МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 27001

Третья редакция
2022-10

Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования

Sécurité de l'information, cybersécurité et protection de la vie privée— Systéms de management de la sécurité de l'information — Exigences

Логотип ISO | Логотип IEC

Номер для ссылки
ISO/IEC 27001:2022 (E)

ДОКУМЕНТ С ЗАЩИЩЕННЫМ АВТОРСКИМ ПРАВОМ

Бюро ISO по охране авторских прав
CЗ 401 • Ch. de Blandonnet 8
CH-1211 Vernier, Geneva
Phone + 41 22 749 01 11
Электронная почта copyright@iso.org
Сайт www.iso.org
Издано в Швейцарии

Содержание

Страница

Предисловие

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Национальные 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, в контакте с ИСО и МЭК также принимают участие в работе.

Процедуры, использованные при разработке этого документа и предназначенные для дальнейшей поддержки, описаны в Директивах ISO/IEC, Часть 1. В частности, должны быть указаны различные критерии утверждения, необходимые для различных типов документов. Данный документ был разработан в соответствии с правилами, изложенными в Директивах ISO/IEC, Часть 2 (см. www.iso.org/directives или www.iec.ch/members_experts/refdocs).

Обращаем внимание на то, что некоторые элементы данного документа могут являться предметом патентных прав. ISO и IEC не должна нести ответственность за идентификацию какого-либо или всех подобных патентных прав. Детали, касающиеся любых патентных прав, установленные в ходе разработки документа, должны быть указаны в разделе Введение и/или в листе патентных деклараций ISO (см. www.iso.org/patents) или IEC (см. http://patents.iec.ch).

Все торговые марки, упомянутые в данном документе, приведены для удобства пользователей и не означают рекомендации (одобрения).

Для понимания добровольного характера стандартов, значений, используемых ISO специфических терминов и выражений, связанных с оценкой соответствия, равно как и информации о соблюдении ISO принципов соглашения Всемирной Торговой Организации (ВТО) по техническим барьерам в торговле (ТБТ) см. по следующей ссылке: www.iso.org/iso/foreword.html. В IEC см. www.iec.ch/understanding-standards.

Данный документ разработан Техническим Комитетом ISO/IEC JNC 1, *Информационные технологии*, *Подкомитет SC 27*, *Информационная безопасность, кибербезопасность и защита персональных данных*.

Эта третья редакция отменяет и заменяет вторую редакцию (ISO/IEC 27001:2013), которая была технически пересмотрена. Она также включает в себя Технические поправки ISO/IEC 27001:2013/Cor.1:2014, . ISO/IEC 27001:2013/Cor.2:2015.

Внесены следующие основные изменения:

— текст был приведен в соответствие с гармонизированной структурой для стандартов на системы менеджмента и ISO/IEC 27002:2022,

Любые отзывы, замечания или вопросы по данному документу следует направлять в национальный орган по стандартизации. Полный перечень таких органов находится по адресу www.iso.org/members.html и www.iec.ch/national-committees

0 Введение

0.1 Общие положения

Данный документ был разработан с целью установить требования для создания, внедрения, поддержания функционирования и постоянного 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 доступности 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.

Данный документ 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 данном документе, 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 с ссылками на стандарты по системе менеджмента информационной безопасности (включая ISO/IEC 27003 [2], ISO/IEC 27004 [3] и ISO/IEC 27005 [4]), а также соответствующие термины и определения.

0.2 Совместимость с другими стандартами системы управления

Данный документ следует структуре высокого 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.

Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования

1 Область применения

Данный документ определяет требования к созданию, внедрению, поддержанию функционирования и постоянному улучшению системы менеджмента информационной безопасности с учетом среды организации. Данный документ также включает требования для оценки и обработки рисков информационной безопасности, адаптированные к потребностям организации. Требования, установленные данным документом, 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 данного документа.

2 Нормативные ссылки

На следующие документы имеются ссылки в тексте таким образом, что в целом или их часть составляет требования данного документа. 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 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

3 Термины и определения

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

ISO и IEC поддерживают терминологическую базу данных для применения в сфере стандартизации по следующим адресам:

— платформа ISO Online browsing platform: доступна на http://www.iso.org/obp

— IEC Electropedia: доступна на http://www.electropedia.org/.

4 Среда организации

4.1 Понимание организации и ее среды

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

ПРИМЕЧАНИЕ Для определения этих факторов при установлении внешней и внутренней среды организации, воспользуйтесь информацией, содержащейся в разделе 5.4.1 ISO 31000:2018 [5].

4.2 Понимание потребностей и ожиданий заинтересованных сторон

Организация должна определить:

a) заинтересованные стороны, которые значимы для системы менеджмента информационной безопасности;

b) значимые требования этих заинтересованных сторон;

c) какие из этих требований будут учитываться в системе менеджмента информационной безопасности.

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

4.3 Определение области применения системы менеджмента информационной безопасности

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

Определяя эту область, организация должна принять во внимание:

a) внешние и внутренние факторы, указанные в разделе 4.1;

b) требования, указанные в разделе 4.2; и

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

Область действия должна быть оформлена как документированная информация.

4.4 Система менеджмента информационной безопасности

Организация должна установить, внедрить, поддерживать функционирование и постоянно улучшать систему менеджмента информационной безопасности, включая необходимые процессы и их взаимодействия, в соответствии с требованиями данного документа.

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) ориентации сотрудников и поддержки их усилий, направленных на обеспечение результативности системы менеджмента информационной безопасности;

g) содействия постоянному совершенствованию; 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 постоянного улучшения системы менеджмента информационной безопасности.

Политика информационной безопасности должна:

e) быть оформлена как документированная информация;

f) быть доведена до сведения сотрудников в организации;

g) быть доступной для заинтересованных сторон в соответствующих случаях.

5.3 Организационные функции, ответственность и полномочия

Высшее руководство должно гарантировать, что для функций, значимых 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 данного документа;

b) отчетности 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 факторы, упомянутые в разделе 4.1, и требования, установленные в разделе 4.2, а также определить риски и возможности, в отношении которых должны быть предприняты действия, чтобы:

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

b) предотвратить или уменьшить нежелательные эффекты;

c) обеспечить постоянное улучшение.

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) применяет процесс оценки рисков информационной безопасности для идентификацию рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках области применения системы менеджмента информационной безопасности; и

2) обеспечивает определение владельцев риска;

d) обеспечивает анализ рисков информационной безопасности:

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

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

3) определение уровня 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 как документированную информацию данные, полученные в ходе процесса оценки рисков информационной безопасности.

6.1.3 Обработка рисков информационной безопасности

Организация должна определить и выполнять процесс обработки рисков информационной безопасности, чтобы:

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 1 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 А, и удостовериться, что никакие из необходимых средств управления не были упущены из виду;

ПРИМЕЧАНИЕ 2 Приложение А содержит перечень возможных средств управления. Пользователям данного документа дана ссылка на Приложение А с тем, чтобы гарантировать, что никакие необходимые средства управления не были пропущены.

ПРИМЕЧАНИЕ 3 Средства управления информационной безопасностью, перечисленные в Приложении А, не являются исчерпывающими и, если необходимо, могут быть добавлены дополнительные средства управления.

d) сформировать Заявление о применимости, которое содержит:

— необходимые средства управления (см.6.1.3 b) и c));

— обоснование их применения;

— указание на то, 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 4 Процессы оценки и обработки рисков информационной безопасности в данном документе согласованы с принципами и общими руководящими указаниями, приведенными в ISO 31000 [5].

6.2 Цели (задачи)[1] в области информационной безопасности и планирование их достижения

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

Цели (задачи) 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) отслеживаться с точки зрения их выполнения;

e) быть сообщены персоналу;

f) соответствующим образом обновляться;

g) быть доступны в документированной форме.

Организация должна сохранять документированную информацию по целям (задачам) в

[1] В оригинале использовано слово «objectives», более точный перевод которого в контексте стандарта – «задачи», а не «цели». Но, учитывая, что термин «цели» уже устоялся, дается двойной перевод [прим. пер.]

области информационной безопасности как.

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

a) что будет сделано;
b) какие ресурсы потребуются;
c) кто будет ответственным за выполнение;
d) когда цели будут достигнуты; и
e) как результаты будут оцениваться.

6.3 Планирование изменений

В случае, если организация выявила необходимость изменений в системе менеджмента информационной безопасности, эти изменения должны быть осуществлены в плановом порядке.

7 Обеспечение

7.1 Ресурсы

Организация должна определить и обеспечить ресурсы, необходимые для разработки, внедрения, поддержания функционирования и постоянного 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 быть осведомлен о:

a) политике в области информационной безопасности,
b) своем вкладе в результативность системы менеджмента информационной безопасности, включая выгоды от улучшения деятельности по обеспечению информационной безопасности, и
c) последствия невыполнения требований 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) каким образом должна осуществляться коммуникация.

7.5 Документированная информация

7.5.1 Общие положения

Система менеджмента информационной безопасности организации должна включать:

a) документированную информацию, требуемую данным документом; 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, графическая форма) и носитель (например, бумага, электронный вид), и
c) пересмотр и утверждение в целях сохранения пригодности и соответствия.

7.5.3 Управление документированной информацией

Документированной информацией, требуемой системой менеджмента информационной безопасности и данным документом, 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:

c) рассылать, обеспечивать доступ, выдачу и применение,
d) хранить и сохранять в надлежащем состоянии, включая сохранение читаемости,
e) управлять изменениями (например, контроль версий), и
f) 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, и выполнять действия, определенные в разделе 6 посредством:

- установления критериев для процессов;
- осуществления управления этими процессами в соответствии с установленными критериями.

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 и поставляемые извне продукты и услуги, значимые для системы менеджмента информационной безопасности, находятся под управлением организации.

8.2 Оценка рисков информационной безопасности

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

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 функционирования

9.1 Мониторинг, измерение, анализ и оценка

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; 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;

f) кто должен анализировать и оценивать эти результаты.

Организация должна сохранять документированную информацию как свидетельство полученных результатов.

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

9.2 Внутренний аудит

9.2.1 Общие положение

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

a) соответствует ли

1) система менеджмента информационной безопасности собственным требованиям организации к системе менеджмента информационной безопасности;

2) требованиям данного документа;

b) что система менеджмента информационной безопасности результативно внедрена и функционирует.

9.2.2 Программа внутреннего аудита

Организация должна планировать, разрабатывать, выполнять и управлять программой(ами) аудитов, включая периодичность их проведения, методы, ответственность, требования к планированию и отчетности. При разработке программ(ы) аудитов организация должна учитывать значимость проверяемых процессов и результаты предыдущих аудитов.

Организация должна:

a) определить критерии и область аудита для каждого аудита;

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

c) гарантировать, что результаты аудитов переданы соответствующим руководителям.

Должна иметься документированная информация как подтверждение выполнения программы аудита и его результатов.

9.3 Анализ системы руководством

9.3.1 Общие положения

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

9.3.2 Исходные данные для анализа

При анализе руководству необходимо учитывать следующее:

a) статус мероприятий, предусмотренных предыдущим анализом;

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

c) изменения в потребностях и ожиданиях заинтересованных сторон, которые значимы для системы менеджмента информационной безопасности;

d) информацию о функционировании системы менеджмента информационной безопасности, включая тенденции в:

   1) несоответствиях и корректирующих действиях;
   2) результатах мониторинга и измерений;
   3) результатах аудитов;
   4) достижении целей (задач) в области информационной безопасности;

e) данные обратной связи от заинтересованных сторон;

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

g) возможности для постоянного улучшения.

9.3.3 Результаты анализа

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

Организация должна сохранять результаты анализа системы менеджмента как документированную информацию.

10 Улучшение

10.1 Постоянное улучшение

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

10.2 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;
   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 несоответствия, 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;

g) результатов любого корректирующего действия.

Приложение А
(нормативное)
Средства управления информационной безопасностью

Средства управления, перечисленные в Таблице А.1, непосредственно взяты из разделов 5 - 8 ISO/IEC 27002:2022 [1] и согласованы с ними, и должны применяться в контексте п. 6.1.3.

Таблица А.1 – Средства управления информационной безопасностью

5 Организационные средства управления		
5.1	Политики информационной безопасности	*Средство управления* Должны быть определены политика информационной безопасности и политики по другим направлениям, утверждены руководством, опубликованы, доведены до сведения и поняты соответствующим персоналом и значимыми заинтересованными сторонами, а также пересматриваться через запланированные интервалы времени и в случае значительных изменений.
5.2	Роли и обязанности, связанные с информационной безопасностью	*Средство управления* Должны быть определены и назначены все роли и обязанности, связанные с информационной безопасностью, в соответствии с потребностями организации.
5.3	Разделение обязанностей	*Средство управления* Вступающие в противоречие друг с другом обязанности и области ответственности должны быть разделены.
5.4	Обязанности руководства	*Средство управления* Руководство должно требовать от всех сотрудников соблюдения требований по информационной безопасности в соответствии с установленными политикой информационной безопасности, иными политиками и процедурами организации.
5.5	Контакты с полномочными органами	*Средство управления* Должны быть установлены и поддерживаться соответствующие контакты с соответствующими органами.
5.6	Контакты с профессиональными сообществами	*Средство управления* Организация должна установить и поддерживать контакты с профессиональными сообществами или иными форумами специалистов по информационной безопасности и профессиональными ассоциациями.

5 Организационные средства управления		
5.7	Изучение угроз	*Средство управления* Должна собираться и анализироваться информация, связанная с угрозами информационной безопасности, для изучения угроз
5.8	Информационная безопасность в управлении проектами	*Средство управления* Обеспечение информационной безопасности должно быть интегрировано в управление проектами.
5.9	Инвентаризация информации и иных связанных с ней активов	*Средство управления* Реестры информационных и иных связанных с этим активов, включая владельцев, должны быть разработаны и поддерживаться в актуальном состоянии
5.10	Надлежащее применение информационных и иных, связанных с ними, активов	*Средство управления* Должны быть определены, документированы и внедрены правила надлежащего применения и процедуры обращения с информационными и иными, связанными с ними, активами
5.11	Возврат активов	*Средство управления* Персонал и представители заинтересованных сторон, насколько это применимо, должны вернуть все активы организации в ее распоряжение при изменении или прекращении трудовых отношений, контрактов и соглашений.
5.12	Классификация информации	*Средство управления* Информация должна быть классифицирована исходя из потребностей информационной безопасности организации на основе требований к конфиденциальности, целостности и доступности и требований заинтересованных сторон.
5.13	Маркировка информации	*Средство управления* Должен быть разработан и внедрен соответствующий набор процедур для маркировки информации в соответствии со схемой классификации информации, принятой в организации.
5.14	Передача информации	*Средство управления* Должны быть внедрены правила, процедуры или соглашения для любого вида средств передачи как внутри организации, так и между организацией и другими сторонами
5.15	Управление доступом	*Средство управления* Должны быть на основе требований бизнеса и требований к информационной безопасности разработаны и внедрены правила физического и логического доступа к информационным и иным, связанным с ними, активам

5 Организационные средства управления		
5.16	Управление идентификацией	*Средство управления* Должно быть обеспечено управление всем жизненным циклом идентификаторов
5.17	Информация для аутентификации	*Средство управления* Назначение и управление информацией для аутентификации должно быть контролируемым в рамках процесса управления, включая консультирование сотрудников по вопросам надлежащего обращения с информацией для аутентификации
5.18	Права доступа	*Средство управления* Права доступа к информационным и иным, связанным с ними, активам должны быть предоставлены, пересматриваться, изменяться и аннулироваться в соответствии с различными политиками организации и правилами контроля доступа
5.19	Информационная безопасность в отношениях с поставщиками	*Средство управления* Должны быть определены и внедрены процессы и процедуры управления рисками для информационной безопасности, связанными с использованием продуктов и услуг, предоставляемых поставщиками
5.20	Обеспечение информационной безопасности в рамках соглашений с поставщиками	*Средство управления* Должны быть установлены сущностные требования к информационной безопасности и согласованы с каждым поставщиком с учетом особенностей отношений с этим поставщиком.
5.21	Управление информационной безопасностью в цепочках поставки в сфере информационно-коммуникационных технологий (ИКТ)	*Средство управления* Должны быть разработаны и внедрены процесс и процедуры управления рисками для информационной безопасности, связанных с цепочкой поставок продуктов и услуг ИКТ.
5.22	Мониторинг, анализ и управление изменениями услуг поставщиков	*Средство управления* Организация должна регулярно вести мониторинг, анализ, оценку и управлять изменениями в деятельности поставщиков в сфере информационной безопасности и поставки услуг.

5 Организационные средства управления		
5.23	Информационная безопасность при использовании облачных сервисов	*Средство управления* Должен быть установлен процесс запроса, использования, управления и прекращения использования облачных сервисов в соответствии с требования организации в области информационной безопасности.
5.24	Планирование и подготовка в части управления инцидентами информационной безопасности	*Средство управления* Организация должна планировать и готовиться к управлению инцидентами информационной безопасности посредством определения, установления и информирования о процессах управления инцидентами информационной безопасности, ролях и обязанностях.
5.25	Оценка событий в области информационной безопасности и принятие решений	*Средство управления* Организация должна оценивать события в области информационной безопасности и решать, следует ли их расценивать как инцидент информационной безопасности.
5.26	Ответные меры по инцидентам информационной безопасности	*Средство управления* Реагирование на инциденты информационной безопасности должно осуществляться в соответствии с документированными процедурами.
5.27	Излечение уроков из инцидентов информационной безопасности	*Средство управления* Знания, полученные из инцидентов информационной безопасности, должны использоваться для усиления и улучшения средств управления информационной безопасностью.
5.28	Сбор свидетельств	*Средство управления* Организация должна установить и внедрить процедуры для идентификации, сбора, накопления и сохранения свидетельств, связанных с событиями информационной безопасности.
5.29	Информационная безопасность при сбое	*Средство управления* Организация должна планировать, каким образом она будет обеспечивать информационную безопасность на соответствующем уровне при сбое.
5.30	Готовность ИКТ к обеспечению непрерывности бизнеса	*Средство управления* Меры по обеспечению готовности ИКТ должны планироваться, внедряться, поддерживаться в актуальном состоянии и тестироваться с точки зрения целей непрерывности бизнеса и требований к непрерывности функционирования ИКТ.

5 Организационные средства управления		
5.31	Законодательные, нормативные и контрактные требования	*Средство управления* Законодательные, нормативные и контрактные требования, значимые для информационной безопасности, а также подход организации к удовлетворению этих требований должны быть определены, документированы и сохраняться актуальными.
5.32	Права интеллектуальной собственности	*Средство управления* Организация должна осуществлять соответствующие процедуры для защиты прав интеллектуальной собственности.
5.33	Защита записей	*Средство управления* Записи должны быть защищены от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированной публикации.
5.34	Приватность и защита персональных данных	*Средство управления* Организация должна установить и выполнять требования, связанные с сохранением приватности и защитой персональных данных (ПД) в соответствии с действующими законодательными, нормативными и контрактными требованиями.
5.35	Независимый анализ информационной безопасности	*Средство управления* Подход организации к управлению информационной безопасностью и его реализация, в том числе. люди, процессы и технологии, должны подвергаться независимому анализу через запланированные интервалы времени или в тех случаях, когда происходят существенные изменения.
5.36	Соответствие политикам, правилам и стандартам информационной безопасности	*Средство управления* Соответствие политике информационной безопасности, политикам в других областях, правилам и стандартам должно регулярно анализироваться.
5.37	Документированные операционные процедуры	*Средство управления* Операционные процедуры для устройств обработки информации должны быть документированы и доступны персоналу, которому они требуются.

6	**Средства управления, связанные с персоналом**	
6.1	Предварительная проверка	*Средство управления* 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.
6.2	Условия трудового соглашения	*Средство управления* Трудовые соглашения с сотрудниками должны устанавливать их и организации ответственность в части информационной безопасности.
6.3	Осведомленность, образование и подготовка в сфере информационной безопасности	*Средство управления* Сотрудники организации и значимые заинтересованные стороны должны быть соответствующим образом информированы, иметь соответствующее образование и подготовку, а также регулярно извещаться об изменениях в политике информационной безопасности организации, политиках по другим направлениям, в той мере, насколько это важно для исполнения их служебных обязанностей.
6.4	Дисциплинарные меры	*Средство управления* Должен быть разработан и доведен до сведения персонала процесс для принятия мер к тем сотрудникам и иным заинтересованным сторонам, которые допустили нарушение требований информационной безопасности.
6.5	Обязанности после прекращения или изменения трудовых отношений	*Средство управления* Ответственность и обязанности по соблюдению информационной безопасности, которые остаются в силе после прекращения или изменения трудовых отношений, должны быть определены и сообщены соответствующему персоналу и иным заинтересованным сторонам, а также обеспечено их выполнение.
6.6	Соглашения о конфиденциальности или неразглашении	*Средство управления* Соглашения о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны быть определены, документированы, регулярно пересматриваться и быть подписанными персоналом и иными заинтересованными сторонами.

6	**Средства управления, связанные с персоналом**	
6.7	Удаленная работа	*Средство управления* Должны осуществляться меры по обеспечению безопасности в тех случаях, когда персонал работает удаленно, чтобы обеспечить защиту информации, к которой есть доступ, которая обрабатывается или хранится в местах за пределами организации.
6.8	Отчетность о событиях информационной безопасности	*Средство управления* Организация должна иметь процедуру для персонала для своевременного информирования о выявленных или предполагаемых событиях информационный безопасности посредством соответствующих каналов.

7	**Средства управления, связанные с физическим доступом**	
7.1	Физические периметры безопасности	*Средство управления* Периметры безопасности должны быть определены и использоваться для защиты зон нахождения информации и иных, связанной с ней, активов.
7.2	Физический вход	*Средство управления* Зоны безопасности должны быть защищены выделением мест прохода и соответствующими средствами контроля прохода .
7.3	Защита офисов, помещений и устройств	*Средство управления* Меры физической защиты безопасности для офисов, помещений и оборудования должны быть разработаны и применяться.
7.4	Мониторинг физической защиты	*Средство управления* Помещения должны находиться под постоянным контролем неавторизованного доступа.
7.5	Защита от физических и природных угроз	*Средство управления* Должны быть разработаны и внедрены меры по защите от физических и природных угроз, таких как стихийные бедствия, а также иные намеренные или непреднамеренные физические угрозы для инфраструктуры.
7.6	Работа в защищенных зонах	*Средство управления* Должны быть разработаны и применяться процедуры для работы в защищенных зонах.

7	**Средства управления, связанные с физическим доступом**	
7.7	Чистый стол и чистый экран	*Средство управления* Должны быть установлены и обеспечено выполнение правил чистого стола для бумажных документов, переносных устройств хранения информации и правил чистого экрана для устройств обработки информации.
7.8	Размещение и защита оборудования	*Средство управления* Оборудование должно быть размещено в безопасном месте и защищено.
7.9	Защита активов вне территории	*Средство управления* Активы, находящиеся вне территории организации, должны быть защищены.
7.10	Устройства хранения	*Средство управления* Управление устройствами хранения должно осуществляться на всем протяжении их жизненного цикла, включающего приобретение, использование, транспортировку и уничтожение, в соответствии с классификационной схемой организации и требованиями к обращению.
7.11	Службы обеспечения	*Средство управления* Устройства обработки информации должны быть защищены от перебоев в электроснабжении и других сбоев, вызываемых перебоями в работе служб обеспечения.
7.12	Защита кабельных сетей	*Средство управления* Питающие кабели и кабели, передающие данные или обеспечивающие работу информационных сервисов, должны быть защищены от перехвата, помех или повреждения.
7.13	Обслуживание оборудования	*Средство управления* Оборудование должно обслуживаться надлежащим образом, чтобы гарантировать конфиденциальность, целостность и доступность информации.
7.14	Безопасная утилизация или повторное использование оборудования	*Средство управления* 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.

8	**Технологические средства управления**	
8.1	Оконечные устройства пользователя	*Средство управления* Информация сохраняемая, обрабатываемая или к которой имеется доступ через оконечные устройства пользователя, должна быть защищена.
8.2	Привилегированные права доступа	*Средство управления* Предоставление и использование привилегированных прав доступа должно быть ограничено и находиться под контролем.
8.3	Ограничение доступа к информации	*Средство управления* Доступ к информации и иным, связанным с нею активам, должен быть ограничен в соответствии установленными политиками по контролю доступа.
8.4	Доступ к исходному коду	*Средство управления* Должно быть обеспечено соответствующее управление доступом на чтение и запись к исходному коду, инструментам разработки и библиотекам.
8.5	Безопасная аутентификация	*Средство управления* Должны быть внедрены технологии и процедуры безопасной аутентификации, основанные на ограничениях доступа к информации и политиках по контролю доступа.
8.6	Управление производительностью	*Средство управления* Использования ресурсов должно быть под контролем и настроено в соответствии с текущими и перспективными требованиями к производительности.
8.7	Защита от вредоносного программного обеспечения	*Средство управления* Должна быть внедрена защита от вредоносного программного обеспечения и сопровождаться соответствующим информированием пользователей.
8.8	Управление техническими уязвимостями	*Средство управления* Должна получаться информация о технических уязвимостях в используемых информационных системах, оцениваться возможное влияние на организацию таких уязвимостей и приниматься соответствующие меры.
8.9	Менеджмент конфигураций	*Средство управления* Конфигурации, включая те, что связаны с безопасностью, оборудования, программного обеспечения, сервисов и сетей должны быть определены, документированы, внедрены, вестись их мониторинг и анализ.

8	**Технологические средства управления**	
8.10	Удаление информации	*Средство управления* Информация, хранящаяся в информационных системах, на устройствах или любых иных носителей данных, должна быть удалена, если она больше не требуется.
8.11	Маскирование данных	*Средство управления* Должно использоваться маскирование данных в соответствии с политиками организации по контролю доступа и иными специализированными политиками, а также требованиями бизнеса, с учетом применимого законодательства.
8.12	Предупреждение утечки данных	*Средство управления* Должны применяться меры по предупреждению утечки данных в системах, сетях и иных устройствах для обработки, хранения и передачи конфиденциальной информации.
8.13	Резервное копирование информации	*Средство управления* Должно выполняться и регулярно тестироваться резервное копирование информации, программного обеспечения и систем в соответствии с принятой политикой резервного копирования.
8.14	Избыточность устройств обработки информации	*Средство управления* Устройства обработки информации должны применяться с избыточностью, достаточной для выполнения требований по доступности.
8.15	Ведение журналов (логов)	*Средство управления* Журналы (логи), фиксирующие действия, исключения, сбои и иные значимые события должны вестись, сохраняться, быть защищенными и анализироваться.
8.16	Мониторинг действий	*Средство управления* Должен осуществляться мониторинг сетей, систем и приложений с целью выявления отклонений от нормального поведения и принятие соответствующих мер для оценки возможных инцидентов информационной безопасности.
8.17	Синхронизация часов	*Средство управления* Время у информационных систем, используемых организацией, должно быть синхронизировано с одобренными источниками точного времени.

8	**Технологические средства управления**	
8.18	Использование утилит с привилегированными правами	*Средство управления* Применение утилит, которые могли бы обходить средства контроля системы и приложений, должно быть ограничено и строго контролироваться.
8.19	Установка приложений в операционной системе	*Средство управления* Должны быть внедрены процедуры и меры для безопасного управления установкой программного обеспечения в операционной системе.
8.20	Безопасность сетей	*Средство управления* Сети и сетевые устройства должны быть защищены, управляться и контролироваться с целью защиты информации в системах и приложениях.
8.21	Безопасность сетевых сервисов	*Средство управления* Должны быть определены, внедрены и контролироваться механизмы обеспечения безопасности, уровни сервиса и требования к обслуживанию сетевых служб.
8.22	Разделение сетей	*Средство управления* Группы информационных сервисов, пользователей и информационных систем должны быть разделены в сетях организации.
8.23	Веб-фильтрация	*Средство управления* Доступ к внешним веб-сайтам должен находиться под управлением для снижения подверженности влиянию вредоносного содержания.
8.24	Использование криптографии	*Средство управления* Должны быть определены и внедрены правила результативного использования криптографии, включая управление криптографическими ключами.
8.25	Жизненный цикл разработки безопасного программного обеспечения	*Средство управления* Должны быть установлены и применяться правила разработки безопасного программного обеспечения и систем.
8.26	Применение требований по безопасности	*Средство управления* Должны быть выявлены, установлены и утверждены требования по информационной безопасности для разработки или приобретения приложений.

8	**Технологические средства управления**	
8.27	Безопасная архитектура систем и принципы разработки	*Средство управления* Принципы разработки безопасных систем должны быть установлены, документированы, поддерживаться в актуальном состоянии и применяться к любым действиям в рамках разработки информационных систем.
8.28	Безопасное кодирование	*Средство управления* Принципы создания безопасного кода должны применяться в ходе разработки программного обеспечения.
8.29	Тестирование обеспечения безопасности при разработке и приемке	*Средство управления* Процессы тестирования обеспечения безопасности должны быть определены и внедрены в рамках жизненного цикла разработки.
8.30	Разработка, переданная на аутсорсинг	*Средство управления* Организация должна управлять, осуществлять мониторинг и анализ деятельности, связанной с разработкой систем, переданной на аутсорсинг.
8.31	Разделение среды разработки, тестирования и эксплуатации	*Средство управления* Среда разработки, тестирования и рабочая среда должны быть отделены друг от друга и обеспечена безопасность.
8.32	Управление изменениями	*Средство управления* Должны быть предусмотрены процедуры управления изменениями в средствах обработки информации и информационных системах.
8.33	Данные для тестирования	*Средство управления* Данные для тестирования должны быть соответствующим образом отобраны, обеспечена их защищенность и управление.
8.34	Защита информационных систем в ходе аудита	*Средство управления* Аудиты и иные действия, направленные на обеспечение гарантий, включающие оценку операционных систем, должны быть спланированы и согласованы проводящим тестирование и соответствующим руководством.

Библиография

[1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[2] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[3] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing Information security risks*

[5] ISO 31000:2018, *Risk management —Guidelines*