CERT academy

Международная тренинговая компания

МЕЖДУНАРОДНЫЙ **СТАНДАРТ**

ISO 27001:2022

Система менеджмента информационной безопасности

Для учебных целей

МЕЖДУНАРОДНЫЙ ISO/IEC СТАНДАРТ 27001

Третье издание
2022-10

Информационная безопасность, кибербезопасность и защита конфиденциальности – Система менеджмента информационной безопасности - Требования

Исходящий номер
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

ДОКУМЕНТ, ЗАЩИЩЕННЫЙ АВТОРСКИМ ПРАВОМ

© ISO/IEC 2022

Все права защищены. Если иное не указано или не требуется в контексте ее реализации, никакая часть данной публикации не может быть воспроизведена или использована иным образом в любой форме или любыми средствами, электронными или механическими, включая ксерокопию или размещение в Интернете или корпоративной сети, без предварительного письменного разрешения. Разрешение можно запросить либо у ISO по указанному ниже адресу, либо у организации-члена ISO в стране заявителя.

Бюро ISO по охране авторских прав
CP 401 • Гл. де Бландонне 8
CH-1214 Вернье, Женева
Телефон: +41 22 749 01 11
Электронная почта: copyright@iso.org
Сайт: www.iso.org

Опубликовано в Швейцарии

Содержание

Страница

Предисловие ... iv
Введение ... v
1 Область применения ... 1
2 Нормативные ссылки ... 1
3 Термины и определения ... 1
4 Контекст организации ... 1
4.1 Понимание организации и ее контекста ... 1
4.2 Понимание потребностей и ожиданий заинтересованных сторон ... 1
4.3 Определение области применения системы менеджмента информационной безопасности ... 2
4.4 Система менеджмента информационной безопасности ... 2
5 Лидерство ... 2
5.1 Лидерство и обязательства ... 2
5.2 Политика ... 3
5.3 Организационные функции, ответственность и полномочия ... 3
6 Планирование ... 3
6.1 Действия по обработке рисков и реализации возможностей ... 3
6.2 Цели в области информационной безопасности и планирование их достижения ... 5
6.3 Планирование изменений ... 5
7 Обеспечение ... 6
7.1 Ресурсы ... 6
7.2 Компетентность ... 6
7.3 Осведомленность ... 6
7.4 Коммуникация ... 6
7.5 Документированная информация ... 6
8 Функционирование ... 7
8.1 Оперативное планирование и управление ... 7
8.2 Оценка рисков информационной безопасности ... 8
8.3 Обработка рисков информационной безопасности ... 8
9 Оценка результатов деятельности ... 8
9.1 Мониторинг, измерение, анализ и оценка ... 8
9.2 Внутренний аудит ... 8
9.3 Анализ менеджмента ... 9
10 Улучшение ... 10
10.1 Непрерывное улучшение ... 10
10.2 Несоответствия и корректирующие действия ... 10
Приложение А (нормативное) **Справочник по средствам управления информационной безопасностью** ... 11
Библиография ... 19

© ISO/IEC 2022 – Все права защищены

ISO/IEC 27001:2022(E)

Предисловие

ISO (Международная организация по стандартизации) и IEC (Международная электротехническая комиссия) образуют специализированную систему всемирной стандартизации. Государственные органы, являющиеся членами ISO или IEC, участвуют в разработке международных стандартов через технические комитеты, созданные соответствующей организацией для работы в конкретных областях технической деятельности. Технические комитеты ISO и IEC сотрудничают в областях взаимного интереса. Другие международные организации, правительственные и неправительственные, во взаимодействии с ISO и IEC также принимают участие в работе.

Процедуры, используемые для разработки этого документа, и процедуры, предназначенные для его дальнейшего обслуживания, описаны в Директивах ISO/IEC, Часть 1. В частности, следует отметить различные критерии утверждения, необходимые для различных типов документов. Этот документ был составлен в соответствии с редакционными правилами Директив ISO/IEC, Часть 2 (см. www.iso.org/directives или www.iec.ch/members expert/refdocs).

Обращаем внимание на возможность того, что некоторые элементы этого документа могут быть предметом патентных прав. ISO и IEC не несут ответственности за идентификацию каких-либо или всех таких патентных прав. Подробная информация о любых патентных правах, выявленных в ходе разработки документа, будет представлена во Введении и/или в списке полученных патентных деклараций ISO (см. www.iso.org/patents) или в списке полученных патентных деклараций IEC (см. https: //патенты.iec.ch).

Любое торговое наименование, используемое в этом документе, является информацией, предоставленной для удобства пользователей, и не является рекламой.

Для объяснения добровольного характера стандартов, значения конкретных терминов и выражений ISO, связанных с оценкой соответствия, а также информации о приверженности ISO принципам Всемирной торговой организации (ВТО) в отношении технических барьеров в торговле (ТБТ) см. www.iso.org/iso/foreword.html. В IEC см. www.iec.ch/understanding-standards.

Этот документ был подготовлен Объединенным техническим комитетом ISO/IEC JTC 1, *Информационные технологии*, Подкомитетом SC 27, *Информационная безопасность, кибербезопасность и защита конфиденциальности.*

Это третье издание отменяет и заменяет второе издание (ISO/IEC 27001:2013), которое было технически пересмотрено. Он также включает технические исправления ISO/IEC 27001:2013/Cor 1:2014 и ISO/IEC 27001:2013/Cor 2:2015.

Основные изменения заключаются в следующем:

- текст приведен в соответствие с согласованной структурой стандартов на системы менеджмента и ISO/IEC 27002:2022.

Любые отзывы или вопросы по этому документу следует направлять в пользовательсикий национальный орган по стандартизации. Полный список этих органов можно найти на сайтах www.iso.org/members.html и www.iec.ch/national-committees.

© ISO/IEC 2022 – Все права защищены

Введение

0.1 Общие положения

Данный документ был разработан с целью установить требования для создания, внедрения, поддержания функционирования и непрерывного улучшения системы менеджмента информационной безопасности. Внедрение системы менеджмента информационной безопасности является стратегическим решением для организации. На создание и внедрение системы менеджмента информационной безопасности организации влияют потребности и цели организации, требования по безопасности, применяемые организационные процессы, а также размер и структура организации. Все эти факторы влияния ожидаемо меняются с течением времени.

Система менеджмента информационной безопасности сохраняет конфиденциальность, целостность и доступность информации, применяя процесс управления рисками, и дает заинтересованным сторонам уверенность в том, что риски управляются надлежащим образом.

Важно, чтобы система менеджмента информационной безопасности была частью процессов организации и интегрирована в общую структуру управления, и чтобы информационная безопасность учитывалась при разработке процессов, информационных систем и средств контроля. Предполагается, что внедрение системы менеджмента информационной безопасности будет масштабироваться в соответствии с потребностями организации.

Данный документ может использоваться внутренними и внешними сторонами для оценки способности организации соответствовать собственным требованиям информационной безопасности организации.

Порядок, в котором требования представлены в данном документе, не отражает их важности и не подразумевает порядок, в котором они должны быть реализованы. Элементы списка перечислены только для справки.

ISO/IEC 27000 содержит обзор и словарь терминов для систем менеджмента информационной безопасности, ссылаясь на серию стандартов системы менеджмента информационной безопасности (включая ISO/IEC 27003[2], ISO/IEC 27004[3] и ISO/IEC 27005[4]), с соответствующими терминами и определениями.

0.2 Совместимость с другими стандартами систем менеджмента

В данном документе применяется структура высшего уровня, идентичные заголовки подразделов, идентичный текст, общие термины и основные определения, определенные в Приложении SL к Директивам ISO/IEC, Часть 1, Сводное приложение ISO, и, следовательно, 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 решили использовать единую систему менеджмента, отвечающую требованиям двух или более стандартов на системы менеджмента.

© ISO/IEC 2022 – Все права защищены

Информационная безопасность, кибербезопасность и защита конфиденциальности - Система менеджмента информационной безопасности – Требования

1 Область применения

Данный документ определяет требования к созданию, внедрению, поддержке и непрерывному улучшению системы менеджмента информационной безопасности в контексте организации. Данный документ также включает требования к оценке и обработке рисков информационной безопасности с учетом потребностей организации. Требования, изложенные в данном документе, являются общими и предназначены для применения ко всем организациям, независимо от их типа, размера или характера. Исключение любого из требований, указанных в разделах 4-10, неприемлемо, если организация заявляет о соответствии данному документу.

2 Нормативные ссылки

Следующие документы упоминаются в тексте таким образом, что часть или все их содержание составляет требования настоящего документа. Для датированных ссылок применяется только цитируемое издание. Для недатированных ссылок применяется последнее издание ссылочного документа (включая любые поправки).

ISO/IEC 27000, *Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Обзор и словарь*

3 Термины и определения

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

ISO и IEC поддерживают терминологические базы данных для использования в стандартизации по следующим адресам:

Платформа просмотра ISO в Интернете: доступна по адресу https://www.iso.org/obp.

IEC Electropedia: доступно на https://www.electropedia.org/

4 Контекст организации

4.1 Понимание организации и ее контекста

Организация должна определить внешние и внутренние проблемы, которые имеют отношение к ее цели и влияют на ее способность достигать намеченных результатов ее системы менеджмента информационной безопасности.

ПРИМЕЧАНИЕ. Определение этих проблем относится к установлению внешнего и внутреннего контекста организации, рассматриваемого в пункте 5.4.1 ISO 31000:2018[5].

4.2 Понимание потребностей и ожиданий заинтересованных сторон

Организация должна определить:

А) заинтересованные стороны, имеющие отношение к системе менеджмента информационной безопасности;

Б) соответствующие требования этих заинтересованных сторон;

В) какие из этих требований будут решаться посредством системы менеджмента информационной безопасности.

© ISO/IEC 2022 – Все права защищены

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

4.3 Определение области применения системы менеджмента информационной безопасности

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

При определении области применения организация должна учитывать:

А) внешние и внутренние проблемы, указанные в пункте 4.1;

Б) требования, указанные в пункте 4.2;

В) взаимосвязи и зависимости между действиями, выполняемыми организацией, и действиями, выполняемыми другими организациями.

Область применения должна быть доступна в виде документированной информации.

4.4 Система менеджмента информационной безопасности

Организация должна установить, внедрить, поддерживать и постоянно совершенствовать систему менеджмента информационной безопасности, включая необходимые процессы и их взаимодействие, в соответствии с требованиями настоящего документа.

5 Лидерство

5.1 Лидерство и обязательства

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

А) обеспечения того, чтобы политика информационной безопасности и цели информационной безопасности были установлены и совместимы со стратегическим направлением организации;

Б) обеспечения интеграции требований системы менеджмента информационной безопасности в процессы организации;

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

Г) информирования о важности эффективного управления информационной безопасностью и соответствия требованиям системы менеджмента информационной безопасности;

Д) обеспечения того, чтобы система менеджмента информационной безопасности достигла намеченных результатов;

Е) направления и поддержки лиц, способствующих повышению эффективности системы менеджмента информационной безопасности;

Ж) содействия непрерывному улучшению; а также

З) поддержка других соответствующих управленческих ролей, чтобы продемонстрировать свое лидерство, поскольку это относится к их сферам ответственности.

ПРИМЕЧАНИЕ. Ссылку на «бизнес» в этом документе можно интерпретировать широко, чтобы обозначить те виды деятельности, которые являются ключевыми для целей существования организации.

© ISO/IEC 2022 – Все права защищены

5.2 Политика

Высшее руководство должно установить политику информационной безопасности, которая:

А) соответствует назначению организации;

Б) включает цели информационной безопасности (см. 6.2) или служит основой для постановки целей информационной безопасности;

В) включает в себя обязательство выполнять применимые требования, связанные с информационной безопасностью;

Г) включает обязательство по непрерывному улучшению системы менеджмента информационной безопасности.

Политика информационной безопасности должна:

Д) быть доступной в виде документированной информации;

Е) быть доведена до сведения сотрудников внутри организации;

Ж) быть доступной для заинтересованных сторон, если это необходимо.

5.3 Организационные функции, ответственность и полномочия

Высшее руководство должно обеспечить, чтобы обязанности и полномочия для функций, относящихся к информационной безопасности, были назначены и доведены до сведения внутри организации.

Высшее руководство должно определить ответственность и полномочия для:

А) обеспечения соответствия системы менеджмента информационной безопасности требованиям настоящего документа;

Б) отчетности о работе системы менеджмента информационной безопасности перед высшим руководством.

ПРИМЕЧАНИЕ. Высшее руководство может также назначать обязанности и полномочия для составления отчетов об эффективности системы менеджмента информационной безопасности в организации.

6 Планирование

6.1 Действия по обработке рисков и реализации возможностей

6.1.1 Общие положения

При планировании системы менеджмента информационной безопасности организация должна учитывать проблемы, указанные в пункте 4.1, и требования, указанные в пункте 4.2, и определять риски и возможности, которые необходимо учесть, чтобы:

А) гарантировать, что система менеджмента информационной безопасности может достичь намеченных результатов;

Б) предотвратить или уменьшить нежелательные эффекты;

В) добиваться непрерывного улучшения.

Организация должна планировать:

Г) действия по устранению этих рисков и реализации возможностей; а также

Д) каким образом

1) интегрировать и внедрять действия в процессы своей системы менеджмента информационной безопасности; а также

2) оценить эффективность этих действий.

© ISO/IEC 2022 – Все права защищены

6.1.2 Оценка рисков информационной безопасности

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

А) устанавливает и обеспечивает применение критериев оценки рисков информационной безопасности, которые включают:

1) критерии приемлемости риска; а также

2) критерии проведения оценок рисков информационной безопасности;

Б) гарантирует, что повторные оценки рисков информационной безопасности дают согласованные, достоверные и сопоставимые результаты;

В) определяет риски информационной безопасности:

1) включает в себя процесс оценки рисков информационной безопасности для выявления рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках системы менеджмента информационной безопасности; а также

2) обеспечивает определение владельцев риска;

Г) анализирует риски информационной безопасности:

1) оценку потенциальных последствий, которые возникнут, если риски, указанные в 6.1.2 В) 1), реализуются;

2) оценку реальной вероятности возникновения рисков, указанных в 6.1.2 В) 1); а также

3) определение уровня риска;

Д) оценивает риски информационной безопасности:

1) сравнение результатов анализа риска с критериями риска, установленными в 6.1.2 А); а также

2) расстановку анализируемых рисков по приоритетам для обработки рисков.

Организация должна сохранять 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 с целью:

А) выбрать соответствующие варианты обработки рисков информационной безопасности с учетом результатов оценки рисков;

Б) определить все элементы управления, необходимые для реализации выбранного(ых) варианта(ов) обработки рисков информационной безопасности;

ПРИМЕЧАНИЕ 1. Организации могут разрабатывать средства управления по мере необходимости или идентифицировать их из любого источника.

В) сравнить меры контроля, определенные в 6.1.3 Б), выше, с теми, что указаны в приложении А, и убедиться, что никакие необходимые меры контроля не были упущены;

ПРИМЕЧАНИЕ 2. Приложение А содержит список возможных средств управления информационной безопасностью. Пользователям данного документа рекомендуется ознакомиться с Приложением А, чтобы убедиться, что не упущены все необходимые средства контроля информационной безопасности.

ПРИМЕЧАНИЕ 3 Меры информационной безопасности, перечисленные в Приложении А, не являются исчерпывающими, и при необходимости могут быть включены дополнительные меры информационной безопасности.

Г) подготовить Заявление о применимости, содержащее:

- необходимые средства управления (см. 6.1.3 Б) и В));

© ISO/IEC 2022 – Все права защищены

- обоснование их применения;

- реализованы ли необходимые средства управления или нет; а также

- обоснование исключения любого из средств управления в Приложении А.

Д) сформировать план обработки рисков информационной безопасности; а также

Е) получить согласие владельцев рисков на план обработки рисков информационной безопасности и принятие остаточных рисков информационной безопасности.

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

ПРИМЕЧАНИЕ 4. Процесс оценки и обработки рисков информационной безопасности, описанный в данном документе, соответствует принципам и общим рекомендациям, приведенным в ISO 31000[5].

6.2 Цели в области информационной безопасности и планирование их достижения

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

Цели информационной безопасности должны:

А) соответствовать политике информационной безопасности;

Б) быть измеримым (если возможно);

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

Г) находиться под наблюдением;

Д) быть сообщены персоналу;

Е) обновляться по мере необходимости;

Ж) быть доступной в виде документированной информации.

Организация должна хранить документированную информацию о целях информационной безопасности.

При планировании достижения целей информационной безопасности организация должна определить:

З) что будет сделано;

И) какие ресурсы потребуются;

К) кто будет нести ответственность;

Л) когда цели будут достигнуты; а также

М) как будут оцениваться результаты.

6.3 Планирование изменений

Когда организация определяет необходимость внесения изменений в систему менеджмента информационной безопасности, изменения должны осуществляться в плановом порядке.

© ISO/IEC 2022 – Все права защищены

7 Обеспечение

7.1 Ресурсы

Организация должна определить и предоставить ресурсы, необходимые для создания, внедрения, обслуживания и непрерывного улучшения системы менеджмента информационной безопасности.

7.2 Компетентность

Организация должна:

А) определить необходимую компетентность лица (лиц), выполняющих подконтрольную ему работу, влияющую на ее показатели информационной безопасности;

Б) обеспечить, чтобы эти лица были компетентны в силу соответствующего образования, подготовки или опыта;

В) при необходимости предпринимать действия для приобретения необходимой компетентности и оценивать эффективность предпринятых действий; а также

Г) сохранять соответствующую документированную информацию в качестве доказательства компетентности.

ПРИМЕЧАНИЕ: Применимые действия могут включать, например: обучение, наставничество или переназначение действующих сотрудников; или наем или заключение контрактов с компетентными лицами.

7.3 Осведомленность

Лица, выполняющие работы под управлением организации, должны знать:

А) политику информационной безопасности;

Б) их вклад в эффективность системы менеджмента информационной безопасности, включая преимущества повышения эффективности информационной безопасности; а также

С) последствия несоответствия требованиям системы менеджмента информационной безопасности.

7.4 Коммуникация

Организация должна определить потребность во внутренних и внешних коммуникациях, относящихся к системе менеджмента информационной безопасности, включая:

А) на какой предмет обмениваться информацией;

Б) когда обмениваться информацией;

В) с кем обмениваться информацией;

Г) как обмениваться информацией.

7.5 Документированная информация

7.5.1 Общие положения

Система менеджмента информационной безопасности организации должна включать:

А) документированную информацию, требуемая настоящим документом; а также

© ISO/IEC 2022 – Все права защищены

Б) документированную информацию, определенную организацией как необходимую для эффективности системы менеджмента информационной безопасности.

ПРИМЕЧАНИЕ. Объем документированной информации для системы менеджмента информационной безопасности может различаться в разных организациях из-за:

1) размера организации и типа ее деятельности, процессов, продуктов и услуг;

2) сложности процессов и их взаимодействия; а также

3) компетентности персонала.

7.5.2 Создание и обновление

При создании и обновлении документированной информации организация должна обеспечить надлежащие:

А) идентификацию и описание (например, название, дата, автор или номер ссылки);

Б) формат (например, язык, версия программного обеспечения, графика) и носитель (например, бумажный, электронный); а также

В) рассмотрение и утверждение на предмет пригодности и соответствия.

7.5.3 Управление документированной информацией

Документированная информация, требуемая системой менеджмента информационной безопасности и настоящим документом, должна контролироваться для обеспечения:

А) он доступен и пригоден для использования, где и когда он нужен; а также

Б) он надлежащим образом защищен (например, от потери конфиденциальности, ненадлежащего использования или потери целостности).

Для управления документированной информацией организация должна осуществлять следующие виды деятельности, если применимо:

В) распространение, доступ, поиск и использование;

Г) хранение и сохранность, в том числе сохранение удобочитаемости;

Д) контроль изменений (например, контроль версий); а также

Е) удержание и распоряжение.

Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и функционирования системы менеджмента информационной безопасности, должна быть надлежащим образом идентифицирована и управляться.

ПРИМЕЧАНИЕ. Доступ может подразумевать решение о разрешении только на просмотр документированной информации или о разрешении и полномочиях на просмотр и изменение документированной информации и т. д.

8 Функционирование

8.1 Оперативное планирование и управление

Организация должна планировать, внедрять и контролировать процессы, необходимые для удовлетворения требований и выполнения действий, определенных в разделе 6, путем:

- установления критериев для процессов;

- осуществления контроля процессов в соответствии с критериями.

Документированная информация должна быть доступна в объеме, необходимом для обеспечения уверенности в том, что процессы выполняются в соответствии с планом.

© ISO/IEC 2022 – Все права защищены

Организация должна контролировать запланированные изменения и анализировать последствия непреднамеренных изменений, при необходимости предпринимая действия для смягчения любых неблагоприятных последствий.

Организация должна гарантировать, что предоставляемые извне процессы, продукты или услуги, которые имеют отношение к системе менеджмента информационной безопасности, находятся под контролем.

8.2 Оценка рисков информационной безопасности

Организация должна проводить оценки рисков информационной безопасности через запланированные интервалы времени или когда предлагаются или происходят значительные изменения, принимая во внимание критерии, установленные в 6.1.2 а).

Организация должна сохранять документированную информацию о результатах оценок рисков информационной безопасности.

8.3 Обработка рисков информационной безопасности

Организация должна реализовать план обработки рисков информационной безопасности.

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

9 Оценка результатов деятельности

9.1 Мониторинг, измерение, анализ и оценка

Организация должна определить:

А) что необходимо отслеживать и измерять, включая процессы и средства управления информационной безопасностью;

Б) методы мониторинга, измерения, анализа и оценки, если применимо, для обеспечения достоверных результатов. Выбранные методы должны давать сопоставимые и воспроизводимые результаты, чтобы их можно было считать действительными;

В) когда должны проводиться мониторинг и измерения;

Г) кто должен проводить мониторинг и измерения;

Д) когда результаты мониторинга и измерений должны быть проанализированы и оценены;

Е) кто будет анализировать и оценивать эти результаты.

Должна быть доступна документированная информация, подтверждающая результаты.

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

9.2 Внутренний аудит

9.2.1 Общие положения

Организация должна проводить внутренние аудиты через запланированные промежутки времени, чтобы предоставить информацию о том, что система менеджмента информационной безопасности:

А) соответствует

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

© ISO/IEC 2022 – Все права защищены

2) требованиям данного документа;

Б) эффективно внедряется и поддерживается.

9.2.2 Программа внутреннего аудита

Организация должна планировать, устанавливать, внедрять и поддерживать программу(ы) аудита, включая периодичность, методы, обязанности, требования к планированию и отчетность.

При разработке программы (программ) внутреннего аудита организация должна учитывать важность соответствующих процессов и результаты предыдущих аудитов.

Организация должна:

А) определить критерии аудита и объем для каждого аудита;

Б) выбирать аудиторов и проводить проверки, обеспечивающие объективность и беспристрастность процесса проверки;

В) обеспечить, чтобы результаты проверок были доведены до сведения соответствующего руководства;

Должна быть доступна документированная информация, подтверждающая выполнение программы (программ) аудита и результаты аудита.

9.3 Анализ менеджмента

9.3.1 Общие положения

Высшее руководство должно пересматривать систему менеджмента информационной безопасности организации через запланированные промежутки времени, чтобы гарантировать ее постоянную пригодность, соответствие и эффективность.

9.3.2 Входные данные для анализа со стороны руководства

Анализ со стороны руководства должен включать рассмотрение:

А) статуса действий из предыдущих обзоров руководства;

Б) изменения внешних и внутренних вопросов, имеющих отношение к системе менеджмента информационной безопасности;

В) изменения потребностей и ожиданий заинтересованных сторон, имеющих отношение к системе менеджмента информационной безопасности;

Г) отзывы о показателях информационной безопасности, включая тенденции в:

1) несоответствиях и корректирующих действиях;

2) результатах мониторинга и измерений;

3) результатах аудитов;

4) выполнении задач информационной безопасности;

Д) обратную связь от заинтересованных сторон;

Е) результаты оценки рисков и состояние плана обработки рисков;

Ж) возможности для непрерывного улучшения.

9.3.3 Результаты проверки руководством

Результаты анализа со стороны руководства должны включать решения, касающиеся возможностей постоянного улучшения и любых потребностей в изменениях системы менеджмента информационной безопасности.

© ISO/IEC 2022 – Все права защищены

Документированная информация должна быть доступна в качестве доказательства результатов анализа со стороны руководства.

10 Улучшение

10.1 Непрерывное улучшение

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

10.2 Несоответствия и корректирующие действия

При возникновении несоответствия организация должна:

А) реагировать на несоответствие и, если применимо:

1) принять меры по его контролю и исправлению;

2) применять меры в отношении последствий;

Б) оценить необходимость действий по устранению причин несоответствия, чтобы оно не повторилось или не произошло где-либо еще, путем:

1) рассмотрения несоответствия;

2) определения причин несоответствия; а также

3) определения наличия или потенциального возникновения подобных несоответствий;

В) выполнить любое необходимое действие;

Г) анализировать эффективность любых предпринятых корректирующих действий; а также

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

Корректирующие действия должны соответствовать последствиям выявленных несоответствий.

Документированная информация должна быть доступна в качестве доказательства:

Е) характера несоответствий и любых последующих предпринятых действий,

Ж) результатов любого корректирующего действия.

© ISO/IEC 2022 – Все права защищены

Приложение А

(нормативное)

Справочник по средствам управления информационной безопасностью

Средства управления информационной безопасностью, перечисленные в таблице А.1, непосредственно получены из средств, перечисленных в ISO/IEC 27002:2022 [1], разделы 5–8, и согласуются с ними, и должны использоваться в контексте с 6.1.3.

Таблица А.1 - Средства управления информационной безопасностью

5	**Организационные средства управления**	
5.1	Политики информационной безопасности	**Средство управления** Политика информационной безопасности и тематические политики должны быть определены, одобрены руководством, опубликованы, доведены до сведения и подтверждены соответствующим персоналом и соответствующими заинтересованными сторонами, а также пересматриваться через запланированные интервалы времени и в случае возникновения существенных изменений.
5.2	Должностные функции и обязанности в области информационной безопасности	**Средство управления** Должностные функции и обязанности в области информационной безопасности должны быть определены и распределены в соответствии с потребностями организации.
5.3	Разделение обязанностей	**Средство управления** Конфликтующие обязанности и конфликтующие области ответственности должны быть разделены.
5.4	Обязанности руководства	**Средство управления** Руководство должно требовать от всего персонала применения информационной безопасности в соответствии с установленной политикой информационной безопасности, конкретными политиками и процедурами организации.
5.5	Контакты с полномочными органами	**Средство управления** Организация должна установить и поддерживать контакт с соответствующими органами.
5.6	Контакты с профессиональными сообществами	**Средство управления** Организация должна устанавливать и поддерживать контакты с профессиональными сообществами или другими специализированными форумами по безопасности и профессиональными ассоциациями.
5.7	Аналитика угроз	**Средство управления** Информация, относящаяся к угрозам информационной безопасности, должна собираться и анализироваться для получения информации об угрозах.
5.8	Информационная безопасность в управлении проектами	**Средство управления** Информационная безопасность должна быть интегрирована в управление проектами.
5.9	Инвентаризация информации и других связанных активов	**Средство управления** Должен быть разработан перечень информации и других связанных активов, включая владельцев, который будет поддерживаться в актуальном состоянии
5.10	Допустимое использование информации и других связанных активов	**Средство управления** Должны быть определены, задокументированы и реализованы правила приемлемого использования и процедуры обращения с информацией и другими связанными активами.
5.11	Возврат активов	**Средство управления** Персонал и другие заинтересованные стороны, в зависимости от обстоятельств, должны вернуть все активы организации, находящиеся в их владении, при изменении или прекращении их работы, контракта или соглашения.

© ISO/IEC 2022 – Все права защищены

Таблица A.1 (продолжение)

5.12	Классификация информации	**Средство управления** Информация должна быть классифицирована в соответствии с потребностями информационной безопасности организации на основе конфиденциальности, целостности, доступности и соответствующих требований заинтересованных сторон.
5.13	Маркировка информации	**Средство управления** Соответствующий набор процедур для маркировки информации должен быть разработан и реализован в соответствии со схемой классификации информации, принятой в организации.
5.14	Передача информации	**Средство управления** Правила передачи информации, процедуры или соглашения должны действовать для всех типов средств передачи внутри организации и между организацией и другими сторонами.
5.15	Контроль доступа	**Средство управления** Правила для контроля физического и логического доступа к информации и другим связанным активам должны быть установлены и реализованы на основе требований бизнеса и информационной безопасности.
5.16	Управление идентификацией	**Средство управления** Должен управляться полный жизненный цикл удостоверений.
5.17	Аутентификационная информация	**Средство управления** Распределение и управление аутентификационной информацией должно контролироваться процессом управления, включая консультирование персонала по надлежащему обращению с аутентификационной информацией.
5.18	Права доступа	**Средство управления** Права доступа к информации и другим связанным с ними активам должны предоставляться, проверяться, модифицироваться и удаляться в соответствии с тематическими политиками и правилами управления доступом организации.
5.19	Информационная безопасность в отношениях с поставщиками	**Средство управления** Процессы и процедуры должны быть определены и внедрены для управления рисками информационной безопасности, связанными с использованием продуктов или услуг поставщика.
5.20	Обеспечение информационной безопасности в рамках соглашений с поставщиками	**Средство управления** Соответствующие требования информационной безопасности должны быть установлены и согласованы с каждым поставщиком в зависимости от типа отношений с поставщиком.
5.21	Управление информационной безопасностью в цепочке поставок информационно-коммуникационных технологий (ИКТ)	**Средство управления** Процессы и процедуры должны быть определены и внедрены для управления рисками информационной безопасности, связанными с цепочкой поставок продуктов и услуг ИКТ.
5.22	Мониторинг, проверка и управление изменениями в услугах поставщиков	**Средство управления** Организация должна регулярно отслеживать, анализировать, оценивать и управлять изменениями в методах информационной безопасности поставщиков и предоставлении услуг.
5.23	Информационная безопасность при использовании облачных сервисов	**Средство управления** Процессы приобретения, использования, управления и выхода из облачных сервисов должны быть установлены в соответствии с требованиями информационной безопасности организации.
5.24	Планирование и подготовка к управлению инцидентами информационной безопасности	**Средство управления** Организация должна планировать и готовиться к управлению инцидентами ИБ, определяя, устанавливая и сообщая процессы управления инцидентами ИБ, роли и обязанности.

© ISO/IEC 2022 – Все права защищены

Таблица A.1 (продолжение)

5.25	Оценка и принятие решений по событиям информационной безопасности	**Средство управления** Организация должна оценивать события информационной безопасности и решать, следует ли их классифицировать как инциденты информационной безопасности.
5.26	Реагирование на инциденты информационной безопасности	**Средство управления** На инциденты информационной безопасности необходимо реагировать в соответствии с документированными процедурами.
5.27	Учимся на инцидентах информационной безопасности	**Средство управления** Знания, полученные в результате инцидентов информационной безопасности, должны использоваться для укрепления и улучшения средств контроля информационной безопасности.
5.28	Сбор доказательств	**Средство управления** Организация должна установить и внедрить процедуры идентификации, сбора, получения и сохранения свидетельств, связанных с событиями информационной безопасности.
5.29	Информационная безопасность во время сбоев	**Средство управления** Организация должна планировать, как поддерживать информационную безопасность на соответствующем уровне во время сбоев.
5.30	Готовность ИКТ к обеспечению непрерывности бизнеса	**Средство управления** Готовность ИКТ должна планироваться, внедряться, поддерживаться и тестироваться на основе целей обеспечения непрерывности бизнеса и требований к обеспечению непрерывности ИКТ.
5.31	Юридические, законодательные, нормативные и договорные требования	**Средство управления** Юридические, законодательные, нормативные и договорные требования, относящиеся к информационной безопасности, и подход организации к выполнению этих требований должны быть идентифицированы, задокументированы и обновлены.
5.32	Права интеллектуальной собственности	**Средство управления** Организация должна внедрить соответствующие процедуры для защиты прав интеллектуальной собственности.
5.33	Защита записей	**Средство управления** Записи должны быть защищены от потери, уничтожения, фальсификации, несанкционированного доступа и несанкционированного раскрытия.
5.34	Конфиденциальность и защита личной информации (PII)	**Средство управления** Организация должна определить и выполнить требования в отношении сохранения конфиденциальности и защиты PII в соответствии с применимыми законами и правилами, а также договорными требованиями.
5.35	Независимая проверка информационной безопасности	**Средство управления** Подход организации к управлению информационной безопасностью и его реализации, включая людей, процессы и технологии, должен пересматриваться независимо через запланированные промежутки времени или при возникновении существенных изменений.
5.36	Соблюдение политик, правил и стандартов информационной безопасности	**Средство управления** Соблюдение политики информационной безопасности организации, тематических политик, правил и стандартов должно регулярно пересматриваться.
5.37	Документированные рабочие процедуры	**Средство управления** Операционные процедуры для средств обработки информации должны быть задокументированы и доступны для персонала, который в них нуждается.

© ISO/IEC 2022 – Все права защищены

Таблица A.1 (продолжение)

6	**Управление людьми**	
6.1	Скрининг	**Средство управления** Проверки биографических данных всех кандидатов на должность персонала должны проводиться до поступления на работу в организацию и на постоянной основе с учетом применимых законов, правил и этических норм и должны быть пропорциональны бизнес-требованиям, классификации информации, к которой необходимо получить доступ, и предполагаемые риски.
6.2	Условия трудоустройства	**Средство управления** В трудовых договорах должны быть указаны обязанности персонала и организации по обеспечению информационной безопасности.
6.3	Осведомленность, образование и обучение в области информационной безопасности	**Средство управления** Персонал организации и соответствующие заинтересованные стороны должны получать соответствующие знания, образование и обучение по информационной безопасности, а также регулярные обновления политики информационной безопасности организации, политик и процедур, относящихся к конкретным темам, в соответствии с их должностными обязанностями.
6.4	Дисциплинарный процесс	**Средство управления** Должно быть формализовано и доведено до сведения дисциплинарное производство для принятия мер в отношении персонала и других соответствующих заинтересованных сторон, допустивших нарушение политики информационной безопасности.
6.5	Обязанности после увольнения или смены места работы	**Средство управления** Обязанности и ответственность по информационной безопасности, которые остаются в силе после увольнения или смены работы, должны быть определены, введены в действие и доведены до сведения соответствующего персонала и других заинтересованных сторон.
6.6	Соглашения о конфиденциальности или неразглашении	**Средство управления** Соглашения о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны быть идентифицированы, задокументированы, регулярно пересматриваться и подписываться персоналом и другими соответствующими заинтересованными сторонами.
6.7	Удаленная работа	**Средство управления** Меры безопасности должны быть реализованы, когда персонал работает удаленно, для защиты информации, к которой осуществляется доступ, которая обрабатывается или хранится за пределами помещений организации.
6.8	Отчетность о событиях информационной безопасности	**Средство управления** Организация должна предоставить персоналу механизм своевременного сообщения о наблюдаемых или предполагаемых событиях информационной безопасности по соответствующим каналам.
7	**Физические средства управления**	
7.1	Периметры физической безопасности	**Средство управления** Периметры безопасности должны быть определены и использоваться для защиты областей, содержащих информацию и другие связанные активы.
7.2	Физический вход	**Средство управления** Безопасные зоны должны быть защищены соответствующими контрольно-пропускными пунктами и точками доступа.
7.3	Охрана офисов, помещений и сооружений	**Средство управления** Должна быть разработана и реализована физическая охрана офисов, помещений и сооружений.
7.4	Мониторинг физической безопасности	**Средство управления** Помещения должны находиться под постоянным контролем на предмет несанкционированного физического доступа.

© ISO/IEC 2022 – Все права защищены

Таблица A.1 (продолжение)

7.5	Защита от физических и экологических угроз	**Средство управления** Должна быть разработана и реализована защита от физических и экологических угроз, таких как стихийные бедствия и другие преднамеренные или непреднамеренные физические угрозы инфраструктуре.
7.6	Работа в безопасных зонах	**Средство управления** Должны быть разработаны и реализованы меры безопасности для работы в безопасных зонах.
7.7	Чистый стол и чистый экран	**Средство управления** Должны быть определены и должным образом применяться правила чистого рабочего стола для бумаги и съемных носителей информации, а также правила чистого экрана для средств обработки информации.
7.8	Размещение и защита оборудования	**Средство управления** Оборудование должно быть надежно закреплено и защищено.
7.9	Безопасность активов вне помещений	**Средство управления** Внешние активы должны быть защищены.
7.10	Носители информации	**Средство управления** Управление носителями информации должно осуществляться на протяжении их жизненного цикла приобретения, использования, транспортировки и утилизации в соответствии со схемой классификации организации и требованиями обращения с ними.
7.11	Вспомогательные энергетические системы	**Средство управления** Средства обработки информации должны быть защищены от перебоев в электроснабжении и других сбоев, вызванных отказами вспомогательных энергетических сетей.
7.12	Безопасность кабелей	**Средство управления** Кабели, передающие энергию, данные или вспомогательные информационные услуги, должны быть защищены от перехвата, вмешательства или повреждения.
7.13	Обслуживание оборудования	**Средство управления** Оборудование должно правильно обслуживаться для обеспечения доступности, целостности и конфиденциальности информации.
7.14	Безопасная утилизация или повторное использование оборудования	**Средство управления** Элементы оборудования, содержащие носители данных, должны быть проверены, чтобы гарантировать, что любые конфиденциальные данные и лицензионное программное обеспечение были удалены или надежно перезаписаны перед утилизацией или повторным использованием.
8	**Технические средства управления**	
8.1	Пользовательские конечные устройства	**Средство управления** Информация, хранящаяся, обрабатываемая или доступная через пользовательские оконечные устройства, должна быть защищена.
8.2	Привилегированные права доступа	**Средство управления** Назначение и использование привилегированных прав доступа должно быть ограниченным и контролируемым.
8.3	Ограничение доступа к информации	**Средство управления** Доступ к информации и другим связанным активам должен быть ограничен в соответствии с установленной политикой управления доступом для конкретной темы.
8.4	Доступ к исходному коду	**Средство управления** Доступ для чтения и записи к исходному коду, средствам разработки и программным библиотекам должен управляться надлежащим образом.

© ISO/IEC 2022 – Все права защищены

Таблица А.1 (продолжение)

8.5	Безопасная аутентификация	**Средство управления** Технологии и процедуры безопасной аутентификации должны быть реализованы на основе ограничений доступа к информации и тематической политики управления доступом.
8.6	Управление мощностями	**Средство управления** Использование ресурсов должно контролироваться и корректироваться в соответствии с текущими и ожидаемыми потребностями в мощности.
8.7	Защита от вредоносных программ	**Средство управления** Защита от вредоносных программ должна быть реализована и поддерживаться соответствующей осведомленностью пользователей.
8.8	Управление техническими уязвимостями	**Средство управления** Должна быть получена информация о технических уязвимостях используемых информационных систем, оценена подверженность организации таким уязвимостям и приняты соответствующие меры.
8.9	Управление конфигурацией	**Средство управления** Конфигурации, включая конфигурации безопасности, аппаратного обеспечения, программного обеспечения, услуг и сетей должны быть установлены, задокументированы, реализованы, отслежены и проверены.
8.10	Удаление информации	**Средство управления** Информация, хранящаяся в информационных системах, устройствах или любых других носителях информации, подлежит удалению, когда она больше не требуется.
8.11	Маскировка данных	**Средство управления** Маскирование данных должно использоваться в соответствии с тематической политикой организации по управлению доступом и другими связанными тематическими политиками, а также бизнес-требованиями с учетом применимого законодательства.
8.12	Предотвращение утечки данных	**Средство управления** Меры по предотвращению утечки данных должны применяться к системам, сетям и любым другим устройствам, которые обрабатывают, хранят или передают конфиденциальную информацию.
8.13	Резервное копирование информации	**Средство управления** Резервные копии информации, программного обеспечения и систем должны поддерживаться и регулярно тестироваться в соответствии с согласованной темой политики резервного копирования.
8.14	Избыточность средств обработки информации	**Средство управления** Средства обработки информации должны быть реализованы с избыточностью, достаточной для удовлетворения требований доступности.
8.15	Ведение журнала	**Средство управления** Должны создаваться, храниться, защищаться и анализироваться журналы, в которых регистрируются действия, исключения, неисправности и другие соответствующие события.
8.16	Деятельность по мониторингу	**Средство управления** Сети, системы и приложения должны отслеживаться на предмет аномального поведения и предприниматься соответствующие действия для оценки потенциальных инцидентов информационной безопасности.
8.17	Синхронизация часов	**Средство управления** Часы систем обработки информации, используемых организацией, должны быть синхронизированы с утвержденными источниками времени.

© ISO/IEC 2022 – Все права защищены

Таблица A.1 (продолжение)

8.18	Использование привилегированных служебных программ	**Средство управления** Использование служебных программ, способных переопределить средства управления системой и приложениями, должно быть ограничено и строго контролироваться.
8.19	Установка ПО на операционные системы	**Средство управления** Должны быть реализованы процедуры и меры для безопасного управления установкой программного обеспечения в операционных системах.
8.20	Безопасность сетей	**Средство управления** Сети и сетевые устройства должны быть защищены, управляться и контролироваться для защиты информации в системах и приложениях.
8.21	Безопасность сетевых сервисов	**Средство управления** Механизмы безопасности, уровни обслуживания и требования к обслуживанию сетевых услуг должны быть идентифицированы, реализованы и проверены.
8.22	Разделение сетей	**Средство управления** Группы информационных служб, пользователей и информационных систем должны быть разделены в сетях организации.
8.23	Веб-фильтрация	**Средство управления** Доступ к внешним веб-сайтам должен регулироваться, чтобы уменьшить подверженность вредоносному контенту.
8.24	Использование криптографии	**Средство управления** Должны быть определены и реализованы правила эффективного использования криптографии, включая управление криптографическими ключами.
8.25	Безопасный жизненный цикл разработки	**Средство управления** Должны быть установлены и применяться правила безопасной разработки программного обеспечения и систем.
8.26	Требования безопасности приложений	**Средство управления** Требования информационной безопасности должны быть идентифицированы, указаны и утверждены при разработке или приобретении приложений.
8.27	Безопасная системная архитектура и инженерные принципы	**Средство управления** Принципы инженерно-безопасных систем должны быть установлены, задокументированы, поддерживаться и применяться к любой деятельности по разработке информационных систем.
8.28	Безопасное кодирование	**Средство управления** При разработке программного обеспечения должны применяться принципы безопасного кодирования.
8.29	Тестирование безопасности в разработке и приемке	**Средство управления** Процессы тестирования безопасности должны быть определены и реализованы в жизненном цикле разработки.
8.30	Аутсорсинговая разработка	**Средство управления** Организация должна направлять, контролировать и анализировать деятельность, связанную с разработкой системы, переданной на аутсорсинг.

© ISO/IEC 2022 – Все права защищены

8.31	Разделение среды разработки, тестирования и производства	**Средство управления** Среды разработки, тестирования и производства должны быть разделены и защищены.
8.32	Управление изменениями	**Средство управления** Изменения в средствах обработки информации и информационных системах подлежат процедурам управления изменениями.
8.33	Информация о тестировании	**Средство управления** Информация о тестировании должна соответствующим образом выбираться, защищаться и управляться.
8.34	Защита информационных систем при аудиторском тестировании	**Средство управления** Аудиторские тесты и другие действия по обеспечению уверенности, связанные с оценкой операционных систем, должны планироваться и согласовываться между тестировщиком и соответствующим руководством.

© ISO/IEC 2022 – Все права защищены

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*

© ISO/IEC 2022 – Все права защищены

ICS 03.100.70; 35.030

© ISO/IEC 2022 – Все права защищены