ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28000— 2025

Безопасность и устойчивость

СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ

Требования

(ISO 28000:2022, IDT)

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 010 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 сентября 2025 г. № 976-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28000:2022 «Безопасность и устойчивость. Системы менеджмента безопасности. Требования» (ISO 28000:2022 «Security and resilience — Security management systems — Requirements», IDT).

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

5 ВЗАМЕН ГОСТ Р ИСО 28000—2019

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

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

© ISO, 2022
© Оформление. ФГБУ «Институт стандартизации», 2025

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Среда организации 3
4.1 Понимание организацией своей среды 3
4.2 Понимание потребностей и ожиданий заинтересованных сторон 3
4.3 Определение области применения системы менеджмента безопасности 5
4.4 Система менеджмента безопасности 5
5 Лидерство 5
5.1 Лидерство и приверженность 5
5.2 Политика в области безопасности 6
5.3 Роли, обязанности, ответственность и полномочия 6
6 Планирование 7
6.1 Действия в отношении рисков и возможностей 7
6.2 Цели в области безопасности и планирование их достижения 7
6.3 Планирование изменений 8
7 Средства обеспечения 8
7.1 Ресурсы 8
7.2 Компетентность 8
7.3 Осведомленность 8
7.4 Обмен информацией 9
7.5 Документированная информация 9
8 Деятельность 10
8.1 Планирование и управление 10
8.2 Идентификация процессов и видов деятельности 10
8.3 Оценка рисков и воздействие на них 10
8.4 Средства управления 10
8.5 Стратегии, процедуры, процессы и подходы к обеспечению безопасности 11
8.6 Планы обеспечения безопасности 11
9 Оценка результатов деятельности 13
9.1 Мониторинг, измерение, анализ и оценка 13
9.2 Внутренний аудит 13
9.3 Анализ со стороны руководства 14
10 Улучшение 14
10.1 Постоянное улучшение 14
10.2 Несоответствие и корректирующее действие 15
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 16
Библиография 17

Введение

Большинство организаций сталкиваются с растущей неопределенностью и нестабильностью в области обеспечения безопасности. Как следствие, организации сталкиваются с проблемами обеспечения безопасности, влияющими на их цели. Эти проблемы организации хотят решать систематизированно в рамках своей системы менеджмента. Применение системы менеджмента безопасности может напрямую способствовать повышению делового потенциала и авторитета организации.

Настоящий стандарт устанавливает требования к системе менеджмента безопасности, включая аспекты, которые являются критическими для обеспечения безопасности цепи поставок. От организации требуется:

- оценить безопасность среды, в которой она работает, включая свою цепь поставок (а также связи и взаимосвязи);
- определить наличие надлежащих мер безопасности для результативного менеджмента рисков, связанных с безопасностью;
- контролировать соблюдение законодательных, нормативных обязательств и добровольных обязательств, к которым присоединяется организация;
- привести в соответствие процессы и средства управления безопасностью, включая соответствующие фазы предконтроля и постконтроля и средства управления цепями поставок, для достижения целей организации.

Менеджмент безопасности связан со множеством аспектов управления деятельностью. Эти аспекты включают виды деятельности, находящиеся под управлением и влиянием организаций, включая, среди прочего, те виды деятельности, которые влияют на цепь поставок. Следует учитывать все виды деятельности, функции и операции, которые оказывают влияние на менеджмент безопасности организации, включая (но не ограничиваясь этим) ее цепь поставок.

Цепи поставок носят динамический характер. Поэтому некоторые организации, управляющие несколькими цепями поставок, могут запросить у поставщиков подтверждение соблюдения ими соответствующих стандартов безопасности в качестве условия включения в эту цепь поставок, чтобы выполнить требования к менеджменту безопасности.

Настоящий стандарт основан на методологии, известной как цикл «Планируй—Делай—Проверяй—Действуй» (PDCA) для планирования, создания, внедрения, функционирования, мониторинга, анализа, поддержания и постоянного улучшения результативности системы менеджмента безопасности организации (см. таблицу 1 и рисунок 1).

Таблица 1 — Пояснение к циклу PDCA

Планируй (установи)	Разработать политику обеспечения безопасности, поставить цели, задачи, обеспечить средства управления, выбрать процессы и процедуры, связанные с повышением безопасности, для достижения результатов, соответствующих общей политике и целям организации
Делай (внедри и функционируй)	Внедрить и применять политику, средства управления, процессы и процедуры в области безопасности
Проверяй (мониторинг и анализ)	Осуществлять мониторинг и анализировать показатели деятельности в соответствии с политикой и целями, сообщать о результатах руководству для анализа, определять и санкционировать действия по исправлению и улучшению
Действуй (поддерживай и улучшай)	Поддерживать и улучшать систему менеджмента безопасности путем осуществления корректирующих действий, основанных на результатах анализа со стороны руководства и пересмотра области применения системы менеджмента безопасности, политики и целей в области безопасности

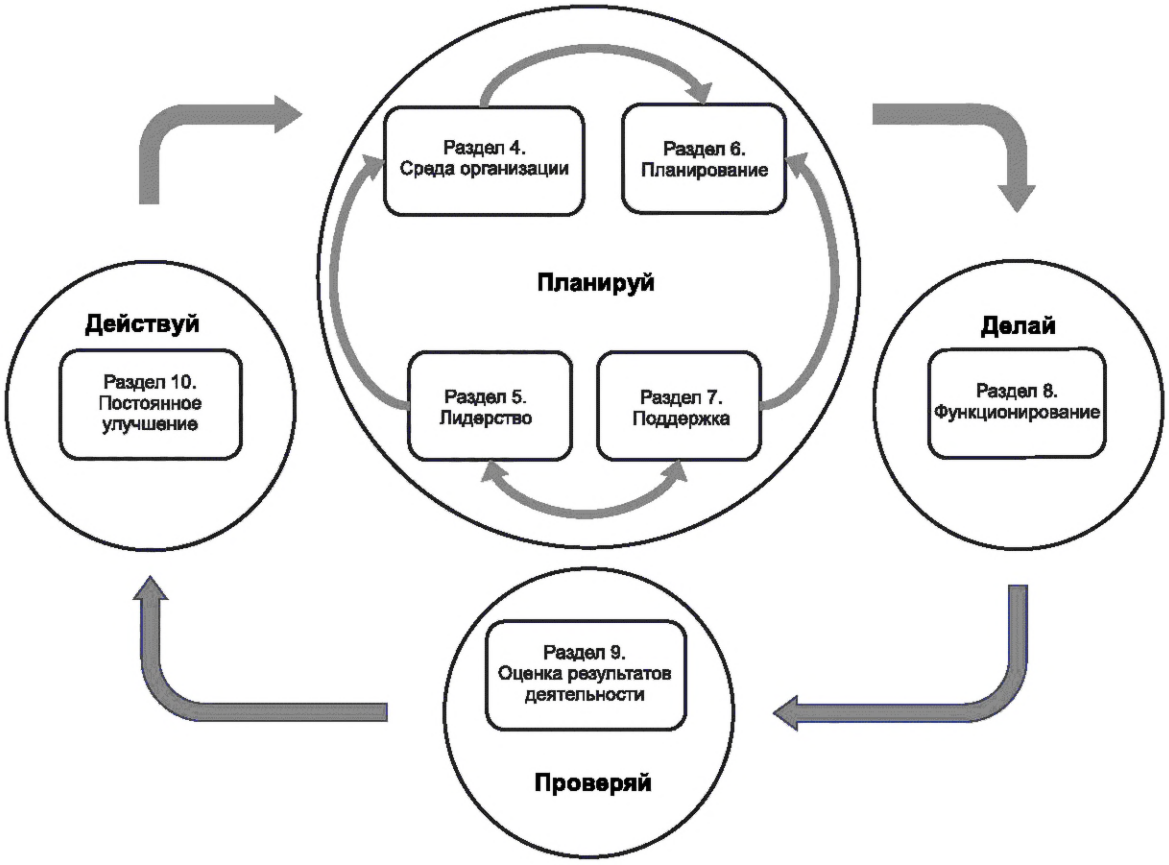

Рисунок 1 — Цикл PDCA, применяемый к системе менеджмента безопасности

Этот цикл обеспечивает согласованность требований настоящего стандарта с другими стандартами на системы менеджмента, а именно с ИСО 9001, ИСО 14001, ИСО 22301, ИСО/МЭК 27001, ИСО 45001 и пр., поддерживая, таким образом, последовательное и комплексное внедрение и применение соответствующих систем менеджмента.

Организации могут подтвердить соответствие системы менеджмента безопасности настоящему стандарту посредством проведения внешнего или внутреннего аудита.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность и устойчивость

СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ

Требования

Security and resilience. Security management systems. Requirements

Дата введения — 2026—03—01

1 Область применения

Настоящий стандарт устанавливает требования к системе менеджмента безопасности, включая аспекты, относящиеся к цепи поставок.

Настоящий стандарт применим к организациям всех типов и размеров (например, коммерческие предприятия, государственные или иные общественные учреждения и некоммерческие организации), которые хотят разработать, применять, поддерживать и улучшать систему менеджмента безопасности. Настоящий стандарт обеспечивает единый и комплексный подход и не относится к конкретной отрасли или сектору экономики.

Настоящий стандарт можно использовать на протяжении всего жизненного цикла организации, он может применяться к любому виду деятельности, внутренней или внешней, на всех уровнях.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт [для датированной ссылки применяют только указанное издание ссылочного стандарта, для недатированной — последнее издание (включая все изменения)]:

ISO 22300, Security and resilience — Vocabulary (Безопасность и устойчивость. Словарь)

3 Термины и определения

В настоящем стандарте применены термины и определения по ИСО 22300, а также следующие термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных для использования в целях стандартизации, находящиеся по следующим адресам:

- платформа онлайн-просмотра ИСО доступна по адресу: gost.e-ecolog.ru ;
- Электропедия МЭК доступна по адресу: gost.e-ecolog.ru .

3.1 **организация** (organization): Лицо или группа людей, связанные определенными отношениями, имеющие ответственность, полномочия и выполняющие свои функции для достижения их *целей* (3.7).

Примечание 1 — Понятие организации включает в себя, но не ограничивается следующими примерами: индивидуальный предприниматель, компания, корпорация, фирма, предприятие, орган власти, товарищество, благотворительная организация, а также их часть или их объединение, являющиеся юридическим лицом или нет, государственные или частные.

Примечание 2 — Если рассматриваемая организация является частью более крупной структуры (организации), термин «организация» относится только к той части более крупной структуры, которая входит в область применения *системы менеджмента безопасности* (3.5).

Издание официальное

3.2 **заинтересованная сторона** (interested party), **стейкхолдер** (stakeholder): Лицо или *организация* (3.1), которые могут влиять на осуществление деятельности или принятие решения, быть подверженными их влиянию или воспринимать себя в качестве последних.

3.3 **высшее руководство** (security management/top management): Лицо или группа людей, осуществляющих руководство и управление *организацией* (3.1) на высшем уровне.

Примечание 1 — Высшее руководство имеет право делегировать полномочия и предоставлять ресурсы в рамках организации.

Примечание 2 — Если область применения системы *менеджмента* (3.4) охватывает только часть организации, под высшим руководством подразумевают тех, кто осуществляет руководство и управляет именно этой частью организации.

3.4 **система менеджмента** (management system): Совокупность взаимосвязанных или взаимодействующих элементов *организации* (3.1) для установления *политик* (3.6), *целей* (3.7) и *процессов* (3.9) для достижения этих целей.

Примечание 1 — Система менеджмента может относиться к одному или нескольким направлениям деятельности.

Примечание 2 — Элементы системы менеджмента включают структуру организации, роли и ответственность, планирование и функционирование.

3.5 **система менеджмента безопасности** (security management system): Система скоординированных *политик* (3.6), *процессов* (3.9) и практик, посредством которых организация осуществляет менеджмент своих *целей* (3.7) безопасности.

3.6 **политика** (policy): Намерения и направление развития *организации* (3.1), официально сформулированные ее высшим руководством (3.3).

3.7 **цель** (objective): Результат, который должен быть достигнут.

Примечание 1 — Цель может быть стратегической, тактической или оперативной.

Примечание 2 — Цели могут относиться к разным аспектам (таким, как финансовые цели, цели в области здоровья и безопасности, экологии), а также применяться на разных уровнях [например, организации в целом, проекта, продукции и *процесса* (3.9)].

Примечание 3 — Цель может быть выражена разными способами, например в виде намеченного результата, намерения, критерия работы, цели в области безопасности или другими словами со схожими значениями (например, целевая установка, заданная величина, задача).

Примечание 4 — В контексте *системы менеджмента безопасности* (3.5), цели в области безопасности, устанавливаемые *организацией* (3.1), согласуют с *политикой* (3.6) в области безопасности для достижения определенных результатов.

3.8 **риск** (risk): Влияние неопределенности на *цели* (3.7).

Примечание 1 — Влияние выражается в отклонении от ожидаемого результата — позитивном и/или негативном и может быть реакцией на возможности и угрозы, создавать их или приводить к их появлению.

Примечание 2 — Цели могут иметь различные аспекты и относиться к разным категориям, а также могут быть поставлены применительно к разным уровням.

Примечание 3 — Риск обычно выражается в терминах источников риска, потенциально возможных событий, их последствий и их вероятности.

3.9 **процесс** (process): Совокупность взаимосвязанных или взаимодействующих видов деятельности, использующих входы для получения результата.

Примечание — В зависимости от контекста «результат» называется выходом, продукцией или услугой.

3.10 **компетентность** (competence): Способность применять знания и навыки для достижения намеченных результатов.

3.11 **документированная информация** (documented information): Информация, которая должна управляться и поддерживаться *организацией* (3.1), и носитель, который ее содержит.

Примечание 1 — Документированная информация может быть любого формата и на любом носителе и может быть получена из любого источника.

Примечание 2 — Документированная информация может относиться:
- к *системе менеджмента* (3.4), включая соответствующие *процессы* (3.9);
- к информации, созданной для функционирования организации (документация);
- к свидетельствам достигнутых результатов (записи).

3.12 **результаты деятельности** (performance): Измеримый итог.

Примечание 1 — Результаты деятельности могут относиться к количественным или качественным полученным данным.

Примечание 2 — Результаты деятельности могут относиться к менеджменту, *процессам* (3.9), продукции, услугам, системам или *организациям* (3.1).

3.13 **постоянное улучшение** (continual improvement): Повторяющаяся деятельность по улучшению *результатов деятельности* (3.12).

3.14 **результативность** (effectiveness): Степень реализации запланированной деятельности и достижения запланированных результатов.

3.15 **требование** (requirement): Потребность или ожидание, которое установлено, обычно предполагается или является обязательным.

Примечание 1 — Слова «обычно предполагается» означают, что это общепринятая практика *организации* (3.1) и *заинтересованных сторон* (3.2), что рассматриваемые потребности или ожидания предполагаются.

Примечание 2 — Установленным является такое требование, которое определено, например, в *документированной информации* (3.11).

3.16 **соответствие** (conformity): Выполнение *требования* (3.15).

3.17 **несоответствие** (nonconformity): Невыполнение *требования* (3.15).

3.18 **корректирующее действие** (corrective action): Действие, предпринятое для устранения причины *несоответствия* (3.17) и предупреждения его повторного возникновения.

3.19 **аудит** (audit): Систематический, независимый и документированный *процесс* (3.9) получения свидетельств аудита и их объективного оценивания для установления степени соответствия критериям аудита.

Примечание 1 — Аудит может быть внутренним (аудит, проводимый первой стороной) или внешним (аудит, проводимый второй или третьей стороной), а также аудит может быть комплексным или совместным.

Примечание 2 — Внутренний аудит проводит сама *организация* (3.1) или внешняя сторона от имени организации.

Примечание 3 — Понятия «свидетельство аудита» и «критерии аудита» установлены в ИСО 19011.

3.20 **измерение** (measurement): *Процесс* (3.9) определения величины.

3.21 **мониторинг** (monitoring): Определение статуса системы, *процесса* (3.9) или действия.

Примечание — Для определения статуса может возникнуть необходимость проверить, проконтролировать или отследить.

4 Среда организации

4.1 Понимание организацией своей среды

Организация должна определить внешние и внутренние факторы, относящиеся к ее намерениям и влияющие на ее способность достигать намеченного(ых) результата(ов) ее системы менеджмента безопасности, включая требования к ее цепи поставок.

4.2 Понимание потребностей и ожиданий заинтересованных сторон

4.2.1 Общие положения

Организация должна определять:
- заинтересованные стороны, имеющие отношение к системе менеджмента безопасности;
- соответствующие требования этих заинтересованных сторон;
- какие из этих требований будут рассмотрены в рамках системы менеджмента безопасности.

4.2.2 Законодательные, нормативные правовые и другие требования

Организация должна:

a) внедрить и поддерживать процесс выявления, получения доступа и оценки применимых законодательных, нормативных правовых и других требований, относящихся к ее безопасности;

b) обеспечить, чтобы эти применимые законодательные, нормативные правовые и другие требования учитывались при внедрении и поддержании системы менеджмента безопасности;

c) документировать эту информацию и поддерживать ее в актуальном состоянии;

d) в той степени, в какой это подходит, сообщать эту информацию соответствующим заинтересованным сторонам.

4.2.3 Принципы

4.2.3.1 Общие положения

Целью менеджмента безопасности в организации является создание ценностей и, особенно, их защита.

Организации следует применять принципы, приведенные на рисунке 2 и описанные в 4.2.3.2—4.2.3.9.



Рисунок 2 — Принципы

4.2.3.2 Лидерство

Руководителям на всех уровнях следует установить единство намерений и направлений развития. Им следует создать условия для согласования стратегий, политик, процессов и ресурсов организации для достижения ее целей. В разделе 5 даны пояснения к этому принципу.

4.2.3.3 Структурированный и целостный подход, основанный на наилучшей имеющейся информации

Структурированному и целостному подходу к менеджменту безопасности, включая цепь поставок, следует способствовать достижению последовательных и сопоставимых результатов более эффективным и результативным образом, когда под деятельностью понимают и ею управляют как взаимосвязанными процессами, функционирующими как согласованная система

4.2.3.4 Соразмерность потребностям

Системе менеджмента безопасности следует быть настроенной и соразмерной внешней и внутренней среде и потребностям организации. Это следует отнести и к ее целям.

4.2.3.5 Всестороннее вовлечение людей

Организации следует надлежащим и своевременным образом вовлекать заинтересованные стороны. Ей следует надлежащим образом учитывать их знания, взгляды и представления для повышения осведомленности и информированного содействия менеджменту безопасности. Организации следует на всех уровнях обеспечить уважение к каждому и его вовлеченность на всех уровнях.

4.2.3.6 Интегрированный подход

Менеджмент безопасности является неотъемлемой частью всех видов деятельности организации. Его следует интегрировать во все другие системы менеджмента организации.

Менеджмент риска, принятый в организации — официально одобренный, неофициальный или применяемый интуитивно — следует интегрировать в систему менеджмента безопасности.

4.2.3.7 Динамичность и постоянное улучшение

Организации следует постоянно фокусироваться на улучшении за счет извлечения уроков и накопления опыта, чтобы поддерживать достигнутый уровень показателей деятельности, реагировать на изменения и создавать новые возможности по мере изменения внешней и внутренней среды организации.

4.2.3.8 Учет человеческих и культурных факторов

Поведение и культура людей существенно влияют на все аспекты менеджмента безопасности и их следует учитывать на каждом уровне и этапе. Решения следует основывать на анализе и оценке данных и информации, чтобы обеспечить в итоге большую объективность, уверенность в принятии решений и большую вероятность достижения желаемых результатов. Следует учитывать восприятия.

4.2.3.9 Менеджмент взаимоотношений

Для устойчивого успеха организации следует управлять отношениями со всеми соответствующими заинтересованными сторонами, поскольку они могут влиять на результаты деятельности организации.

4.3 Определение области применения системы менеджмента безопасности

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

При определении этой области организация должна рассмотреть:

- внешние и внутренние факторы, о которых говорится в 4.1;
- требования, о которых говорится в 4.2.

Область применения должна быть в наличии в виде документированной информации.

Если организация выбирает, чтобы процесс, влияющий на соответствие ее системы менеджмента безопасности, предоставлялся извне, она должна обеспечить управление этим процессом. В рамках системы менеджмента безопасности должны быть определены необходимые средства управления и ответственность за предоставляемые извне процессы.

4.4 Система менеджмента безопасности

Организация должна создать, применять поддерживать и постоянно улучшать систему менеджмента безопасности, включая необходимые процессы и их взаимодействие, в соответствии с требованиями настоящего стандарта.

5 Лидерство

5.1 Лидерство и приверженность

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

- установления политики в области безопасности и целей в области безопасности, согласующихся со стратегией развития организации;
- выявления и мониторинга требований и ожиданий заинтересованных сторон, связанных с организацией, и осуществления соответствующих своевременных действий для управления этими ожида-

ниями, чтобы обеспечить интеграцию требований к системе менеджмента безопасности в бизнес-процессы организации;

- обеспечения интеграции требований к системе менеджмента безопасности в бизнес-процессы организации;
- обеспечения ресурсами, необходимыми для системы менеджмента безопасности;
- информирования о важности результативного менеджмента безопасности и соответствия требованиям к системе менеджмента безопасности;
- обеспечения достижения системой менеджмента безопасности намеченного(ых) результата(ов);
- обеспечения дееспособности целей, задач и программ в области менеджмента безопасности;
- дополнения системы менеджмента безопасности программами обеспечения безопасности, созданными другими подразделениями организации;
- руководства и оказания поддержки лиц в их участии в обеспечении результативности системы менеджмента безопасности;
- содействия постоянному улучшению имеющейся в организации системы менеджмента безопасности;
- поддержания других соответствующих должностных лиц в демонстрации ими лидерства в их областях.

Примечание — Понятие «бизнес» в настоящем стандарте в широком смысле можно интерпретировать как обозначающее те виды деятельности, которые являются ключевыми для целей существования организации.

5.2 Политика в области безопасности

5.2.1 Создание политики в области безопасности

Высшее руководство организации должно установить политику в области безопасности. Политика должна:

a) соответствовать намерениям организации;

b) создавать основу для установления целей в области безопасности;

c) включать в себя обязательство соответствовать применимым требованиям;

d) включать в себя обязательство постоянно улучшать систему менеджмента безопасности;

e) учитывать неблагоприятное влияние, которое политика, цели, задачи, программы и т. д. могут оказывать на другие аспекты деятельности организации.

5.2.2 Требования к политике в области безопасности

Политика в области безопасности должна:

- быть согласована с другими политиками организации;
- быть согласована с обобщенной оценкой рисков организации в области безопасности;
- обеспечивать пересмотр политики в случае ее приобретения или слияния с другими организациями или другого изменения в области бизнес-деятельности организации, которая может повлиять на целостность или приемлемость системы менеджмента безопасности;
- описывать и устанавливать первичную подотчетность и ответственность за результаты;
- быть в наличии в виде документированной информации;
- быть доведенной до сведения персонала организации;
- в том виде, как это подходит, быть доступной для заинтересованных сторон.

Примечание — Организации могут решить для себя разработать подробную политику в области менеджмента безопасности для внутреннего использования, которая предоставляла бы достаточно информации и указаний для управления системой менеджмента безопасности (части которой могут быть конфиденциальными), и иметь обобщенную (неконфиденциальную) версию, содержащую цели в широком смысле, для распространения среди ее заинтересованных сторон.

5.3 Роли, обязанности, ответственность и полномочия

Высшее руководство должно обеспечить определение и доведение до персонала организации сведений об обязанностях, ответственности и полномочиях для выполнения соответствующих ролей.

Высшее руководство должно установить обязанности, ответственность и полномочия:

a) для обеспечения соответствия системы менеджмента безопасности требованиям настоящего стандарта;

b) предоставления отчетов высшему руководству о результатах функционирования системы менеджмента безопасности.

6 Планирование

6.1 Действия в отношении рисков и возможностей

6.1.1 Общие положения

При планировании в системе менеджмента безопасности организация должна рассмотреть факторы, о которых говорится в 4.1, и требования, о которых говорится в 4.2, и определить риски и возможности, подлежащие рассмотрению:

- для обеспечения уверенности в том, что система менеджмента безопасности может получить свой(и) намеченный результат(ы);
- предотвращения или уменьшения нежелательного влияния;
- достижения постоянного улучшения.

Организация должна планировать:

a) действия в отношении рисков и возможностей;

b) каким образом:

- интегрировать эти действия в процессы системы менеджмента безопасности и осуществлять их;
- оценивать результативность этих действий.

Намерением менеджмента рисков является создание и защита ценности. Менеджмент рисков должен быть интегрирован в систему менеджмента безопасности. Риски, связанные с безопасностью организации и ее заинтересованных сторон, рассматриваются в 8.3.

6.1.2 Определение рисков, относящихся к безопасности, и выявление возможностей

Определение рисков, связанных с безопасностью, и выявление и использование возможностей требуют упреждающей оценки рисков, которая должна включать рассмотрение (но не ограничиваться этим):

a) физических или функциональных сбоев и злонамеренных или преступных действий;

b) экологических, человеческих и культурных факторов и других внутренних или внешних условий среды, включая факторы, находящиеся вне управления со стороны организации, влияющие на безопасность организации;

c) проектирования, монтажа, технического обслуживания и замены оборудования, обеспечивающего безопасность;

d) менеджмента информации, данных, знаний и обмена информацией организации;

e) информации, относящейся к угрозам и уязвимости безопасности;

f) взаимозависимостей между поставщиками.

6.1.3 Реагирование на риски, относящиеся к безопасности, и реализация возможностей

Оценивание выявленного риска, относящегося к безопасности, должно служить исходной информацией (но не ограничиваться только этим) для:

a) менеджмента рисков в целом по организации;

b) воздействия на риск;

c) установления целей в области менеджмента безопасности;

d) процессов менеджмента безопасности;

e) разработки, установления требований и применения системы менеджмента безопасности;

f) определения адекватных ресурсов, включая персонал;

g) определения потребностей в подготовке и требуемого уровня компетентности.

6.2 Цели в области безопасности и планирование их достижения

6.2.1 Установление целей в области безопасности

Организация должна установить цели в области безопасности для соответствующих функциональных структур и уровней организации.

Цели в области безопасности должны:

a) быть согласованными с политикой в области безопасности;

b) быть измеримыми (если это осуществимо на практике);

c) учитывать применимые требования;

d) подлежать мониторингу;

e) быть доведенными до сведения персонала;

f) актуализироваться по мере необходимости;

g) быть в наличии в виде документированной информации.

6.2.2 Определение целей в области безопасности

При планировании действий по достижению целей в области безопасности организация должна определить:

- что должно быть сделано;
- какие потребуются ресурсы;
- кто будет нести ответственность;
- когда эти действия будут завершены;
- каким образом будут оцениваться результаты.

При установлении и анализе целей в области безопасности организация должна учесть:

a) технологические, кадровые, административные и другие возможности;

b) мнения соответствующих заинтересованных сторон и влияние на них.

Цели в области безопасности должны соответствовать приверженности организации постоянному улучшению.

6.3 Планирование изменений

Когда организация выявляет необходимость в изменениях в системе менеджмента безопасности, включая изменения, выявленные в ходе реализации требований раздела 10, эти изменения должны осуществляться запланированным образом.

Организация должна рассмотреть:

a) цель изменений и их возможные последствия;

b) сохранение целостности системы менеджмента безопасности;

c) наличие ресурсов;

d) распределение или перераспределение обязанностей, ответственности и полномочий.

7 Средства обеспечения

7.1 Ресурсы

Организация должна определить и предоставить ресурсы, необходимые для создания, применения поддержания в работоспособном состоянии и постоянного улучшения системы менеджмента безопасности.

7.2 Компетентность

Организация должна:

- определять необходимую компетентность лиц(а), выполняющих(его) работу под ее управлением, которая оказывает влияние на показатели деятельности в области безопасности;
- обеспечить, чтобы эти лица были компетентны на основе соответствующего образования, подготовки или опыта и прошли соответствующую проверку с точки зрения безопасности;
- если применимо, предпринять действия для приобретения необходимой компетенции и оценить результативность предпринятых действий.

Должна быть в наличии соответствующая документированная информация, подтверждающая компетентность.

Примечание — Применяемые действия могут включать, например: проведение подготовки, наставничество или перевод работников на другую должность; или наем или заключение контрактов с компетентными лицами.

7.3 Осведомленность

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

- о политике в области безопасности;
- своем вкладе в обеспечение результативности системы менеджмента безопасности, включая преимущества от улучшения показателей деятельности в области безопасности;
- последствиях несоответствия требованиям системы менеджмента безопасности;
- своей роли и обязанностях и ответственности в достижении согласованности с политикой менеджмента безопасности и процедурами, а также с требованиями системы менеджмента безопасности, включая требования готовности к чрезвычайным ситуациям и реагированию на них.

7.4 Обмен информацией

Организация должна определить внутренний и внешний обмен информацией, имеющей отношение к системе менеджмента безопасности, включая:

- какая информация будет передаваться;
- когда будет передаваться информация;
- кому будет передаваться информация;
- каким образом будет передаваться информация;
- степень конфиденциальности информации до ее передачи.

7.5 Документированная информация

7.5.1 Общие положения

Система менеджмента безопасности организации должна включать в себя:

a) документированную информацию, требуемую настоящим стандартом;

b) документированную информацию, определенную организацией как необходимую для обеспечения результативности системы менеджмента безопасности.

Документированная информация должна описывать обязанности, ответственность и полномочия для достижения целей и решения задач в области менеджмента безопасности, включая средства и сроки достижения этих целей и решения этих задач.

Примечание — Степень потребности и объем документированной информации в системе менеджмента безопасности одной организации может отличаться от другой в зависимости от:

- размера организации и вида ее деятельности, процессов, продукции и услуг;
- сложности процессов и их взаимосвязи;
- компетентност и персонала.

Организация должна определить ценность информации, установить требуемый уровень сохранения ее целостности, а также средства управления безопасностью для предотвращения несанкционированного доступа к ней.

7.5.2 Создание и актуализация

При создании и актуализации документированной информации организация должна соответствующим образом обеспечить:

- ее идентификацию и описание (например, название, дата, автор, ссылочный номер);
- формат (например, язык, версия программного обеспечения, графические средства) и носитель (например, бумажный или электронный);
- анализ и официальное одобрение с точки зрения пригодности и адекватности.

7.5.3 Управление документированной информацией

Документированной информацией, требуемой системой менеджмента безопасности и настоящим стандартом, необходимо управлять для обеспечения:

a) наличия и пригодности — в том случае, где и когда она необходима;

b) достаточной защищенности (например, от несоблюдения конфиденциальности, от ненадлежащего использования или потери целостности);

c) периодического анализа и пересмотра по мере необходимости и утверждения с точки зрения ее адекватности уполномоченным персоналом;

d) незамедлительного удаления устаревших документов, данных и информации из всех мест и областей, где они применяются, или обеспечения иной защиты от непреднамеренного использования;

e) соответствующей идентификации архивных документов, данных и информации, сохраняемых в соответствии с законодательными требованиями и/или в целях обеспечения сохранности знаний.

Для управления документированной информацией организация должна в той степени, насколько это применимо, рассмотреть следующее:

- распределение, обеспечение доступности, возможность получения и использование информации;
- накопление и сохранение, включая сохранение разборчивости;
- управление изменениями (например, управление версиями);
- сохранение информации в течение установленных сроков, а также ее уничтожение.

Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и функционирования системы менеджмента безопасности, должна быть соответствующим образом идентифицирована и находиться под управлением.

Примечание — Доступ подразумевает разрешение просмотра документированной информации или разрешение просмотра с полномочиями по внесению изменений в документированную информацию.

8 Деятельность

8.1 Планирование и управление

Организация должна планировать, применять процессы, необходимые для выполнения требований и для выполнения действий, определенных в разделе 6, и осуществлять управление этими процессами посредством:

- установления критериев приемлемости для процессов:
- управления процессами в соответствии с установленными критериями.

Документированная информация должна быть в наличии в объеме, необходимом для уверенности в том, что процессы были осуществлены в соответствии с тем, как было запланировано.

8.2 Идентификация процессов и видов деятельности

Организация должна идентифицировать процессы и виды деятельности, необходимые для достижения:

a) соответствия ее политике в области безопасности;

b) соответствия законодательным и нормативным правовым требованиям к обеспечению безопасности;

c) целей в области менеджмента безопасности;

d) функционирования своей системы менеджмента безопасности;

e) требуемого уровня безопасности цепи поставок.

8.3 Оценка рисков и воздействие на них

Организация должна внедрить и поддерживать процесс оценки рисков и воздействия на них.

Примечание — Процесс оценки рисков и воздействия на них описан в ISO 31000.

Организации следует:

a) выявить риски, относящиеся к безопасности, расставить приоритеты с точки зрения ресурсов, необходимых для менеджмента безопасности;

b) проанализировать и оценить выявленные риски;

c) определить, какие риски требуют воздействия на них;

d) выбрать и реализовать варианты реагирования на эти риски;

e) подготовить и исполнить планы воздействия на риски.

Примечание — Риски в данном подразделе относятся к безопасности организации и ее заинтересованных сторон. Риски и возможности, связанные с результативностью системы менеджмента безопасности, рассматриваются в 6.1.

8.4 Средства управления

Процессы, перечисленные в 8.2, должны, в зависимости от обстоятельств, включать средства менеджмента человеческих ресурсов, а также менеджмента проектирования, монтажа, эксплуатации, реконструкции и модификации оборудования, приборов и информационных технологий, связанных с обеспечением безопасности. В тех случаях, когда существующие механизмы пересматриваются или вводятся новые механизмы, которые могут повлиять на менеджмент безопасности, организация должна рассмотреть соответствующие риски, относящиеся к безопасности, до внедрения этих механизмов. Новые или пересмотренные методы, подлежащие рассмотрению, должны включать:

a) пересмотренные структуру организации, роли или обязанности и ответственность;

b) подготовку персонала, его осведомленность и менеджмент человеческих ресурсов;

c) пересмотренные политику, цели, задачи или программы в области менеджмента безопасности;

d) пересмотренные процессы и процедуры;

e) введение новой инфраструктуры, оборудования или технологий в области обеспечения безопасности, которые могут включать аппаратное и/или программное обеспечение;

f) использование (в том объеме, в котором это подходит) новых подрядчиков, поставщиков или персонала;

g) требования к обеспечению безопасности внешними поставщиками.

Организация должна управлять плановыми изменениями и анализировать последствия непреднамеренных изменений, принимая, при необходимости, меры по ослаблению неблагоприятных влияний.

Организация должна обеспечить управление поставляемыми извне процессами, продукцией и услугами, имеющими отношение к системе менеджмента безопасности.

8.5 Стратегии, процедуры, процессы и подходы к обеспечению безопасности

8.5.1 Идентификация и выбор стратегий и подходов

Организации следует внедрить и поддерживать систематические процессы для анализа уязвимости и угроз, связанных с безопасностью. На основе такого анализа и последующей оценки рисков организации следует идентифицировать и выбрать стратегию обеспечения безопасности, которая будет включать одну или несколько процедур, процессов и подходов.

Идентификацию следует основывать на степени, в которой стратегии, процедуры, процессы и подходы:

a) поддерживают безопасность организации;

b) уменьшают вероятность уязвимости системы безопасности;

c) уменьшают вероятность воплощения угрозы в реальность;

d) сокращают период действия любых недостатков в подходах к обеспечению безопасности и ограничивают их влияние;

e) обеспечивают наличие соответствующих ресурсов.

Выбор следует основывать на степени, в которой стратегии, процедуры, процессы и подходы:

- соблюдают требования к защите безопасности организации;
- учитывают степень и тип риска, который организация может или не может принять;
- учитывают связанные с этим затраты и выгоды.

8.5.2 Требования к ресурсам

Организация должна определить требования к ресурсам, чтобы применять выбранные процедуры, процессы и походы к обеспечению безопасности.

8.5.3 Применение подходов

Организация должна применять и поддерживать выбранные подходы к обеспечению безопасности.

8.6 Планы обеспечения безопасности

8.6.1 Общие положения

Организация должна разработать и документировать планы и процедуры обеспечения безопасности на основе выбранных стратегий и подходов. Организация должна создать и поддерживать структуру реагирования, которая позволит своевременно и результативно предупреждать и сообщать соответствующим заинтересованным сторонам об уязвимостях, связанных с безопасностью, и о неизбежных угрозах безопасности или продолжающихся нарушениях безопасности. Структура реагирования должна обеспечить разработку планов и процедур управления организацией во время неминуемой угрозы безопасности или продолжающегося нарушения безопасности.

8.6.2 Структура реагирования

Организация должна создать и поддерживать структуру, определяя назначенное лицо или одну или нескольких групп (команд), ответственных за реагирование на уязвимости и угрозы, относящиеся к безопасности. Роли, а также обязанности и ответственность назначенного лица или каждой команды, а также взаимоотношения с этим лицом или командами должны быть четко определены, доведены до сведения и задокументированы.

В совокупности командам следует быть компетентными, для того чтобы:

a) оценить характер и степень угрозы безопасности и ее потенциального влияния;

b) оценить воздействие с учетом заранее определенных пороговых значений, которые оправдывают инициирование официальной реакции;

c) инициировать соответствующую реакцию для обеспечения безопасности;

d) планировать действия, которые необходимо предпринять;

e) расставить приоритеты, используя в качестве первоочередного приоритета — обеспечение безопасности для жизни;

f) осуществлять мониторинг влияний любых изменений в уязвимостях, относящихся к безопасности, изменений в намерениях и возможностях субъектов угроз, в нарушениях безопасности, а также в ответных мерах организации;

g) активировать подходы к обеспечению безопасности;

h) обмениваться информацией с соответствующими заинтересованными сторонами, органами власти и средствами массовой информации;

i) внести вклад в план обмена информацией с помощью управления обменом информацией.

Следует обеспечить, чтобы у каждого назначенного лица или команды:

- был определенный персонал, включая заместителей, обладающий необходимыми обязанностями, ответственностью, полномочиями и компетентностью для выполнения возложенных на них функций;

- были документированные процедуры для руководства их действиями, включая процедуры активации, реализации, координации мер реагирования и передачи информации о них.

8.6.3 Предупреждение и обмен информацией

Организация должна документировать и поддерживать в актуальном состоянии процедуры:

a) обмена информацией внутри и вне организации с соответствующими заинтересованными сторонами, включая, какими данными, когда, с кем и каким образом осуществлять обмен.

Примечание — Организация может документировать и поддерживать процедуры, описывающие то, как и при каких обстоятельствах организация взаимодействует с сотрудниками и их контакты для коммуникации в чрезвычайных ситуациях;

b) получения, документирования сообщений от заинтересованных сторон и реагирование на них, включая любую национальную или региональную систему консультирования по вопросам рисков или аналогичную систему;

c) обеспечения доступности средств связи во время нарушения безопасности, выявления уязвимости или угрозы для безопасности;

d) содействия структурированному обмену информацией с лицами, ответственными за реагирование на угрозы и/или нарушения безопасности;

e) предоставления подробной инструкции по реагированию средств массовой информации организации на нарушение безопасности, включая стратегии обмена информацией;

f) фиксации подробной информации о нарушении безопасности, предпринятых действиях и принятых решениях.

Там, где это применимо, также следует рассмотреть и реализовать следующее:

- оповещать заинтересованные стороны, потенциально затрагиваемые фактическим или надвигающимся нарушением безопасности;

- обеспечение надлежащей координации действий и обмена информацией между многочисленными организациями, на которые возложена ответственность за соответствующее реагирование.

Процедуры предупреждения и обмена информацией должны подвергаться практической проверке в качестве части программ организации по тестированию, а также по подготовке персонала.

8.6.4 Содержание планов обеспечения безопасности

Организация должна документировать и поддерживать в актуальном состоянии планы обеспечения безопасности. Эти планы должны содержать руководства и информацию, помогающие командам реагировать на уязвимость, угрозу и/или нарушение безопасности, а также помогать организации в реагировании и восстановлении ее безопасности.

В совокупности планам обеспечения безопасности следует содержать:

a) подробное описание действий, которые команды должны выполнять, чтобы:

1) сохранить или восстановить согласованный статус безопасности;
2) осуществлять мониторинг влияния реальных или надвигающихся угроз, уязвимостей или нарушений в области безопасности и реакции организации на них;

b) ссылку на заранее определенные пороговые значения и процесс инициирования действий по реагированию;

c) процедуры восстановления безопасности организации;

d) подробную информацию по управлению немедленно возникающими последствиями уязвимости и угрозами безопасности или фактического или надвигающегося нарушения безопасности с учетом того, как это повлияет на:

1) благосостояние отдельных людей;
2) ценность активов, информацию и персонал, потенциально могущих быть подвергнутыми риску/угрозе;
3) предотвращение (в дальнейшем) потери или невозможности осуществления ключевых видов деятельности.

В каждый план следует включать:

- его предназначение, область применения и цели;
- роли, обязанности и ответственность команды исполнителей этого плана;
- действия, предпринимаемые для исполнения решений;
- информацию, необходимую для инициирования (включая критерии инициирования), функционирования, координации действий команды и обмена информацией об этом;
- внутренние и внешние взаимозависимости;
- требования к ресурсам;
- требования к отчетности;
- действия на случай остановки работ.

Каждый план должен быть пригодным и быть в наличии в том месте и в то время, когда он требуется.

8.6.5 Восстановление

Организация должна иметь документированные процессы восстановления безопасности организации после любых временных мер, принимаемых до, во время и после нарушения безопасности

9 Оценка результатов деятельности

9.1 Мониторинг, измерение, анализ и оценка

Организация должна определить:

- что необходимо подвергать мониторингу и измерять;
- в том объеме, в котором это подходит, методы мониторинга, измерения, анализа и оценки, для получения достоверных результатов;
- когда выполнять мониторинг и измерения;
- когда анализировать и оценивать результаты мониторинга и измерений.

Организация должна иметь в наличии соответствующую документированную информацию как свидетельство полученных результатов.

Организация должна оценивать показатели функционирования и результативность системы менеджмента безопасности.

9.2 Внутренний аудит

9.2.1 Общие положения

Организация должна проводить внутренние аудиты через запланированные промежутки времени для получения информации о том:

a) является ли система менеджмента безопасности соответствующей:
   1) собственным требованиям организации к своей системе менеджмента безопасности;
   2) требованиям настоящего стандарта;

b) результативно ли внедрена система менеджмента безопасности и поддерживается ли она в актуальном состоянии.

9.2.2 Программа внутреннего аудита

Организация должна планировать, разрабатывать, реализовывать и поддерживать в актуальном состоянии программу(ы) аудитов, включая частоту и методы проведения аудита, обязанности и ответственность, планируемые для проверки требования, а также отчетность об аудитах.

Программа аудитов должна разрабатываться с учетом важности проверяемых процессов и результатов предыдущих аудитов.

Организация должна:

a) определять цели, критерии и область аудита для каждого аудита;

b) отбирать аудиторов и проводить аудиты так, чтобы обеспечивались объективность и беспристрастность процесса аудита;

c) обеспечивать передачу информации о результатах аудитов соответствующим руководителям;

d) верифицировать, что оборудование и персонал службы безопасности используются надлежащим образом;

e) обеспечивать выполнение необходимых корректирующих действий без неоправданной задержки для устранения обнаруженных несоответствий и их причин;

f) обеспечивать включение в последующие действия по аудиту верификацию принятых мер и отчетность о результатах верификации.

Организация должна обеспечить наличие документированной информации как свидетельства, подтверждающего реализацию программы аудитов и полученные результаты аудитов.

Программа аудита, включая все планы-графики, должна основываться на результатах оценки рисков для деятельности организации и результатах предыдущих аудитов. Процедуры проведения аудита должны охватывать область, частоту и методы аудитов, требования к компетентности, обязанностям и ответственности аудиторов, требования к проведению аудитов и представлению отчетности о результатах.

9.3 Анализ со стороны руководства

9.3.1 Общие положения

Высшее руководство должно анализировать систему менеджмента безопасности организации через запланированные интервалы времени в целях обеспечения ее сохраняющейся пригодности, адекватности и результативности.

Организация должна рассмотреть результаты анализа и оценки, а также результаты анализа со стороны руководства, чтобы определить, существуют ли потребности или возможности, связанные с бизнесом или системой менеджмента безопасности, которые необходимо рассмотреть как часть деятельности по постоянному улучшению.

Примечание — Организация может использовать процессы системы менеджмента безопасности, такие как лидерство, планирование и оценка результатов деятельности, для достижения улучшения.

9.3.2 Исходные данные для анализа со стороны руководства

Анализ со стороны руководства должен включать в себя рассмотрение:

a) статуса действий по результатам предыдущих анализов со стороны руководства;

b) изменений во внешних и внутренних факторах, имеющих отношение к системе менеджмента безопасности;

c) изменений потребностей или ожиданий заинтересованных сторон, имеющих отношение к системе менеджмента безопасности;

d) информации о результатах деятельности в области безопасности, включая тенденции, относящиеся к:

1) несоответствиям и корректирующим действиям;
2) результатам мониторинга и измерений;
3) результатам аудита;

e) возможностей для постоянного улучшения;

f) результатов аудитов и оценок соответствия законодательным требованиям, а также другим требованиям, с которыми организация согласилась;

g) обмена информацией с внешними заинтересованными сторонами, включая жалобы;

h) результатов деятельности организации в области обеспечения безопасности;

i) степени достижения целей и решения задач;

j) статуса корректирующих действий;

k) действий по итогам предыдущих анализов со стороны руководства;

l) изменений в обстоятельствах, включая изменения в законодательных, нормативных правовых и других требованиях (см. 4.2.2), относящихся к аспектам безопасности;

m) рекомендаций по улучшению.

9.3.3 Результаты анализа со стороны руководства

Результаты анализа со стороны руководства должны включать в себя решения, относящиеся к возможностям для постоянного улучшения и ко всем необходимым изменениям в системе менеджмента безопасности.

Документированная информация, служащая свидетельством результатов анализов со стороны руководства, должна быть в наличии.

10 Улучшение

10.1 Постоянное улучшение

Организация должна постоянно повышать пригодность, адекватность и результативность системы менеджмента безопасности. Организации следует активно искать возможности для улучшения,

даже если это не вызвано уязвимостями, связанными с безопасностью, и неизбежными угрозами безопасности или продолжающимися нарушениями безопасности для соответствующих заинтересованных сторон.

10.2 Несоответствие и корректирующее действие

При появлении несоответствия организация должна:

a) отреагировать на данное несоответствие и, насколько это возможно и целесообразно:
   1) предпринять действия по управлению несоответствием и его коррекции;
   2) предпринять действия в отношении последствий несоответствия;

b) оценить необходимость действий по устранению причин(ы) несоответствия, с тем чтобы избежать его повторного появления или появления в другом месте, посредством:
   1) анализа несоответствия;
   2) определения причин, вызвавших появление несоответствия;
   3) определения наличия другого аналогичного несоответствия или возможности его возникновения;

c) выполнить все необходимые действия;

d) проанализировать результативность всех осуществленных корректирующих действий;

e) внести при необходимости изменения в систему менеджмента безопасности.

Корректирующие действия должны соответствовать степени влияния выявленных несоответствий.

Должно быть обеспечено наличие информации, являющейся свидетельством:

- характера несоответствий и последующих предпринятых действий;
- результатов всех корректирующих действий;
- расследования вопросов, связанных с безопасностью:
  - сбои, включая почти случившиеся сбои и ложные срабатывания;
  - инциденты и чрезвычайные ситуации;
  - несоответствия;
- принятия мер по смягчению любых последствий, возникающих в результате таких сбоев, инцидентов или несоответствий.

Процедуры должны требовать, чтобы все предлагаемые корректирующие действия были проанализированы в процессе оценки рисков, относящихся к безопасности, до их внедрения, если только немедленное внедрение не предотвратит неминуемую угрозу жизни или общественной безопасности.

Любые корректирующие действия, предпринятые для устранения причин фактических и потенциальных несоответствий, должны соответствовать масштабу проблем и соответствовать рискам, относящимся к менеджменту безопасности, которые могут возникнуть.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 22300	IDT	ГОСТ Р 22.0.12—2015/ИСО 22300:2012 «Безопасность в чрезвычайных ситуациях. Международные термины и определения»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

Библиография

[1] ISO 9001, Quality management systems — Requirements (Системы менеджмента качества. Требования)

[2] ISO 14001, Environmental management systems — Requirements with guidance for use (Системы экологического менеджмента. Требования и руководство по применению)

[3] ISO 19011, Guidelines for auditing management systems (Руководящие указания по аудиту систем менеджмент)

[4] ISO 22301, Security and resilience — Business continuity management systems — Requirements (Безопасность и устойчивость. Системы менеджмента непрерывности деятельности. Требования)

[5] ISO/IEC 27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements (Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования)

[6] ISO 28001, Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance (Системы менеджмента безопасности цепи поставок. Наилучшие практики осуществления безопасности цепи поставок, оценки и планов безопасности. Требования и руководство по применению)

[7] ISO 28002, Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use (Системы менеджмента безопасности цепи поставок. Устойчивость цепи поставок. Требования и руководство по применению)[1)]

[8] ISO 28003, Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems (Системы менеджмента безопасности для цепи поставок. Требования к органам аудита и сертификации систем менеджмента безопасности цепи поставок)

[9] ISO 28004-1, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles (Системы менеджмента безопасности цепи поставок. Руководство по внедрению ISO 28000. Часть 1. Основные принципы)

[10] ISO 28004-3, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports) [Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000. Часть 3. Дополнительное специальное руководство по принятию ISO 28000 для использования в операциях среднего и малого бизнеса (кроме морских портов)]

[11] ISO 28004-4, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective (Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000. Часть 4. Дополнительное специальное руководство по внедрению ISO 28000, когда соответствие ISO 28001 является предметом менеджмента)

[12] ISO 31000, Risk management — Guidelines (Менеджмент риска. Принципы и руководство)

[13] ISO 45001, Occupational health and safety management systems — Requirements with guidance for use (Системы менеджмента охраны здоровья и безопасности труда. Требования и рекомендации по применению)

[14] ISO Guide 73, Risk management — Vocabulary (Менеджмент риска. Термины и определения)[2)]

[1)] Отменен.

[2)] Отменен. Действует ISO 31073:2022 «Risk management — Vocabulary».

УДК 656.614.3.004:006.354

ОКС 03.100.01
03.100.70

Ключевые слова: система менеджмента, безопасность, цепь поставок

Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 03.09.2025. Подписано в печать 29.09.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,37.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru