ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28000— 2019

ТЕХНИЧЕСКИЕ УСЛОВИЯ ДЛЯ СИСТЕМ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

(ISO 28000:2007, IDT)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Международный менеджмент, качество, сертификация» (АНО «ММКС») совместно с Обществом с ограниченной ответственностью «Палекс» (ООО «Палекс») и Ассоциацией по сертификации «Русский Регистр» 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 23 декабря 2019 г. № 1432-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28000:2007 «Спецификация на системы менеджмента безопасности цепи поставок» (ISO 28000:2007 «Specification for security management systems for the supply chain», IDT)

5 ВЗАМЕН ГОСТ Р 53663—2009 (ИСО 28000:2005)

*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, 2007 — Все права сохраняются
© Стандартинформ, оформление, 2020

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 Требования к системе менеджмента безопасности цепи поставок 3
4.1 Общие требования 3
4.2 Политика в области менеджмента безопасности 3
4.3 Оценка рисков безопасности и планирование 4
4.4 Внедрение и функционирование 5
4.5 Контроль и корректирующие действия 8
4.6 Анализ со стороны руководства и постоянное улучшение 9
Приложение А (справочное) Соответствие между стандартами ИСО 28000:2007, ИСО 14001:2004 и ИСО 9001:2000 11
Библиография 14

Введение

Настоящий стандарт подготовлен в связи с существующей в промышленности потребностью в стандарте на менеджмент безопасности. Конечной целью настоящего стандарта является повышение безопасности цепи поставок. Настоящий стандарт является стандартом управления высокого уровня, который позволяет организации создать общую систему менеджмента безопасности цепи поставок. В соответствии с требованиями настоящего стандарта организация должна оценить свою рабочую среду с точки зрения обеспечения безопасности, а также определить, являются ли меры по обеспечению безопасности, принимаемые на месте, адекватными и существуют ли уже обязательные требования к обеспечению безопасности, которые организация выполняет. Если этим процессом определены потребности в безопасности, организация должна внедрить механизмы и процессы для удовлетворения этих потребностей. Поскольку цепи поставок носят динамический характер, некоторые организации, управляющие несколькими цепями поставок, могут запросить у поставщиков услуг подтверждение соблюдения ими государственных требований соответствия или требований стандартов ИСО по безопасности цепи поставок в качестве условия включения в эту цепь поставок, чтобы упростить управление безопасностью, как показано на рисунке 1.

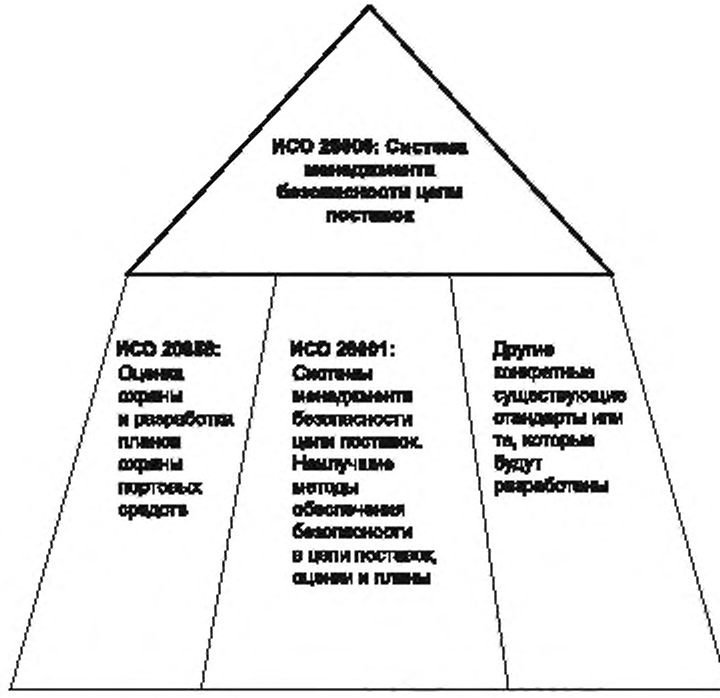

Рисунок 1 — Взаимосвязь стандарта ИСО 28000 с другими аналогичными стандартами

Настоящий стандарт предназначен для применения в тех случаях, когда управление цепями поставок организации необходимо осуществлять безопасным образом. Формализованный подход к управлению безопасностью может внести непосредственный вклад в деловые возможности и авторитет организации.

Соответствие стандарту само по себе не дает освобождения от законодательных обязательств. Для организаций, которые этого пожелают, соответствие системы менеджмента безопасности цепи поставок настоящему стандарту может быть подтверждено посредствам проведения внешнего или внутреннего аудита.

Стандарт основан на подходе ИСО к системам управления, принятом в ИСО 14001:2004, основанном на оценке риска. Однако организации, которые приняли процессный подход к системам управления (например, ИСО 9001:2000), могут использовать свою существующую систему менеджмента качества как основу для системы управления безопасностью согласно настоящему стандарту. Настоящий стандарт не предназначен для дублирования законодательных, нормативных требований и стандартов, касающихся управления безопасностью цепи поставок, по которым организация уже была сертифицирована или проверена на соответствие. Может проводиться аудит первой, второй и третьей сторон.

Примечание — Настоящий стандарт основан на методологии, известной как «Планируй—Делай—Проверяй—Действуй» (PDCA).

PDCA состоит в следующем:

- планировать: определить цели и процессы, необходимые для достижения результатов в соответствии с политикой менеджмента безопасности организации;
- делать: внедрить процессы;
- проверять: отслеживать и оценивать процессы в соответствии с политикой безопасности, целями, задачами, законодательными и другими требованиями и сообщать о результатах;
- действовать: принимать меры для постоянного улучшения результативности системы управления безопасностью.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕХНИЧЕСКИЕ УСЛОВИЯ ДЛЯ СИСТЕМ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Specification for security management systems for the supply chain

Дата введения — 2020—07—01

1 Область применения

Настоящий стандарт определяет требования к системе управления безопасностью, включая аспекты, являющиеся критическими для обеспечения безопасности цепи поставок. Менеджмент безопасности связан со многими другими аспектами управления деятельностью. Данные аспекты включают в себя все виды деятельности, управляемые или находящиеся под влиянием организации, которые воздействуют на безопасность цепи поставок. Эти другие аспекты должны рассматриваться непосредственно там и тогда, где и когда они оказывают влияние на менеджмент безопасности, включая транспортирования этих товаров в цепи поставок.

Настоящий стандарт применим к организациям всех размеров (от малых до многонациональных), занятых в производстве, обслуживании, хранении, транспортированием на любом этапе производства или цепи поставок, которые заинтересованы в том, чтобы:

a) создавать, внедрять, поддерживать и улучшать систему менеджмента безопасности;

b) обеспечивать соответствие заявленной политике менеджмента безопасности;

c) демонстрировать такое соответствие другим;

d) добиться сертификации/регистрации системы менеджмента безопасности аккредитованным органом сертификации третьей стороны;

e) самостоятельно определять и декларировать соответствие настоящему стандарту.

Существуют нормативные и законодательные требования и кодексы, которые касаются некоторых требований настоящего стандарта. Требование дублирующей демонстрации соответствия не является целью настоящего стандарта.

Организации, выбирающие сертификацию третьей стороной, могут дополнительно продемонстрировать, что они вносят значительный вклад в безопасность цепи поставок.

2 Нормативные ссылки

В настоящем стандарте нормативные ссылки отсутствуют. Этот пункт включен для того, чтобы сохранить нумерацию, аналогичную другим стандартам систем менеджмента.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **средство** (facility): Установки, машины, имущество, здания, транспортные средства, корабли, портовые сооружения и другие объекты инфраструктуры или установки и связанные с ними системы, которые имеют четко выраженную и поддающуюся количественной оценке функцию деятельности или услуги.

Примечание — Данный термин включает любой программный продукт, имеющий решающее значение для обеспечения безопасности и применения менеджмента безопасности.

Издание официальное

3.2 **безопасность** (security): Противодействие преднамеренному, несанкционированному действию (действиям), предназначенному для причинения вреда или повреждения цепи поставок.

3.3 **менеджмент безопасности** (security management): Систематическая и скоординированная деятельность и практики, посредством которых организация оптимально управляет своими рисками, а также связанными с ними потенциальными угрозами и их влиянием.

3.4 **цель менеджмента безопасности** (security management objective): Конкретный результат или достижение требуемого уровня безопасности в целях соответствия политике менеджмента безопасности.

Примечание — Крайне важно, чтобы такие результаты были прямо или косвенно связаны с реализацией продуктов, товаров или услуг, предоставляемых всей компанией своим клиентам или конечным потребителям.

3.5 **политика менеджмента безопасности** (security management policy): Общие намерения и направления деятельности организации, связанные с безопасностью и структурой для контроля процессов и деятельности, связанных с безопасностью, которые вытекают из политики и нормативных требований организации и согласуются с ними.

3.6 **программы менеджмента безопасности** (security management programmes): Средства, с использованием которых достигается цель управления безопасностью.

3.7 **целевые показатели менеджмента безопасности** (security management target): Определенный уровень результатов деятельности, необходимый для достижения цели менеджмента безопасности.

3.8 **заинтересованная сторона/стейкхолдер** (stakeholder): Физическое или юридическое лицо, заинтересованное в эффективности, успехе или результативности деятельности организации.

Примечание — Например, клиенты, акционеры, финансовые компании, страховые компании, регулирующие органы, государственные органы, сотрудники, подрядчики, поставщики, профсоюзы или общество.

3.9 **цепь поставок** (supply chain): Набор взаимосвязанных ресурсов и процессов, который начинается с поиска сырья и распространяется через доставку продуктов или услуг конечному потребителю посредством различных видов транспорта.

Примечание — Цепь поставок может включать поставщиков логистических услуг, производственные мощности, внутренние распределительные центры, дистрибьюторов, оптовых торговцев и другие организации, которые ведут к конечному пользователю.

3.9.1 **фаза постконтроля** (downstream): Действия, процессы и движения груза в цепи поставок, которые происходят после того, как груз выходит из-под непосредственного оперативного контроля организации, включая страхование, финансирование, управление данными, а также упаковку, хранение и перемещение груза, но не ограничиваются этим.

3.9.2 **фаза предконтроля** (upstream): Действия, процессы и движения груза в цепи поставок, которые происходят прежде, чем груз оказывается под непосредственным оперативным контролем организации, включая страхование, финансирование, управление данными, а также упаковку, хранение и перемещение груза, но не ограничиваются этим.

3.10 **высшее руководство** (top management): Лицо или группа людей, осуществляющих руководство и управление организацией на самом высоком уровне.

Примечание — Высшее руководство (особенно большой транснациональной организации) может не рассматриваться в личном плане как элемент, входящий в систему, описываемую настоящим стандартом. Однако ответственность высшего руководства на всех уровнях системы должна четко прослеживаться.

3.11 **постоянное улучшение** (continual improvement)**:** Повторяющийся процесс совершенствования системы менеджмента безопасности с целью улучшения общих показателей безопасности в соответствии с политикой безопасности организации.

4 Требования к системе менеджмента безопасности цепи поставок



Рисунок 2 — Элементы системы менеджмента безопасности

4.1 Общие требования

Организация должна разработать, задокументировать, внедрять, поддерживать в рабочем состоянии систему менеджмента безопасности, постоянно улучшать ее результативность для выявления угроз безопасности, оценки рисков, контроля и смягчения их последствий.

Организация должна постоянно повышать эффективность своей деятельности в целом в соответствии с требованиями, изложенными в настоящем разделе.

Организация должна определить область применения своей системы менеджмента безопасности. Если организация решает передать на аутсорсинг определенный процесс, влияющий на соответствие требованиям настоящего стандарта, то она должна обеспечить контроль таких процессов. Необходимые средства контроля и обязанности по контролю за выполнением данных процессов должны быть определены в системе менеджмента безопасности.

4.2 Политика в области менеджмента безопасности

Высшее руководство организации должно утвердить общую политику менеджмента в области безопасности. Политика должна:

a) соответствовать другим политикам организации;

b) определять структуру, которая позволяет разрабатывать конкретные цели, целевые показатели и программы менеджмента безопасности;

c) соответствовать общей структуре управления угрозами и рисками безопасности в организации;

d) соответствовать угрозам организации, характеру и масштабам ее деятельности;

e) четко формулировать общие цели управления безопасностью;

f) включать обязательство постоянно улучшать процесс управления безопасностью;

g) включать обязательство соблюдать действующие нормативно-законодательные и иные требования, применимые к организации;

h) быть официально одобренной высшим руководством;

i) быть задокументирована, внедрена и поддерживаться в рабочем состоянии;

j) быть доведена до сведения всего соответствующего персонала и третьих лиц, включая подрядчиков и посетителей, с целью ознакомления этих лиц с их индивидуальными обязательствами, связанными с менеджментом безопасности;

k) быть доступной для заинтересованных сторон, если это необходимо;

l) обеспечивать пересмотр политики в случае приобретения или слияния с другими организациями или другого изменения сферы деятельности организации, которая может повлиять на непрерывность или актуальность системы менеджмента безопасности.

Примечание — Для внутреннего использования в организации допускается детализированная политика менеджмента безопасности, которая содержит цели по направлениям деятельности организации для управления системой менеджмента безопасности (части которой могут быть конфиденциальными), и общедоступная (не конфиденциальная) версия, содержащая общие цели для распространения среди основных заинтересованных сторон и других заинтересованных лиц.

4.3 Оценка рисков безопасности и планирование

4.3.1 Оценка риска безопасности

Организация должна устанавливать и поддерживать в рабочем состоянии процедуры постоянной идентификации и оценки угроз безопасности и рисков, связанных с менеджментом безопасности, а также определения и реализации необходимых мер управления. Необходимо, чтобы методы идентификации, оценки и управления угрозами безопасности и рисками соответствовали характеру и масштабу операций. Эта оценка должна учитывать вероятность события и все его последствия, включая:

a) угрозы и риски физического отказа, такие как функциональный сбой, случайный ущерб, злонамеренный ущерб, террористические или преступные действия;

b) угрозы и риски операционного характера, включая контроль безопасности, человеческий фактор и другие действия, которые влияют на результаты деятельности, состояние или безопасность организации;

c) события природного характера (штормы, наводнения и т. д.), которые могут сделать мероприятия по безопасности и технические средства охраны неэффективными;

d) внешние факторы, находящиеся под контролем организации, такие как сбои в поставляемом извне оборудовании и услугах;

e) угрозы и риски заинтересованных сторон, такие как несоблюдение нормативных требований или ущерб репутации или бренду;

f) проектирование и установка охранного оборудования, включая замену, техническое обслуживание и т. д.;

g) управление информацией и данными, связь;

h) угрозы непрерывности деятельности организации.

Организация должна обеспечить, чтобы результаты этих оценок и влияние этих мер управления учитывались и, при необходимости, вносили вклад в:

a) цели и целевые показатели менеджмента безопасности;

b) программы менеджмента безопасности;

c) определение требований к проектированию, спецификации и установке;

d) определение адекватных ресурсов, включая штатное расписание;

e) определение потребностей в обучении и навыках (см. 4.4.2);

f) разработку оперативного управления (см. 4.4.6);

g) общую структуру менеджмента угроз и рисков организации.

Организация должна документировать и поддерживать вышеуказанную информацию в актуальном состоянии.

Методология идентификации угроз и рисков организации должна:

a) быть выбрана в соответствии с областью применения, спецификой деятельности и сроками, чтобы гарантировать проактивный, а не реактивный характер действий;

b) включать сбор информации, связанной с угрозами и рисками безопасности;

c) предусматривать классификацию путей выявления тех угроз и рисков, которых следует избегать, устранять или которыми необходимо управлять;

d) обеспечить мониторинг действий для обеспечения эффективности и своевременности их реализации (см. 4.5.1).

4.3.2 Нормативно-законодательные и другие требования по безопасности

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры:

a) по идентификации и обеспечению доступа к применимым нормативно-законодательным и иным требованиям, связанным с угрозой ее безопасности и рисками, которые установлены для организации;

b) определению того, как данные требования применяются к угрозам и рискам безопасности.

Организация должна поддерживать эту информацию в актуальном состоянии. Организация должна передавать соответствующую информацию о нормативно-законодательных и иных требованиях своим сотрудникам и другим соответствующим третьим сторонам, включая подрядчиков.

4.3.3 Цели в области менеджмента безопасности

Организация должна разработать, внедрить и поддерживать в рабочем состоянии документированные цели менеджмента безопасности для соответствующих функций и уровней управления внутри организации. Цели должны быть определены и согласованы с политикой. При установлении и пересмотре своих целей организация должна учитывать:

a) действующие нормативно-законодательные требования по безопасности;

b) угрозы и риски, связанные с безопасностью;

c) технологические и другие факторы;

d) финансовые, операционные и другие требования организации;

e) мнения соответствующих заинтересованных сторон.

Цели менеджмента безопасности должны:

a) соответствовать обязательствам организации по постоянному улучшению;

b) быть измеримыми (где это возможно);

c) быть доведены до сведения всех соответствующих сотрудников и третьих лиц, включая подрядчиков, с целью обеспечения их осведомленности об индивидуальных обязанностях;

d) периодически пересматриваться для обеспечения актуальности и соответствия политике менеджмента безопасности. При необходимости цели менеджмента безопасности должны быть соответствующим образом изменены.

4.3.4 Целевые показатели в области менеджмента безопасности

Организация должна установить, внедрить и поддерживать в рабочем состоянии документированные целевые показатели менеджмента безопасности, соответствующие потребностям организации. Целевые показатели должны быть развернуты и соответствовать целям менеджмента безопасности.

Эти целевые показатели должны быть:

a) развернутыми, конкретными, измеримыми, достижимыми, реалистичными и ограниченными во времени (где это практически осуществимо) (SMART);

b) доведенными до сведения всех соответствующих сотрудников и третьих лиц, включая подрядчиков, с целью обеспечения их осведомленности об индивидуальных обязанностях;

c) периодически пересматриваемыми, чтобы убедиться в том, что они остаются актуальными и соответствуют целям менеджмента безопасности. При необходимости целевые показатели должны быть соответствующим образом изменены.

4.3.5 Программы менеджмента безопасности

Организация должна установить, внедрить и поддерживать в рабочем состоянии программы менеджмента безопасности для достижения своих целей и выполнения целевых показателей.

Программы должны быть оптимизированы, расставлены по приоритетам, и организация должна обеспечить результативную и экономически эффективную реализацию этих программ.

Программы должны включать документацию, которая описывает:

a) распределение ответственности и полномочий для достижения целей и целевых показателей менеджмента безопасности;

b) средства и сроки достижения целей и целевых показателей менеджмента безопасности.

Программы менеджмента безопасности должны периодически пересматриваться на предмет их пригодности для обеспечения эффективности и соответствия целям и задачам. При необходимости в программы должны быть внесены соответствующие изменения.

4.4 Внедрение и функционирование

4.4.1 Структура, ответственность и полномочия по менеджменту безопасности

Для выполнения политики, целей, целевых показателей и программ менеджмента безопасности организация должна установить и поддерживать организационную структуру, распределение ответственности и полномочий.

Данные организационная структура, ответственность и полномочия должны быть определены, задокументированы и доведены до сведения лиц, ответственных за внедрение и поддержание системы в рабочем состоянии.

Высшее руководство должно предоставить свидетельства своей приверженности разработке и внедрению системы (процессов) менеджмента безопасности и постоянному повышению ее эффективности за счет:

a) назначения представителя высшего руководства, который (независимо от других обязанностей) несет ответственность за общее проектирование, обслуживание, документирование и улучшение системы менеджмента безопасности организации;

b) назначения представителя (представителей) руководства с необходимыми полномочиями для обеспечения реализации целей и целевых показателей;

c) выявления и мониторинга требований и ожиданий заинтересованных сторон организации и принятие надлежащих и своевременных мер для управления этими ожиданиями;

d) обеспечения необходимыми ресурсами;

e) учета негативного влияния, которое могут оказать политика менеджмента в области безопасности, цели, целевые показатели, программы и т. д. на другие аспекты деятельности организации;

f) обеспечения того, чтобы любые программы по безопасности, созданные в любом подразделении организации, дополняли систему менеджмента безопасности организации;

g) информирования организации о важности соблюдения требований управления безопасностью и выполнения политики;

h) обеспечения того, чтобы угрозы и риски, связанные с безопасностью, оценивались и включались в систему менеджмента риска и угроз организации, если это применимо;

i) обеспечение жизнеспособности целей, целевых показателей и программ менеджмента безопасности.

4.4.2 Компетентность, обучение и осведомленность

Организация должна гарантировать, что персонал, ответственный за проектирование, эксплуатацию и управление оборудованием и процессами безопасности, имеет соответствующую квалификацию на основе образования, обучения и/или опыта. Организация должна устанавливать и поддерживать процедуры для того, чтобы сотрудники и лица, работающие от имени организации, были осведомлены о следующем:

a) важности соблюдения политики и программ менеджмента безопасности и требований системы менеджмента безопасности;

b) своих обязанностях, ответственности и полномочиях в достижении соответствия политике и программам менеджмента безопасности, а также требованиям системы менеджмента безопасности, включая требования готовности к чрезвычайным обстоятельствам и реагированию на них;

c) потенциальных последствиях для безопасности организации при отклонении от определенных операционных процедур.

Организация должна сохранять соответствующие записи по компетентности и обучению персонала.

4.4.3 Обмен информацией

Организация должна установить, внедрить и поддерживать процедуры для обеспечения того, чтобы необходимая информация по менеджменту безопасности передавалась соответствующим сотрудникам, подрядчикам и другим заинтересованным сторонам.

В связи с тем, что определенная информация, связанная с безопасностью, имеет секретный характер, следует должным образом учитывать конфиденциальность информации до начала ее распространения.

4.4.4 Документирование

Организация должна разработать и поддерживать в рабочем состоянии документацию системы менеджмента безопасности, которая включает:

a) политику, цели и целевые показатели;

b) описание области распространения системы менеджмента безопасности;

c) описание основных элементов системы менеджмента безопасности, их взаимодействия со ссылками на соответствующие документы;

d) записи, определенные настоящим стандартом;

e) записи, определенные организацией как необходимые для обеспечения результативного планирования, функционирования и контроля процессов, связанных со значительными угрозами и рисками безопасности.

Организация должна определить конфиденциальность информации и предпринять шаги для предотвращения несанкционированного доступа.

4.4.5 Управление документацией и данными

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры управления всеми документами, данными и информацией, регламентированными в разделе 4, для обеспечения следующего:

a) документы, данные и информация хранятся в защищенном месте и доступны только уполномоченным лицам,

b) документы, данные и информация периодически пересматриваются, анализируются и актуализируются (по мере необходимости) и утверждаются на пригодность уполномоченным лицом;

c) текущие версии соответствующих документов, данных и информации доступны во всех местах, где выполняются действия для результативного функционирования системы менеджмента безопасности;

d) устаревшие документы, данные и информация незамедлительно удаляются из всех мест и областей, где они применяются, или иным образом гарантируется защита от их непреднамеренного использования;

e) архивные документы, данные и информация, сохраненные в соответствии с законодательными требованиями или в целях сохранения знаний, или и те, и другие, надлежащим образом идентифицированы;

f) документы, данные и информация находятся в безопасности и, если они находятся в электронном виде, надлежащим образом защищены, а также обеспечено резервное копирование с возможностью восстановления.

4.4.6 Управление деятельностью

Организация должна определить те операции и действия, которые необходимы для достижения:

a) политики в области менеджмента безопасности,

b) управления действиями для снижения угроз, определенных как имеющих значительный риск;

c) соблюдения нормативно-законодательных и иных требований по безопасности;

d) целей в области менеджмента безопасности;

e) реализации программ менеджмента безопасности;

f) обеспечения требуемого уровня безопасности цепи поставок.

Организация должна обеспечить условия для возможности осуществления операций и действий посредством:

a) разработки, внедрения и поддержания в рабочем состоянии документированных процедур для управления ситуациями, в которых отсутствие этих процедур может привести к невозможности выполнения операций и действий, указанных выше в перечислениях a), f);

b) оценки любых угроз, исходящих от деятельности в цепи поставок на фазе предконтроля, и применения мероприятий по управлению для смягчения влияния этих воздействий на организацию и других операторов цепи поставок в фазе постконтроля;

c) установление и поддержание требований к товарам или услугам, влияющим на безопасность, и доведение этих требований до поставщиков и подрядчиков.

Данные процедуры должны включать средства управления для проектирования, установки, эксплуатации, восстановления и модификации элементов, связанных с безопасностью оборудования, приборов и т. д., если это применимо. Если существующие договоренности пересматриваются или вводятся новые договоренности, которые могут повлиять на операции и действия в области менеджмента безопасности, организация должна рассмотреть связанные с безопасностью угрозы и риски до реализации договоренностей. Новые или пересмотренные договоренности должны включать:

a) пересмотренную организационную структуру, полномочия и ответственность;

b) пересмотренную политику, цели, целевые показатели или программы менеджмента безопасности;

c) пересмотренные процессы и процедуры;

d) внедрение новой инфраструктуры, оборудования или технологий безопасности, которые могут включать аппаратное и/или программное обеспечение;

e) введение новых подрядчиков, поставщиков или персонала, если это применимо.

4.4.7 Готовность к действиям в чрезвычайной ситуации, реагирование и восстановление безопасности

Организация должна разработать, внедрить и поддерживать в рабочем состоянии соответствующие планы и процедуры для выявления потенциальной возможности возникновения инцидентов, свя-

занных с безопасностью, и чрезвычайных ситуаций, реагирования на них, а также для предотвращения и смягчения возможных последствий, которые могут быть связаны с ними. Планы и процедуры должны включать информацию о предоставлении и обслуживании любого идентифицированного оборудования, средств или услуг, которые могут потребоваться во время или после инцидентов или чрезвычайных ситуаций.

Организация должна периодически проверять эффективность планов и процедур своей готовности к действию в чрезвычайных обстоятельствах, реагированию на них и восстановлению безопасности, особенно после возникновения инцидентов или чрезвычайных ситуаций, вызванных нарушениями безопасности и угрозами. Организация должна периодически проводить учения по этим процедурам, где это применимо.

4.5 Контроль и корректирующие действия

4.5.1 Измерение и мониторинг результатов деятельности по безопасности

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры для мониторинга и измерения результатов деятельности всей системы менеджмента безопасности. Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры мониторинга и измерения результатов деятельности по безопасности. При определении периодичности мониторинга и измерений результатов деятельности организация должна учитывать угрозы и риски, связанные с безопасностью, включая потенциальные механизмы ухудшения и их последствия. Данные процедуры должны предусматривать:

a) как качественные, так и количественные измерения, соответствующие потребностям организации;

b) мониторинг степени выполнения политики, целей и целевых показателей в области менеджмента безопасности организации;

c) упреждающие измерения результатов, которые контролируют выполнение программ менеджмента безопасности, критериев выполнения операций и соблюдение нормативно-законодательных и иных требований по безопасности,

d) измерение результатов реагирования для мониторинга нарушений, сбоев, инцидентов, несоответствий, связанных с безопасностью (в том числе случайных и ложных срабатываний) и других ретроспективных свидетельств недостаточного уровня результативности системы менеджмента безопасности;

e) записи данных и результатов мониторинга и измерений, существенных для облегчения последующего анализа корректирующих и предупреждающих действий. Если для контроля результатов деятельности или измерений и мониторинга требуется контрольное оборудование, организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры калибровки и технического обслуживания такого оборудования. Записи о калибровке и техническом обслуживании и их результатах должны храниться в течение определенного времени, достаточного, чтобы соответствовать нормативно-законодательным требованиям и политике организации.

4.5.2 Оценка системы

Организация должна оценивать планы, процедуры и возможности менеджмента безопасности с использованием периодического анализа, тестирования, отчетов после инцидентов, извлеченных уроков, оценок результатов деятельности, результативности учений. Значительные изменения в этих факторах должны быть немедленно отражены в процедуре (процедурах).

Организация должна периодически оценивать соблюдение нормативно-законодательных требований, соответствие лучшим отраслевым практикам и своей собственной политике и целям.

Организация должна вести учет результатов периодических оценок.

4.5.3 Сбои, инциденты, несоответствия, корректирующие и предупреждающие действия, связанные с безопасностью

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры определения ответственности и полномочий для:

a) оценки и инициирования предупреждающих действий для выявления потенциальных сбоев в безопасности, чтобы не допустить их возникновения;

b) расследований, связанных с безопасностью:

- действий в ситуации сбоев, в том числе при «почти-ошибках» и ложных срабатываниях;
- действий при возникновении инцидентов и чрезвычайных ситуаций;
- действий при возникновении несоответствий;

c) принятия мер по смягчению любых последствий, возникающих в результате таких сбоев, инцидентов или несоответствий;

d) инициирования и завершения корректирующих действий,

e) подтверждения эффективности предпринятых корректирующих действий.

Эти процедуры следует регламентировать, чтобы все предлагаемые корректирующие и предупреждающие действия были рассмотрены в процессе оценки угроз и рисков безопасности перед внедрением, если только немедленное внедрение не предотвратит неизбежное воздействие на жизнь или общественную безопасность.

Любые корректирующие или предупреждающие действия, предпринимаемые для устранения причин фактических и потенциальных несоответствий, которые могут возникнуть, должны соответствовать масштабу проблем и соответствовать угрозам и рискам, связанным с менеджментом безопасности. Организация должна внедрить любые изменения в документированных процедурах, возникающие в результате корректирующих и предупреждающих действий и обеспечить их идентификацию. Корректирующие и предупреждающие действия должны включать в себя необходимое обучение, где это применимо.

4.5.4 Управление записями

Организация должна установить и поддерживать в рабочем состоянии записи, необходимые для демонстрации соответствия системы менеджмента безопасности требованиям настоящего стандарта, а также достижения запланированных результатов.

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуру(ы) для идентификации, хранения, защиты, поиска и удаления записей.

Записи должны быть разборчивыми, идентифицируемыми и прослеживаемыми.

Электронная и цифровая документация должна быть защищена от несанкционированного доступа, иметь резервное копирование с возможностью восстановления и должна быть доступна только авторизованному персоналу.

4.5.5 Аудит

Организация должна планировать, разрабатывать, реализовывать и поддерживать в актуальном состоянии программу аудита менеджмента безопасности и обеспечивать проведение аудитов системы менеджмента безопасности через запланированные интервалы времени, чтобы:

a) определить, действительно ли система менеджмента безопасности:

- соответствует запланированным мероприятиям, включая требования всего раздела 4;
- должным образом внедрена и поддерживается в рабочем состоянии;
- является результативной в выполнении политики и целей менеджмента безопасности организации;

b) рассмотреть результаты предыдущих аудитов и действия, предпринятые для устранения несоответствий;

c) предоставить информацию о результатах аудитов руководству;

d) убедиться, что оборудование и персонал, оказывающий влияние на безопасность, должным образом развернуты на предприятии.

Программа аудита, включая любой график, должна основываться на результатах оценки угроз и рисков в деятельности организации, а также на результатах предыдущих аудитов. Процедуры проведения аудита должны охватывать область применения, частоту и методы аудитов, требования к компетентности и обязанностям аудиторов, требования по проведению аудитов и представлению отчетности по результатам. По возможности, аудит должен проводиться независимым персоналом, т. е. теми, кто несет прямую ответственность за проверяемую деятельность.

Примечание — Фраза «независимый персонал» не обязательно означает внешний для организации персонал.

4.6 Анализ со стороны руководства и постоянное улучшение

Высшее руководство должно анализировать систему менеджмента безопасности организации через запланированные интервалы времени в целях обеспечения ее постоянной пригодности, адекватности и результативности. Анализ должен включать оценку возможностей для улучшения и необходимости внесения изменений в систему менеджмента безопасности, включая политику и цели в области безопасности, угрозы и риски. Организация должна сохранять записи анализа со стороны руководства.

Входные данные для анализа со стороны руководства должны включать:

a) результаты аудитов и оценок соответствия нормативно-законодательным и иным требованиям, которые относятся к организации;

b) обмен информацией с внешними заинтересованными сторонами, включая жалобы;

c) показатели результатов деятельности в области безопасности организации;

d) степень достижения целей и целевых показателей;

e) статус корректирующих и предупреждающих действий;

f) статус действий по результатам предыдущих анализов со стороны руководства;

g) изменение условий, включая изменения в нормативно-законодательных и иных требованиях, связанных с аспектами безопасности организации;

h) рекомендации по улучшению.

Результаты анализа со стороны руководства должны включать любые решения и действия, связанные с возможными изменениями политики, целей, целевых показателей в области безопасности и других элементов системы менеджмента безопасности в соответствии с обязательством постоянного улучшения.

Приложение А
(справочное)

Соответствие между стандартами ИСО 28000:2007, ИСО 14001:2004 и ИСО 9001:2000

Таблица А.1

ИСО 28000:2007		ИСО 14001:2004		ИСО 9001:2000	
Требования к системе менеджмента безопасности цепи поставок	4	Требования к системе экологического менеджмента	4	Система менеджмента качества	4
Общие требования	4.1	Общие требования	4.1	Общие требования	4.1
Политика в области менеджмента безопасности	4.2	Экологическая политика	4.2	Обязательства руководства Политика в области качества Непрерывное улучшение	5.1 5.3 8.5.1
Оценка рисков безопасности и планирование	4.3	Планирование	4.3	Планирование	5.4
Оценка риска безопасности	4.3.1	Экологические аспекты	4.3.1	Ориентация на потребителя Определение требований, относящихся к продукции Анализ требований, относящийся к продукции	5.2 7.2.1 7.2.2
Нормативно-законодательные и другие требования по безопасности	4.3.2	Законодательные и прочие требования	4.3.2	Ориентация на потребителя Определение требований, относящихся к продукции	5.2 7.2.1
Цели в области менеджмента безопасности	4.3.3	Цели, задачи и программа(ы)	4.3.3	Цели в области качества Планирование в рамках системы менеджмента качества Непрерывное улучшение	5.4.1 5.4.2 8.5.1
Целевые показатели в области менеджмента безопасности	4.3.4	Цели, задачи и программа(ы)	4.3.3	Цели в области качества Планирование в рамках системы менеджмента качества Непрерывное улучшение	5.4.1 5.4.2 8.5.1
Программы менеджмента безопасности	4.3.5	Цели, задачи и программа(ы)	4.3.3	Цели в области качества Планирование в рамках системы менеджмента качества Непрерывное улучшение	5.4.1 5.4.2 8.5.1
Внедрение и функционирование	4.4	Внедрение и функционирование	4.4	Выпуск продукции	7

Продолжение таблицы А.1

ИСО 28000:2007		ИСО 14001:2004		ИСО 9001:2000	
Структура, ответственность и полномочия по менеджменту безопасности	4.4.1	Структура и ответственность	4.4.1	Обязательства руководства	5.1
				Ответственность и полномочия	5.5.1
				Представитель руководства	5.5.2
				Обеспечение ресурсами	6.1
				Инфраструктура	6.3
Компетентность, обучение и осведомленность	4.4.2	Обучение, осведомленность и компетентность	4.4.2	Человеческие ресурсы. Общие положения	6.2.1
				Компетентность, осведомленность и подготовка	6.2.2
Обмен информацией	4.4.3	Коммуникации	4.4.3	Внутренние коммуникации	5.5.3
				Связь с потребителями	7.2.3
Документирование	4.4.4	Документация	4.4.4	Требования к документации. Общие требования	4.2.1
Управление документацией и данными	4.4.5	Контроль документации	4.4.5	Управление документацией	4.2.3
Управление деятельностью	4.4.6	Контроль деятельности	4.4.6	Планирование выпуска продукции	7.1
				Определение требований, относящихся к продукции	7.2.1
				Анализ требований, относящихся к продукции	7.2.2
				Планирование проектирования и разработки	7.3.1
				Входные данные проектирования и разработки	7.3.2
				Выходные данные проектирования и разработки	7.3.3
				Анализ проекта и разработки	7.3.4
				Проверка проекта и разработки	7.3.5
				Утверждение проекта и разработки	7.3.6
				Управление изменениями проекта и разработки	7.3.7
				Процесс закупок	7.4.1
				Информация по закупкам	7.4.2
				Проверка закупленной продукции	7.4.3
				Управление производством и предоставлением услуг	7.5.1
				Утверждение процессов производства и предоставления услуг	7.5.2
				Сохранение продукции	7.5.5

Окончание таблицы А.1

ИСО 28000:2007		ИСО 14001:2004		ИСО 9001:2000	
Готовность к действиям в чрезвычайной ситуации, реагирование и восстановление безопасности	4.4.7	Подготовленность к аварийным ситуациям и реагирование на них	4.4.7	Управление несоответствующей продукцией	8.3
Контроль и корректирующие действия	4.5	Проверки	4.5	Мониторинг и измерение	8
Измерение и мониторинг результатов деятельности по безопасности	4.5.1	Мониторинг и измерения	4.5.1	Управление контрольными и измерительными приборами Общие положения (измерение, анализ и улучшение) Мониторинг и измерение процессов Мониторинг и измерение продукции Анализ данных	7.6 8.1 8.2.3 8.2.4 8.4
Оценка системы	4.5.2	Оценка соответствия	4.5.2	Мониторинг и измерение процессов Мониторинг и измерение продукции	8.2.3 8.2.4
Сбои, инциденты, несоответствия, корректирующие и предупреждающие действия, связанные с безопасностью	4.5.3	Несоответствия, корректирующие и предупреждающие действия	4.5.3	Управление несоответствующей продукцией Анализ данных Корректирующие действия Предупреждающие действия	8.3 8.4 8.5.2 8.5.3
Управление записями	4.5.4	Контроль записей	4.5.4	Управление записями	4.2.4
Аудит	4.5.5	Внутренний аудит	4.5.5	Внутренние аудиты	8.2.2
Анализ со стороны руководства и постоянное улучшение	4.6	Анализ со стороны руководства	4.6	Обязательства руководства Анализ со стороны руководства Общие положения Входные данные анализа Выходные данные анализа Непрерывное улучшение	5.1 5.6 5.6.1 5.6.2 5.6.3 8.5.1

Библиография

[1] ISO 9001:2000 — Quality management systems — Requirements (Система менеджмента качества. Требования)

[2] ISO 14001:2004 — Environmental management systems — Requirements with guidance for use (Системы экологического менеджмента. Требования с руководством использованием)

[3] ISO 19011:2002 — Guidelines for quality and/or environmental management systems auditing (Рекомендации по аудиту систем менеджмента качества и/или охраны окружающей среды)

[4] ISO/PAS 20858:2004 — Ships and marine technology — Maritime port facility security assessments and security plan development (Суда и морские технологии. Оценка охраны и разработка планов охраны портовых средств)

[5] ISO/PAS 28001 — Security management systems for the supply chain — Best practices for implementing supply chain security — Assessments and plans (Система менеджмента безопасности цепи поставок — Наилучшие методы обеспечения безопасности цепи поставок. Оценки и планы)

[6] ISO/PAS 28004:2006 — Security management systems for the supply chain — Guidelines for the implementation of ISO/PAS 28000 (Система менеджмента безопасности цепи поставок — Руководство по внедрению ISO/PAS 2800)

УДК 656.614.3.004:006.354 ОКС 13.310 47.020.99 IDT

Ключевые слова: технические условия, система менеджмента, безопасность, цепь поставок

БЗ 2—2020/38

Редактор *Л.И. Нахимова*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 03.03.2020. Подписано в печать 10.03.2020. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,90.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11
www.jurizdat.ru gost.e-ecolog.ru

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31. к. 2.
gost.e-ecolog.ru ıstinfo.ru

gost.e-ecolog.ru