ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28004-1— 2019

СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководящие указания по внедрению ИСО 28000

Часть 1

Общие принципы

(ISO 28004-1:2007/Cor.1:2012, 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»), 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. № 1436-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28004-1:2007/Изм.1:2012 «Системы менеджмента безопасности цепи поставок — Руководство по внедрению ИСО 28000 — Часть 1. Общие принципы» (ISO 28004-1:2007/Cor.1:2012 «Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles», IDT), включая изменения и техническую поправку Cor.1:2012

5 ВЗАМЕН ГОСТ Р 53661—2009 (ИСО 28004:2006)

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*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 2
3 Термины, определения и сокращения 2
4 Требования к системе менеджмента безопасности цепи поставок 3
4.1 Общие требования 4
4.2 Политика в области менеджмента безопасности 4
4.3 Оценка рисков безопасности и планирование 7
4.4 Внедрение и функционирование 16
4.5 Контроль и корректирующие действия 26
4.6 Анализ со стороны руководства и постоянное улучшение 37
Приложение А (справочное) Соответствие между стандартами ИСО 28000:2007, ИСО 14001:2004 и ИСО 9001:2000 40
Библиография 44

Введение

ИСО 28000:2007 «Спецификация для систем менеджмента безопасности цепи поставок» и настоящий стандарт разработаны в связи с необходимостью разработки унифицированного стандарта системы управления цепями поставок с целью оценки и сертификации системы управления безопасностью, а также руководства по реализации данного стандарта.

ИСО 28000 согласован со стандартами систем менеджмента ИСО 9001:2000 «Качество» и ИСО14001:2004 «Экология», что будет способствовать интеграции систем качества, охраны окружающей среды и управления цепями поставок организаций.

Каждый пункт/подпункт настоящего стандарта предваряет полные требования ИСО 28000, после которых следует соответствующее руководство. Нумерация разделов и пунктов настоящего стандарта соответствует нумерации разделов и пунктов ИСО 28000.

При целесообразности настоящий стандарт может быть пересмотрен или изменен, в случае пересмотра положений ИСО 28000.

Настоящий стандарт не подразумевает включение всех необходимых положений договора, заключенного между операторами цепи поставок, поставщиками и заинтересованными сторонами, однако пользователи несут ответственность за его правильное применение.

Соблюдение требований настоящего стандарта не освобождает от исполнения юридических обязательств.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководящие указания по внедрению ИСО 28000

Часть 1

Общие принципы

Security management systems for the supply chain.
Guidelines for the implementation of ISO 28000. Part 1. General principles

Дата введения — 2020—07—01

1 Область применения

Настоящий стандарт содержит общие рекомендации по применению ИСО 28000:2007 «Спецификация для систем управления безопасностью для цепи поставок».

В настоящем стандарте приведены основные принципы ИСО 28000, отражающие намерения, типовые входные данные, процессы и типовые выходные данные требований ИСО 28000, что направлено на четкое толкование и эффективное внедрение ИСО 28000.

Настоящий стандарт не распространяется на дополнительные требования к указанным в ИСО 28000 и не предусматривает обязательных способов для внедрения ИСО 28000.

ИСО 28000

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 аспекты должны рассматриваться непосредственно там и тогда, где и когда они оказывают влияние на менеджмент безопасности, включая транспортирование этих товаров в цепи поставок.

Настоящий стандарт применим к организациям всех размеров (от малых до многонациональных), занятым в производстве, обслуживании, хранении, транспортировании 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.

Издание официальное

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

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 ИСО 28000.

3 Термины, определения и сокращения

В настоящем стандарте используются 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.

3.2 **безопасность** (security): Противодействие преднамеренному, несанкционированному действию, 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.

В настоящем стандарте применены термины и определения по ИСО 28000, а также следующие термины с соответствующими определениями:

3.12 **риск** (risk): Вероятность возникновения угрозы безопасности организации и ее последствия.

3.13 **проверка благонадежности** (security cleared): Процесс верификации надежности людей, которые будут иметь доступ к конфиденциальным материалам в отношении безопасности организации.

3.14 **угроза** (threat): Возможное преднамеренное действие или ряд действий, которые могут нанести ущерб любой из заинтересованных сторон, объектам, операциям, цепи поставок, обществу, экономической стабильности или непрерывности деятельности и целостности организации.

4 Требования к системе менеджмента безопасности цепи поставок



Рисунок 1 — Элементы системы менеджмента безопасности

4.1 Общие требования

a) Требования ИСО 28000

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.

b) Намерения

Организация должна разработать и поддерживать в рабочем состоянии систему менеджмента, которая соответствует всем требованиям ИСО 28000. Это может помочь организации в соблюдении правил безопасности и нормативно-законодательных требований.

Уровень детализации и сложности системы менеджмента безопасности, объем документации и выделенные ей ресурсы зависят от размера и специфики структуры организации, а также характера ее деятельности.

Организация, руководствуясь свободой выбора и гибкостью в определении своих границ, может принять решение о внедрении ИСО 28000 в полном объеме исключительно в конкретных подразделениях или для определенных видов деятельности.

Организации следует взвешенно относиться к вопросам определения границ и области применения системы менеджмента, чтобы не ограничивать свою сферу деятельности, исключая из оценки операцию или вид деятельности, необходимые для осуществления деятельности организации в целом или влияющие на безопасность ее сотрудников и других заинтересованных сторон.

Если требования ИСО 28000 применяют для проведения конкретной операции, то политика безопасности, разработанная другими подразделениями организации, может быть использована отдельным блоком операций/видов деятельности, способствующим выполнению требований ИСО 28000. В этом случае политика безопасности может быть подвергнута незначительному пересмотру или изменению для обеспечения ее применимости к осуществлению работы конкретного операционного подразделения или к виду деятельности организации

c) Типовые входные данные

Все требования, указанные в ИСО 28000.

d) Типовые выходные данные/результат

Типовым результатом является эффективно внедренная и поддерживаемая система управления безопасностью, которая помогает организации осуществлять улучшение.

4.2 Политика в области менеджмента безопасности

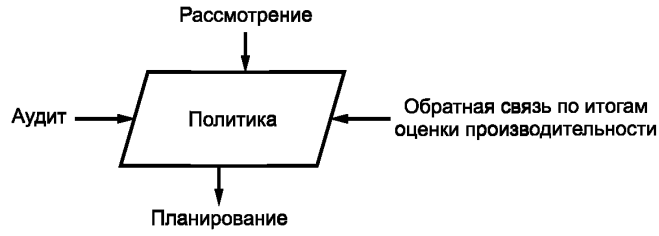


Рисунок 2 — Политика менеджмента безопасности

a) Требования ИСО 28000

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.

b) Намерения

Политика безопасности — это краткое изложение обязательств высшего руководства по обеспечению безопасности деятельности организации. Политика безопасности формирует общие направления и устанавливает принципы действий для организации, определяет цели безопасности и результаты деятельности всей организации. Политика безопасности должна быть разработана, утверждена высшим руководством организации и документально оформлена.

c) Типовые входные данные

При разработке политики в области безопасности руководство должно рассмотреть следующие вопросы в отношении своей цепи поставок:

- политика и цели деятельности организации представляет собой единое целое;
- рассмотрение прошлых и настоящих результатов деятельности в области безопасности с целью стабильности организации;
- потребности заинтересованных сторон;
- необходимость и возможность постоянного улучшения и эффективного роста;
- потребность в ресурсах;
- вклад сотрудников;
- участие подрядчиков, заинтересованных сторон и другого внештатного персонала.

d) Процесс

При разработке и утверждении политики в области безопасности высшее руководство должно учитывать пункты, перечисленные ниже.

Эффективно сформулированная и доведенная до персонала политика в области безопасности должна:

1) соответствовать характеру и масштабу рисков безопасности организации.

Идентификация угроз, оценка риска и управление рисками должны быть отражены в политике безопасности организации, что является основой эффективной системы менеджмента безопасности.

Политика безопасности должна включать видение будущего организации. Оно должно быть реалистичным и не учитывать природу рисков, с которыми сталкивается организация;

2) включать обязательства относительно постоянного улучшения.

Глобальные угрозы в сфере безопасности усиливают давление на организацию с целью снижения риска инцидентов в цепи поставок. Помимо исполнения национальных правовых и нормативных обязательств, а также других нормативно-законодательных требований и руководств, подготовленных соответствующими организациями, такими как Всемирная торговая организация (ВТО), организация должна стремиться к улучшению своих показателей безопасности и совершенствованию собственной системы менеджмента безопасности эффективным и действенным образом для удовлетворения меняющихся глобальных торговых, деловых и нормативно-законодательных требований.

Планируемые результаты улучшений должны быть отражены в целях по безопасности (см. 4.3.2) и программах менеджмента безопасности (см. 4.3.5), а также в политике в области безопасности. При этом заявление о политике безопасности может включать в себя обязательства в расширенной области действия;

3) включать обязательство, как минимум, соответствовать действующим нормативно-законодательным и другим требованиям, относящимся к организации.

Необходимо, чтобы организация соответствовала применимым регуляторным требованиям. Обязательство политики в области безопасности — это публичное признание организацией того, что она обязана соблюдать законодательные или другие юридически обязательные требования или принятые добровольно, такие как рамочные стандарты безопасности ВТО.

Примечание — Термин «другие юридически обязательные требования» может означать, например, корпоративные политики или политики объединений, собственные внутренние стандарты организации, спецификации и коды надлежащей практики, которые организация обязалась выполнять);

4) документироваться, внедряться и поддерживаться в рабочем состоянии.

Планирование и подготовка — это основной способ эффективного внедрения. Часто предложения о политике безопасности, а также цели в области безопасности являются нереалистичными, так как на них не выделяются соответствующие средства и компетентный персонал. Перед публичным декларированием политики следует предусмотреть, чтобы все необходимые финансовые ресурсы, другие источники и высокопрофессиональные сотрудники были задействованы в реализации целей в области безопасности в запланированный период.

Для того чтобы обеспечить результативность политики в области безопасности, необходимо, чтобы она была документально оформлена, актуализировалась и периодически пересматривалась на предмет ее приемлемости;

5) доводиться до всего персонала для информирования сотрудников об их персональной ответственности за безопасность.

Вовлечение и ответственность персонала является важнейшим условием эффективной безопасности организации.

Сотрудники должны быть осведомлены о влиянии управления безопасностью на качество их собственной рабочей среды. Сотрудников следует поощрять к активному участию в управлении безопасностью.

Персонал (на всех уровнях, включая уровни управления) не сможет внести эффективный вклад в управление безопасностью, если он не вполне четко понимает политику безопасности организации и свои обязанности и не обладает в полной мере компетентностью для выполнения необходимых задач.

Для того чтобы сотрудники вносили эффективный вклад в управление безопасностью, необходимо, чтобы организация доводила до сведения всех сотрудников свою политику и цели безопасности и предоставляла инструментарий, чтобы у них была структура, с помощью которого они могли бы оценить свои результаты в области безопасности;

6) быть доступной для заинтересованных сторон.

Лицо или группа лиц (как внутренние, так и внешние), работа которых связана с показателями безопасности организации или попадающие под их влияние, будут заинтересованы в заявлении о политике безопасности. Следовательно, должен существовать процесс для доведения до них политики безопасности и обеспечивать ознакомление с политикой безопасности заинтересованных сторон при необходимости;

7) пересматриваться на предмет постоянной пригодности и соответствия деятельности организации.

В связи с изменениями правовых и законодательных норм политику в области безопасности и систему менеджмента безопасности организации следует регулярно пересматривать для обеспечения их актуальности и эффективности.

При внесении изменений в политику и систему менеджмента безопасности организации они должны быть доведены до сведения всех заинтересованных сторон.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты являются всеобъемлющей, кратко изложенной, понятной политикой в области безопасности, которая сообщается всей организации и заинтересованным сторонам, при необходимости

4.3 Оценка рисков безопасности и планирование

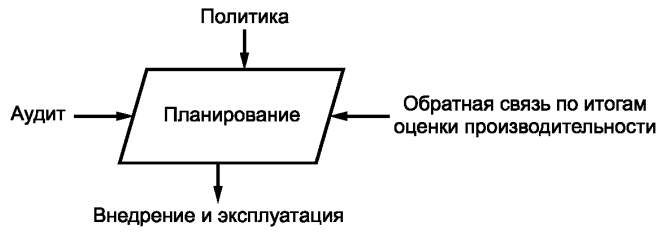


Рисунок 3 — Планирование

4.3.1 Оценка риска безопасности

a) Требования ИСО 28000

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. Методы идентификации, оценки и управления угрозами безопасности и рисками должны соответствовать 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:

a) в 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).

b) Намерения

После осуществления процесса идентификации угроз, оценки рисков и менеджмента рисков организация должна иметь общее представление о значительном риске, угрозах безопасности и уязвимостях в своей области деятельности.

Процессы идентификации угроз, оценки риска и менеджмента риска и их результаты должны стать основой всей системы безопасности. Следует обратить особое внимание на то, чтобы взаимосвязи между процессами идентификации угроз безопасности, оценки риска, менеджмента риска и другими элементами системы менеджмента безопасности были четко проработаны и были очевидными.

Целью настоящего стандарта является установление принципов, по которым организация может определить, являются ли подходящими и достаточными для работы процессы идентификации угроз, оценки рисков и управления рисками. Выдача рекомендации относительно того, каким образом следует осуществить эти действия, не является целью настоящего стандарта.

Использование организацией процессов идентификации угроз безопасности, оценки риска и управления рисками должно способствовать постоянному и своевременному выявлению, оценке и контролю своих рисков безопасности.

Во всех случаях следует учитывать возможность стандартных и нестандартных операций внутри организации и возникновения чрезвычайных ситуаций.

Сложность процессов идентификации угроз безопасности, оценки рисков менеджмента риска в значительной степени зависит от таких факторов, как размер организации, ситуация на рабочих местах, характер, сложность и значимость угроз безопасности. Цель ИСО 28000:2007 (см. п. 4.3.1) заключается в том, чтобы небольшие организации с низким риском для безопасности не проводили сложную идентификацию угроз безопасности, оценку риска, управления рисками и масштабные учения.

При внедрении процессов идентификации угроз, оценки риска и менеджмента риска организация должна принимать во внимание затраты и время на выполнение данных процессов, а также доступность достоверных данных.

Информация, уже разработанная для нормативных или других целей, может быть использована в регулировании этих процессов. Организация также может принимать во внимание степень существующего управления практического контроля рассматриваемой угрозой безопасности. С этой целью следует определить масштаб угрозы безопасности, учитывая входные и выходные данные (результаты), связанные с ее текущими и прежними действиями, процессами, продуктами и/или услугами организации.

Оценку риска безопасности должен проводить квалифицированный персонал с использованием признанных документированных методик.

Организация без существующей системы менеджмента безопасности может руководствоваться своей текущей позицией в отношении рисков безопасности посредством оценки риска. С целью реализации этой позиции должны быть рассмотрены угрозы безопасности, с которыми сталкивается организация, в качестве основы для создания системы менеджмента безопасности. Организация должна рассмотреть возможность включения (но не ограничиваясь этим) следующих пунктов при проведении первого анализа:

- нормативно-законодательные требования;
- идентификация угроз безопасности, с которыми сталкивается организация;
- идентификация угроз безопасности и информации о рисках в соответствующих организациях (полиция, службы безопасности);
- изучение всех существующих практик, процессов и процедур менеджмента безопасности;
- оценка обратной связи по результатам расследований предыдущих инцидентов и чрезвычайных ситуаций.

Целесообразный подход к оценке риска может включать чек-листы (контрольные списки), собеседования, непосредственные инспекции и измерения, результаты предыдущих аудитов системы менеджмента или другие проверки в зависимости от характера деятельности организации. Данные действия следует осуществлять по документированной и воспроизводимой методологии.

Необходимо отметить, что первичный обзор рекомендуется для создания базового направления, но он не заменяет реализацию структурированного систематического подхода, приведенного в 4.3.1.

c) Типовые входные данные

Типовые входные данные включают следующие аспекты:

- нормативно-законодательные и другие требования по безопасности (см. 4.3.2);
- политику в области безопасности (см. 4.2);
- записи об инцидентах;
- несоответствия (см. 4.5.3);
- результаты аудитов системы менеджмента безопасности (см. 4.5.5);
- обмен информацией с персоналом и другими заинтересованными сторонами (см. 4.4.3);
- информацию, полученную от привлеченных консультантов по безопасности, анализ и улучшение деятельности на рабочих местах (эта информация может иметь проактивный и реактивный характер реагирования);
- информацию о наиболее эффективных методиках, типичных случаях в отношении рисков безопасности организации, инцидентах и чрезвычайных ситуациях в других организациях;
- отраслевые стандарты;
- предписания со стороны федеральных органов;
- информацию об объектах, средствах организации, процессах, деятельности организации, включая:
  - детали изменений процедур,
  - планы расположения предприятия,
  - руководства по процессам и операционные процедуры,
  - данные по безопасности,
  - данные мониторинга (см. 4.5.1).

d) Процесс

1) Идентификация угроз, оценка риска и управление рисками

i) Общие положения

Меры по управлению риском должны отражать принцип устранения или снижения до практически достижимого минимального риска безопасности, где это практически осуществимо, либо путем уменьшения вероятности возникновения, либо потенциальной серьезности последствий от инцидента, связанного с безопасностью. Процессы идентификации угроз, оценки рисков и управления рисками являются ключевыми инструментами менеджмента риска.

Процессы идентификации угроз, оценки рисков и управления рисками значительно различаются в разных отраслях — от простых оценок до сложного количественного анализа с внушительной документацией. Организация должна планировать и внедрять такие процессы идентификации угроз, оценки рисков, управления рисками, которые отвечают ее потребностям и ситуациям на рабочем месте и обеспечивают соответствие законодательным требованиям в области безопасности.

Процессы выявления угроз безопасности, оценки рисков и менеджмента риска должны быть позиционированы как проактивные, а не как реактивные меры, т. е должны предшествовать введению новых или пересмотренных действий или процедур. Любое необходимое снижение риска и мероприятия по управлению рисками, которые определены, должны быть внедрены до реализации изменений.

Организация должна обеспечивать надлежащую квалификацию персонала, постоянно актуализировать свою методологию, документацию, данные и записи об идентификации угроз, оценке риска и управлении риском в отношении текущей деятельности, а также расширять их для того, чтобы проанализировать новые события и новые (или измененные) виды деятельности, прежде чем эти нововведения будут реализованы.

Процессы идентификации угроз, оценки рисков и менеджмента риска должны применяться не только к текущим операциям/видам детальности объекта и процедурам, но также к периодическим или случайным видам деятельности/процедурам.

Наряду с учетом рисков безопасности и рисков, связанных с деятельностью, осуществляемой собственным персоналом, организация должна принимать во внимание риски для безопасности и ри-

ски, возникающие в связи с деятельностью подрядчиков и посетителей, а также с использованием продуктов или услуг, предоставляемых ей другими организациями.

ii) Процессы

Процессы идентификации угроз, оценки риска и менеджмента риска должны быть документированы и включать следующие элементы:

- идентификацию угроз безопасности;
- оценку рисков с применением существующих (или предполагаемых) мероприятий по управлению рисками (с учетом подверженности конкретной угрозе безопасности, вероятности возникновения, сбоев в мероприятиях по управлению, потенциальной серьезности последствий, травм, повреждений и непрерывности работы);
- оценку приемлемости текущего и остаточного риска;
- определение необходимых дополнительных мер по управлению риском;
- оценку того, являются ли мероприятия менеджмента риска достаточными для снижения риска до приемлемого уровня.

Дополнительно процессы должны учитывать следующее:

- характер, сроки, объем и методологию для любой формы идентификации угроз, оценки рисков и менеджмента риска;
- применимые нормативно-законодательные требования по безопасности или другие требования;
- функции и полномочия персонала, ответственного за выполнение процессов;
- уровень компетентности и потребности в обучении (см. 4.4.2) для персонала, который должен выполнять процессы. В зависимости от характера или типа используемых процессов организации может потребоваться оказание внешних рекомендаций или услуг;
- информацию, представленную сотрудниками безопасности, относительно проверок и действий по непрерывному улучшению (эти действия могут быть реактивными или проактивными).

iii) Последующие действия

После реализации процессов идентификации угроз, оценки рисков и менеджмента риска:

- должны быть четкие доказательства того, что любые корректирующие или предупреждающие действия (см. 4.5.2), определенные как необходимые, отслеживаются на предмет их своевременного завершения. Для этого может потребоваться дальнейшая идентификация угроз и оценка риска для того, чтобы отразить предложенные изменения в мерах по управлению рисками и определить пересмотренные оценки остаточного риска;
- обратная связь о результатах и ходе выполнения корректирующих или предупреждающих действий должна быть направлена руководству в качестве исходных данных для анализа установления пересмотренных или новых целей по безопасности (см. 4.6);
- организация должна самостоятельно устанавливать соответствие компетенции персонала, выполняющего конкретные задания по безопасности, тому уровню, который определен процессом оценки риска при осуществлении необходимых мероприятий менеджмента риска;
- должна быть обратная связь по использованию опыта эксплуатации в будущем вышеперечисленных процессов для внесения поправок в них или в данные, на которых они основаны, если это применимо.

2) Действия после первоначальной идентификации угроз, оценки рисков и менеджмента рисков (см. также 4.6)

Процессы идентификации угроз безопасности, оценки рисков и менеджмента рисков следует пересматривать в заранее установленное время или в тот период, который указан в заявлении о политике безопасности. Допустимо, если заранее установленное время определяется руководством и может являться частью процесса анализа, проводимого со стороны руководства (см. 4.6).

Этот период может варьироваться в зависимости от следующих соображений:

- характер угрозы безопасности;
- степень риска;
- изменения в деятельности организации.

Анализ следует также проводить в том случае, если изменения, осуществляемые в организации, ставят под сомнение обоснованность действующих оценок рисков. Такие изменения могут включать в себя следующие элементы:

- расширение, сокращение, реструктуризация, изменения в объектах/инфраструктуре или аспектах цепи поставок;
- перераспределение обязанностей;

- изменение методов работы или моделей поведения при угрозах безопасности со стороны внешних источников.

e) Типовые выходные данные/результаты

Должны быть разработаны документированные процедуры для следующих элементов:

- идентификация угроз безопасности;
- определение рисков, связанных с идентифицированными угрозами. Указание уровня рисков, связанных с каждой угрозой безопасности, и их допустимости;
- описание или ссылка на мероприятия по мониторингу и управлению рисками (см. 4.4.6 и 4.5.1), особенно тех рисков, которые неприемлемы;
- цель безопасности и действия по снижению выявленных рисков (см. 4.3.3) и любые последующие действия для мониторинга прогресса в их снижении, при необходимости;
- определение требований к компетентности и обучению для реализации мероприятий по управлению (см. 4.4.2);
- необходимые мероприятия по управлению, описанные как элементы управления операциями/деятельностью системы (4.4.6);
- записи, генерируемые каждой из вышеупомянутых процедур.

4.3.2 Нормативно-законодательные и другие требования по безопасности

a) Требования ИСО 28000

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.

b) Намерения

Организация должна знать и надлежащим образом реагировать на вводимые нормативно-законодательные и другие требования и доводить до соответствующего персонала данную информацию.

Данное требование 4.3.2 из ИСО 28000:2007 предназначено для повышения осведомленности и понимания нормативно-законодательных требований и обязательств, однако не является обязанностью по созданию библиотек юридических или иных документов, потребность в которых минимальна.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- сведения о цепи поставок организации;
- результаты идентификации угроз безопасности, оценки рисков и менеджмента риска (см. 4.3.1);
- лучшие практики (например, кодексы, рекомендации отраслевых ассоциаций);
- законодательные требования, правительственные кодексы, надлежащие методики и правила межправительственных и торговых ассоциаций;
- список источников информации;
- национальные, региональные или международные стандарты;
- требования по внутренней работе организации;
- требования заинтересованных сторон;
- процессы управления динамикой цепи поставок.

d) Процесс

Должны быть идентифицированы существующие нормативно-законодательные и другие требования в области безопасности. Организация должна определить наиболее соответствующие средства для доступа и сохранения информации, включая средства медиаподдержки (например, бумага, компакт-диск, дисковод, Интернет), а также оценить, какие и где именно требования применяются и кому предназначены.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают следующие аспекты:

- процедуры идентификации и оценки информации и ее поддержания в актуальном состоянии;

- идентификация требований, которые применимы, и где именно они применимы (может быть в виде реестров);
- требования (фактический текст, резюме или анализ, где это уместно), находящиеся на местах, определенных организацией;
- процедура мониторинга новых законодательных требований по безопасности.

4.3.3 Цели в области менеджмента безопасности

a) Требования ИСО 28000

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.

b) Намерения

Необходимо обеспечить, чтобы во всей организации (где это практически возможно) были определены измеримые цели безопасности в соответствии с политикой безопасности.

c) Типовые входные данные

Типовые входные данные включают следующие аспекты:

- политика и цели, относящиеся к деятельности организации в целом;
- политика безопасности, включая обязательства по постоянному улучшению (см. 4.2);
- результаты идентификации угроз безопасности, оценки рисков и менеджмента риска (см. 4.3.1);
- нормативно-законодательные и другие требования (см. 4.3.2);
- технологические варианты;
- финансовые, операционные и бизнес-требования;
- проблемы сотрудников и заинтересованных сторон (см. 4.4.3);
- информация, поступающая от сотрудников по безопасности, относительно оценки и действий по улучшению ситуации на рабочем месте (эти действия могут быть реактивными или проактивными по своему характеру);
- анализ установленных целей безопасности;
- записи о выявленных несоответствиях безопасности, инцидентах и материальном ущербе;
- результаты анализа со стороны руководства (см. 4.6).

d) Процесс

Используя входные данные, руководство организации должно идентифицировать, разработать и определить приоритеты по целям в области безопасности.

При установлении целей по безопасности особое внимание следует уделять информации или данным, поступающим от тех лиц, которых это может персонально касаться, в связи с тем, что подобные обращения могут помочь обеспечить их разумность и более широкое признание. Также полезно рассмотреть информацию или данные, полученные от источника, внешнего по отношению к организации, например: от подрядчиков, поставщиков, деловых партнеров, полиции и спецслужб или заинтересованных сторон.

Совещания соответствующих уровней руководства управления для разработки целей по безопасности следует проводить регулярно (например, на ежегодной основе). В некоторых организациях при необходимости допустимо документировать процесс разработки целей по безопасности.

Цели по безопасности должны охватывать как проблемы корпоративной безопасности в целом, так и проблемы безопасности, специфичные для цепи поставок, отдельных функций и уровней в организации.

Для каждой цели по безопасности должны быть определены измеримые показатели, при наличии возможности, позволяющие контролировать выполнение цели по безопасности.

Цели по безопасности должны быть разумными и достижимыми для организации, а также позволяющими осуществлять их контроль, направленный на программу производственной деятельности. В организации должен быть график выполнения для реализации каждой цели по безопасности.

Цели по безопасности могут быть разбиты на отдельные подцели в зависимости от размера организации, сложности цели безопасности и времени ее достижения. Должны быть четкие связи между различными уровнями целей и измеримыми показателями по безопасности.

Примеры целей безопасности по безопасности включают в себя:

- снижение уровня риска;
- внедрение дополнительных функций в систему менеджмента безопасности;
- шаги, предпринятые для улучшения существующих объектов;
- устранение или уменьшение частоты конкретного инцидента.

Цели по безопасности должны быть доведены до соответствующего персонала [например, посредством обучения или групповых инструктажей (см. 4.4.2)] и подробно изложены через программы менеджмента безопасности (см. 4.3.4).

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают документированные, измеримые (где это практически реализуемо) цели по безопасности относительно каждой функции в организации.

4.3.4 Целевые показатели в области менеджмента безопасности

Требования ИСО 28000

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.

b) Намерения

Целевые показатели устанавливаются для достижения целей организации в пределах ограниченного промежутка времени.

c) Типовые входные данные

Типовые входные данные включают в себя:

- политику и цели, относящиеся к деятельности организации в целом;
- политику безопасности, включая обязательства по постоянному улучшению (см. 4.2);
- результаты идентификации угроз, оценки риска и менеджмента риска (см. 4.3.1);
- нормативно-законодательные требования (см. 4.3.2);
- технологические варианты;
- финансовые, операционные требования и бизнес-требования;
- проблемы сотрудников и заинтересованных сторон (см. 4.4.3);
- информацию, полученную от сотрудников, по безопасности, оценке и улучшению работы на местах (эта деятельность может быть реактивной и проактивной по своему характеру);
- анализ разработанных целей по безопасности;
- записи о прошлых несоответствиях и инцидентах, связанных с безопасностью;
- результаты анализа со стороны руководства (см. 4.6).

d) Процесс

Процесс определен в программах безопасности и представляет собой достижимые целевые показатели для выполнения целей.

Используя входные данные организации, соответствующее руководство должно определить и установить приоритеты для достижения целевых показателей. Целевые показатели должны быть конкретными, основанными на временной шкале и измеримыми.

При установлении целевых показателей безопасности особое внимание следует уделять информации или данным, полученным от тех лиц, у кого с наибольшей вероятностью будут персональные целевые показатели безопасности, так как это способствует разумности установления показателей и облегчению их восприятия в организации. Также полезно рассмотреть входные данные, поступающие от внешних источников, например: от подрядчиков, поставщиков, деловых партнеров, представителей федеральных органов или заинтересованных сторон.

Совещания соответствующих уровней руководства по разработке целевых показателей безопасности следует проводить после изменения целей по безопасности. В некоторых организациях допускается документировать процесс установления целевых показателей безопасности.

Целевые показатели безопасности должны охватывать как проблемы корпоративной безопасности в целом, так и проблемы безопасности, характерные для цепи поставок, отдельных функций и определенных уровней в организации.

Для каждого целевого показателя должен быть разработан конкретный количественный индикатор. Этот индикатор должен обеспечивать возможность мониторинга выполнения целевых показателей безопасности.

Целевые показатели безопасности должны быть разумными и достижимыми для организации, а также позволяющими осуществлять их контроль, направленный на производственную деятельность. Следует установить временную шкалу для реализации каждого целевого показателя по безопасности.

Целевые показатели по безопасности могут быть подразделены на отдельные подпоказатели в зависимости от размера организации, сложности целевого показателя безопасности и временной шкалы. Должна быть установлена четкая взаимосвязь между различными уровнями целей и целевых показателей.

Примеры типов целей безопасности включают в себя:

- снижение уровня риска в течение определенного периода времени;
- внедрение конкретных новых технологий для снижения риска или смягчения воздействия угроз безопасности;
- конкретные шаги, предпринимаемые для улучшения существующих объектов в конкретные сроки;
- устранение или уменьшение частоты возникновения конкретного инцидента.

Целевые показатели безопасности должны быть доведены до соответствующего персонала (например, посредством обучения или групповых инструктажей; см. 4.4.2) и подробно изложены в программе менеджмента безопасности (см. 4.3.4).

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя документированные, измеримые, где это практически возможно, целевые показатели безопасности относительно каждой функции в организации.

4.3.5 Программы менеджмента безопасности

a) Требования ИСО 28000

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.

b) Намерения

Программы менеджмента безопасности должны быть напрямую связаны с целями и целевыми показателями. В каждой программе должно быть описано, как организация преобразует свои цели и обязательства в политике в определенные действия для достижения цели безопасности и целевых показателей. Программа потребует разработки стратегий и планов действий, которые должны быть документированы и доведены до сведения персонала. Прогресс реализации программы в отношении достижения заявленной цели должен находиться под контролем, анализироваться и документально оформляться. Стратегия программы сдерживания и минимизации последствий должна быть основана на результатах идентификации угроз и опасностей, оценке рисков (например, анализ воздействия, оценка программы, оперативный опыт).

c) Типовые входные данные

Типовые входные данные включают в себя следующие элементы:

- цели и целевые показатели по безопасности;
- нормативно-законодательные и другие требования;
- результаты идентификации угроз безопасности, оценки рисков и менеджмента рисков;
- сведения о деятельности организации;
- информация, полученная на основе выполненных работ по обеспечению безопасности, проверке и улучшению деятельности работников на рабочем месте (эти действия могут быть реактивными или проактивными по своей природе);
- анализ реальных возможностей с учетом новых различных или действующих технологических вариантов;
- действия по постоянному улучшению деятельности;
- ресурсы, необходимые для достижения целей безопасности организации.

d) Процесс

Программы менеджмента безопасности должны определять:

- ответственность за достижение целей;
- средства для достижения целей;
- временные рамки достижения целей.

В рамках программы следует рассмотреть возможность снижения угрозы с помощью методологических и технологических вариантов и опыта других организаций, принимая во внимание финансовые, операционные и бизнес-требования, а также мнения партнеров и заинтересованных сторон.

В программе должно быть предусмотрено распределение соответствующей ответственности и полномочий относительно каждой задачи и определены временные рамки для каждого отдельного задания для соответствия общей шкале времени установленной цели безопасности. Следует также предусмотреть распределение необходимых ресурсов из наиболее адекватных источников (например, финансовые, человеческие, оборудование, логистика) для каждого задания.

В тех случаях, когда предполагается внесение значительных изменений или модификаций в методах работы, процессах, оборудовании или средствах, в программе должны быть предусмотрены учения по идентификации новых угроз безопасности и оценке рисков. В курсе программы управления безопасностью следует уделить внимание консультациям с соответствующим персоналом относительно ожидаемых изменений.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают разработанные и документированные программы менеджмента безопасности для достижения целей и целевых показателей (см. 4.3.3 и 4.3.4).

4.4 Внедрение и функционирование

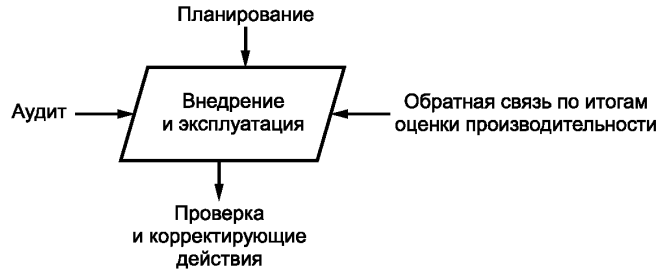


Рисунок 4 — Внедрение и функционирование

4.4.1 Структура, ответственность и полномочия по менеджменту безопасности

a) Требования ИСО 28000

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) обеспечения жизнеспособности целей, целевых показателей и программ менеджмента безопасности.

b) Намерения

Для облегчения эффективного управления безопасностью необходимо, чтобы роли, обязанности и полномочия были определены, задокументированы и доведены до соответствующего персонала. Только ответственный за безопасность персонал (см. определение в разделе 3) должен быть задействован для реализации критических задач безопасности. Должны быть предоставлены адекватные источники ресурсов для четкого выполнения заданий по безопасности

c) Типовые входные данные

Типовые входные данные включают следующее:

- организационную структуру;

- идентификацию рисков, оценку рисков и результаты управления рисками;
- цели, целевые показатели и программы по безопасности;
- нормативные и законодательные требования;
- должностные инструкции;
- перечень квалифицированных сотрудников службы безопасности, которые прошли и/или должны пройти оценку благонадежности.

d) Процесс

1) Обзор

Должны быть определены обязанности и полномочия тех лиц, на которых возложена ответственность в системе менеджмента безопасности, включая четкое определение обязанностей на пересечении различных функций.

Такие определения могут, в частности, потребоваться для следующих категорий сотрудников:

- высшее руководство;
- руководители среднего звена на всех уровнях организации;
- ответственные за подрядчиков и посетителей, которые имеют доступ к помещению и его работникам;
- ответственные за обучение по безопасности;
- ответственные за оборудование и операции, которые имеют решающее значение для безопасности;
- сотрудники, прошедшие оценку благонадежности, или другие специалисты по безопасности внутри организации;
- сотрудники службы безопасности, предоставляющие консультации на проводимых форумах.

Однако организация должна доводить до сведения сотрудников информацию и непреложность ее реализации относительно того, что безопасность — это ответственность каждого сотрудника организации, а не только ответственность тех, кто наделен определенными обязанностями в системе менеджмента безопасности.

2) Определение ответственности высшего руководства

В обязанности высшего руководства должны входить разработка политики организации в области безопасности и обеспечение внедрения системы менеджмента безопасности. В рамках этого обязательства высшее руководство должно провести выборы и назначить конкретного представителя руководства с определенными обязанностями и полномочиями для внедрения системы менеджмента безопасности. В крупных или сложных по структуре организациях может быть назначено несколько ответственных представителей.

3) Определение ответственности представителя руководства

Представитель руководства в области менеджмента безопасности должен нести ответственность и иметь полномочия по обеспечению того, чтобы система менеджмента безопасности была внедрена и документирована. Представитель руководства в области менеджмента безопасности должен иметь постоянный доступ к высшему руководству и поддерживаться другим персоналом, которому делегированы обязанности по мониторингу работы всех функций безопасности организации. Представитель руководства должен регулярно получать информацию о функционировании системы и активно участвовать в регулярном рассмотрении и определении целей безопасности. Следует обеспечить, чтобы любые другие обязанности или функции, возложенные на этих сотрудников, не вступали в противоречие с выполнением ими обязанностей по обеспечению безопасности.

4) Определение ответственности линейного руководства (менеджеров среднего звена)

Ответственность руководителей среднего звена должна включать обеспечение того, что управление безопасностью осуществляется в пределах его зоны действия. В тех случаях, когда ответственность за вопросы безопасности возложена исключительно на руководителе среднего звена, роль и обязанности отдельной функции безопасности в организации должны быть надлежащим образом определены во избежание двусмысленности в отношении ответственности и полномочий. С этой целью следует проводить мероприятия по разрешению любого конфликта, возникающего из-за проблем безопасности, с одной стороны, и соображений производительности — с другой, путем перехода на более высокий уровень управления.

5) Документирование ролей и ответственности

Ответственность и полномочия по безопасности должны быть задокументированы по форме, выбранной организацией. Это может быть одна или несколько из следующих форм (при этом организация может выбрать альтернативную форму):

- руководство по системе менеджмента безопасности;
- процедура и описание задач;
- должностные инструкции;
- вводный обучающий пакет и информационные программы.

Если в организации сочтут необходимым документально оформить должностные инструкции, охватывающие другие аспекты ролей и обязанностей сотрудников, то в эти должностные инструкции должны быть включены обязанности по обеспечению безопасности.

6) Информация о ролях и ответственности

До сведения сотрудников должна быть доведена информация об обязанностях и полномочиях, которые непосредственно их касаются. Это направлено на четкое понимание сферы деятельности и связи между различными функциями и каналами, использованными для инициирования действий.

7) Ресурсы

Руководство должно обеспечить наличие необходимых ресурсов для поддержания безопасной цепи поставок, включая оборудование, человеческие ресурсы, экспертные знания и обучение.

Ресурсы следует считать адекватными, если они достаточны для выполнения программ и мероприятий по обеспечению безопасности, включая измерение результатов и мониторинг.

В той организации, в которой внедрены системы менеджмента безопасности, адекватность источника ресурса можно оценить путем сравнения запланированных целей по безопасности и фактических результатов.

8) Ответственность руководства

Высшее руководство должно наглядно продемонстрировать свою приверженность целям безопасности. Средства демонстрации могут включать посещение и осмотр производственных площадок, участие в расследовании инцидентов безопасности и предоставление источников ресурсов в контексте корректирующих действий, посещение собраний по безопасности и выпуск сообщений поддержки.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты:

- определение обязанностей по обеспечению безопасности и полномочий для всего соответствующего персонала;
- документирование ролей/обязанностей в руководствах/процедурах/учебных пакетах;
- процесс передачи ролей и обязанностей всем сотрудникам и другим соответствующим сторонам;
- активное участие руководства и поддержка безопасности на всех уровнях.

4.4.2 Компетентность, обучение и осведомленность

a) Требования ИСО 28000

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.

b) Намерения

Организация должна иметь эффективную процедуру для обеспечения компетентности персонала при выполнении возложенных на них функций по обеспечению безопасности, а также их осведомленности о рисках безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя следующие аспекты:

- определения ролей и обязанностей;
- должностные инструкции (включая детали задач безопасности, которые должны быть выполнены);
- оценка результатов работы сотрудников;
- идентификация риска безопасности, оценка риска и результаты управления рисками;
- процедура и инструкция по эксплуатации;
- политика безопасности и цели безопасности;
- программы безопасности.

d) Процесс

Следующие элементы должны быть включены в процесс:

- систематическое определение осведомленности о безопасности и компетенциях, необходимых на каждом уровне и функции в организации;
- меры по выявлению и устранению выявленных недостатков между уровнем ответственности, которым в настоящее время наделено физическое лицо, и надлежащей осведомленностью и компетентностью в области безопасности;
- своевременное и систематическое проведение любого обучения, признанного необходимым;
- оценка персонала для того, чтобы удостовериться в том, что персонал приобрел и поддерживает необходимые знания и уровень компетентности;
- ведение соответствующей записи об обучении и компетентности сотрудников.

Примечание — Особое внимание должно быть уделено осведомленности о безопасности во всей организации, что крайне важно для успешной работы системы менеджмента безопасности и ее эффективного внедрения.

Должна быть создана и поддерживаться программа повышения осведомленности и обучения в области безопасности по следующим аспектам:

- осведомленность о рисках и угрозах безопасности на систематической основе;
- понимание механизмов безопасности в организации и конкретных функций и обязанностей отдельных лиц;
- систематическая программа вводного и непрерывного обучения для сотрудников и тех лиц, кто меняет место работы в пределах организации или решает задачи внутри организации;
- обучение принятию мер безопасности противодействию и рискам безопасности на конкретных местах, а также рискам, мерам предосторожности и процедурам, которые необходимо соблюдать (причем это обучение проводят до начала работы в организации или непосредственно на рабочем месте);
- обучение выполнению идентификации риска безопасности, оценки риска и управления риском (см. 4.3.1 d);
- специальное внутреннее или внешнее обучение, которое может потребоваться сотрудникам с определенными ролями в системе безопасности, включая представителей по безопасности;
- обучение ответственных лиц, под управлением которых находятся другие сотрудники, подрядчики и другие лица (например, временные работники), их обязанностям по обеспечению безопасности. Это делается для того, чтобы данные ответственные лица и те, кто находится под их управлением, понимали угрозы безопасности и риски, связанные с выполнением работ, за которые они несут ответственность, вне зависимости от места их проведения. Кроме того, необходимо гарантировать, что персонал обладает компетенциями, необходимыми для безопасного выполнения действий, следуя процедурам безопасности;
- роли и обязанности (включая корпоративные и индивидуальные юридические обязанности) высшего руководства по обеспечению функционирования системы менеджмента безопасности для управления рисками и сведения к минимуму заболеваний, травм и других потерь для организации;
- программы обучения и повышения осведомленности подрядчиков, временных работников и посетителей в соответствии с уровнем риска, которому они подвергаются.

Результативность программ обучения и повышения осведомленности следует оценивать, например, в виде оценки при проведении тестирований (учений) и/или соответствующих проверок на месте, для определения того, были ли достигнуты компетентность и достаточная осведомленность. Также результативность может быть оценена в виде долгосрочного мониторинга воздействия проведенного обучения.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- требования к компетентности для выполнения отдельных функций;

- анализ потребностей в обучении;
- учебные программы/планы;
- диапазон учебных курсов/продуктов, доступных для использования в организации;
- записи об обучении, записи оценки результативности обучения;
- программы информирования о безопасности;
- оценка осведомленности о безопасности.

4.4.3 Обмен информацией

a) Требования ИСО 28000

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.

b) Намерения

Организация должна поощрять участие всех, кто вовлечен в ее деятельность, в изучении передовых практик по безопасности и оказывать поддержку в продвижении своей политики безопасности и целей безопасности в процессе консультаций и делового общения.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- политика безопасности и цели безопасности;
- соответствующая документация системы управления безопасностью;
- идентификация рисков безопасности, оценка рисков и процедуры контроля рисков;
- определение ролей по безопасности и обязанностей;
- результаты официальных и неофициальных консультаций по вопросам безопасности сотрудников с руководством;
- детали программы обучения;
- соответствующая информация, полученная из внешних источников.

d) Процесс

Организация должна документировать и способствовать продвижению договоренностей, с помощью которых проводит консультации и доводит до сведения соответствующую информацию о безопасности своих сотрудников и других заинтересованных сторон (например, подрядчиков, посетителей, деловых партнеров, органы власти).

Меры по вовлечению сотрудников включают в себя следующие процессы:

- консультации по разработке и анализу политик, разработке и рассмотрению целей безопасности, решений по внедрению процессов и процедур менеджмента рисков, включая проведение оценки рисков безопасности и контроля рисков, связанных с их собственной деятельностью; консультации по вопросам внесения изменений, влияющих на безопасность на рабочем месте, таких как введение нового или модифицированного оборудования, оснащение, использование химических веществ, а также внедрение необходимых технологий, процессов, процедур или схем работы;
- сотрудники должны быть осведомлены по вопросам безопасности и проинформированы об определенной схеме управления, действующей для обеспечения безопасности.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующее:

- официальное руководство и консультации сотрудников путем задействования советов безопасности или аналогичных органов;
- участие сотрудников в идентификации рисков безопасности, оценке рисков и управлении рисками;
- инициативы по поощрению консультаций сотрудников по вопросам безопасности, проверок и улучшений на рабочем месте и обратной связи с руководством по вопросам безопасности;
- распределение ролей, порядок и механизмы взаимодействия с руководством, установленные для сотрудников при расследовании происшествий и инцидентов, инспекции безопасности на площадке и т. д.;
- инструктажи по безопасности для сотрудников и других заинтересованных сторон, например подрядчиков или посетителей;

- доски объявлений, содержащие информацию о безопасности;
- бюллетень по безопасности;
- наглядную информацию по безопасности;
- другие средства для обмена конфиденциальной информацией и отчетами о безопасности с соответствующими органами власти и партнерами по цепи поставок.

4.4.4 Документирование

a) Требования ИСО 28000

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.

b) Намерения

Организация должна документировать и поддерживать данные в актуальном состоянии для того, чтобы гарантировать, что ее система менеджмента безопасности доведена до сведения персонала, результативно внедрена и находится в рабочем состоянии.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- детали документации и информационных систем, которые организация разрабатывает для поддержки своей системы менеджмента безопасности и деятельности по обеспечению безопасности, а также для выполнения требований ИСО 28000;
- обязанности и полномочия;
- информацию об объектах, в которых используется документация или информация, и об ограничениях, которые это может накладывать на физическую природу документации, или о применении электронных или других носителей.

d) Процесс

Организация должна идентифицировать данные и информацию, которые необходимы для системы менеджмента безопасности, прежде чем разрабатывать документацию, необходимую для поддержки ее процессов безопасности и системы менеджмента безопасности.

Необходимость разрабатывать документацию в определенном формате, соответствующую ИСО 28000, отсутствует, точно так же как и заменять существующую документацию, например руководства, процедуры или рабочие инструкции, если они объективно описывают действующие мероприятия по обеспечению безопасности. Если организация уже обладает установленной документированной системой менеджмента безопасности, то более удобно и эффективно будет разработать документ перекрестных ссылок, отражающий взаимосвязь между ее существующей процедурой и требованиями ИСО 28000.

При этом необходимо учитывать следующее:

- обязанности и полномочия пользователей документации и информации, определяющие степень безопасности и доступности, которые должны быть установлены;
- способ использования физической документации в бумажном виде и среда, в которой она используется. Аналогичное внимание следует уделить использованию электронного оборудования, предназначенного для информационных систем.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- обзорная документация по системе менеджмента безопасности;
- перечни документов, основные списки или указатели;
- процедуры;
- рабочие инструкции.

4.4.5 Управление документами и данными

a) Требования ИСО 28000

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.

b) Намерения

Все документы и данные, содержащие информацию, критически важную для работы системы менеджмента безопасности и эффективности деятельности организации, должны быть идентифицированы и находиться под управлением.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- детали документации и систем данных, которые организация разрабатывает для поддержки своей системы менеджмента безопасности и деятельности по обеспечению безопасности, а также для выполнения требований ИСО 28000;
- детальное описание обязанностей и полномочий.

d) Процесс

Должна быть разработана и внедрена письменная процедура, в которой определены средства контроля для идентификации, утверждения, выдачи, доступа и удаления документации по безопасности и контроль безопасности данных. Эта процедура должна четко определять категории документации и данных, к которым она применяется, и уровень классификации, основанный на степени конфиденциальности информации.

Документация и данные должны быть в наличии и доступны для уполномоченного персонала при необходимости в стандартных и нестандартных условиях, включая чрезвычайные ситуации.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- процедуру управления документацией, включая распределение обязанностей и полномочий;
- список документов, номенклатура дел;
- список контролируемой документации и ее местонахождение;
- архив записей.

4.4.6 Управление операциями

a) Требования ИСО 28000

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 имеющие 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.

b) Намерения

Организация должна разработать и поддерживать в рабочем состоянии механизмы, обеспечивающие эффективное проведение мероприятий по управлению и принятие контрольных мер для контроля операционных рисков безопасности, выполнения политики и целей безопасности, достижения целевых показателей безопасности и соответствия нормативно-законодательным и другим требованиям.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- политика безопасности и цели безопасности;
- идентификация угроз безопасности и оценка рисков;
- применимые нормативно-законодательные и другие требования.

d) Процесс

Организация должна установить процедуру для управления выявленными рисками, в том числе теми, которые могут возникать в связи с действиями подрядчиков, деловых партнеров или посетителей. Документирование данной процедуры необходимо в тех случаях, когда это может привести к инцидентам, чрезвычайным ситуациям или другим отклонениям от политики безопасности и реализации целей безопасности. Процедуры менеджмента риска следует регулярно проверять на предмет их продолжающейся пригодности и результативности. В случае необходимости в данные процедуры должны быть внесены изменения.

Процедуры должны учитывать такие ситуации, когда риски распространяются на помещения клиентов или других внешних сторон либо зоны контроля в других частях цепи поставок (например, когда сотрудники организации работают на площадке клиента). В отдельных случаях может потребоваться консультация с внешней стороной по вопросам безопасности.

Ниже приведены примеры областей, в которых, как правило, возникают риски, а также примеры мер борьбы с ними.

1) Покупка или перемещение товаров и услуг и использование внешнего ресурса

Это включает в себя следующие элементы:

- оценка и периодическая переоценка компетентности подрядчиков в области безопасности;
- утверждение проекта мероприятий безопасности для нового завода или оборудования.

2) Чувствительные к безопасности задачи (конфиденциальные)

Это включает в себя, например, следующее:

- выявление чувствительных к безопасности (конфиденциальных) задач;
- предварительное определение и утверждение безопасных методов работы;
- предварительная квалификация персонала для выполнения ответственных задач безопасности;
- процедура контроля за входом персонала в зоны безопасности.

3) Техническое обслуживание охранного оборудования

Это включает в себя следующее:

- разделение и контроль доступа;
- проверка и тестирование охранного оборудования и систем с высокой целостностью.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- процедуры;
- инструкцию по эксплуатации и техническому обслуживанию.

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

a) Требования ИСО 28000

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

b) Намерения

В этом пункте рассмотрены готовность, реагирование и восстановление политики безопасности после инцидента. Термин «готовность к чрезвычайным ситуациям» означает планирование, подготовку и принятие мер предосторожности после незапланированных событий, угрожающих безопасности, или кризисов.

Организация должна активно оценивать потенциально возможные инциденты и потребности в реагировании на события, угрожающие безопасности и выявленные в процессе идентификации угроз и оценки риска (см. 4.3.1). Должны быть разработаны планы реагирования, процедуры и процессы для устранения последствий и аудит отработанных мер по реагированию с целью повышения результативности.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- идентификацию угроз безопасности и оценку рисков;
- участие местных служб экстренной помощи и служб безопасности, а также подробную информацию о согласованных мерах реагирования или проведение консультаций в случае чрезвычайной ситуации;
- нормативно-законодательные или иные требования;
- опыт и анализ ранее произошедших инцидентов и чрезвычайных ситуаций и результатов принятых действий;
- опыт организаций с аналогичными видами деятельности из предыдущих инцидентов и чрезвычайных ситуаций (извлеченные уроки, лучшие практики);
- материалы федеральных органов власти и служб экстренного реагирования;
- обзор проведенных учений и занятий.

d) Процесс

Организация должна разработать план(ы) действий в чрезвычайных ситуациях, определить и предоставить план принятия соответствующих аварийных мер и предусмотреть регулярную проверку своих возможностей путем тренировок. Планы аварийной готовности, реагирования и восстановления безопасности должны включать меры по восстановлению безопасности, защите данных и средств и обеспечению непрерывного действия безопасности.

Практические занятия должны подтвердить результативность наиболее важных частей плана(ов) реагирования на предмет безопасности и полноту процесса планирования на случай чрезвычайной ситуации. В то время как теоретические упражнения могут быть полезны в процессе планирования, далее следует проводить практические учения. Результаты аварийных и практических учений должны быть оценены и при необходимости внесены изменения.

1) Реагирование на чрезвычайные ситуации и план восстановления безопасности

План(ы) реагирования на чрезвычайные ситуации и восстановления безопасности должен (должны) содержать описание действий, которые необходимо предпринять при возникновении указанных ситуаций, и эти планы должны включать следующее:

- выявление потенциальных инцидентов и чрезвычайных ситуаций;
- идентификацию лица, ответственного за действия в чрезвычайной ситуации;
- детали действий, которые должны быть предприняты персоналом во время чрезвычайной ситуации, включая те действия, которые должны быть осуществлены внешним персоналом, в случае его присутствия на месте чрезвычайной ситуации, таким как подрядчики или посетители (которым может потребоваться, например, перейти на указанный пункт сбора для эвакуации);
- ответственность, полномочия и обязанности персонала, выполняющего определенные функции во время чрезвычайной ситуации (например, охрана, пожарные, персонал скорой помощи, специалисты по радиологической утечке/токсическому загрязнению);
- процедуры эвакуации;
- процедуры, содержащие способы восстановления безопасности и условий безопасности в краткосрочной и среднесрочной перспективе;
- идентификацию, расположение и защиту секретных данных, конфиденциальные записи и оборудование, а также необходимые действия в чрезвычайной ситуации;
- взаимодействие с аварийными службами и службами первой помощи;
- обмен информацией с заинтересованными сторонами;
- наличие необходимой информации во время чрезвычайной ситуации, например: чертежи компоновки завода, данные по безопасности, процедуры, рабочие инструкции и контактные телефоны;
- взаимодействие с деловыми/торговыми партнерами;
- обеспечение целостности систем связи.

Участие внешних агентств в планировании и реагировании на чрезвычайные ситуации должно быть четко задокументировано. Эти учреждения должны быть проинформированы о возможных обстоятельствах их участия и снабжены такой информацией, которая требует их содействия в деятельности по принятию мер реагирования.

2) Охранное оборудование

Необходимо определить потребности в оборудовании для обеспечения безопасности и предоставить его в достаточном количестве. Следует проводить проверки для выявления случаев повреждения работоспособности оборудования.

3) Практические занятия и учения

Практические занятия и учения должны проводиться по заранее установленному графику. При целесообразности и осуществлении на практике следует поощрять участие внешних служб безопасности в проводимых организацией учениях.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают следующее:

- документированные аварийные планы и процедуры реагирования на чрезвычайные ситуации, планы восстановления безопасности;
- список охранного оборудования;
- протоколы испытаний охранного оборудования;
- практические занятия и учения;
- обзор/анализ тренировочных занятий и учений;

- рекомендуемые действия на основе проведенного анализа;
- прогресс в достижении рекомендуемых действий;
- принятые действия.

4.5 Контроль и корректирующие действия

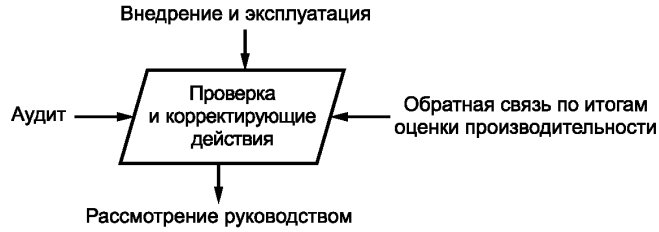


Рисунок 5 — Контроль и корректирующие действия

4.5.1 Измерение и мониторинг результатов деятельности по безопасности

a) Требования ИСО 28000

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры мониторинга и измерения результатов деятельности всей системы менеджмента безопасности, а также процедуры мониторинга и измерения результатов деятельности 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) проактивные 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.

b) Намерения

Организация должна определить ключевые показатели деятельности (KPI) в области безопасности в пределах организации, цепи поставок, которыми она управляет и которые находятся в сфере ее влияния. Эти показатели должны включать, но не ограничиваться следующим:

- достижение политики и целей в области безопасности;
- результаты управления/снижения угроз, в зависимости от обстоятельств, контрмеры, а также оценка их результативности;
- извлеченные уроки из сбоев системы менеджмента безопасности, в том числе инцидентов безопасности и ошибок;

- оценка результативности программ информирования, обучения, обмена информацией и консультирования сотрудников и заинтересованных сторон;
- получение и использование информации, которая может быть применена для анализа и улучшения аспектов системы менеджмента безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя следующее:

- идентификацию угрозы безопасности, оценку риска и управление риском (см. 4.3.1);
- требования законодательства, правила, лучшие действующие практики (при их наличии);
- политику и цели безопасности;
- процедуру управления несоответствиями;
- протоколы испытаний и калибровки охранного оборудования, включая оборудование, принадлежащее подрядчикам;
- отчеты об обучении (включая подрядчиков);
- отчеты руководства.

d) Процесс

1) Проактивный и реактивный мониторинг

Система менеджмента безопасности организации должна включать как проактивный, так и реактивный мониторинг, осуществляемый нижеприведенным образом.

Проактивный мониторинг следует использовать для проверки соответствия деятельности организации в области безопасности, например путем мониторинга результативности частоты и эффективности проверок безопасности.

Реактивный мониторинг следует использовать для расследования, анализа и регистрации нарушений, выявленных в системе менеджмента безопасности, включая аварийные ситуации и инциденты безопасности.

Как проактивные, так и реактивные данные мониторинга часто применяют для определения того, достигнуты ли цели в области безопасности.

2) Технологии измерения

Ниже приведены те примеры методов, которые можно использовать для измерения результатов деятельности по безопасности:

- результаты идентификации риска безопасности, оценки риска и процессов управления риском, таких как соблюдение рамочных стандартов безопасности ВТО и Таможенно-торгового партнерства США против терроризма (C-TPAT), Постановления уполномоченного экономического оператора Европейской комиссии (УЭО);
- систематические проверки с использованием контрольных списков (чек-листов);
- инспекции по безопасности;
- оценка новых логистических систем цепи поставок;
- рассмотрение и оценка полученных статистических моделей логистики;
- осмотр охранного оборудования для проверки его исправного состояния;
- доступность и эффективность использования персонала с признанным опытом в области безопасности или официальной квалификацией;
- оценка поведения работников для выявления ненадлежащих мер безопасности, которые могут потребовать исправления;
- анализ документации и записей;
- сравнение с надлежащей практикой безопасности в других организациях;
- опросы для определения отношения сотрудников к выявлению подозрительного поведения;
- обратная связь с заинтересованными сторонами.

Организация должна решить, что контролировать и как часто следует проводить мониторинг в зависимости от уровня риска (см. 4.3.1). Должен быть подготовлен график проверок, основанный на результатах идентификации угроз, оценке рисков и нормативно-законодательных требованиях, в качестве части системы менеджмента безопасности.

Регулярный мониторинг безопасности процессов, логистических узлов, деловых партнеров, действий цепи поставок и практики следует проводить в соответствии с документированной схемой мониторинга уполномоченным персоналом, в обязанности которого включены и выборочные проверки критических задач для обеспечения соответствия процедурам безопасности и кодексам практики. Для оказания помощи в проведении систематических проверок и мониторинга могут быть использованы контрольные списки (чек-листы).

3) Охранное оборудование

Должен быть составлен перечень охранного оборудования, которое используют для мониторинга и обеспечения безопасности (например, камеры, заборы, ворота, сигнализация и т. д.). Оборудование должно быть идентифицировано и тщательно контролироваться. Точность показаний этого оборудования должна быть известна. При необходимости должна быть доступна письменная процедура, описывающая, как проведены измерения по безопасности. Оборудование, используемое для обеспечения безопасности, должно поддерживаться в надлежащем порядке и должно быть способно функционировать в соответствии с установленными требованиями.

При необходимости график калибровки, поверки и технического обслуживания для охранного оборудования должен быть документирован и внедрен. Этот график должен включать следующие пункты:

- частота калибровки и технического обслуживания;
- ссылка на методы испытаний, где это применимо;
- идентификация оборудования, которое будет использовано для калибровки;
- действия, которые необходимо предпринять, если указанное оборудование для обеспечения безопасности не соответствует калибровке.

Калибровка, поверка и техническое обслуживание должны быть проведены в надлежащих условиях. Процедура должна быть подготовлена для критических или сложных калибровок.

Оборудование, используемое для калибровки, должно соответствовать национальным стандартам, при их наличии. В случае отсутствия данных стандартов основу для используемых уровней следует задокументировать.

Необходимо вести записи всех калибровок, работ по техническому обслуживанию и результатов. Записи должны содержать подробности измерений до и после калибровки.

Статус калибровки и поверки охранного оборудования должен быть четко определен для пользователей.

Не следует использовать охранное оборудование, статус калибровки или поверки которого неизвестен или известно, что оно не соответствует калибровке/поверке. Кроме того, оборудование должно быть снято с эксплуатации и четко обозначено, маркировано или иным образом отмечено для предупреждения случайного использования. Такая маркировка должна быть осуществлена в соответствии с письменной(ыми) процедурой(рами). Процедура должна включать определение статуса калибровки/поверки оборудования. Несоответствие должно быть выдано для документирования предпринятых действий. Процедура должна включать план действий в случае обнаружения оборудования, не прошедшего калибровку/поверку.

4) Инспекция

i) Оборудование

Инвентаризация (с использованием уникальной идентификации всех предметов) должна быть проведена для всего охранного оборудования. Такое оборудование должно быть проверено по мере необходимости и включено в схемы проверки.

ii) Инспекции по безопасности

Следует проводить инспекции по безопасности, но они не должны освобождать уполномоченный персонал от проведения регулярных проверок или выявления угроз безопасности.

iii) Записи о проведении инспекций

Каждая инспекция по безопасности должна быть документально оформлена. Записи должны указывать, выполнялась ли документированная процедура безопасности. Должны быть отобраны записи инспекций по безопасности, обходов, опросов и аудитов системы менеджмента безопасности для выявления причин несоответствия и повторяющихся рисков безопасности. Должны быть предприняты необходимые предупреждающие действия. Угрозы безопасности, вызывающие подозрение, обстоятельства и несоответствующее оборудование, выявленные в ходе проверок, должны быть задокументированы как несоответствия, оценены как риск и исправлены в соответствии с процедурой управления несоответствиями.

5) Оборудование поставщиков/подрядчиков

Охранное оборудование, используемое подрядчиками, должно быть подвергнуто такому же контролю, как и внутреннее оборудование. Подрядчики должны предоставить гарантии того, что их оборудование соответствует этим требованиям. Перед началом работы поставщик должен предоставить копию своей записи испытаний и технического обслуживания оборудования для идентифицированного критического оборудования. Если какие-либо задачи требуют специальной подготовки, соответствующая запись должна быть предоставлена заказчику для ознакомления.

6) Статистические или другие теоретические аналитические методы

Статистическая или другая теоретическая аналитическая методика, используемая для оценки ситуации, связанной с безопасностью, для расследования инцидента безопасности, сбоя или для оказания помощи в принятии решений в отношении безопасности, должна быть основана на заслуживающих доверие научных принципах. Высшее руководство должно обеспечить выявление необходимости в таких методах. Руководящие принципы их использования должны быть задокументированы с указанием обстоятельств, при которых они уместны.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- процедуру наблюдения за эффективностью мер безопасности;
- графики инспекций и контрольные списки (чек-листы);
- контрольные списки (чек-листы) проверки оборудования;
- списки охранного оборудования;
- калибровочные устройства и записи по калибровке/поверке;
- ремонтные работы и их результаты;
- заполненные контрольные списки, отчеты об инспекциях (о результатах аудита системы менеджмента безопасности см. 4.5.4);
- отчеты о несоответствии;
- подтверждение результатов внедрения данной процедуры.

4.5.2 Оценка системы

a) Требования ИСО 28000

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.

b) Намерения

Организация должна иметь результативную процедуру для рассмотрения и оценки планов управления, процедур и возможностей своей организации в соответствии с ее политикой, целями, целевыми показателями. Организация также должна периодически пересматривать их соответствие применимым нормативно-законодательным требованиям.

Основная цель этих процедур — это обеспечение актуальности планов и процедур безопасности и их соответствия изменяющимся требованиям и потребностям. Эти изменения должны быть своевременными и в полной мере учитывать любые изменения в правилах цепи поставок, передовой практике и извлеченных уроках.

c) Типовые входные данные

Типовые входные данные должны включать:

- отчеты об инцидентах;
- результаты планирования инцидентов, готовности к ним и проведение учений;
- идентификацию угроз, оценку риска и отчеты по управлению риском;
- отчеты аудита системы менеджмента безопасности, включая отчеты о несоответствии;
- отчеты об инцидентах и/или опасностях;
- отчеты и действия по анализу со стороны руководства (см. 4.6);
- прогресс в достижении целей;
- изменение нормативных требований;
- коррекция ожиданий заинтересованных сторон и других вовлеченных лиц;
- изменения в объеме работ, деятельности и клиентской базе организации.

d) Процесс

Руководству организации следует через определенные промежутки времени проводить анализ своей системы менеджмента безопасности для того, чтобы установить и обеспечить ее постоянную

пригодность и эффективность. Интервалы должны быть достаточно короткими, чтобы можно было выявить отказы системы до того, как возникнут косвенные повреждения.

Результатом внедрения системы безопасности, достижения целей, установленных в политике, является постоянное улучшение — это один из основных принципов ИСО 28000. Процесс и процедуры согласно 4.5.2 должны способствовать достижению поставленных целей.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты и результаты включают в себя:

- улучшенные процессы и производительность;
- сокращение фактов несоответствий;
- соблюдение правовых норм;
- обновленные отчеты об идентификации угроз, оценке рисков и реестры рисков;
- улучшенные процессы;
- доказательства оценки результативности предпринятых корректирующих и предупреждающих действий.

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

a) Требования ИСО 28000

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

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

b) расследований, связанных с безопасностью:

1) действия в ситуации сбоев, в том числе при «почти ошибках» и ложных срабатываниях;

2) действия при возникновении инцидентов и чрезвычайных ситуаций;

3) при возникновении несоответствий;

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

d) инициирование и завершение корректирующих действий;

e) подтверждение эффективности предпринятых корректирующих действий.

Эти процедуры должны 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.

b) Намерения

Организация должна обладать результативной процедурой для сообщения и оценки и/или расследования чрезвычайных ситуаций, инцидентов безопасности и несоответствий. Основная цель процедуры состоит в том, чтобы предотвратить дальнейшее возникновение ситуации путем выявления и устранения ключевой причины. Кроме того, процедура должна позволять обнаруживать, анализировать и устранять потенциальные причины несоответствий, в том числе возникающие в результате сбоев, человеческих ошибок, сбоев системы, процесса или оборудования.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- общую процедуру;
- чрезвычайные действия в чрезвычайной ситуации;
- идентификацию угроз безопасности, оценку рисков и управление рисками;
- отчеты аудита системы менеджмента безопасности, включая отчеты о несоответствии;

- отчеты об инцидентах безопасности и угрозах безопасности;
- отчеты о техническом обслуживании и поверке/калибровке охранного оборудования.

d) Процесс

Организация должна разработать документированную процедуру, чтобы обеспечить расследование инцидента безопасности и несоответствия и инициировать корректирующие и/или предупреждающие действия. Необходимо следить за прогрессом при выполнении корректирующих и предупреждающих действий и оценить результативность таких действий.

1) Процедуры

Процедура должна включать рассмотрение следующих пунктов:

i) общее

При исполнении процедуры следует:

- определять обязанности и полномочия лиц, вовлеченных в реализацию, отчетность, расследование, последующие действия и мониторинг корректирующих и предупреждающих действий;
- требовать, чтобы осуществлялось информирование обо всех несоответствиях, инцидентах безопасности и угрозах безопасности;
- привлекать весь персонал (сотрудников, временных работников, персонал, подрядчиков, посетителей и всех других лиц, участвующих в цепи поставок);
- учитывать влияние на заинтересованные стороны;
- обеспечивать отсутствие критики в адрес сотрудника, сообщившего об инциденте безопасности;
- четко определять порядок действий, которые необходимо предпринять после несоответствий, выявленных в системе управления безопасностью;

ii) незамедлительные действия

При обнаружении несоответствий, инцидентов безопасности или угрозы необходимо немедленно принять меры для исправления инцидента безопасности. Процедура должна отразить порядок того, как:

- определять процесс уведомления;
- где это уместно, включать координацию планов и процедур действий в чрезвычайных ситуациях;
- определять масштабы расследования в отношении потенциальной или реальной угрозы (например, оповестить руководство о серьезных инцидентах безопасности);

iii) записи

Следует использовать соответствующие средства для записи фактической информации и результатов немедленного расследования и последующего подробного расследования. Организация должна обеспечить соблюдение процедур:

- для записи сведений о несоответствии, инциденте безопасности или угрозах безопасности;
- определения места хранения записей и ответственности за хранение;

iv) расследование

Процедура должна определять, каким образом следует проводить процесс расследования:

- тип событий, подлежащих расследованию (например, инциденты, которые могли бы привести к серьезной угрозе);
- цели расследования;
- кто должен проводить расследование, полномочия лиц, привлекаемых к расследованию, требуемая квалификация (включая, при необходимости, руководителя среднего звена);
- корневую причину несоответствия;
- проведение опросов свидетелей;
- решение практических вопросов, таких как наличие камер и хранение доказательств;
- механизмы отчетности о расследовании, включая отчетность перед заинтересованными сторонами.

Персонал, проводящий расследование, должен начать предварительный анализ фактов во время сбора информации по расследованию. Сбор и анализ данных должны продолжаться до тех пор, пока не будет получено адекватное и достаточно полное объяснение;

v) корректирующие действия

Корректирующие действия — это действия, предпринимаемые для выявления корневой причины несоответствий и инцидентов безопасности и для принятия мер с целью предотвращения их повторения. Примеры элементов, которые следует учитывать при создании и поддержании процедуры корректирующих действий, включают:

- выявление и реализация корректирующих и предупреждающих мер как на краткосрочную, так и на долгосрочную перспективу (это может также включать использование соответствующего источника информации, такого как рекомендации опытных сотрудников в области безопасности);

- оценку любого воздействия на результаты идентификации угроз и оценки рисков, необходимость обновления отчета об идентификации угроз, оценки рисков и менеджмента риска;

- запись необходимых изменений, вносимых в процедуру по результатам корректирующих действий или идентификации угроз, оценки рисков и управления рисками;

- применение системы менеджмента риска или изменение существующего менеджмента риска для того, чтобы обеспечить реализацию корректирующих действий и оценить их результативность;

vi) предупреждающие действия

Предупреждающие действия — это действия, предпринимаемые для предотвращения возможных нарушений безопасности.

Примеры элементов, которые следует учитывать при установлении и поддержании процедуры предупреждающих действий, включают:

- использование внушающего доверие источника информации, таких как результаты корректирующих действий, тенденции/тренды инцидентов безопасности, отчеты по аудиту системы менеджмента безопасности, обновленная оценка рисков, новая информация о безопасности, консультирование сотрудников и заинтересованных сторон, экспертиза безопасности и т. д.;

- инициирование и осуществление предупреждающих действий и применение мероприятий по управлению для обеспечения их результативности;

- регистрацию любых изменений в процедурах, возникающих в результате предупреждающих действий, и представление их на утверждение;

vii) последующие действия

Предпринятые корректирующие или предупреждающие действия должны быть максимально результативными. Следует оценивать результативность предпринятых корректирующих/предупреждающих действий. О нерешенных/потерявших актуальность действиях следует сообщать высшему руководству при первой возможности.

2) Анализ несоответствий и инцидентов, связанных с безопасностью

Причины несоответствий и инцидентов, связанных с безопасностью, следует систематизировать и анализировать на регулярной основе для выполнения анализа корневых причин. Частота и сложность анализа должны быть продемонстрированы другим заинтересованным сторонам.

В категоризацию и анализ должны быть включены:

- частота или сложность инцидентов по безопасности;

- местонахождение, деятельность, представительство, день, время суток (в зависимости от того, что подходит);

- тип и степень или влияние на объекты, цепь поставок и т. д.;

- случайные и корневые причины.

Инциденту безопасности следует уделять должное внимание. Все инциденты по безопасности могут быть показателем угрозы безопасности или уязвимости.

Должны быть сформированы обоснованные выводы и предприняты корректирующие действия. Этот анализ должен быть представлен высшему руководству и включен в анализ со стороны руководства (см. 4.6).

3) Мониторинг и информирование о результатах

Следует оценивать эффективность расследований и отчетность по вопросам безопасности. Оценка должна быть объективной и, по возможности, сопровождаться количественным результатом.

Организация, извлекая уроки из расследования, должна:

- выявить корневые причины недостатков, выявленных в системе менеджмента безопасности и общем управлении организацией, где это применимо;

- сообщить выводы и рекомендации руководству и заинтересованным сторонам (см.4.4.3);

- включить соответствующие выводы и рекомендации расследований в непрерывный процесс анализа безопасности;

- следить за своевременным внедрением корректирующих действий и их последующей оценки результативности с течением времени;

- применять уроки, извлеченные из расследования несоответствий и инцидентов безопасности, во всей своей организации, цепи поставок, которой она управляет и на которую оказывает влияние.

Нужно сосредоточиться на общих принципах, а не на конкретных действиях, призванных избежать повторения аналогичного события в одной и той же области организации.

4) Сохранность записей

Обеспечение сохранности записей может быть достигнуто быстро и с минимальным формальным планированием или может быть более сложной деятельностью в долгосрочной перспективе. Эта документация должна соответствовать уровню корректирующих действий.

Отчеты и предложения следует отправлять представителю высшего руководства для их анализа и хранения (см. 4.5.4).

Организация должна вести записи инцидентов безопасности, так как они могут потребоваться тем, кто управляет цепью поставок.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- инциденты безопасности и процедуры несоответствия;
- отчеты о несоответствии;
- реестр несоответствий;
- отчеты о расследованиях;
- обновленные отчеты по выявлению рисков безопасности, оценке рисков и управлению рисками;
- анализ входных данных со стороны руководства;
- доказательства оценки результативности предпринятых корректирующих и предупреждающих действий.

4.5.4 Управление записями

a) Требования ИСО 28000

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.

b) Намерения

Записи следует хранить для того, чтобы продемонстрировать, что система менеджмента безопасности работает результативно. Записи по безопасности, которые поддерживают систему менеджмента и ее соответствие требованиям, должны быть подготовлены, поддерживаться в рабочем состоянии, быть разборчивыми и надлежащим образом идентифицированными.

c) Типовые входные данные

Записи, используемые для демонстрации соответствия требованиям, которые должны храниться, включают в себя следующие пункты:

- записи об обучении и компетенции;
- отчеты об инспекциях по безопасности;
- несоответствия в области безопасности;
- результаты предупреждающих и корректирующих действий;
- отчеты по аудиту системы менеджмента безопасности;
- протоколы собраний по безопасности;
- протоколы занятий/учений по безопасности;
- анализ со стороны руководства;
- записи идентификации угроз безопасности, оценки рисков и менеджмента риска.

d) Процесс

Очевидность требования ИСО 28000 достаточно обоснованна. Тем не менее дополнительное внимание должно быть уделено следующим пунктам:

- полномочиям на удаление записей по безопасности;
- конфиденциальности (защитная маркировка) записи по безопасности;

- правовым и иным требованиям к хранению записи в журнале;
- вопросам, связанным с использованием электронных записей.

Записи по безопасности должны быть полностью заполнены, разборчивы и надлежащим образом идентифицированы. Должно быть определено время хранения записей по безопасности. Записи следует хранить в безопасном месте, они должны быть легкодоступны и защищены от порчи. Наиболее важные записи безопасности должны быть защищены от возможного пожара и других повреждений, в зависимости от ситуации и в соответствии с требованиями действующего законодательства.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- процедуру идентификации, ведения и распоряжения записями по безопасности;
- хранение надлежащим образом, обеспечивающее комфортное извлечение записей по безопасности.

4.5.5 Аудит

a) Требования ИСО 28000

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.

b) Намерения

Внутренние аудиты системы менеджмента безопасности организации следует проводить через запланированные промежутки времени для предоставления руководству информации о том, соответствует ли система требованиям процедур и требованиям раздела 4 ИСО 28000:2007 и разработана ли, внедрена ли и поддерживается ли система в рабочем состоянии. Аудиты также можно проводить для определения возможностей улучшения системы менеджмента безопасности организации. В целом аудиты системы менеджмента безопасности должны учитывать политику безопасности, процедуры, а также условия и практики, применимые к цепи поставок.

Следует создать программу внутреннего аудита системы менеджмента безопасности для обеспечения возможности организации по анализу соответствия своей системы менеджмента безопасности требованиям ИСО 28000 и другим требованиям, определенным в рамках проведения ее операций. Плановые аудиты системы менеджмента безопасности должны проводиться персоналом организации и/или внешним персоналом, выбранным организацией, для установления степени соответствия документированным процедурам безопасности и оценке результативности системы в достижении целей безопасности организации. Персонал, проводящий аудит системы менеджмента безопасности, должен иметь возможность дать беспристрастную и объективную оценку.

Примечание — Внутренний аудит системы менеджмента безопасности фокусируется на результатах деятельности системы менеджмента безопасности. Аудит не следует путать с инспекцией по безопасности, анализом, оценками или другими проверками безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- заявление о политике безопасности;
- цели безопасности;
- процедуры безопасности и инструкции;
- идентификацию угроз безопасности, оценку рисков и управление рисками;
- требования действующего законодательства и лучшие практики (если применимо);
- отчеты о несоответствии;
- процедуру аудита системы менеджмента безопасности;
- участие компетентного(ых), независимого(ых), внутреннего(их)/внешнего(их) аудитора(ов);
- процедуру управления несоответствиями;
- занятия и учения по безопасности;
- информацию, полученную от внешних организаций, об угрозах безопасности.

d) Процесс

1) Аудиты

Аудиты системы менеджмента безопасности обеспечивают всестороннюю и формализованную оценку соответствия организации процедурам и практикам безопасности.

Аудит системы менеджмента безопасности следует проводить в соответствии с запланированными мероприятиями. Дополнительные аудиты должны проводиться в зависимости от обстоятельств, например: после инцидента, который влияет на систему безопасности, изменения в организации, средствах или объеме цепи поставок.

Аудит системы менеджмента безопасности проводится исключительно компетентным, независимым персоналом с соответствующим разрешением по безопасности для проверяемых областей.

Результаты аудита системы менеджмента безопасности должны включать подробные оценки результативности процедур безопасности, уровня соответствия процедурам и, при необходимости, определять корректирующие действия. Результаты аудитов системы менеджмента безопасности должны быть оформлены как записи и своевременно сообщены руководству.

Примечание — Общие принципы и методология, описанные в ИСО 19011, подходят для аудита системы менеджмента безопасности.

2) Планирование

Должен быть подготовлен план, как правило, на ежегодной основе, который предусматривает проведение внутренних аудитов менеджмента безопасности. Аудит менеджмента безопасности должен охватывать всю деятельность, входящую в область распространения системы менеджмента безопасности, и оценивать ее соответствие требованиям ИСО 28000.

Периодичность и область аудитов системы менеджмента безопасности должны быть связаны с рисками, характерными для различных элементов системы менеджмента безопасности, фактическими данными о результатах деятельности системы менеджмента безопасности, результатами анализа со стороны руководства и той степенью, в которой управление безопасностью системы менеджмента безопасности или среда, в которой она работает, могут быть изменены.

Дополнительные, внеплановые аудиты системы менеджмента безопасности должны проводиться в том случае, если возникают ситуации, которые оправдывают цель их проведения, например после инцидента с безопасностью.

3) Поддержка со стороны руководства

Для того чтобы аудит системы менеджмента безопасности приносил добавочную стоимость, необходимо, чтобы высшее руководство полностью поддерживало концепции аудита и его результативное внедрение в организации. Высшее руководство должно учитывать выводы и рекомендации аудиторов и предпринимать, по мере необходимости, соответствующие действия в надлежащие сроки. Как только принято решение, что должен быть выполнен аудит системы менеджмента безопасности, он должен быть проведен беспристрастным способом. Весь персонал должен быть проинформирован о целях аудита и его преимуществах. Следует поощрять персонал к открытому сотрудничеству с аудиторами и достоверным и конструктивным ответам на их вопросы.

4) Аудиторы

Один или несколько человек могут проводить аудит системы менеджмента безопасности. Групповой подход может расширить вовлеченность и улучшить сотрудничество. Групповой подход также позволяет использовать более широкий спектр специальных навыков и знаний.

Аудиторы должны быть независимыми от части организации или от деятельности, подлежащей аудиту, и при необходимости должны быть проверены на безопасность для аудируемых областей.

Аудиторы должны понимать свою задачу и быть компетентными в ее выполнении. Они должны иметь опыт и знания соответствующих стандартов, кодексов практики и систем, которые они проверяют для того, чтобы они смогли оценить эффективность деятельности организации и выявить ее недостатки. Аудиторы должны быть знакомы с требованиями, изложенными в действующем законодательстве. Кроме того, аудиторы должны знать и иметь доступ к стандартам и руководящим указаниям, относящимся к работе, которой они занимаются.

5) Сбор и интерпретация данных

Методы и средства, используемые при сборе информации, будут зависеть от характера проводимого аудита системы менеджмента безопасности. Аудит системы менеджмента безопасности должен гарантировать, что в ходе аудита использована репрезентативная выборка основных видов деятельности и опрос полномочного персонала (в том числе и представителей службы безопасности сотрудников). Соответствующая документация должна быть изучена. Это может включать следующую документацию:

- документация системы менеджмента безопасности;
- заявление о политике безопасности;
- цели безопасности;
- результаты занятий и учений безопасности;
- процедуры;
- протоколы совещаний по безопасности;
- сообщения или информирование от правоохранительных органов или других регулирующих органов (устные, письма, уведомления и т. д.);
- уставные документы и сертификаты;
- записи по обучению;
- предыдущие отчеты по аудитам системы менеджмента безопасности;
- запросы на корректирующие действия;
- отчеты о несоответствии.

По возможности проверки должны быть встроены в процедуру аудита системы менеджмента безопасности для того, чтобы помочь избежать неправильного толкования или неправильного использования собранных данных, информации или других записей.

6) Результаты аудита

Содержание окончательного отчета об аудите системы менеджмента безопасности должно быть четким, точным и полным. Оно должно быть датировано и подписано аудитором.

Отчет должен, в зависимости от ситуации, содержать следующие элементы:

- цели и задачи аудита системы менеджмента безопасности;
- сведения о плане аудита системы менеджмента безопасности, определение членов аудиторской группы и проверяемых представителях, даты проведения аудита и определение областей, подлежащих аудиту;
- идентификация справочных документов, используемых для проведения аудита системы управления безопасностью (например, ИСО 28000, руководство по менеджменту безопасности);
- подробности выявленных несоответствий;
- аудиторскую оценку степени соответствия ИСО 28000;
- способность системы менеджмента безопасности достигать заявленных целей в области безопасности;
- распространение итогового отчета по аудиту системы менеджмента безопасности.

По результатам аудитов системы менеджмента безопасности должны быть незамедлительно предприняты корректирующие действия. Следует разработать план согласованных действий по исправлению положения с указанием ответственных лиц, дат завершения и требований по отчетности. Для обеспечения удовлетворительного выполнения рекомендаций должны быть созданы механизмы последующего мониторинга.

Анализ результатов и результативности корректирующих действий должен проводиться руководством (при необходимости).

Последующие (внеплановые) аудиты должны проводиться для проверки результативности реализации корректирующих действий.

Конфиденциальность сведений следует учитывать при регистрации и записи информации, содержащейся в отчетах аудита системы менеджмента безопасности.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- план/программу аудита системы менеджмента безопасности;
- процедуру аудита системы менеджмента безопасности;
- отчет об аудите системы менеджмента безопасности, включая отчеты о несоответствиях, рекомендации и запросы на корректирующие действия;
- подписанные/закрытые отчеты о несоответствии;
- подтверждение отчетности руководству о результатах аудитов системы менеджмента безопасности.

4.6 Анализ со стороны руководства и постоянное улучшение

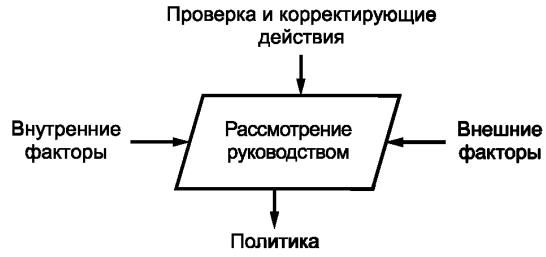


Рисунок 6 — Анализ со стороны руководства

a) Требования ИСО 28000

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.

b) Намерения

Высшее руководство должно анализировать работу системы менеджмента безопасности для того, чтобы оценить, полностью ли она реализована и остается ли она соответствующей результативной для достижения заявленной политики организации и целей безопасности. В анализе со стороны руководств следует рассмотреть вопрос о том, является ли политика безопасности приемлемой. Анализ должен установить новые или обновленные цели безопасности, соответствующие будущему периоду, для демонстрации постоянного улучшения, и рассмотреть необходимость внесения изменений в определенные элементы системы менеджмента безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя следующие позиции:

- результаты внутреннего и внешнего аудита системы менеджмента безопасности;
- корректирующие действия, выполняемые в системе со времени предыдущего анализа;
- протоколы занятий и учений по безопасности;
- отчет представителя высшего руководства об общих результатах деятельности и системы в целом;
- отчеты других организаций и заинтересованных сторон о результативности системы, так как она влияет на цепь поставок;
- отчеты о процессах идентификации угроз, оценки рисков и управлении рисками;
- эффективность программ обучения и повышения осведомленности;
- прогресс и результативность целей менеджмента безопасности.

d) Процесс

Процесс анализа со стороны руководства, как правило, включает в себя совещание, проводимое высшим руководством на регулярной основе, например ежегодно. Анализ должен быть сосредоточен на общих результатах деятельности системы менеджмента безопасности, а не на конкретных деталях, поскольку они должны обрабатываться обычными средствами в системе менеджмента безопасности.

При планировании анализа со стороны руководства следует учитывать следующее:

- темы для обсуждения;
- перечень присутствующих (руководители, специалисты по безопасности, другой персонал);
- обязанности отдельных участников в отношении анализа; информация, которая будет представлена на рассмотрение.

В анализе должны быть рассмотрены следующие темы:

- пригодность действующей политики безопасности;
- установление или обновление целей безопасности для постоянного улучшения в предстоящий период;
- адекватность текущих процессов идентификации угроз, оценки рисков и менеджмента риска;
- текущий уровень риска и эффективность существующих мероприятий по управлению;
- адекватность источника ресурсов;
- эффективность процесса инспекций безопасности;
- эффективность процесса отчетности по рискам безопасности;
- данные, относящиеся к безопасности и происшествиям;
- записи о том, что конкретные процедуры нерезультативны;
- результаты внутренних и внешних аудитов системы менеджмента безопасности, проведенных после предыдущего анализа со стороны руководства, и их результативность;
- состояние готовности к чрезвычайным ситуациям и мероприятиям по обеспечению безопасности;
- усовершенствование системы менеджмента безопасности;
- результаты любых расследований инцидентов по безопасности;
- оценка последствий прогнозируемых изменений в законодательстве, нормативных актах, технологиях и информации в области безопасности.

Высшее руководство должно гарантировать, что общие результаты деятельности системы менеджмента безопасности сообщаются на совещании по анализу со стороны руководства. Отдельные проверки результативности системы менеджмента безопасности следует проводить с более частыми интервалами, если это необходимо.

Анализ со стороны руководства может включать анализ интегрированной системы менеджмента, поэтому результаты анализа безопасности, качества и других элементов системы управления могут рассматриваться на одном и том же совещании или в ходе одного и того же процесса. Если этот подход

будет принят, он не должен умалять важность любой из составных частей интегрированной системы менеджмента организации.

e) Типовые выходные данные/результаты

Типовые выходные данные/результаты включают в себя следующие позиции:

- протоколы любых собраний по анализу со стороны руководства;
- пересмотр политики и целей по безопасности;
- конкретные корректирующие действия для отдельных менеджеров с целевыми показателями и датами завершения;
- конкретные действия по улучшению с назначенными обязанностями и целевыми показателями для завершения;
- даты анализа корректирующих действий;
- области, на которые следует обратить внимание при планировании будущих внутренних аудитов системы менеджмента безопасности.

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	5.1
				Политика в области качества	5.3
				Непрерывное улучшение	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	5.2
				Определение требований, относящихся к продукции	7.2.1
				Анализ требований, относящийся к продукции	7.2.2
Нормативно-законодательные и другие требования по безопасности	4.3.2	Законодательные и прочие требования	4.3.2	Ориентация на потребителя	5.2
				Определение требований, относящихся к продукции	7.2.1
Цели в области менеджмента безопасности	4.3.3	Цели, задачи и программа(ы)	4.3.3	Цели в области качества	5.4.1
				Планирование в рамках системы менеджмента качества	5.4.2
				Непрерывное улучшение	8.5.1
Целевые показатели в области менеджмента безопасности	4.3.4	Цели, задачи и программа(ы)	4.3.3	Цели в области качества	5.4.1
				Планирование в рамках системы менеджмента качества	5.4.2
				Непрерывное улучшение	8.5.1
Программы менеджмента безопасности	4.3.5	Цели, задачи и программа(ы)	4.3.3	Цели в области качества	5.4.1
				Планирование в рамках системы менеджмента качества	5.4.2
				Непрерывное улучшение	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
Документация	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	7.6
				Общие положения (Измерение, анализ и улучшение)	8.1
				Мониторинг и измерение процессов	8.2.3
				Мониторинг и измерение продукции	8.2.4
				Анализ данных	8.4
Оценка системы	4.5.2	Оценка соответствия	4.5.2	Мониторинг и измерение процессов	8.2.3
				Мониторинг и измерение продукции	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	8.3
				Анализ данных	8.4
				Корректирующие действия	8.5.2
				Предупреждающие действия	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	5.1
				Анализ со стороны руководства	5.6
				Общие положения	5.6.1
				Входные данные анализа	5.6.2
				Выходные данные анализа	5.6.3
				Непрерывное улучшение	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 по использованию)

[3] ISO 17021:2006 Conformity assessment — Requirements for bodies providing audit and certification of management systems (Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента)

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

[5] ISO 28000:2007 Specification for security management systems for the supply chain
(Спецификация на системы менеджмента безопасности цепи поставок)

УДК 656.614.3.004:006:354 ОКС 03.100.01 IDT

Ключевые слова: система менеджмента, безопасность, цепь поставок, руководство по внедрению

БЗ 2—2020/40

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 27.02.2020. Подписано в печать 05.03.2020. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 4,74.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru