ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53661— 2009 (ИСО 28004:2006)

СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководство по внедрению

ISO 28004:2006
Security management systems for the supply chain — Guidelines for the implementation of ISO/PAS 28000 (MOD)

Издание официальное

БЗ 7—2009/344

Москва
Стандартинформ
2010

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Служба морской безопасности» (ФГУ СМБ) на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 1026-ст

4 Настоящий стандарт является модифицированным международному стандарту ИСО 28004:2006 «Системы менеджмента безопасности сети поставок. Руководство по внедрению ISO/PAS 28000» (ISO 28004:2006 «Security management systems for the supply chain — Guidelines for the implementation of ISO/PAS 28000») путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения его в соответствие с ГОСТ Р 1.5 (пункт 3.5).

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

© Стандартинформ, 2010

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 и определения 2
4 Элементы системы менеджмента безопасности 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 Проверка и корректирующие действия 25
4.6 Анализ со стороны руководства и постоянное улучшение 37
Приложение А (справочное) Соответствие структуры настоящего стандарта со структурой ГОСТ Р ИСО 14001—2007 и ГОСТ Р ИСО 9001—2008 39
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 42
Библиография 42

Введение

ГОСТ Р 53663—2009 «Система менеджмента безопасности цепи поставок. Требования» и настоящий стандарт подготовлены в связи с возникшей потребностью в наличии унифицированного стандарта системы менеджмента в области безопасности цепи поставок и руководства по внедрению такой системы менеджмента безопасности на предприятиях с тем, чтобы получить возможность проводить оценку соответствия и сертификацию таких систем менеджмента.

ГОСТ Р 53663—2009 согласован со стандартами ГОСТ Р ИСО 9001—2008 (система менеджмента качества) и ГОСТ Р ИСО 14001—2007 (система экологического менеджмента), что позволяет организации согласовать или интегрировать свою собственную систему менеджмента в системы менеджмента качества, экологии и безопасности цепи поставок.

В начале каждого раздела настоящего стандарта отдельным блоком приведены требования ГОСТ Р 53663—2009, за которыми следуют соответствующие им рекомендации. Нумерация разделов настоящего стандарта совпадает с нумерацией ГОСТ Р 53663—2009.

Соответствие настоящему стандарту не освобождает от последующего выполнения положений *законодательных и иных нормативных правовых актов в области обеспечения безопасности.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководство по внедрению

Security management system for the supply chain. Guidelines for the implementation

Дата введения — 2010—07—01

1 Область применения

Настоящий стандарт содержит основные положения и рекомендации по внедрению *ГОСТ Р 53663*.

В настоящем стандарте отражены основные принципы, рассматривающие намерения, типовые входные данные, процессы и типовые выходные данные по каждому разделу *ГОСТ Р 53663*. Это способствует лучшему пониманию и внедрению *ГОСТ Р 53663*.

Настоящий стандарт не содержит дополнительные требования к уже установленным в *ГОСТ Р 53663* и не предписывает обязательные к выполнению требования ИСО 28000.

1 Область применения

Данный стандарт устанавливает требования к системам менеджмента безопасности, охватывая важные аспекты обеспечения безопасности цепи поставок. Эти аспекты включают в себя, но не ограничиваются вопросами финансирования, производства, управления информированием, а также средствами упаковки, хранения и передачи товаров между различными видами транспорта и местами нахождения. Менеджмент безопасности связан со многими другими аспектами бизнеса-менеджмента. Эти другие аспекты нужно рассматривать непосредственно там и тогда, где и когда они оказывают влияние на менеджмент безопасности, включая передачу товаров по всей цепи поставок.

Эти требования применимы ко всем организациям (от малых до многонациональных), занятых в производстве, обслуживании, хранении или транспортировке, на любом этапе производства или цепи поставок, которые желают:

a) разрабатывать, внедрять, поддерживать в рабочем состоянии и улучшать систему менеджмента безопасности,

b) обеспечивать соответствие с утвержденной политикой в области менеджмента безопасности,

e) демонстрировать такое соответствие другим организациям;

d) получать подтверждение соответствия своей системы менеджмента безопасности у аккредитованного органа по сертификации;

e) самостоятельно определять и декларировать соответствие настоящему стандарту.

Организации, которые в дальнейшем выбирают подтверждение соответствия у аккредитованного органа по сертификации, могут продемонстрировать, что они значительно способствуют обеспечению безопасности цепи поставок.

[ГОСТ Р 53663—2009]

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО 9001—2008 Системы менеджмента качества. Требования

ГОСТ Р ИСО 14001—2007 Системы экологического менеджмента. Требования и руководство по применению

ГОСТ Р ИСО 19011—2003 Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента

Примечание — *При пользовании настоящим стандартом целесообразно проверить действия ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.*

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **средство** (facility): Предназначенный для выполнения определенной функции или оказания услуги технологический комплекс в том числе предприятие, обеспечивающее его функционирование, здание, сооружение, устройство или оборудование, а также транспортное средство.

Примечание — Данное определение включает в себя любой код программного обеспечения, являющийся ключевым для обеспечения безопасности и применения менеджмента безопасности.

3.2 **безопасность** (security): Сопротивление преднамеренному акту незаконного вмешательства, рассчитанному на нанесение вреда или ущерба цепи поставок или посредством цепи поставок.

3.3 **менеджмент безопасности** (security management): Систематизированные и скоординированные действия и методы, с помощью которых организация оптимально управляет своими рисками и связанными с ними потенциальными угрозами и воздействиями.

3.4 **цель в области менеджмента безопасности** (security management objective): Требуемый в интересах безопасности определенный результат или достижение, удовлетворяющее политику в области менеджмента безопасности.

Примечание — Важно, чтобы такие результаты были прямо или косвенно связаны с обеспечением продукции, поставок или услуг, предоставляемых всем бизнесом его клиентам или конечным пользователям.

3.5 **политика в области менеджмента безопасности** (security management policy): Совокупность намерений и стремлений организации в отношении безопасности, а также структура управления процессами и деятельностью в области безопасности, которые соответствуют политике организации и нормативным требованиям.

3.6 **программы в области менеджмента безопасности** (security management programmes): Методы, с помощью которых достигаются цели в области менеджмента безопасности.

3.7 **задача в области менеджмента безопасности** (security management target): Специальный уровень эксплуатации, который требуется для достижения цели в области менеджмента безопасности.

3.8 **заинтересованное лицо** (stakeholder): Физическое или юридическое лицо, заинтересованное в исполнении организацией своих функций, достижении успеха или влияющее на ее деятельность.

Примечание — Примерами таких лиц являются клиенты, акционеры, финансисты, страховщики, инспекторы, органы, учрежденные в соответствии с уставом, персонал, подрядчики, поставщики, общественные организации.

3.9 **цепь поставок** (supply chain): Взаимосвязанный набор ресурсов и процессов, начинающийся с получения сырья и простирающийся через доставку продукции или услуг конечному пользователю посредством транспортных систем.

Примечание — Цепь поставок может включать в себя продавцов, промышленные предприятия, логистические центры, внутренние центры распределения, дистрибьюторов, оптовых продавцов и других юридических лиц, ведущих 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 ограничиваясь 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 ограничиваясь этим.

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.

3.10 **постоянное улучшение** (continual improvement): Периодически повторяющийся процесс усиления системы менеджмента безопасности для усовершенствования всей работы в отношении безопасности, соответствующей политике организации в этой области.

[ГОСТ Р 53663—2009]

3.11 **риск** (risk): Вероятность реализации акта незаконного вмешательства и его последствия.

3.12 **проверка на допуск** (security cleared): Процесс проверки надежности людей, которые получат доступ к конфиденциальным материалам по вопросам безопасности.

3.13 **угроза** (threat): Любое возможное преднамеренное действие или ряд действий разрушающего характера в отношении каких-либо заинтересованных сторон, средств, операций, цепей поставок, общества, экономической устойчивости, целостности бизнеса и хозяйственной деятельности.

4 Элементы системы менеджмента безопасности

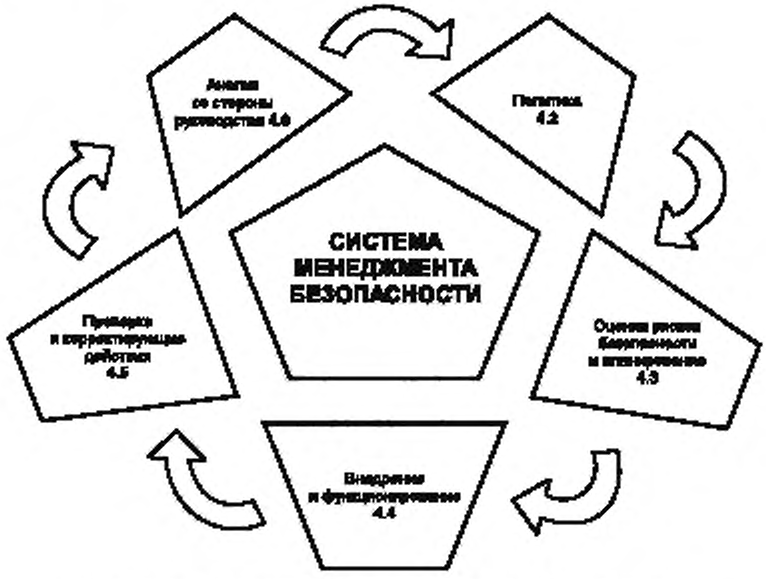

Рисунок 1 — Элементы успешного менеджмента безопасности

4.1 Общие требования

a) Требования

Организация должна разрабатывать, документировать, внедрять, поддерживать в рабочем состоянии и постоянно улучшать результативность системы менеджмента безопасности с тем, чтобы идентифицировать риски в области безопасности, управлять ими, а также смягчать их последствия.

Организация должна постоянно улучшать эффективность своей деятельности в соответствии с требованиями, изложенными в разделе 4.

Организация должна определить область применения своей системы менеджмента безопасности. Если организация принимает решение о передаче сторонней организации какого-либо процесса, влияющего на соответствие требованиям данного стандарта, она должна обеспечить со своей стороны контроль за таким процессом. Необходимые рычаги управления и ответственность за выполнение таких процессов должны быть определены в рамках системы менеджмента безопасности.

[ГОСТ Р 53663—2009]

b) Намерение

Организация должна разрабатывать и поддерживать в рабочем состоянии систему менеджмента, которая соответствует требованиям *ГОСТ Р 53663*. Это позволяет организации соблюдать законодательные и иные нормативные правовые акты в области обеспечения безопасности и охраны.

Уровень детализации и сложность системы менеджмента безопасности, а также объемы документации и используемых ресурсов зависят от размера и структуры организации и специфики ее деятельности.

Организация обладает свободой и гибкостью в определении области применения *ГОСТ Р 53663* и может избрать внедрение стандарта как применительно ко всей организации в целом, так и к отдельным структурным подразделениям или определенным услугам, предоставляемым организацией.

При определении области применения и масштаба системы менеджмента безопасности необходимо соблюдать осторожность. Организациям не следует пытаться ограничивать область применения таким образом, чтобы исключать из оценки структурные подразделения или услуги, деятельность которых необходима для общего функционирования организации в целом, а также исключать те аспекты, которые могут напрямую влиять на обеспечение безопасности персонала и других заинтересованных сторон.

При внедрении *ГОСТ Р 53663* в отдельном структурном подразделении или для определенной услуги, предоставляемой организацией, могут быть использованы существующие в организации политика и процедуры в области обеспечения безопасности, разработанные для иных подразделений. Эти политика и процедуры потребуют пересмотра и внесения соответствующих изменений, учитывающих специфику функционирования такого структурного подразделения или особенности предоставляемой услуги.

c) Типовые входные данные

Все требования по входным данным определены в *ГОСТ Р 53663*.

d) Типовые выходные данные

Типовым выходным данным является эффективно внедренная и поддерживаемая в рабочем состоянии система менеджмента безопасности, которая помогает организации в постоянном стремлении к улучшению.

4.2 Политика в области менеджмента безопасности

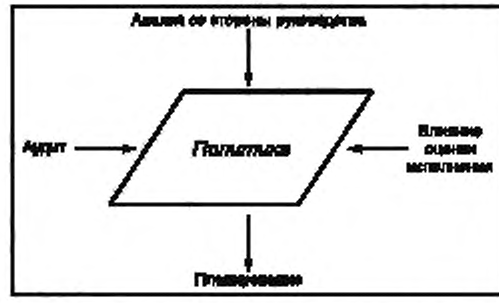

Рисунок 2 — Политика в области менеджмента безопасности

a) Требования

Высшее руководство организации должно официально определять общую политику в области менеджмента безопасности. Эта политика должна:

a) быть согласованна с политикой организации в других областях;

b) предусматривать структуру, которая позволяет достигать цели и выполнять задачи и программы, специфичные для менеджмента безопасности;

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

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

e) четко определять все или основные цели в области менеджмента безопасности;

f) включать в себя обязательство постоянного улучшения процесса менеджмента безопасности;

g) включать в себя обязательство соответствовать законодательным, нормативным и уставным требованиям, применяемым в настоящее время, а также иным требованиям, предписанным для организации;

h) быть официально одобренной высшим руководством;

i) документироваться, внедряться и поддерживаться в рабочем состоянии;

j) доводиться до сведения всего соответствующего персонала и третьих лиц, включая подрядчиков и посетителей, имея в виду, что эти лица должны знать свои индивидуальные обязательства в отношении менеджмента безопасности;

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

l) предусматривать ее анализ в случае приобретения другой организации или слияния с другими организациями, или при других изменениях области бизнеса организации, которые могут повлиять на стабильность или пригодность системы менеджмента безопасности.

Примечание — Для внутреннего использования организации допускается выбрать детально разработанную политику в области менеджмента безопасности, которая содержала бы достаточную информацию по направлениям деятельности системы менеджмента безопасности (некоторые разделы которой могут носить конфиденциальный характер), а также имела бы обобщенную (неконфиденциальную) версию, отражающую общие цели, которые доводятся до сведения персонала и других заинтересованных сторон.

[ГОСТ Р 53663—2009]

b) Намерение

Политика в области менеджмента безопасности — краткое программное заявление высшего руководства об обязательствах в отношении обеспечения безопасности и охраны. Политика в области менеджмента безопасности устанавливает общие намерения и направление деятельности организации. Она обеспечивает основу для постановки целей в области обеспечения безопасности и охраны для всей организации в целом.

Документированная политика в области менеджмента безопасности должна быть сформулирована и утверждена высшим руководством организации.

c) Типовые входные данные

При разработке политики в области менеджмента безопасности высшему руководству, особенно в отношении собственных цепей поставок, следует учитывать:

- политику и цели, согласующиеся с деятельностью организации в целом;
- историческую и текущую деятельность организации в области обеспечения безопасности;
- потребности заинтересованных сторон;
- возможности и потребность в постоянном улучшении;
- необходимые ресурсы;
- содействие персонала;
- содействие подрядчиков, заинтересованных сторон и другого стороннего персонала.

d) Процесс

При разработке и утверждении политики в области менеджмента безопасности высшему руководству следует учитывать нижеприведенные требования.

Эффективно сформулированная и понятная политика в области менеджмента безопасности должна:

1) соответствовать характеру и масштабам рисков для организации.

Идентификация угроз, оценка рисков и риска-менеджмента, являясь основой эффективной системы менеджмента безопасности, должны найти отражение в политике в области менеджмента безопасности.

Политика в области менеджмента безопасности должна учитывать потенциал организации, соответствовать действительности, а также исключать преувеличение или приуменьшение рисков для организации;

2) содержать обязательство по постоянному улучшению эффективности системы менеджмента безопасности.

Глобальные угрозы в сфере безопасности и охраны увеличивают давление на организации, вынуждая их приуменьшать риски в цепи поставок. Помимо выполнения нормативных правовых актов, а также инструкций и руководств, подготовленных такими органами, как Всемирная Таможенная Организация (ВТО), организация должна стремиться к постоянному улучшению системы менеджмента безопасности для обеспечения соответствия собственной деятельности обязательным требованиям в области обеспечения безопасности и охраны с тем, чтобы эффективно реагировать на изменение потребностей мировой торговли.

Планируемое улучшение эффективности функционирования должно быть представлено в целях в области менеджмента безопасности (см. 4.3.2) и управляться программами в области менеджмента безопасности (см. 4.3.5), хотя изложение политики может включать более обширные сферы деятельности;

3) содержать обязательство, по меньшей мере, соответствовать существующим применимым нормативным требованиям в области обеспечения безопасности и охраны, выполнение которых предписано организации.

От организаций требуется соответствие применимым нормативным требованиям в области обеспечения безопасности и охраны. Политика в области менеджмента безопасности — публичное подтверждение организацией своего долга соответствовать, если не усиливать требования, законодательных нормативных правовых актов и других требований или добровольно принятых норм, таким как Рамочные стандарты безопасности и облегчения мировой торговли ВТО [1].

Примечание — термин «другие требования» может означать корпоративные обязательства, отраслевые стандарты, технические условия либо регламенты, принятые организацией.

4) документироваться, внедряться и поддерживаться в рабочем состоянии.

Ключом успешного внедрения является планирование и подготовка. Часто формулировки, используемые в политике и целях в области менеджмента безопасности, не соответствуют действительности из-за отсутствия достаточных ресурсов у организации для их осуществления. Прежде, чем делать любые публичные заявления, организация должна убедиться в наличии ресурсов, персонала, компетенции и опыта для достижения устанавливаемых целей в области менеджмента безопасности, обеспечения безопасности и охраны в рамках собственной структуры.

Для достижения эффективности политика в области менеджмента безопасности должна быть документально оформлена, поддерживаться в рабочем состоянии и, по мере необходимости, актуализироваться;

5) доводиться до всего персонала в целях достижения понимания своих обязанностей в части обеспечения безопасности и охраны.

Вовлеченность и понимание со стороны персонала — условие успешного обеспечения безопасности организации.

Необходимо обеспечивать осведомленность персонала о влиянии менеджмента безопасности на окружающие условия работы и качество собственной деятельности, а также мотивировать персонал к активному содействию менеджменту безопасности.

Персонал (на всех уровнях, включая уровни управления) вряд ли будет в состоянии эффективно способствовать менеджменту безопасности, если не будет достигнуто понимание политики организации в области менеджмента безопасности и собственной ответственности и компетенции для выполнения поставленных задач.

Это потребует от организации четкого доведения до персонала собственной политики и целей в области менеджмента безопасности с тем, чтобы создавать условия для понимания персоналом своих персональных обязанностей при выполнении задач по обеспечению безопасности;

6) быть доступной для заинтересованных лиц.

Любой человек или группа (внутри или вне организации), заинтересованные в деятельности организации в части обеспечения безопасности, уделяют особое внимание политике этой организации в

области менеджмента безопасности. Поэтому должен быть предусмотрен соответствующий процесс доведения сведений о политике всем заинтересованным лицам, где это необходимо;

7) периодически анализироваться с тем, чтобы оставаться актуальной и соответствовать направлениям деятельности организации.

В связи с периодическими изменениями законодательных и иных нормативных правовых актов в сфере обеспечения безопасности и охраны, а также возрастающими потребностями со стороны заинтересованных лиц политика и система менеджмента безопасности цепи поставок нуждаются в регулярном анализе и пересмотре в целях обеспечения собственной эффективности и постоянной пригодности.

Все изменения должны быть доведены заинтересованными лицами в возможно короткие сроки.

e) Типовые выходные данные

Всесторонняя, кратко сформулированная и понятная политика организации в области менеджмента безопасности, доведенная до всего персонала и, при необходимости, до заинтересованных лиц.

4.3 Оценка рисков безопасности и планирование

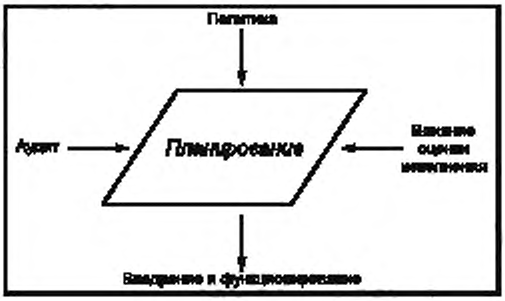

Рисунок 3 — Планирование

4.3.1 Оценка рисков безопасности

a) Требования

Организация должна разрабатывать и поддерживать в рабочем состоянии процедуры по своевременной идентификации угроз и оценке рисков, в том числе касающихся менеджмента безопасности, а также по определению и реализации необходимых мер административного управления. Идентификация угроз, отнесенных к охране и рискам, оценка и методы управления должны, как минимум, соответствовать характеру и масштабу выполняемой организацией деятельности. Эта оценка должна учитывать вероятность случая и все его последствия, включая:

a) угрозы и риски физического воздействия или повреждения, такие как функциональный отказ, непредвиденное повреждение, злонамеренное причинение вреда, террористический акт или преступное деяние;

b) угрозы и риски оперативного характера, включая контроль безопасности, человеческого фактора и других действий, которые влияют на деятельность, условия или безопасность организации;

c) события природного характера (бурю, наводнение и т.д.), из-за которых меры по обеспечению безопасности и технические средства охраны могут оказаться неэффективными;

d) внешние факторы, управляемые организацией, такие как непредоставление услуг и неисправность оборудования внешних поставщиков;

e) угрозы и риски со стороны заинтересованного лица, такие как отказ соблюдать нормативные требования или нанесение ущерба репутации или бренду;

f) конструкцию и установку средств охраны (замену, обслуживание и т.д.);

g) управление информацией и данными, а также связь;

h) угрозу непрерывности производственной деятельности.

Организация должна быть уверена в том, что результаты оценки и эффект от такого контроля принимаются во внимание и, где это необходимо, оказывают влияние на:

a) цели и задачи в области менеджмента безопасности;

b) программы в области менеджмента безопасности;

c) определение требований к конструкции, спецификации и установке;

d) определение достаточности ресурсов, включая степень укомплектованности персоналом;

e) определение потребности в подготовке и приобретении необходимых навыков (см. 4.4.2);

f) развитие управления документами и данными (см. 4.4.6);

g) всю структуру управления организацией в отношении угроз и рисков.

Организация должна документировать и актуализировать вышеуказанную информацию.

Методология организации по идентификации и оценке угроз и рисков должна:

a) быть выбрана в соответствии с областью применения, характером и сроками с тем, чтобы иметь предупреждающий характер, а не подтверждающей факт случившегося;

b) включать в себя сбор информации, имеющей отношение к угрозам, отнесенным к охране и рискам;

c) предусматривать классификацию угроз и рисков и выбор соответствующих действий по предотвращению, устранению или управлению ими;

d) предусматривать мониторинг действий с тем, чтобы определить результативность и своевременность их выполнения (см. 4.5.1).

[ГОСТ Р 53663—2009]

b) Намерение

Организация должна определять наиболее значимые угрозы, риски и уязвимые места, связанные со своей деятельностью с тем, чтобы применять процессы идентификации угроз, оценки рисков и риска-менеджмента.

Процессы идентификации угроз, оценки рисков, риска-менеджмента и их выходные данные должны стать основой для всей системы менеджмента безопасности. Особенно важно четкое установление взаимосвязи между процессами идентификации угроз, оценки рисков и риска-менеджмента с другими элементами системы менеджмента безопасности.

Цель настоящего стандарта установить общие принципы, по которым организация сможет определять применимость и достаточность идентификации угроз, оценки рисков и риска-менеджмента.

Процессы идентификации угроз, оценки рисков и риска-менеджмента должны позволять организации определять, оценивать и управлять рисками в области обеспечения безопасности и охраны, используя имеющиеся возможности.

В любом случае необходимо уделять внимание свойственной и несвойственной деятельности в рамках организации, а также потенциальным чрезвычайным ситуациям.

Сложность процессов идентификации угроз, оценки рисков и риска-менеджмента в основном зависит от размеров и видов деятельности организации, а также от характера, сложности и значимости рисков. *ГОСТ Р 53663* (подпункт 4.3.1) не призван принуждать маленькие организации с меньшими рисками их безопасности внедрять и реализовывать сложный комплекс процессов по идентификации угроз, оценке рисков и риску-менеджменту.

Процессы идентификации угроз, оценки рисков и риску-менеджмента должны учитывать стоимость и сроки их реализации, а также надежность используемых данных. В перечисленных процессах может использоваться уже имеющаяся информация, подготовленная для распорядительных или иных целей. Организация также может учитывать степень существующего практического управления угрозами в области обеспечения безопасности и охраны. Организация должна определять угрозы, которые будут принимать во внимание входные и выходные данные, связанные с текущей и соответствующей прошлой деятельностью, процессами, продукцией и/или услугами.

Проведение оценки рисков в области обеспечения безопасности должно осуществляться квалифицированным персоналом, использующим признанные методики, которые могут быть документально оформлены.

Организация, не имеющая систему менеджмента безопасности, может определять свое текущее состояние в отношении рисков посредством проведения их оценки. Основанием для разработки системы менеджмента безопасности должны быть намерения организации учитывать угрозы, перед которыми она оказалась. Организация должна (но не ограничиваться этим):

- выполнять законодательные и нормативные требования;

- идентифицировать угрозы, перед которыми оказалась организация;

- осуществлять поиск информации об угрозах и рисках у соответствующих федеральных органов исполнительной власти;

- проводить анализ всех существующих процессов и процедур в отношении менеджмента безопасности;

- учитывать результаты расследований происшествий и чрезвычайных ситуаций, связанных с обеспечением безопасности.

В зависимости от характера деятельности организации для удобства в проведении оценки допускается использовать опросные листы, проводить собеседования, непосредственные измерения, учитывать результаты предыдущих аудитов системы менеджмента безопасности или иные данные для анализа. Все эти действия следует проводить регулярно и должны быть документально оформлены.

Следует подчеркнуть, что при проведении первоначальной оценки рекомендуется выработать основное направление, которое не подменяет формирование структурированного системного подхода, указанного в 4.3.1.

c) Типовые входные данные

Типовые входные данные включают в себя следующее:

- законодательные и нормативные требования в области обеспечения безопасности и охраны (см. 4.3.2);

- политику в области безопасности (см. 4.2);

- записи происшествий, связанных с обеспечением безопасности;

- несоответствия (см. 4.5.2);

- результаты аудитов системы менеджмента безопасности (см. 4.5.4);

- сообщения от персонала и других заинтересованных лиц (см. 4.4.3);

- информацию из консультаций персонала в части обеспечения безопасности, по вопросам анализа и действий по улучшению рабочих мест (такие действия могут носить предупредительный характер или быть мерами реагирования);

- информацию о положительном опыте, типовых рисках для организации, происшествиях и чрезвычайных ситуациях, имевших место в похожих организациях;

- отраслевые стандарты;

- предписания *федеральных органов исполнительной власти;*

- информацию о средствах, процессах и деятельности организации, включая:

детали изменений процедур управления,

схемы,

руководства и процедуры по эксплуатации,

данные об охране,

мониторинг данных (см. 4.5.1);

d) Процесс

1) Идентификация угроз, оценка рисков и риска-менеджмента

i) основное

Мероприятия риска-менеджмента должны отражать принципы устранения или снижения рисков до практического минимума там, где это возможно, или уменьшения вероятности или последствий потенциальных актов незаконного вмешательства. Процессы идентификации угроз, оценки рисков и риска-менеджмента являются главными инструментами управления рисками.

Процессы идентификации угроз, оценки рисков и риска-менеджмента для разных отраслей деятельности особо различны: начиная от простых оценок, вплоть до сложных количественных анализов с использованием обширной документации. Организация планирует и внедряет соответствующие процессы идентификации угроз, оценки рисков и риска-менеджмента таким образом, чтобы удовлетворять собственным потребностям и своему месторасположению, а также обеспечивать соответствие законодательным и нормативным требованиям в области обеспечения безопасности.

Процессы идентификации угроз, оценки рисков и риска-менеджмента должны быть позиционированы как предупредительные меры, а не как меры реагирования, то есть они должны предварять введение новых или пересмотренных действий или процедур. Любые необходимые меры по управлению или уменьшению рисков следует внедрять прежде, чем вводятся такие изменения.

Организация должна поддерживать квалификацию персонала и периодически актуализировать методики, документацию, данные и записи по процессам идентификации угроз, оценки рисков и риска-менеджмента для обеспечения их соответствия текущей деятельности организации, а также принимать во внимание развитие, расширение и освоение новых видов деятельности организации для своевременного внедрения этих процессов.

Процессы идентификации угроз, оценки рисков и риска-менеджмента следует применять не только для условий повседневной эксплуатации средств и процедур, но и в случаях внеплановой их эксплуатации.

Наряду с учетом рисков обеспечения безопасности и рисков, создаваемых действиями собственного персонала, организация должна учитывать риски, возникающие вследствие действий подрядчиков и посетителей, а также при пользовании продукцией или услугами, поставляемыми иными организациями;

ii) процессы

Процессы идентификации угроз безопасности, оценки рисков и риска-менеджмента должны быть документально оформлены и включать в себя:

- идентификацию угроз в области обеспечения безопасности и охраны;
- определение рисков с существующими (или предполагаемыми) мерами по их управлению на местах (принимая во внимание открытость конкретных угроз, вероятность несрабатывания мер по управлению рисками и серьезность потенциальных последствий возможных повреждений, разрушений или нарушений устойчивости деятельности организации);
- определение приемлемости текущих и остаточных рисков;
- идентификацию потребностей в дополнительных мерах риска-менеджмента;
- определение мер риска-менеджмента, достаточных для уменьшения рисков до приемлемого уровня.

Помимо отмеченного следует учитывать:

- характер, время, область применения и методы осуществления любых форм идентификации угроз, оценки рисков и риска-менеджмента,
- применимые законодательные и нормативные акты в области обеспечения безопасности и охраны,
- роли и полномочия персонала, ответственного за реализацию таких процессов,
- уровень компетентности и потребность в подготовке персонала (см. 4.4.2), ответственного за реализацию таких процессов. (В зависимости от характера и типа осуществляемых процессов организации может потребоваться приобретение сторонних услуг или консультаций),
- информацию, касающуюся обеспечения безопасности и охраны, получаемую от службы охраны, входных данных, анализа и действий по улучшению (такие действия могут носить предупредительный характер или быть мерами реагирования);

iii) последующие действия

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

- должно быть четкое свидетельство того, что любые корректирующие или предупреждающие действия (см. 4.5.2), определенные как необходимые, контролировались на предмет их своевременного выполнения. (Эти действия могут потребовать проведения дальнейшей идентификации угроз и оценки рисков с тем, чтобы отражать возможные изменения в мероприятиях по риску-менеджменту и для определения остаточных рисков);
- результаты, достигнутые в ходе реализации корректирующих или предупреждающих действий, должны быть представлены в качестве входных данных для проведения анализа эффективности системы менеджмента безопасности со стороны руководства (см. 4.6), а также для установления новых или пересмотра текущих целей в области менеджмента безопасности;
- организация должна иметь возможность определять квалификацию персонала, осуществляющего деятельность по обеспечению безопасности и охраны, на соответствие компетентности, определенной в ходе оценки рисков, для установления необходимого риска-менеджмента;
- результаты опыта, получаемого в ходе внедрения и последующей эксплуатации упомянутых процессов, должны накапливаться и быть использованы для их улучшения.

2) Мероприятия, проводимые после первоначального определения идентификации угроз, оценки рисков и риска-менеджмента (см. 4.6)

Процессы идентификации угроз, оценки рисков и риска-менеджмента должны анализироваться в определенный период времени, который устанавливается либо политикой в области менеджмента безопасности, либо руководством организации. Такой анализ может быть частью анализа эффективности системы менеджмента безопасности со стороны руководства (см. 4.6). Время проведения анализа упомянутых процессов может изменяться в зависимости от:

- характера угроз;
- величины рисков;
- изменений в деятельности организации.

Анализ процессов следует проводить также в случае таких изменений в деятельности организации, при которых ставится под сомнение обоснованность существующих оценок. Такие изменения могут включать в себя:

- расширение, сужение, реструктуризацию средств или аспектов цепи поставок;
- перераспределение обязанностей;
- изменение методов работы или моделей поведения при угрозах со стороны внешних источников.

e) Типовые выходные данные

Процедуры должны быть документально оформлены, содержать:

- идентификацию угроз безопасности;
- определение рисков, связанных с идентифицированными угрозами безопасности;
- указание уровня рисков, связанных с каждой угрозой безопасности, и их приемлемости;
- описание или ссылку на меры по мониторингу и управлению рисками (см. 4.4.6 и 4.5.1), в особенности неприемлемыми рисками;
- соответствующие цели в области менеджмента безопасности и действия по снижению идентифицированных рисков (см. 4.3.3), а также любые последующие действия по отслеживанию процесса их снижения;
- идентификацию потребностей в компетентности и подготовке, необходимых для реализации мер управления (см. 4.4.2);
- необходимые меры управления, детализированные как часть контроля операций в элементах системы (см. 4.4.6);
- записи, относящиеся к каждому из вышеперечисленных процессов.

4.3.2 Законодательные, нормативные и иные требования, регламентирующие обеспечение безопасности

a) Требования

Организация должна разрабатывать, внедрять и поддерживать в рабочем состоянии процедуру по:

a) идентификации и доступу к применимым законодательным, нормативным и иным требованиям, регламентирующим безопасность, которые установлены для организации в отношении угроз, отнесенных к охране и рискам;

b) определению применения этих требований в отношении своих угроз и рисков.

Организация должна хранить и актуализировать эту информацию. Она должна доводить значимую информацию о законодательных и других требованиях всему персоналу и, при необходимости, третьим лицам, включая подрядчиков.

[ГОСТ Р 53663—2009]

b) Намерение

Организации необходимо осознавать влияние законодательных и иных требований на собственную деятельность в настоящее время и в будущем и доводить эту информацию до соответствующего персонала.

Требования *ГОСТ Р 53663* (подпункт 4.3.2) способствуют пониманию законодательной и нормативной ответственности. Но это не является призывом к созданию библиотеки нормативной документации, обращение к которой носит эпизодический характер.

c) Типовые входные данные

Типовые входные данные включают в себя:

- подробные сведения о цепи поставок организации;
- результаты идентификации угроз, оценки рисков и риска-менеджмента (см. 4.3.1);
- положительный опыт (кодексы, отраслевые руководства и т.д.);
- законодательные и нормативные требования, а также требования правительственных, межправительственных органов, международных торговых ассоциаций, кодексы, методики и правила;
- перечень источников информации;
- национальные, европейские, региональные или международные стандарты;
- внутренние требования организации;
- потребности заинтересованных лиц;
- процессы управления динамикой цепи поставок.

d) Процесс

Должны быть определены и идентифицированы законодательные и иные требования в области обеспечения безопасности и охраны, наиболее приемлемые способы получения такой информации,

включая средства массовой информации (газеты, компакт-диски, интернет), а также объем применимых требований.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- процедуры по идентификации, получению и обновлению информации;
- идентифицированные объемы применимых требований (это может принять форму учета);
- требования (в виде актуализируемого перечня), которые доступны в местах, установленных организацией;
- процедуры мониторинга выполнения указаний вследствие новых нормативных актов, регламентирующих безопасность.

4.3.3 Цели в области менеджмента безопасности

a) Требования

Организация должна разрабатывать, документировать, внедрять и поддерживать в рабочем состоянии цели в области менеджмента безопасности с учетом соответствующих функций и уровней внутри организации. Цели должны исходить из политики в области менеджмента безопасности и соответствовать ей. В процессе разработки и анализа своих целей организация должна учитывать:

a) законодательные, нормативные и другие требования, регламентирующие безопасность;
b) угрозы и риски, влияющие на безопасность;
c) технологические и другие факторы;
d) финансовые, эксплуатационные и деловые требования;
e) мнения соответствующих заинтересованных лиц.

Цели в области менеджмента безопасности должны:

a) соответствовать обязательству организации по постоянному улучшению;
b) быть измеримыми (где применимо);
c) доводиться до сведения всего соответствующего персонала и третьих лиц, включая подрядчиков, имея в виду, что эти лица должны знать свои индивидуальные обязательства;
d) периодически анализироваться с тем, чтобы сохранять актуальность и согласованность с политикой в области менеджмента безопасности. Цели должны соответственно корректироваться там, где это необходимо.

[ГОСТ Р 53663—2009]

b) Намерение

Необходимо обеспечивать, чтобы во всей организации (где это практически необходимо) были установлены измеримые цели в области менеджмента безопасности, согласующиеся с политикой.

c) Типовые входные данные

Типовые входные данные включают в себя:

- политику и цели, соответствующие бизнесу организации в целом;
- политику в области менеджмента безопасности, включая намерения по постоянному улучшению (см. 4.2);
- результаты идентификации угроз, оценок рисков и риска-менеджмента (см. 4.3.1);
- законодательные и другие требования (см. 4.3.2);
- технологические особенности;
- финансовые, эксплуатационные и деловые потребности;
- участие персонала и заинтересованных лиц (см. 4.4.3);

информацию от консультаций персонала в части обеспечения безопасности, по вопросам анализа и действий по улучшению рабочих мест (такие действия могут носить предупредительный характер или быть мерами реагирования);

- анализ установленных целей в области менеджмента безопасности;
- записи о несоответствиях, происшествиях и ущербах собственности, касающиеся обеспечения безопасности и охраны;
- результаты анализа со стороны руководства (см. 4.6).

d) Процесс

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

Для достижения адекватности и понимания при установлении целей в области менеджмента безопасности особое внимание следует уделять входным данным, получаемым от источников, которые с наибольшей вероятностью будут затронуты такими целями. Также эффективно использовать

входные данные, получаемые от внешних источников, таких как заказчиков, подрядчиков, поставщиков и *федеральных органов исполнительной власти* или заинтересованных лиц.

Совещания по определению целей в области менеджмента безопасности должно проводить руководство не реже одного раза в год. Для некоторых организаций процесс установления целей в области менеджмента безопасности допускается оформлять документально.

Цели в области менеджмента безопасности должны охватывать как всеобщие проблемы обеспечения безопасности и охраны организации в целом, так и те проблемы, которые являются специфическими для цепи поставок, отдельных подразделений или предоставляемых услуг.

Для каждой цели в области менеджмента безопасности должен быть определен соответствующий показатель, который позволяет контролировать процесс достижения установленных целей.

Цели в области менеджмента безопасности должны быть разумными и достижимыми с тем, чтобы обеспечивать организации возможность их реализации и отслеживания процесса их исполнения. По каждой цели должен быть определен график реализации.

Цели в области менеджмента безопасности допускается подразделять на отдельные направления в зависимости от размера организации, сложности самой цели и времени ее достижения. Должна быть установлена четкая взаимосвязь между такими направлениями и целями в области менеджмента безопасности.

Например, типы целей в области менеджмента безопасности могут включать в себя:

- снижение уровня риска;
- введение дополнительных возможностей в систему менеджмента безопасности;
- мероприятия по улучшению существующих средств охраны;
- устранение или уменьшение вероятности реализации акта незаконного вмешательства.

Цели в области менеджмента безопасности должны быть доведены до соответствующего персонала (в ходе проведения учений и тренировок см. 4.4.2) и детализированы в программах в области менеджмента безопасности (см. 4.3.4).

e) Типовые выходные данные

Типовыми выходными данными являются установленные организацией для каждой своей функции измеримые и документально оформленные цели в области менеджмента безопасности.

4.3.4 Задачи в области менеджмента безопасности

a) Требования

Организация должна разрабатывать, документировать, внедрять и поддерживать в рабочем состоянии задачи в области менеджмента безопасности, соответствующие потребностям организации. Задачи должны исходить из целей в области менеджмента безопасности и соответствовать им.

Эти задачи должны:

a) быть на уровне необходимой детализации;

b) быть конкретными, измеримыми, решаемыми, значимыми и имеющими показатели времени (где это применимо);

c) быть доведены до сведения всего соответствующего персонала и третьих лиц, включая подрядчиков, имея в виду, что эти лица должны знать свои индивидуальные обязательства;

d) периодически анализироваться с тем, чтобы сохранить актуальность и соответствие целям в области менеджмента безопасности. Задачи должны соответственно корректироваться там, где это необходимо.

[ГОСТ Р 53663—2009]

b) Намерение

Задачи в области менеджмента безопасности устанавливают для достижения целей в пределах определенного организацией времени.

c) Типовые входные данные

Типовые входные данные включают в себя:

- политику и цели, соответствующие бизнесу организации в целом;
- политику в области менеджмента безопасности, включая намерения по постоянному улучшению (см. 4.2);
- результаты идентификации угроз, оценок рисков и риска-менеджмента (см. 4.3.1);
- законодательные и другие требования (см. 4.3.2);
- технологические особенности;
- финансовые, эксплуатационные и деловые потребности;
- участие персонала и заинтересованных лиц (см. 4.4.3);

- информацию от консультаций персонала в части обеспечения безопасности, по вопросам анализа и действий по улучшению рабочих мест (такие действия могут носить предупредительный характер или быть мерами реагирования);
- анализ установленных целей в области менеджмента безопасности;
- записи о несоответствиях и актах незаконного вмешательства;
- результаты анализа со стороны руководства (см. 4.6).

d) Процесс

Процесс определен в программах в области менеджмента безопасности и представляет собой достижение задач, соответствующих целям.

Используя входные данные, руководство организации должно идентифицировать и устанавливать приоритеты по задачам в области менеджмента безопасности. Задачи должны быть измеримы, конкретизированы и соотнесены по времени.

Для достижения адекватности и понимания при установлении задач в области менеджмента безопасности особое внимание следует уделять входным данным, получаемым от источников, которые с наибольшей вероятностью будут затронуты при реализации таких задач. Также эффективно использовать входные данные, получаемые от внешних источников, таких как заказчиков, подрядчиков, поставщиков и *федеральных органов исполнительной власти* или заинтересованных лиц.

Совещания по определению задач в области менеджмента безопасности должно проводить руководство после внесения изменений в цели в области менеджмента безопасности. Для некоторых организаций процесс установления задач в области менеджмента безопасности допускается оформлять документально.

Задачи в области менеджмента безопасности должны охватывать как всеобщие проблемы обеспечения безопасности и охраны организации в целом, так и те проблемы, которые являются специфическими для цепи поставок, отдельных подразделений или предоставляемых услуг.

Для каждой задачи в области менеджмента безопасности должен быть определен соответствующий показатель, который позволяет контролировать реализацию поставленных задач.

Задачи в области менеджмента безопасности должны быть разумными и решаемыми с тем, чтобы обеспечивать организации возможность их реализации и наблюдения за процессом их выполнения. По каждой задаче должен быть определен график реализации.

Задачи в области менеджмента безопасности допускается подразделять на отдельные направления в зависимости от размера организации, сложности поставленной задачи и времени ее выполнения. Должна быть установлена четкая взаимосвязь между такими направлениями и задачами в области менеджмента безопасности.

Например, типы задач в области менеджмента безопасности могут включать в себя:

- снижение уровня риска в определенный срок;
- внедрение новых технологий по уменьшению риска или снижению воздействий от угроз безопасности;
- мероприятия по улучшению существующих средств охраны;
- устранение или уменьшение вероятности реализации акта незаконного вмешательства.

Задачи в области менеджмента безопасности должны быть доведены до соответствующего персонала (в ходе проведения учений и тренировок см. 4.4.2) и детализированы в программах в области менеджмента безопасности (см. 4.3.4).

e) Типовые выходные данные

Типовыми выходными данными являются установленные организацией для каждой своей функции измеримые и документально оформленные задачи в области менеджмента безопасности.

4.3.5 Программы в области менеджмента безопасности

a) Требования

Организация должна разрабатывать, внедрять и поддерживать в рабочем состоянии программы в области менеджмента безопасности для достижения своих целей и решения соответствующих задач.

Программы должны быть оптимизированы и затем расставлены по приоритетам, а организация должна предусматривать результативное и рентабельное по затратам выполнения этих программ.

Программы должны включать документацию, содержащую описание:

а) ответственности и полномочий по достижению целей и решению задач в области менеджмента безопасности;

b) способов и сроков достижения целей и решения задач в области менеджмента безопасности.

Программы в области менеджмента безопасности должны периодически актуализироваться с тем, чтобы сохранять результативность и соответствие целям и задачам организации в области менеджмента безопасности. Программы должны соответственно корректироваться там, где это необходимо.

[ГОСТ Р 53663—2009]

b) Намерение

Программы в области менеджмента безопасности должны быть взаимосвязаны с целями и задачами. Каждая программа должна содержать описание того, как организация понимает собственные обязательства и политику по определению действий для достижения целей и задач в области менеджмента безопасности. Программа потребует разработки стратегии и планирования принимаемых действий, которые должны быть документально оформлены и согласованы. Процесс выполнения программы по достижению установленных целей следует контролировать и анализировать с ведением соответствующих записей. Стратегия программы должна быть основана на результатах идентификации угроз и оценки рисков.

c) Типовые входные данные

Типовые входные данные включают в себя:

- цели и задачи в области менеджмента безопасности;
- законодательные и другие требования;
- результаты идентификации угроз, оценки рисков и риска-менеджмента;
- подробные сведения о деятельности организации;
- информацию от консультаций персонала в части обеспечения безопасности, по вопросам анализа и действий по улучшению рабочих мест (такие действия могут носить предупредительный характер или быть мерами реагирования);
- анализ имеющихся возможностей с учетом новых или разных технологических решений;
- действия по постоянному улучшению;
- наличие ресурсов, необходимых для достижения целей в области менеджмента безопасности организации.

d) Процесс

Программа менеджмента безопасности должна определять:

- обязанности по достижению целей;
- средства для достижения целей;
- установленный период времени для достижения целей.

Программа должна рассматривать снижение угроз безопасности посредством методологических и технологических решений, а также опыта других организаций. При этом программа должна учитывать финансовые, эксплуатационные и деловые требования, а также потребности организаций-партнеров и заинтересованных лиц.

Программа должна предусматривать распределение соответствующей ответственности и полномочий, а также установление времени выполнения по каждому направлению решения задач с тем, чтобы составлять график реализации соответствующей цели в области менеджмента безопасности. По решению каждой задачи программа также должна предусматривать распределение соответствующих ресурсов (экономических, технических, человеческих).

Для случаев существенных изменений или реструктуризации деятельности организации, методов работы, оборудования и средств охраны программа должна предусматривать проведение новой идентификации угроз и оценки рисков. Программа в области менеджмента безопасности должна предусматривать консультации соответствующего персонала по ожидаемым изменениям.

e) Типовые выходные данные

Типовыми выходными данными являются определенные организацией и документально оформленные программы в области менеджмента безопасности по достижению целей и решению задач, описанных в 4.3.3 и 4.3.4.

4.4 Внедрение и функционирование



Рисунок 4 — Внедрение и функционирование

4.4.1 Структура, полномочия и ответственность в менеджменте безопасности

a) Требования

Организация должна разрабатывать и поддерживать в рабочем состоянии организационную структуру ролей, ответственности и полномочий, которая бы согласовывалась с политикой, целями, задачами и программами в области менеджмента безопасности.

Эти роли, ответственность и полномочия должны быть идентифицированы, документированы и доведены до сведения каждого лица с персональной ответственностью за внедрение и улучшение.

Высшее руководство должно обеспечить наличие свидетельства принятия обязательств по разработке и внедрению системы менеджмента безопасности, а также постоянному улучшению ее результативности посредством:

a) назначения одного из членов высшего руководства, независимо от его прочих обязанностей, ответственным за всеобщее проектирование, документирование, поддержание в рабочем состоянии и улучшение системы менеджмента безопасности организации;

b) назначения одного или нескольких членов руководства с наделением необходимыми полномочиями для обеспечения достижения целей и выполнения задач;

c) идентификации и мониторинга требований и ожиданий от заинтересованных организации и лиц и принятия надлежащих и своевременных действий по управлению этими ожиданиями;

d) обеспечения наличия достаточных ресурсов;

e) учета возможных неблагоприятных воздействий политики, целей, задач и программ в области менеджмента безопасности на другие аспекты работы организации;

f) обеспечения участия любых, подготовленных другими подразделениями организации, программ по безопасности в системе менеджмента безопасности в качестве дополнений;

g) информирования организации о важности соблюдения требований системы менеджмента безопасности и соответствия собственной политике;

h) обеспечения включения угроз в отношении охраны и рисков в оценку угроз и рисков организации в целом;

i) обеспечения жизнеспособности целей, задач и программ в области менеджмента безопасности.

[ГОСТ Р 53663—2009]

b) Намерение

Для обеспечения эффективности менеджмента безопасности необходимо, чтобы роли, ответственность и полномочия были определены и оформлены документально. Только персонал, прошедший проверку на допуск, можно привлекать для решения задач по обеспечению безопасности и охраны. Выполнение этих задач должно обеспечиваться адекватными ресурсами.

c) Типовые входные данные

Типовые входные данные включают в себя:

- организационную структуру;
- результаты идентификации угроз, оценку рисков и риска-менеджмента;
- цели, задачи и программы в области менеджмента безопасности;
- законодательные и другие требования;

- описания работ;
- перечень компетентного персонала, нуждающегося или прошедшего проверку на допуск.

d) Процесс

1) Общее представление

Должны быть определены ответственность и полномочия всех лиц, выполняющих обязанности по системе менеджмента безопасности, включая четкое определение обязанностей по взаимодействию между различными функциями.

Такое определение, помимо прочих, может потребоваться для следующих категорий лиц:

- высшего руководства;
- руководства среднего звена;
- лиц, ответственных за подрядчиков и посетителей, имеющих доступ в помещения организации и к работающему персоналу;
- лиц, ответственных за проведение учений и тренировок в области обеспечения безопасности;
- лиц, ответственных за технические средства охраны и их эксплуатацию;
- персонала, прошедшего проверку на допуск, или персонала службы охраны организации;
- персонала, привлекаемого для консультаций по вопросам безопасности.

Тем не менее организация должна доводить и продвигать мысль о том, что безопасность — это ответственность каждого в организации, а не только тех лиц, чьи обязанности непосредственно определены в системе менеджмента безопасности.

2) Определение ответственности высшего руководства

Ответственность высшего руководства должна включать в себя определение политики в области менеджмента безопасности и предусматривать внедрение системы менеджмента безопасности в организации. Как часть этого обязательства, высшим руководством должен быть определен и назначен представитель руководства по безопасности с определенной ответственностью и полномочиями по внедрению системы менеджмента безопасности цепи поставок (в крупных организациях может быть более одного назначенного представителя).

3) Определение ответственности представителя руководства по безопасности

Представитель руководства по безопасности должен нести ответственность и обладать полномочиями по внедрению и документированию системы менеджмента безопасности; должен иметь прямой доступ к высшему руководству и пользоваться поддержкой других лиц, наделенных обязанностями по мониторингу эффективности функционирования системы менеджмента безопасности.

Представитель руководства по безопасности должен регулярно получать информацию относительно работы системы и принимать активное участие в проведении анализов результативности функционирования системы менеджмента безопасности для определения целей в этой области. Необходимо обеспечивать, чтобы любые другие обязанности или функции этих лиц не противоречили выполнению их обязанностей в области обеспечения безопасности.

4) Определение ответственности руководства среднего звена

Ответственность руководства среднего звена должна включать в себя обеспечение безопасности в пределах области их деятельности. Там, где основная ответственность за деятельность по обеспечению безопасности и охраны лежит на руководителях среднего звена, должны быть соответственно определены роли и ответственность любого специалиста, осуществляющего функции по обеспечению безопасности в пределах организации во избежание двусмысленного толкования их обязанностей и полномочий. Следует предусматривать меры по разрешению любых конфликтов между проблемами обеспечения безопасности и производственной деятельности путем вынесения их на более высокий уровень руководства.

5) Документирование ответственности и полномочий

Ответственность и полномочия в области обеспечения безопасности должны быть документально оформлены и соответствовать установленной в организации форме. Для этого организация может использовать одну или более из нижеприведенных форм или воспользоваться альтернативной формой по своему выбору:

- руководство по системе менеджмента безопасности;
- рабочие процедуры и правила;
- должностные инструкции;
- программы обучения и подготовки.

Если в организации предусмотрено ведение должностных инструкций персонала, в которых изложены ответственность и полномочия, касающиеся производственной деятельности организации, тогда

в эти должностные инструкции должны быть включены ответственность и полномочия, касающиеся обеспечения безопасности и охраны.

6) Информирование об ответственности и полномочиях

Ответственность и полномочия должны быть доведены до тех лиц, которых они касаются. Это должно обеспечивать понимание людьми границ и взаимодействия между различными функциями и каналами, которые следует использовать для инициирования надлежащих действий.

7) Ресурсы

Руководство должно обеспечивать наличие адекватных ресурсов, достаточных для обеспечения безопасности цепи поставок, включая оборудование, необходимые экспертизы, человеческие ресурсы и обучение.

Ресурсы считают адекватными, если они достаточны для реализации программ в области менеджмента безопасности, включая проведение мониторинга и измерений. Для организаций с уже внедренной системой менеджмента безопасности адекватность ресурсов определяют путем сравнения запланированных целей в области менеджмента безопасности с полученными результатами их реализации.

8) Обязательства руководства

Руководство должно демонстрировать свои обязательства по обеспечению безопасности и охраны. Способы демонстрации могут включать в себя посещение и осмотр охраняемых объектов, участие в расследовании актов незаконного вмешательства, предоставление ресурсов для реализации корректирующих действий, участие в совещаниях и конференциях по обеспечению безопасности и охраны, а также издание соответствующих документов.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- ответственность и полномочия, которые определены для всего персонала, имеющего отношение к обеспечению безопасности;
- ответственность и полномочия, оформленные документально в соответствующих руководствах, процедурах, инструкциях и программах обучения;
- методы доведения информации об ответственности и полномочиях до всего соответствующего персонала;
- активное участие и содействие в вопросах обеспечения безопасности и охраны со стороны руководства на всех уровнях управления.

4.4.2 Компетентность, подготовка и осведомленность

a) Требования

Организация должна заботиться о том, чтобы персонал, ответственный за планирование, функционирование и управление процессами обеспечения безопасности и техническими средствами охраны, имел должную квалификацию с точки зрения образования, подготовки и/или опыта. Организация должна разрабатывать и поддерживать в рабочем состоянии соответствующие процедуры с тем, чтобы персонал, работающий для нее или от ее имени, был осведомлен о:

a) важности соответствия политики и процедур в области менеджмента безопасности требованиям системы менеджмента безопасности;

b) своей роли и ответственности за достижение соответствия политике и процедурам в области менеджмента безопасности, а также требованиях системы менеджмента безопасности, включая готовность к реагированию и действиям в чрезвычайных ситуациях;

e) потенциальных последствиях для безопасности организации при несоблюдении специальных процедур.

Записи о компетенции и подготовке персонала должны поддерживаться в рабочем состоянии.

[ГОСТ Р 53663—2009]

b) Намерение

Организация должна иметь эффективные процедуры для обеспечения осведомленности персонала в отношении рисков и поддержания необходимой компетентности для реализации своих функций по обеспечению безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя:

- определение ответственности и полномочий;
- должностные инструкции (содержащие описание работ по обеспечению безопасности);
- оценки деятельности персонала;

- результаты идентификации угроз, оценки рисков и риска-менеджмента;
- руководства, процедуры и инструкции;
- политику и цели в области менеджмента безопасности;
- программы в области менеджмента безопасности.

d) Процесс

В процесс следует включать:

- систематическую идентификацию осведомленности и компетентности в области обеспечения безопасности и охраны, которые требуются для каждого уровня и каждой функции, осуществляемой организацией;
- меры по выявлению и устранению недостатков компетентности у персонала, имеющего отношение к обеспечению безопасности;
- своевременное проведение необходимого обучения;
- оценку отдельных лиц на предмет приобретения и поддержания ими требуемых знаний и компетентности;
- ведение соответствующих записей об образовании, подготовке, навыках и опыте каждого члена персонала.

Примечание — Для успешной системы менеджмента безопасности и ее эффективного функционирования важно уделять особое внимание вопросам осведомленности в области обеспечения безопасности и охраны во всей организации.

Следует разрабатывать и поддерживать в рабочем состоянии программы подготовки и проведения инструктажа по:

- осведомленности по существующим угрозам безопасности и рискам;
- пониманию мер обеспечения безопасности и охраны, предпринимаемых организацией, а также обязанностям и полномочиям отдельных лиц;
- обеспечению мер безопасности при назначении на должность или смене места работы внутри организации (систематический инструктаж);
- обеспечению мер безопасности при выполнении конкретных видов работ (вводный инструктаж);
- проведению идентификации угроз, оценки рисков и риска-менеджмента (см. 4.3.1 d);
- обязанностям персонала, деятельность которого непосредственно связана с обеспечением безопасности (обучающие семинары, тренинги или занятия в системе дополнительной профессиональной подготовки);
- обязанностям и полномочиям руководителей среднего звена по вопросам обеспечения безопасности и охраны;
- роли и ответственности высшего руководства, в том числе корпоративной, индивидуальной и юридической;
- обязанностям подрядчиков, временных рабочих и посетителей.

Эффективность программ подготовки и проведения инструктажа следует подвергать оценке. В целях определения эффективности и результативности данных программ такая оценка может осуществляться в процессе проведения подготовки или инструктажа.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- требования компетентности в соответствии с обязанностями;
- анализ потребности в подготовке;
- программы/планы подготовки;
- набор обучающих программ и учебных материалов, доступных для использования в пределах организации;
- записи по проведению подготовки и анализу ее эффективности;
- ознакомительные программы по обеспечению безопасности и охраны;
- оценку осведомленности и понимания.

4.4.3 Связь

a) Требования

Организация должна иметь процедуры, обеспечивающие передачу и обмен информацией, относящейся к менеджменту безопасности, между соответствующим персоналом, подрядчиками и другими заинтересованными лицами.

Ввиду конфиденциального характера определенной информации, относящейся к безопасности, должное внимание должно быть уделено такой информации перед ее распространением.
[ГОСТ Р 53663—2009]

b) Намерение

В процессе взаимодействия со своими партнерами организация при реализации своей деятельности должна поддерживать и распространять положительный опыт обеспечения безопасности, основывающийся на собственных политике и целях в области менеджмента безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя:

- политику и цели в области менеджмента безопасности;
- соответствующую документацию системы менеджмента безопасности;
- процедуры идентификации угроз, оценки рисков и риска-менеджмента;
- определения ролей и ответственности по обеспечению безопасности и охраны;
- результаты официальных и неофициальных консультаций руководства с персоналом;
- особенности программ подготовки;
- важную информацию от внешних источников.

d) Процесс

Организация должна документально оформлять и способствовать мерам по получению и обмену информацией, непосредственно связанной с обеспечением безопасности и охраны, среди персонала и заинтересованных лиц.

Эти меры должны способствовать участию персонала в:

- предоставлении рекомендаций в части разработки и проведения анализа политики и целей в области менеджмента безопасности, решении по внедрению процессов и процедур риска-менеджмента, включая проведение оценки рисков и управление рисками, которые связаны с их собственной деятельностью;
- предоставлении рекомендаций в части повышения обеспечения безопасности на рабочем месте, таких как применение новых технологий, модернизации средств охраны или усовершенствований процедур или схем работы.

Необходимо обеспечивать понимание персоналом важности наличия системы менеджмента безопасности и поощрять его стремление к содействию в области обеспечения безопасности и охраны.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- проведение протоколируемых совещаний высшего руководства с персоналом организации по вопросам обеспечения безопасности и охраны;
- привлечение персонала к проведению идентификации угроз, оценке рисков и риску-менеджменту;
- поощрение персонала, участвующего в представлении рекомендаций в части обеспечения безопасности и улучшения деятельности рабочих мест;
- назначение представителя руководства по безопасности с определением роли и взаимосвязей с руководством, включая, например, привлечение его к расследованию произошедших актов незаконного вмешательства, проведению осмотров охраняемых участков и т.д.
- проведение совещаний, касающихся вопросов обеспечения безопасности и охраны, для персонала, других заинтересованных лиц или посетителей;
- объявления, помещаемые на доски, содержащие информацию по вопросам обеспечения безопасности и охраны;
- информационные бюллетени;
- программу использования плакатов, посвященных вопросам безопасности;
- другие способы обмена конфиденциальной информацией по вопросам обеспечения безопасности и охраны с соответствующими *федеральными органами исполнительной власти* и партнерами по цепи поставок.

4.4.4 Документация

a) Требования

Организация должна разрабатывать и поддерживать в рабочем состоянии систему документирования менеджмента безопасности, которая включает в себя (но не ограничивается этим):

a) политику, цели и задачи в области менеджмента безопасности;
b) описание и область применения системы менеджмента безопасности;

c) описание главных элементов системы менеджмента безопасности и их взаимодействие, а также ссылки на соответствующие документы;

d) документы (включая записи), требуемые данным стандартом, и

e) другую документацию, определяемую организацией, как необходимую в обеспечении эффективного планирования, функционирования и управления процессами, относящимися к значительным угрозам и рискам ее безопасности.

Организация должна определять степень конфиденциальности информации и предпринимать шаги для предотвращения несанкционированного доступа к ней.

[ГОСТ Р 53663—2009]

b) Намерение

Для обеспечения понимания, эффективного внедрения и функционирования систему менеджмента безопасности следует документально оформлять и поддерживать в рабочем состоянии.

c) Типовые входные данные

Типовые входные данные включают в себя:

- документацию и информационные системы, используемые организацией, для поддержания системы менеджмента безопасности и своей деятельности в области обеспечения безопасности и охраны в соответствии с требованиями ГОСТ Р *53663*;
- распределение ответственности и полномочий;
- сведения о средствах, в которых используемые данные могут быть представлены как в печатном, так и в электронном виде.

d) Процесс

До разработки документации системы менеджмента безопасности организация должна определять те данные (информацию), которые необходимы для ее успешного функционирования.

Для обеспечения соответствия *ГОСТ Р 53663* не требуется разработка документации определенного формата. Нет также необходимости в замене существующих руководств, процедур или должностных инструкций, если они адекватно описывают текущую деятельность и меры по обеспечению безопасности и охраны в организации. Если в организации уже внедрена документированная система менеджмента безопасности, то наиболее целесообразно будет разработать документ, содержащий взаимосвязи и ссылки существующих процедур с требованиями *ГОСТ Р 53663*.

Необходимо учитывать:

- ответственность и степень допуска к документам и данным, содержащим информацию об обеспечении безопасности и охраны;
- способы и места работы с документами и данными, содержащимися на бумажных носителях. Аналогичные меры должны быть предусмотрены при работе с электронными носителями.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- обзорный документ по системе менеджмента безопасности;
- перечень сведений, содержащих информацию, отнесенную к конфиденциальной;
- руководства, процедуры и правила;
- должностные инструкции.

4.4.5 Управление документами и данными

a) Требования

Организация должна разрабатывать и поддерживать в рабочем состоянии процедуры управления всей документацией, данными и информацией, указанными в разделе 4 с тем, чтобы:

a) хранение и доступ к этим документам, данным и информации осуществлялись только уполномоченным на то персоналом;

b) документы, данные и информация периодически анализировались, при необходимости, актуализировались и подтверждались как пригодные уполномоченным на то персоналом;

c) последние версии соответствующих документов, данных и информации были в наличии во всех местах деятельности, значимых для результативного функционирования системы менеджмента безопасности;

d) устаревшие документы, данные и информация своевременно удалялись из всех источников выпуска и пунктов использования с тем, чтобы предотвратить их непреднамеренное использование;

e) архивные документы, данные и информация, оставленные на хранение по юридическим соображениям или для сохранения знаний, были должным образом идентифицированы и систематизированы;

f) документы, данные и информация сохранялись и обеспечивалась актуализация и возможность их восстановления при хранении в электронном виде.

[ГОСТ Р 53663—2009]

b) Намерение

Вся документация и данные, содержащие информацию о функционировании системы менеджмента безопасности и действиях организации по обеспечению безопасности и охраны, должны быть идентифицированы. Должно быть обеспечено управление ими.

c) Типовые входные данные

Типовые входные данные включают в себя:

- подробные сведения о документации и информационных системах, используемых организацией для обеспечения функционирования своей системы менеджмента безопасности, деятельности по обеспечению безопасности и охраны, а также соответствия требованиям *ГОСТ Р 53663*;
- подробные сведения об ответственности и полномочиях.

d) Процесс

Процедуры должны предусматривать средства управления документацией и данными по обеспечению безопасности и охраны в части их идентификации, одобрения, доступа, выдачи, пересмотра и замены. Эти процедуры должны четко определять степень доступа к документации и данным, содержащим конфиденциальную информацию в зависимости от ее значимости.

Должно обеспечиваться наличие и доступ к документации и данным уполномоченному на то персоналу в случае необходимости как в условиях повседневной деятельности организации, так и в чрезвычайных ситуациях.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- процедуру управления документацией, включая распределение ответственности и предоставления доступа к работе с документацией и данными, содержащими конфиденциальную информацию;
- номенклатуру дел;
- перечень управляемой документации с ее местонахождением;
- хранение записей.

4.4.6 Управление операциями

a) Требования

Организация должна идентифицировать операции и действия, необходимые для:

a) достижения собственной политики в области менеджмента безопасности;

b) управления идентифицированными угрозами и рисками безопасности;

c) соответствия нормативным и иным требованиям, регламентирующим безопасность;

d) решения собственных задач в области менеджмента безопасности;

e) выполнения собственных программ в области менеджмента безопасности;

f) достижения требуемого уровня безопасности цепи поставок.

Организация должна обеспечивать реализацию этих операций и действий в особых условиях путем:

a) разработки, внедрения и поддержания в рабочем состоянии документированных процедур по управлению ситуациями, когда отсутствие таких процедур может привести к сбою в осуществлении операций и деятельности (см. вышеприведенные перечисления);

b) оценки любых угроз, возникающих в результате деятельности на фазе «предконтроля» в цепи поставок, и использования рычагов управления для смягчения их воздействия на организацию и других операторов цепи на фазе «постконтроля»;

c) разработки и внедрения требований в отношении товаров или услуг, которые влияют на безопасность, и доведения их до сведения поставщиков и подрядчиков.

Эти процедуры должны включать в себя управление проектированием, установкой, функционированием, восстановлением и модификацией элементов оборудования, средств и т.д., которые имеют отношение к безопасности. Если пересматриваются существующие договоренности или вводятся новые, то это может повлиять на функционирование и действия менеджмента безопасности. Поэтому организация должна заранее учитывать все связанные с этим угрозы и риски в отношении

безопасности. Новые или пересмотренные договоренности или меры, подлежащие такому учету, включают в себя:

a) пересмотренные структуру, роли или ответственность в рамках организации;

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

c) пересмотренные процессы и процедуры;

d) введение новой инфраструктуры, средств охраны или технологии, которые могут включать технику и/или программное обеспечение;

e) введение новых подрядчиков, поставщиков или персонала.

[ГОСТ Р 53663—2009]

b) Намерение

Организация должна внедрять и поддерживать в рабочем состоянии мероприятия по обеспечению эффективного применения мер управления рисками, достижения политики и целей организации, исполнения задач в области менеджмента безопасности в соответствии с законодательными и другими требованиями, регламентирующими обеспечение безопасности и охраны.

c) Типовые входные данные

Типовые входные данные включают в себя:

- политику и цели в области менеджмента безопасности;
- результаты идентификации угроз и оценки рисков;
- применимые законодательные и другие требования, регламентирующие обеспечение безопасности и охраны.

d) Процесс

Организация должна внедрять процедуры по управлению идентифицированными рисками (включая риски, возникающие при взаимодействии с поставщиками, другими партнерами или операторами цепи поставок, а также посетителями). Следует документировать только те риски, реализация которых может привести к актам незаконного вмешательства или другим отклонениям от политики и целей в области менеджмента безопасности. Процедуры риска-менеджмента следует регулярно анализировать на адекватность и результативность. Изменения, идентифицированные как необходимые, следует внедрять в систему менеджмента безопасности.

В процедурах следует учитывать риски, возникающие на участках цепи поставок, контролируемых другими операторами, например, когда персонал организации непосредственно осуществляет свою деятельность на таких участках, что может потребовать проведения консультаций по вопросам обеспечения безопасности и охраны с такими операторами цепи поставок.

Ниже приведены некоторые примеры областей, в которых типичным образом возникают риски, а также примеры управления такими рисками.

1) Закупка или передача товаров и услуг и использование внешних ресурсов

Например:

- периодическое проведение оценки компетентности поставщиков по вопросам обеспечения безопасности;
- одобрение проектов оборудования или дооборудования техническими средствами охраны.

2) Формирование условий конфиденциальности самой деятельности

Например:

- определение условий конфиденциальности;
- предварительное определение и одобрение методов соблюдения конфиденциальности своей деятельности;
- предварительная оценка квалификации персонала для соблюдения конфиденциальности своей деятельности;
- процедуры контроля доступа в зоны осуществления деятельности, требующей конфиденциальности.

3) Обслуживание технических средств охраны

Например:

- введение ограничений и контроля доступа;
- проведение тестирования и технического обслуживания.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- процедуры;

- руководства по эксплуатации и техническому обслуживанию.

4.4.7 Готовность к действиям в чрезвычайных ситуациях, реагирование и восстановление безопасности

a) Требования

Организация должна разрабатывать, внедрять и поддерживать в рабочем состоянии соответствующие планы и процедуры по определению потенциала и степени реагирования на происшествия, связанные с безопасностью и чрезвычайными ситуациями, а также для предотвращения и смягчения вероятных последствий, которые могут быть связаны с ними. Планы и процедуры должны содержать сведения по обеспечению и обслуживанию любого идентифицированного оборудования, средства или услуги. Такие сведения могут потребоваться во время или после реализации акта незаконного вмешательства или чрезвычайной ситуации.

Организация должна периодически анализировать эффективность своей готовности к действиям в чрезвычайных ситуациях, а также планы и процедуры реагирования и восстановления безопасности. Это особенно важно после акта незаконного вмешательства или чрезвычайной ситуации, произошедших в результате нарушений в области охраны или реализации угрозы. Организация должна периодически подвергать проверке эти процедуры, оценивая их результативность.

[ГОСТ Р 53663—2009]

b) Намерение

Настоящий раздел затрагивает готовность, реагирование и восстановление после реализации акта незаконного вмешательства. Готовность к действиям в чрезвычайных ситуациях означает планирование, подготовку и предупреждающие действия, которые осуществляются вслед за актом незаконного вмешательства.

Организация должна активно оценивать угрозы и потребности реагирования по всем потенциальным актам незаконного вмешательства, определенным в процессе идентификации угроз и оценки рисков (см. 4.3.1). Для повышения эффективного реагирования организацией должны быть разработаны планы и процедуры реагирования, а также порядок действий в случае реализации акта незаконного вмешательства.

c) Типовые входные данные

Типовые входные данные включают в себя:

- идентификацию угроз и оценку рисков;

- наличие *региональных федеральных органов исполнительной власти,* осуществляющих свою деятельность в области обеспечения безопасности, а также подробные сведения о применимых мерах реагирования;

- законодательные, нормативные и другие требования;

- приобретенный опыт и анализ предыдущих актов незаконного вмешательства и чрезвычайных ситуаций, а также результаты последующих действий;

- положительный опыт, полученный другими подобными организациями после актов незаконного вмешательства и чрезвычайных ситуаций;

- данные о *федеральных органах исполнительной власти,* осуществляющих свою деятельность в области обеспечения безопасности;

- обзор проведенных учений и тренировок.

d) Процесс

Организация должна разрабатывать планы действий в чрезвычайных ситуациях, в которых должно быть определено и обеспечено проведение соответствующих мероприятий, а также предусмотрена регулярная проверка собственных способностей организации посредством проведения учений и тренировок. Планы готовности, реагирования и восстановления безопасности организации должны включать меры по восстановлению охраны, защите данных и оборудования, а также устойчивого обеспечения функционирования обеспечения безопасности и охраны.

Проведение учений и тренировок должно демонстрировать эффективность наиболее значимых разделов планов реагирования, а также завершенность процесса планирования. Наряду с теоретическими тренировками, которые могут быть полезны в процессе планирования, необходимо проводить практические учения. Результаты проведенных учений и тренировок должны анализироваться, а изменения в планы действий в чрезвычайных ситуациях, идентифицированные как необходимые, должны внедряться.

1) План реагирования и восстановления безопасности

Планы реагирования и восстановления безопасности должны содержать краткое описание действий в случае возникновения специфических ситуаций и включать в себя:

- идентификацию потенциальных актов незаконного вмешательства и чрезвычайных ситуаций;
- идентификацию лиц, принимающих на себя управление во время чрезвычайных ситуаций;
- подробные сведения о действиях персонала в чрезвычайной ситуации, включая действия сторонних лиц (подрядчиков, клиентов, посетителей), находящихся в зоне действия чрезвычайной ситуации, для которых может потребоваться эвакуация;
- ответственность, полномочия и обязанности персонала с определенными ролями в чрезвычайных ситуациях (например, персонал охраны, пожарной безопасности, персонал для оказания первой помощи, специалисты по радиоактивному или химическому заражению);
- процесс эвакуации;
- процессы, в которых описываются мероприятия по восстановлению условий безопасности и охраны в предельно короткие сроки;
- необходимые действия по идентификации, расположению и охране материалов, записей, данных и оборудования, имеющих отношение к обеспечению безопасности;
- взаимодействие с *федеральными органами исполнительной власти;*
- связь с заинтересованными лицами;
- информацию, необходимую во время чрезвычайных ситуаций, например схемы, данные по охране, процедуры, рабочие инструкции и данные по связи при оповещении;
- взаимодействие и связь с другими деловыми партнерами по цепи поставок;
- обеспечение целостности систем связи.

Привлечение сторонних организаций к планированию действий и реагированию в чрезвычайных ситуациях должно быть четко отражено в документах. Эти организации должны быть предупреждены о возможных обстоятельствах их участия и обеспечены всей необходимой информацией для содействия в подготовке планов участия в реагировании.

2) Технические средства охраны

Организация должна определять потребности в технических средствах охраны и обеспечивать их наличие в достаточном количестве. Технические средства охраны должны проходить периодическое тестирование и техническое обслуживание для обеспечения их постоянной пригодности.

3) Практические учения и тренировки

Практические учения и тренировки следует проводить согласно заранее установленным графикам. Где это возможно, должно поощряться проведение совместных учений с привлечением деловых партнеров по цепи поставок или *федеральных органов исполнительной власти.*

е) Типовые выходные данные

Типовые выходные данные включают в себя:

- документально оформленные планы и процедуры действий в чрезвычайных ситуациях при реагировании и восстановлении безопасности;
- перечень технических средств охраны;
- записи о проведенных проверках и тарировках технических средств охраны;
- проведение учений и тренировок;
- анализ проводимых учений и тренировок;
- выработку рекомендации по результатам проведенных анализов;
- улучшение вследствие внедрения рекомендаций;
- завершающие действия.

4.5 Проверка и корректирующие действия



Рисунок 5 — Проверка и корректирующие действия

4.5.1 Мониторинг и измерение функционирования безопасности

a) Требования

Организация должна разрабатывать и поддерживать в рабочем состоянии процедуры мониторинга и измерений показателей функционирования собственной системы менеджмента безопасности, а также процедуры мониторинга и измерений показателей функционирования самой безопасности. При установлении частоты оценки качества и мониторинга ключевых параметров работы организация должна учитывать угрозы и риски в отношении безопасности, включая потенциальные механизмы ее ухудшения и их последствия. Эти процедуры должны предусматривать:

a) оценку количественных и качественных измерений, отвечающих нуждам организации;

b) мониторинг области применения, в пределах которого должны реализовываться политика, цели и задачи в области менеджмента безопасности организации;

c) предварительные измерения показателей функционирования для мониторинга соответствия программ в области менеджмента безопасности критериям управления операциями, а также применимым законодательным, нормативным и другим требованиям, регламентирующим безопасность;

d) последующие измерения показателей функционирования для мониторинга ухудшений, относящихся к безопасности, произошедших сбоев, инцидентов, отказов (включая несрабатывания и ложные тревоги) и других случаев, свидетельствующих о недостатках в функционировании системы менеджмента безопасности;

e) записи данных по результатам измерений и мониторинга, достаточных для облегчения последующего анализа корректирующих и предупреждающих действий. Если для ведения мониторинга и/или измерений требуется специальное оборудование, организация должна разрабатывать и внедрять процедуры, связанные с калибровкой и обслуживанием такого оборудования. Записи по калибровкам, обслуживанию и результаты мониторинга следует хранить в течение достаточного времени в соответствии с нормативными требованиями и политикой организации.

[ГОСТ Р 53663—2009]

b) Намерение

Организация должна определять ключевые показатели результативности обеспечения безопасности и охраны как для всей организации в целом, так и для цепей поставок, которые управляются организацией или находятся в сфере ее влияния. Показатели должны быть измеримыми и демонстрировать:

- выполнение политики и достижение целей в области менеджмента безопасности;
- соответствующее управление и/или снижение уровня угроз безопасности и результативность эффективности применения контрмер;
- учет выводов и рекомендаций, полученных в ходе проведенных анализов чрезвычайных происшествий, актов незаконного вмешательства и сбоев в системе менеджмента безопасности;
- эффективность применения программ подготовки, осведомленности и оповещения персонала и заинтересованных лиц;
- продуктивность и применимость информации, используемой для анализа и улучшения системы менеджмента безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя:

- идентификацию угроз, оценку рисков и риск-менеджмент (см. 4.3.1);
- законодательные требования, нормативные акты, а также положительный опыт других организаций;
- политику и цели в области менеджмента безопасности;
- процедуру устранения несоответствий;
- записи о проверках, калибровках и тарировках технических средств охраны;
- записи о подготовке и обучении персонала;
- отчеты руководителей среднего звена.

d) Процесс

1) Пассивный и активный мониторинг

Система менеджмента безопасности организации должна объединять в себе пассивный и активный мониторинги:

- пассивный мониторинг следует использовать при проверке соответствия деятельности организации в области обеспечения безопасности и охраны, например контроль частоты и эффективности проведенных проверок по вопросам обеспечения безопасности;

- активный мониторинг следует использовать при проведении расследований, анализа и ведении записей о сбоях в системе менеджмента безопасности, в том числе чрезвычайных ситуаций и актов незаконного вмешательства.

Данные пассивного и активного мониторингов обычно используют при определении достижимости целей в области менеджмента безопасности.

2) Методы измерений

При измерении параметров обеспечения безопасности могут быть использованы:

- результаты процессов идентификации угроз, оценки рисков и риска-менеджмента, и их соответствия Рамочным стандартам безопасности и облегчения мировой торговли Всемирной таможенной организации [1] и требованиям программы США Таможенно-торговое партнерство против терроризма (С-ТРАТ) [2];

- проведение периодических проверок с использованием опросных листов;

- оценка новых цепей поставок логистических систем;

- анализ и оценка полученных схем логистики;

- проверка технических средств охраны на пригодность;

- эффективное привлечение персонала, обладающего признанным опытом или официальной квалификацией в области обеспечения безопасности и охраны;

- примеры поведения: оценка поведения персонала для выявления слабых мест в системе менеджмента безопасности, нуждающихся в корректировке;

- анализ документации и записей;

- сравнение собственного опыта внедрения и функционирования системы менеджмента безопасности с положительным опытом других организаций;

- опрос персонала для определения его отношения к выявлению лиц, вызывающих подозрение;

- обратная связь с заинтересованными лицами.

Организации необходимо принять решение о типе и частоте применимого мониторинга в зависимости от значимости рисков (см. 4.3.1). Графики проведения проверок, основанные на результатах идентификации угроз, оценки рисков и требованиях нормативных актов, должны быть подготовлены как часть системы менеджмента безопасности.

Мониторинг обеспечения безопасности процессов эксплуатации, логистических схем, деятельности деловых партнеров и цепей поставок следует осуществлять в соответствии с документально оформленными и утвержденными схемами мониторинга уполномоченным на то персоналом, который также может привлекаться к проведению выборочных проверок критических элементов обеспечения безопасности и охраны на соответствие требованиям системы менеджмента безопасности. При проведении мониторинга и выборочных проверок допускается использовать опросные листы.

3) Технические средства охраны

Инженерно-технические средства охраны, используемые для мониторинга и обеспечения безопасности, должны быть однозначно идентифицированы, внесены в реестр и находиться под контролем. Точность показаний технических средств должна быть известна. Там, где необходимо, организации должны обеспечивать наличие процедур, содержащих описание порядка проведения соответствующего мониторинга и измерений. Инженерно-технические средства, используемые для обеспечения безопасности и охраны, должны содержаться в пригодном состоянии и использоваться по назначению.

При необходимости для технических средств охраны должны быть разработаны и документально оформлены схемы проведения калибровок и технических осмотров. Такие схемы должны включать в себя:

- частоту проведения калибровок и технического обслуживания;

- ссылку на нормативный акт, в соответствии с которым осуществляют проверку;

- идентификационные данные измерительных устройств, используемых для калибровки;

- описание действий, предпринимаемых в случае выявления показаний, не соответствующих эксплуатационным.

Калибровку и техническое обслуживание следует проводить в соответствующих условиях. Для проведения сложных калибровок должны быть разработаны процедуры.

Измерительные устройства, используемые для калибровки, должны соответствовать метрологическим правилам и нормам.

Записи о результатах проведения калибровок и технического обслуживания должны поддерживаться в рабочем состоянии. Они также должны содержать подробные сведения об измерениях, сделанных как до, так и после проведения регулировок технических средств охраны.

Статус калибровок технических средств охраны должен четко идентифицироваться.

Технические средства охраны, статус калибровки и технического обслуживания которых неизвестен либо просрочен, должны быть запрещены к эксплуатации. Кроме того, такие средства должны быть изъяты из области эксплуатации либо соответствующим образом идентифицированы с целью предотвращения их непреднамеренного использования. Порядок такой идентификации должен быть задокументирован в процедурах. Процедуры также должны включать в себя порядок действий в случае обнаружения несоответствий, связанных с калибровкой и техническим обслуживанием средств охраны.

4) Инспектирование

i) оборудование

Должен быть составлен перечень всех инженерно-технических средств охраны. Их следует проверять в соответствии с установленными требованиями, и они должны быть включены в планы проведения инспекционных проверок.

ii) инспекционные проверки

Проведение инспекционных проверок не освобождает уполномоченный персонал от проведения регламентных работ по обслуживанию инженерно-технических средств охраны или проведения идентификации угроз.

iii) записи об инспекционных проверках

О каждой проведенной инспекционной проверке ведут соответствующие записи. Записи должны демонстрировать действительность соблюдения процедур, установленных системой менеджмента безопасности. Записи об инспекциях, осмотрах, проверках, а также проведенных аудитах системы менеджмента безопасности следует применять для выявления причин несоответствий и возникновения дублирования рисков. Следует применять любые необходимые предупреждающие действия. Уязвимые места и неисправности технических средств охраны, выявленные в период проведения инспекционной проверки, оформляют как несоответствие, которое устраняется в соответствии с процедурой управления несоответствующей продукцией *ГОСТ Р ИСО 9001*.

5) Технические средства охраны, эксплуатируемые подрядчиками

Технические средства охраны, эксплуатируемые подрядчиками, должны управляться так же, как и средства, эксплуатируемые персоналом организации. Подрядчик должен гарантировать, что эти средства охраны будут эксплуатироваться в соответствии с установленными в организации требованиями. Перед началом работ подрядчик предоставляет копии записей о проведении проверок и технического обслуживания тех технических средств охраны, для которых ведение таких записей обязательно. Если для работ с техническими средствами требуется соответствующая подготовка, то подрядчик также предоставляет записи о прохождении его персоналом такой подготовки для анализа.

6) Статистические или другие аналитические методики

Любые статистические или другие аналитические методики, используемые для оценки обеспечения безопасности, расследования актов незаконного вмешательства и нарушений режима охраны или для принятия решений, должны основываться на устойчивых научных принципах. Высшее руководство должно удовлетворять потребности в определении таких методик. При необходимости инструкции по их применению, в зависимости от сложившихся обстоятельств, должны быть документально оформлены.

е) Типовые выходные данные

Типовые выходные данные включают в себя:

- процедуры мониторинга эффективности мероприятий по обеспечению безопасности и охраны;
- планы инспекционных проверок и опросные листы;
- опросные листы проверок состояния инженерно-технических средств охраны;
- перечни инженерно-технических средств охраны;
- мероприятия и записи по калибровке;
- результаты деятельности по техническому обслуживанию;
- заполненные опросные листы, акты проведенных инспекционных проверок [выходные данные аудита системы менеджмента безопасности (см. 4.5.4)];
- акты о несоответствии;
- объективные доказательства внедрения таких процедур.

4.5.2 Оценка системы

a) Требования

Организация должна оценивать планы, процедуры и возможности менеджмента безопасности посредством периодических пересмотров, тестирований, анализа сообщений о происшествиях, связанных с охраной, полученных уроков, оценок работы и результатов учений. Существенные изменения в этих аспектах должны немедленно находить отражение в процедурах.

Организация должна периодически оценивать соответствие системы менеджмента безопасности применимым нормам и правилам, наилучшим производственным примерам, собственной политике и целям.

Организация должна вести соответствующие записи по учету результатов таких оценок.

[ГОСТ Р 53663—2009]

b) Намерение

Организация должна иметь эффективные процедуры для анализа и оценки планов обеспечения безопасности и охраны, а также своих способностей соответствовать достижению политики, целей и задач, установленных в области менеджмента безопасности. Также необходимо проводить периодический анализ соответствия деятельности организации применимым законодательным и другим нормативным требованиям.

Основной целью этих процедур является обеспечение поддержания документации системы менеджмента безопасности на современном уровне в соответствии с законодательными и другими требованиями в области обеспечения безопасности и охраны. Этот уровень должен учитывать положительный опыт внедрения систем менеджмента безопасности, а также любые изменения требований, регламентирующие обеспечение безопасности цепи поставок.

c) Типовые входные данные

Типовые входные данные включают в себя:

- сведения об актах незаконного вмешательства;
- результаты планирования и предупреждающих действий;
- сведения об идентификации угроз, оценке рисков и риска-менеджмента;
- отчеты аудитов системы менеджмента безопасности, включая акты несоответствий;
- сведения о чрезвычайных происшествиях;
- анализ со стороны руководства (см. 4.6);
- прогресс в достижении целей в области менеджмента безопасности;
- изменения законодательных требований, регламентирующих обеспечение безопасности и охраны;
- изменения потребностей заинтересованных лиц;
- изменения условий, размеров или инфраструктуры деятельности организации.

d) Процесс

Руководство организации через определенные интервалы времени должно проводить оценку своей системы менеджмента безопасности для демонстрации ее пригодности и результативности. Интервалы следует устанавливать таким образом, чтобы иметь возможность выявлять сбои в системе менеджмента безопасности прежде, чем они приведут к убыткам.

Результатом эффективного внедрения системы менеджмента безопасности является успешное достижение целей и претворение политики в области менеджмента безопасности при условии ее постоянного улучшения. Это один из основных принципов *ГОСТ Р 53663*. Необходимые для обеспечения этого процессы и процедуры приведены в 4.5.2.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- улучшенные процессы и деятельность;
- уменьшение количества несоответствий;
- соответствие существующим нормам и правилам;
- поддержание на современном уровне процессов идентификации угроз, оценки рисков и риска-менеджмента;
- демонстрацию оценки эффективности принятых корректирующих и предупреждающих действий.

4.5.3 Сбои, инциденты, несоответствия в отношении безопасности, корректирующие и предупреждающие действия

a) Требования

Организация должна разрабатывать, внедрять и поддерживать в рабочем состоянии процедуры по определению ответственности и полномочий в отношении:

a) оценки и принятия предупреждающих действий по определению потенциальных сбоев в системе безопасности для того, чтобы не допустить их;

b) расследований, связанных с безопасностью:

1) отказов, включая несрабатывания и ложные тревоги,

2) актов незаконного вмешательства и чрезвычайных ситуаций,

3) несоответствий;

c) принятия действий по смягчению последствий таких сбоев, происшествий или несоответствий;

d) инициирования и выполнения корректирующих действий;

e) подтверждения результативности принятых корректирующих действий.

Эти процедуры должны требовать анализа всех предложенных корректирующих и предупреждающих мер в части оценки угроз, отнесенных к охране, и рисков до их внедрения, за исключением случаев, когда требуется немедленное их принятие в интересах жизни людей или общественной безопасности.

Любое корректирующее или предупреждающее действие, предпринятое для устранения причины фактических и потенциальных несоответствий, должно быть адекватным величине проблемы и соразмерным тем угрозам и рискам, с проявлением которых может вероятно столкнуться менеджмент безопасности. Организация должна вести записи о любых изменениях в документируемых процедурах, являющихся результатом корректирующих и предупреждающих действий, а при необходимости должна предусмотреть проведение тренировок.

[ГОСТ Р 53663—2009]

b) Намерение

Организация должна обладать эффективными процедурами по анализу и проведению расследований сбоев системы менеджмента безопасности, актов незаконного вмешательства и чрезвычайных ситуаций. Основная цель этих процедур — предотвращение нежелательных ситуаций путем выявления и устранения причин их возникновения. Кроме того, эти процедуры должны позволять определять, анализировать и устранять потенциальные причины несоответствий, включая влияние человеческого фактора, ошибок и неисправностей технических средств охраны.

c) Типовые входные данные

Типовые входные данные включают в себя:

- общесистемные процедуры;
- планы действий в чрезвычайных ситуациях;
- идентификацию угроз, оценку рисков и риска-менеджмента;
- отчеты аудитов системы менеджмента безопасности, включая акты несоответствий;
- сведения об актах незаконного вмешательства и чрезвычайных случаях;
- сведения о проведенных технических осмотрах и калибровках инженерно-технических средств охраны.

d) Процесс

От организации потребуется разработка процедур, гарантирующих, что по каждому акту незаконного вмешательства и чрезвычайной ситуации будет проведено расследование и предприняты соответствующие предупреждающие или корректирующие действия. Процесс реализации корректирующих и предупреждающих действий следует контролировать, а результаты — анализировать на их эффективность.

1) Процедуры

В процедуры должно быть включено рассмотрение следующих вопросов:

i) основное

Процедура должна:

- определять ответственность и полномочия персонала, непосредственно связанного с обеспечением, оповещением, расследованием, доработкой и мониторингом корректирующих и предупреждающих действий;

- требовать обязательное уведомление по каждому несоответствию, акту незаконного вмешательства или чрезвычайному случаю;
- применяться ко всему персоналу (персоналу организации, подрядчикам, посетителям, другим лицам, вовлеченным в цепи поставок);
- учитывать влияние заинтересованных лиц;
- гарантировать персоналу отсутствие критики за предоставление сведений об актах незаконного вмешательства;
- четко определять действия, предпринимаемые после выявления несоответствия в системе менеджмента безопасности;

ii) немедленные действия

В случае идентификации несоответствия следует предпринимать немедленные действия по исправлению возможных актов незаконного вмешательства. Процедуры в этом отношении должны:

- определять порядок оповещения;
- иметь взаимосвязь с планами и процедурами действий в чрезвычайных ситуациях, где применимо;
- определять объем проведения расследования в зависимости от потенциальной или фактической угрозы (например, привлечение высшего руководства или руководителей среднего звена к расследованию значительных актов незаконного вмешательства);

iii) ведение записей

Для регистрации сведений о проведении и результатах предварительных и последующих расследований следует использовать соответствующие способы управления записями. Организация должна обеспечивать наличие в процедурах:

- ведения записи сведений о несоответствиях, актах незаконного вмешательства, чрезвычайных случаях;
- определения мест хранения и ответственности за хранение записей;

iv) расследование

В процедурах должен быть определен порядок проведения расследований и должны быть установлены:

- тип событий, подлежащих расследованию (например, события, приводящие к значительным угрозам);
- цели расследования;
- ответственность, требования к компетентности и перечень лиц, привлекаемых к ведению расследований (включая руководителей среднего звена, где это применимо);
- причины несоответствия;
- мероприятия по опросу свидетелей;
- подтверждающие материалы, такие как наличие видео-, фотокамер или других специальных средств;
- мероприятия по информированию о результатах проведенных расследований, включая информирование соответствующих заинтересованных лиц.

Расследование персонал должен начинать с предварительного анализа фактов во время сбора данных. Сбор данных и анализ следует проводить до тех пор, пока не будут установлены достаточно полные объяснения случившегося;

v) корректирующее действие

Корректирующее действие — это действие, предпринимаемое для определения причин несоответствия или акта незаконного вмешательства, и предупреждения повторного их возникновения. Процедуры по разработке и реализации корректирующего действия должны учитывать:

- идентификацию и внедрение корректирующих и предупреждающих как краткосрочных, так и долгосрочных мер (включая использование соответствующих источников информации, таких как рекомендации персонала охраны);
- оценку любого влияния на результаты идентификации угроз и оценки рисков (а также потребностей поддержания на современном уровне сведений об идентификации угроз, оценке рисков и риска-менеджмента);
- ведение записей о любых изменениях в процедурах, вызванных корректирующим действием, идентификациями угроз, оценками риска и риска-менеджмента;
- использование процессов риска-менеджмента или изменение существующих процедур риска-менеджмента для обеспечения эффективности предпринимаемых корректирующих действий;

vi) предупреждающее действие

Предупреждающее действие — это действие, предпринимаемое для предупреждения появления потенциальных несоответствий в области обеспечения безопасности и охраны.

Процедуры по разработке и реализации предупреждающего действия должны учитывать:

- использование соответствующих источников информации, таких как результаты корректирующих действий, тенденции возникновения актов незаконного вмешательства, сведения об аудитах системы менеджмента безопасности, обновленные оценки рисков, новая информация по обеспечению безопасности, рекомендации персонала охраны и т.д.;
- инициирование и внедрение предупреждающего действия, а также обеспечение контроля эффективности его реализации;
- ведение записей об одобрении изменений и изменениях в процедурах, вызванных предупреждающим действием;

vii) дополнение

Корректирующие или предупреждающие действия должны быть эффективными и практически реализуемыми. По каждому такому действию следует проводить проверку его эффективности. Случаи невыполнения или несоблюдения сроков следует докладывать высшему руководству в возможно короткие сроки.

2) Анализ несоответствий и актов незаконного вмешательства

Выявленные несоответствия и акты незаконного вмешательства должны периодически категорироваться и анализироваться для определения причин их возникновения. Частота и сложность анализа должна демонстрироваться заинтересованным по цепи поставок лицам.

При категорировании и анализе следует учитывать:

- частоту и сложность рассматриваемых происшествий;
- дату, время, место происшествия, а также деятельность, услугу или подразделение, затронутое происшествием;
- тип и степень или характер воздействия на средства, цепь поставок и т.д.;
- направленность и причины возникновения.

Особое внимание следует уделять актам незаконного вмешательства, которые могут рассматриваться как показатель угроз обеспечению безопасности или уязвимости охранных мероприятий.

Должны быть выработаны обоснованные выводы и корректирующие действия. Такой анализ следует довести до высшего руководства организации и должен быть включен в анализ обеспечения безопасности со стороны руководства (см. 4.6).

3) Мониторинг и оповещение результатов

Эффективность проведения расследований в области менеджмента безопасности и процесс оповещения результатов расследования следует подвергать оценке. Оценка должна быть объективной и по возможности иметь количественные показатели.

При оценке расследования организация должна:

- идентифицировать причины несоответствий в системе менеджмента безопасности и в системе менеджмента организации в целом, насколько это возможно;
- оповестить руководство и заинтересованных лиц о полученных данных и рекомендациях (см. 4.4.3);
- включать соответствующие полученные данные и рекомендации в непрерывный процесс анализа обеспечения безопасности;
- контролировать своевременное внедрение изменений в управлении и их дальнейшую эффективность;
- применять опыт, приобретенный в ходе расследований чрезвычайных ситуаций и актов незаконного вмешательства как для всей организации в целом, так и для подконтрольных цепей поставок. При этом необходимо концентрироваться на устранении принципиальных причин появления несоответствий, а не ограничиваться отдельными действиями по устранению схожих несоответствий в подобных частях организации.

4) Ведение записей

Ведение записей может быть быстрым с наименьшим формальным планированием или более сложным и рассчитанным на долгосрочные действия. Сопутствующая документация должна соответствовать уровню корректирующего действия.

Сведения и рекомендации следует направлять представителю руководства по безопасности для сбора и анализа (см. 4.5.4).

Записи проведения расследований актов незаконного вмешательства должны поддерживаться в рабочем состоянии. Такие записи могут потребоваться операторам цепи поставок.

е) Типовые выходные данные

Типовые выходные данные включают в себя:

- процедуру расследования актов незаконного вмешательства и чрезвычайных ситуаций;

- сведения о несоответствиях;
- журнал регистрации несоответствий;
- сведения о расследованиях;
- сведения об обновлении идентификации угроз, оценки рисков и риска-менеджмента;
- входные данные для анализа со стороны руководства;
- объективные доказательства проведения оценки эффективности корректирующих и предупреждающих действий.

4.5.4 Управление записями

a) Требования

Организация должна разрабатывать и поддерживать в рабочем состоянии ведение записей в объеме, необходимом для демонстрации соответствия собственной системы менеджмента безопасности требованиям стандарта, а также для демонстрации достигнутых результатов.

Организация должна разрабатывать, внедрять и поддерживать в рабочем состоянии процедуру(ы) идентификации, хранения, защиты, восстановления, сроков хранения и изъятия записей.

Записи должны оставаться четкими, легкоидентифицируемыми, опознаваемыми и прослеживаемыми.

Документация в электронном и цифровом форматах должна быть защищена от неумелого обращения, надежно поддерживаться и быть доступной только для уполномоченного персонала.

[ГОСТ Р 53663—2009]

b) Намерение

Ведение записей осуществляют для демонстрации свидетельств соответствия требованиям и результативности функционирования системы менеджмента безопасности. Записи должны быть определены, поддерживаться в рабочем состоянии, быть четкими, легкоидентифицируемыми и восстанавливаемыми.

c) Типовые входные данные

Записи, демонстрирующие соответствие требованиям, включают в себя:

- записи о подготовке и компетентности;
- сведения об инспекционных проверках обеспечения безопасности и охраны;
- записи о несоответствиях;
- результаты корректирующих и предупреждающих действий;
- сведения об аудитах системы менеджмента безопасности;
- протоколы совещаний по вопросам обеспечения безопасности и охраны;
- сведения о проведенных учениях и тренировках;
- анализ со стороны руководства;
- записи, касающиеся идентификации угроз, оценки рисков и риска-менеджмента.

d) Процесс

Требования *ГОСТ Р 53663* очевидны. Однако следует дополнительно рассмотреть:

- полномочия по распоряжению записями;
- обеспечение конфиденциальности записей;
- законодательные и другие требования в сфере сохранности записей;
- порядок ведения записей в электронном виде.

Записи должны быть четкими и легкоидентифицируемыми. Должно быть определено время их хранения. Записи следует хранить в безопасном месте, должны быть легковосстанавливаемыми и защищенными от износа. Важные записи должны быть защищены соответствующим образом от возможного пожара и других повреждений в соответствии с применимыми нормативными требованиями.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- процедуру управления записями;
- соответственно хранимые и легковосстановимые записи.

4.5.5 Аудит

a) Требования

Организация должна разрабатывать, внедрять и поддерживать в рабочем состоянии программу аудита менеджмента безопасности и обеспечивать проведение аудита через запланированные интервалы времени для того, чтобы:

a) определить, что система менеджмента безопасности:
   1) соответствует запланированным мероприятиям менеджмента безопасности, включая требования раздела 4,
   2) внедрена и поддерживается в рабочем состоянии,
   3) результативна в реализации политики и достижении целей в области менеджмента безопасности;
b) проанализировать результаты предыдущих аудитов и принятых корректирующих действий;
c) предоставить высшему руководству информацию о результатах аудита;
d) удостовериться в том, что технические средства охраны и персонал задействованы должным образом.

Программа аудита, включая график аудиторских проверок, должна основываться на результатах оценок угроз и рисков деятельности организации и результатах предыдущих аудиторских проверок. Процедуры аудита должны определять объем, частоту, методы проведения, компетенцию, ответственность, критерии к проведению аудита и отображению его результатов. Там, где возможно, аудит должен проводить персонал, не зависимый от тех лиц, которые несут непосредственную ответственность за проверяемую деятельность.

Примечание — Термин «независимый персонал» необязательно означает персонал, не относящийся к организации.

[ГОСТ Р 53663—2009]

b) Намерение

Внутренние аудиты следует проводить через запланированные интервалы времени для определения того, что система менеджмента безопасности внедрена результативно и поддерживается в рабочем состоянии; а также для предоставления высшему руководству сведений о соответствии всем требованиям *ГОСТ Р 53663* (*раздел 4*) и требованиям к системе менеджмента, разработанным организацией. Аудит также может осуществляться для определения способностей организации к постоянному улучшению. В целом в ходе проведения внутренних аудитов необходимо рассмотрение политики и целей в области менеджмента безопасности, а также состояния условий и процессов, затрагивающих цепи поставок.

Программа проведения внутренних аудитов должна позволять организации проводить анализ функционирования системы менеджмента безопасности на соответствие *ГОСТ Р 53663* и другим установленным требованиям в рамках своей деятельности. Запланированные аудиты следует проводить силами персонала организации или привлеченных специалистов для установления степени соответствия деятельности организации задокументированным процедурам, а также для оценки эффективности системы менеджмента по достижению целей в области менеджмента безопасности. Персонал, проводящий аудиты системы менеджмента безопасности, должен обеспечивать объективность и беспристрастность процесса аудита.

Примечание — Внутренний аудит системы менеджмента безопасности фокусируется на функционировании системы менеджмента безопасности. Вместе с тем такой аудит не следует путать с проведением анализов, оценок и других инспекторских проверок обеспечения безопасности и охраны.

c) Типовые входные данные

Типовые входные данные включают в себя:
- политику в области менеджмента безопасности;
- цели в области менеджмента безопасности;
- процедуры и руководства, касающиеся обеспечения безопасности и охраны;
- результаты идентификации угроз, оценки рисков и риск-менеджмента;
- нормативные требования и положительный опыт;
- сведения о несоответствиях;
- процедуры проведения аудита системы менеджмента безопасности;
- компетентных, независимых, внутренних/внешних аудиторов;
- процедуры управления несоответствиями;
- учения и тренировки по обеспечению безопасности и охраны;
- информацию об угрозах от внешних источников.

d) Процесс

1) Аудиты системы менеджмента безопасности

Аудит дает всестороннюю и документально оформленную оценку соответствия деятельности организации установленным процедурам и методам.

Аудит следует проводить в соответствии с установленным планом. Дополнительные аудиты проводят в зависимости от сложившихся обстоятельств, например после инцидентов, повлиявших на систему менеджмента безопасности, изменений деятельности организации, инженерно-технических средств охраны или размеров цепи поставок.

Аудит должен проводить только компетентный, независимый персонал, который прошел соответствующую проверку на допуск для работы в проверяемых областях.

Выходные данные аудита должны включать в себя подробную оценку эффективности процедур обеспечения безопасности и охраны, уровень их соответствия фактической деятельности и, при необходимости, определять корректирующие действия. Записи о результатах проведенных аудитов должны поддерживаться в рабочем состоянии и своевременно доводиться до высшего руководства.

Примечание — Основные принципы и методы, изложенные в *ГОСТ Р ИСО 19011*, применимы при проведении аудитов системы менеджмента безопасности.

2) Планирование

График проведения внутренних проверок следует планировать на ежегодной основе. Аудит должен охватывать всю деятельность организации, затрагиваемую системой менеджментов безопасности, и оценивать ее соответствие *ГОСТ Р 53663*.

Частоту и объемы проводимых аудитов следует планировать с учетом рисков, связанных с различными элементами системы менеджмента безопасности, существующими сведениями о функционировании системы, выходными данными анализа со стороны руководства, а также области применения системы менеджмента безопасности, в пределах которой она может изменяться.

Основанием к проведению внеочередных, незапланированных аудитов может быть, например, реализация акта незаконного вмешательства.

3) Содействие руководства

Для обеспечения эффективного внедрения и результативного проведения аудитов необходимо тесное участие со стороны высшего руководства организации. Высшее руководство должно учитывать выводы и рекомендации, выработанные в ходе аудита, и предпринимать соответствующие действия по мере необходимости в соответствующие сроки. Аудиты следует проводить в строгом соответствии с установленными планами. Персонал должен быть проинформирован о целях и актуальности проводимых аудитов. Во время проведения аудита аудируемый персонал должен оказывать полное содействие в предоставлении необходимых сведений и данных.

4) Аудиторы

Аудит может проводиться одним или несколькими аудиторами. Командный подход поможет расширить рамки участия и улучшить сотрудничество, а также позволит использовать более широкий диапазон необходимых навыков и знаний.

Выбор аудиторов должен обеспечивать объективность и беспристрастность процесса аудита. Аудиторы не должны проверять свою собственную работу, а при необходимости должны получать допуск для проведения аудита таких работ.

Аудитор должен четко понимать свои задачи и быть достаточно компетентным для их выполнения. Он должен обладать опытом и знаниями соответствующих нормативных правовых актов, регламентирующих обеспечение безопасности и охраны, достаточными для ведения аудита, оценки функционирования системы менеджмента безопасности и идентификации несоответствий. Кроме того, аудитор должен быть осведомлен и иметь доступ к процедурам и руководствам, касающимся проверяемой деятельности.

5) Сбор и толкование данных

Способы, используемые при сборе информации о функционировании системы менеджмента безопасности, зависят от характера проводимых аудитов. Аудит должен обеспечивать получение объективных свидетельств осуществления соответствующих действий и опрос персонала (при необходимости — персонала подрядчика), непосредственно связанного с обеспечением безопасности и охраны организации. Соответствующую документацию следует проверять, к ней может относиться:

- документация системы менеджмента безопасности;
- политика в области менеджмента безопасности;
- цели в области менеджмента безопасности;
- результаты проводимых учений и тренировок;
- процедуры;
- протоколы совещаний по вопросам обеспечения безопасности и охраны;
- любые сведения, полученные от *федеральных органов исполнительной власти*;
- перечни и планы;
- записи о подготовках персонала;
- результаты предыдущих аудитов системы менеджмента безопасности;
- сведения о корректирующих действиях;
- сведения о несоответствиях.

Для исключения возможности неправильного использования или толкования собранных при проведении аудита сведений в процедуру проведения внутренних аудитов организации должна быть включена обязательная проверка получаемой информации на объективность, непротиворечивость и адекватность.

6) Результаты аудита

Содержание акта о результатах внутреннего аудита системы менеджмента безопасности организации должно быть понятным, точным и завершенным. Акт должен содержать дату и подпись аудитора и в зависимости от обстоятельств содержать:

- цели и объемы аудита;
- сведения о плане проведения аудита, информацию о членах комиссии и аудируемом персонале, даты проведения и наименование подразделений;
- сведения о деятельности или услугах, подвергаемых аудиту;
- ссылки на документы, на соответствие требований которых проводился аудит;
- сведения о выявленных несоответствиях;
- оценку аудитором степени соответствия *ГОСТ Р 53663*;
- способность системы менеджмента безопасности достигать установленные цели в области менеджмента безопасности;
- адресаты рассылки копий акта о результатах внутреннего аудита системы менеджмента безопасности.

Результаты аудита следует доводить до всех лиц, имеющих к этому отношение, в возможно короткие сроки для обеспечения принятия корректирующих действий. Должен быть подготовлен план совместных корректирующих действий с указанием ответственных лиц, сроков и способов доклада об исполнении. Для обеспечения гарантий успешного внедрения рекомендаций следует применять меры мониторинга.

Руководство должно проанализировать результаты и, при необходимости, предпринять эффективные корректирующие действия.

В дальнейшем может потребоваться проведение внепланового аудита для анализа эффективности предпринятых корректирующих действий.

При ведении записей, связанных с проведением внутренних аудитов системы менеджмента безопасности, должен соблюдаться режим конфиденциальности.

е) Типовые выходные данные

Типовые выходные данные включают в себя:

- план/программу аудита системы менеджмента безопасности;
- процедуру проведения внутренних аудитов системы менеджмента безопасности;
- акт о результатах внутреннего аудита системы менеджмента безопасности, включая сведения о несоответствиях, выводах, рекомендациях и корректирующих действиях;
- сведения об устранении выявленных несоответствий;
- объективное свидетельство доведения до высшего руководства результатов аудита системы менеджмента безопасности.

4.6 Анализ со стороны руководства и постоянное улучшение



Рисунок 6 — Анализ со стороны руководства

a) Требования

Высшее руководство должно анализировать систему менеджмента безопасности организации с запланированной периодичностью с тем, чтобы обеспечивать ее постоянную пригодность, адекватность и результативность. Анализ должен включать оценку возможностей по улучшению и потребностей в изменениях системы менеджмента безопасности, включая политику и цели в области менеджмента безопасности, а также угрозы и риски. Записи по анализам со стороны руководства следует сохранять. Анализ со стороны руководства должен учитывать:

a) результаты аудита и оценок соответствия законодательным и иным требованиям, предписанным для организации;

b) сообщения от внешних заинтересованных сторон, включая жалобы;

c) исполнительность в выполнении мер по обеспечению безопасности организации;

d) сроки достижения целей и выполнения задач;

e) статус корректирующих и предупреждающих действий;

f) действия, последовавшие после предыдущего анализа менеджмента;

g) изменяющиеся обстоятельства, включая развитие нормативных и иных требований, регламентирующих обеспечение безопасности в отношении организации;

h) рекомендации по улучшению.

Результаты анализа со стороны руководства должны включать в себя любые решения и действия, относящиеся к возможным изменениям в политике, целях, задачах и других элементах системы менеджмента безопасности, согласующиеся с обязательством постоянного улучшения.

[ГОСТ Р 53663—2009]

b) Намерение

Высшее руководство должно анализировать систему менеджмента безопасности с целью обеспечения ее постоянной пригодности, достаточности и результативности в эффективном проведении заявленной политики и достижения целей в области менеджмента безопасности.

В ходе анализа также следует рассматривать соответствие существующей политики. Она должна позволять устанавливать новые или пересматривать существующие цели для обеспечения постоянного улучшения и определять потребности в изменениях системы менеджмента безопасности.

c) Типовые входные данные

Типовые входные данные включают в себя:

- сведения о результатах внутреннего и внешнего аудитов системы менеджмента безопасности;
- корректирующие действия, вытекающие из предыдущих анализов со стороны руководства;
- сведения о проведенных учениях и тренировках;
- сведения от представителя руководства по безопасности о функционировании системы менеджмента безопасности в целом;
- сведения, полученные от других организаций или заинтересованных лиц, об эффективности системы менеджмента безопасности, влияющие на цепь поставок;
- сведения о процессах идентификации угроз, оценки рисков и риска-менеджмента;

- эффективность программ подготовки и ознакомления;
- статус и эффективность целей в области менеджмента безопасности.

d) Процесс

Процесс анализа со стороны руководства обычно включает проведение совещаний высшим руководством через запланированные интервалы времени. Анализ должен фокусироваться на функционировании системы менеджмента безопасности в целом, а не на отдельных деталях системы, управление которыми возможно в рамках существующей системы менеджмента безопасности.

При планировании совещания по анализу со стороны руководства следует уделять внимание:

- темам для рассмотрения;
- участникам совещания (руководителям среднего звена, персоналу службы охраны, другому персоналу);
- ответственности отдельных участников в связи с проводимым анализом;
- используемой для анализа информации.

Совещание по анализу должно охватывать:

- пригодность текущей политики в области менеджмента безопасности;
- установление или пересмотр целей в области менеджмента безопасности для постоянного улучшения в предстоящий период;
- адекватность существующих процессов идентификации угроз, оценки рисков и риска-менеджмента;
- существующий уровень рисков и эффективность мер управления ими;
- достаточность ресурсов;
- результативность процесса инспекторских проверок;
- результативность процесса оповещения;
- сведения об актах незаконного вмешательства и чрезвычайных случаях;
- зарегистрированные примеры неэффективности процедур;
- результаты внутреннего и внешнего аудитов системы менеджмента безопасности, проведенных после предыдущего анализа со стороны руководства, и их эффективность;
- статус готовности к действиям в чрезвычайных ситуациях и мер восстановления безопасности;
- улучшения системы менеджмента безопасности;
- выходные данные проведенных расследований актов незаконного вмешательства и чрезвычайных случаев;
- оценку влияния предполагаемых изменений в законодательных нормативных актах и технологиях или сведениях и информации.

Высшее руководство должно гарантировать, что на совещании была доведена вся информация, касающаяся функционирования системы менеджмента безопасности. При необходимости возможно проведение анализа функционирования отдельных частей системы менеджмента безопасности с меньшими интервалами времени проведения.

Анализ со стороны руководства может включать анализ интегрированной системы менеджмента; при этом выходные данные анализа систем менеджмента безопасности, качества *ГОСТ Р ИСО 9001*, экологии *ГОСТ Р ИСО 14001* и других систем менеджмента могут рассматриваться на том же совещании или в ходе схожего процесса. В случае принятия такого подхода, необходимо исключать принижение важности любой из составных частей интегрированной системы менеджмента организации.

e) Типовые выходные данные

Типовые выходные данные включают в себя:

- протокол проведенного совещания по анализу;
- обновление политики и целей в области менеджмента безопасности;
- определение ответственных за реализацию корректирующих действий с установлением сроков их выполнения;
- определение ответственных за улучшение с установлением сроков их выполнения;
- даты анализа результативности проведенных корректирующих действий;
- области, которые следует выделять при планировании будущего внутреннего аудита системы менеджмента безопасности.

Приложение А
(справочное)

Сопоставление структуры настоящего стандарта со структурой *ГОСТ Р ИСО 14001:2007* и *ГОСТ Р ИСО 9001:2008*

Таблица А.1

Структура настоящего стандарта		Структура *ГОСТ Р ИСО 14001:2007*		Структура *ГОСТ Р ИСО 9001:2008*	
Требования к системе менеджмента безопасности цепи поставок (только заглавие)	4	Требования к системе управления окружающей средой (только заглавие)	4	Требования к системе менеджмента качества (только заглавие)	4
Общие требования	4.1	Общие требования	4.1	Общие требования	4.1
Политика в области менеджмента безопасности	4.2	Экологическая политика	4.2	Обязательство руководства Политика в области качества Постоянное улучшение	5.1 5.3 8.5.1
Оценка рисков безопасности и планирование (только заглавие)	4.3	Планирование (только заглавие)	4.3	Планирование (только заглавие)	5.4
Оценка рисков безопасности	4.3.1	Экологические аспекты	4.3.1	Ориентация на потребителя Определение требований, относящихся к продукции Анализ требований, относящихся к продукции	5.2 7.2.1 7.2.2
Законодательные нормативные и прочие требования к обеспечению безопасности	4.3.2	Требования законодательных актов и другие требования	4.3.2	Ориентация на потребителя Определение требований, относящихся к продукции	5.2 7.2.1
Цели в области менеджмента безопасности	4.3.3	Цели, задачи и программы	4.3.3	Цели в области качества Планирование создания и развития системы менеджмента качества Постоянное улучшение	5.4.1 5.4.2 8.5.1
Задачи в области менеджмента безопасности	4.3.4	Цели, задачи и программы	4.3.3	Цели в области качества Планирование создания и развития системы менеджмента качества Постоянное улучшение	5.4.1 5.4.2 8.5.1
Программы в области менеджмента безопасности	4.3.5	Цели, задачи и программы	4.3.3	Цели в области качества Планирование создания и развития системы менеджмента качества Постоянное улучшение	5.4.1 5.4.2 8.5.1
Внедрение и функционирование (только заглавие)	4.4	Внедрение и функционирование (только заглавие)	4.4	Процессы жизненного цикла продукции (только заглавие)	7
Структура, полномочия и ответственность в менеджменте безопасности	4.4.1	Ресурсы, роли, ответственность и полномочия	4.4.1	Обязательства руководства Ответственность и полномочия Представитель руководства Обеспечение ресурсами Инфраструктура	5.1 5.5.1 5.5.2 6.1 6.3
Компетентность, подготовка и осведомленность	4.4.2	Компетентность, подготовка и осведомленность	4.4.2	(Человеческие ресурсы) Общие положения Компетентность, осведомленность и подготовка	6.2.1 6.2.2

Продолжение таблицы А.1

Структура настоящего стандарта		Структура *ГОСТ Р ИСО 14001:2007*		Структура *ГОСТ Р ИСО 9001:2008*	
Связь	4.4.3	Связь	4.4.3	Внутренний обмен информацией Связь с потребителями	5.5.3 7.2.3
Документация	4.4.4	Документирование	4.4.4	(Требования к документации) Общие положения	4.2.1
Управление документами и данными	4.4.5	Управление документацией	4.4.5	Управление документацией	4.2.3
Управление операциями	4.4.6	Управление операциями	4.4.6	Планирование процессов жизненного цикла продукции Определение требований, относящихся к продукции Анализ требований, относящихся к продукции Планирование проектирования и разработки Входные данные для проектирования и разработки Выходные данные проектирования и разработки Анализ проекта и разработки Верификация проекта и разработки Валидация проекта и разработки Управление изменениями проекта и разработки Процесс закупок Информация по закупкам Верификация закупленной продукции Управление производством и обслуживанием Валидация процессов производства и обслуживания Сохранение соответствия продукции	7.1 7.2.1 7.2.2 7.3.1 7.3.2 7.3.3 7.3.4 7.3.5 7.3.6 7.3.7 7.4.1 7.4.2 7.4.3 7.5.1 7.5.2 7.5.5
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
Проверка и корректирующие действия (только заглавие)	4.5	Проверка (только заглавие)	4.5	Измерение, анализ и улучшения (только заглавие)	8
Мониторинг и измерение функционирования безопасности	4.5.1	Мониторинг и измерения	4.5.1	Управление устройствами для мониторинга и измерений Общие положения (Измерение, анализ и улучшение) Мониторинг и измерение процессов Мониторинг и измерение продукции Анализ данных	7.6 8.1 8.2.3 8.2.4 8.4
Оценка системы	4.5.2	Оценка соответствия	4.5.2	Мониторинг и измерение процессов Мониторинг и измерение продукции	8.2.3 8.2.4

Окончание таблицы А.1

Структура настоящего стандарта		Структура *ГОСТ Р ИСО 14001:2007*		Структура *ГОСТ Р ИСО 9001:2008*	
Сбои, инциденты, несоответствия в отношении безопасности и корректирующие и предупреждающие действия	4.5.3	Несоответствия, корректирующие и предупреждающие действия	4.5.3	Управление несоответствующей продукцией Анализ данных Корректирующие действия Предупреждающие действия	8.3 8.4 8.5.2 8.5.3
Управление записями	4.5.4	Управление записями	4.5.4	Управление записями	4.2.4
Аудит	4.5.5	Внутренний аудит	4.5.5	Внутренний аудит	8.2.2
Анализ со стороны руководства и постоянное улучшение	4.6	Анализ со стороны руководства	4.6	Обязательства руководства Анализ со стороны руководства (только заглавие) Общие положения Входные данные для анализа Выходные данные анализа Постоянное улучшение	5.1 5.6 5.6.1 5.6.2 5.6.3 8.5.1

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО 9001—2008	IDT	ИСО 9001:2008 «Системы менеджмента качества. Требования»
ГОСТ Р ИСО 14001—2007	IDT	ИСО 14001:2004 «Системы экологического менеджмента. Требования и руководство по применению»
ГОСТ Р ИСО 19011—2003	IDT	ИСО 19011:2002 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] SAFE Framework of Standards, WCO, 2007 (Рамочные стандарты безопасности и облегчения мировой торговли Всемирной таможенной организации)

[2] Customs-Trade Partnership Against Terrorism, C-TPAT (Программа США Таможенно-торговое партнерство против терроризма)

УДК 656.614.3.004:006.354 ОКС 13.310, 47.020.99 Т51

Ключевые слова: менеджмент безопасности, цепь поставок, программы и задачи в области менеджмента безопасности, угрозы, риск-менеджмент

Редактор *Р.Г. Говердовская*
Технический редактор *В.Н. Прусакова*
Корректор *Т.И. Кононенко*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 09.07.2010. Подписано в печать 29.07.2010. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 5,12. Уч.-изд. л. 5,10. Тираж 191 экз. Зак. 608.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru