ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53663— 2009 (ИСО 28000:2005)

Система менеджмента безопасности цепи поставок

ТРЕБОВАНИЯ

ISO 28000:2005
Specification for security management system for the supply chain
(MOD)

Издание официальное

БЗ 5—2009/236

Москва
Стандартинформ
2010

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. № 1028-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО 28000:2005 «Технические условия на системы менеджмента безопасности в цепочке поставок» (ISO 28000:2005 «Specification for security management system for the supply chain») 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—2004 (пункт 3.5).

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

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 1
3 Термины и определения 2
4 Элементы системы менеджмента безопасности 3
4.1 Общие требования 3
4.2 Политика в области менеджмента безопасности 3
4.3 Оценка рисков безопасности и планирование 4
4.4 Внедрение и функционирование 5
4.5 Проверка и корректирующие действия 8
4.6 Анализ со стороны руководства и постоянное улучшение 9
Приложение А (справочное) Сопоставление структуры настоящего стандарта со структурой ГОСТ Р ИСО 14001—2007 и ГОСТ Р ИСО 9001—2008 10
Приложение ДА (обязательное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 13

Введение

Настоящий стандарт подготовлен в ответ на спрос промышленности на стандарт менеджмента безопасности. Его конечная цель состоит в том, чтобы улучшить безопасность цепей поставок. Стандарт менеджмента высокого уровня, который позволяет организации установить систему менеджмента безопасности для всей цепи поставок.

Это потребует от организации проводить анализ обстановки, в которой она осуществляет свою деятельность, на предмет определения адекватности принимаемых мер охраны, а также наличия других регламентирующих безопасность требований, которым должна соответствовать организация. Если в процессе такого анализа обнаруживаются потребности в части улучшения охраны, организация должна задействовать методики и процедуры для удовлетворения таких потребностей.

Поскольку цепи поставок несут динамический характер, некоторые организации, управляющие многочисленными цепями поставок, могут принимать во внимание соответствие услуг, предоставляемых поставщиками, национальным стандартам безопасности или стандартам Международной организации по стандартизации в области безопасности как условие включения их в собственную систему менеджмента безопасности цепи поставок (см. рисунок 1).

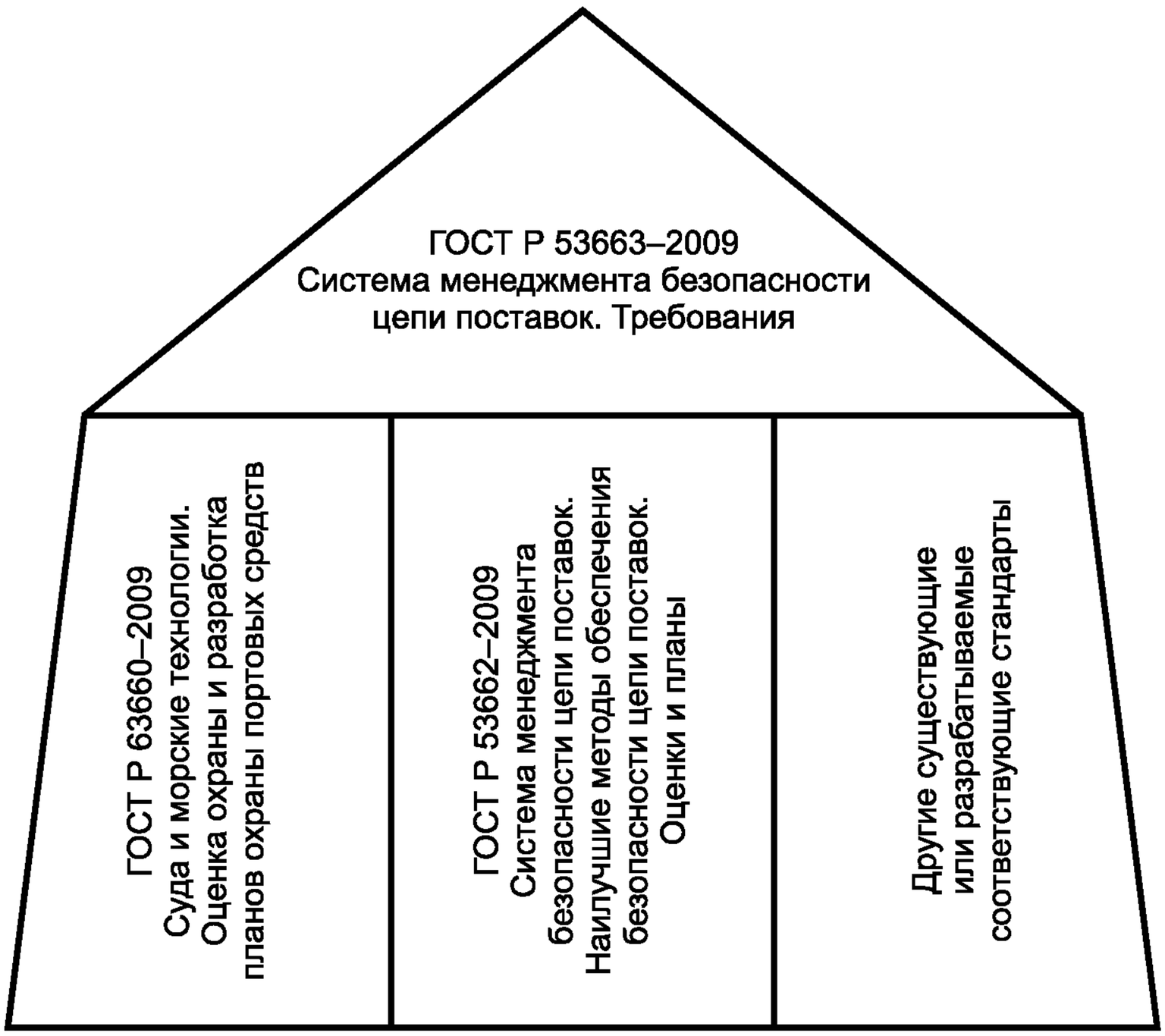

Рисунок 1 — Соотношение между настоящим стандартом и другими соответствующими стандартами

Данные требования предназначены для применения в тех случаях, когда организации требуется надежный менеджмент цепей поставок. Официальный подход к менеджменту безопасности может непосредственно способствовать деловым возможностям организации и доверию к ней.

Соответствие требованиям не освобождает от юридических обязательств. По желанию организации соответствие своей системы менеджмента безопасности положениям данных требований может быть проверено в процессе внешнего или внутреннего аудита.

Эти требования основаны на формате Международной организации по стандартизации, принятом как ГОСТ Р ИСО 14001—2007, который предусматривает подход к системам менеджмента на основе риска. Однако организации, которые приняли последовательный подход к системам менеджмента

(например, ГОСТ Р ИСО 9001—2008), могут использовать существующую систему менеджмента как фундамент для внедрения системы менеджмента безопасности, изложенные в данных требованиях.

Данные требования не призваны дублировать требования *федеральных органов исполнительной власти* и стандарты относительно менеджмента безопасности цепи поставок, по которым организация была уже сертифицирована или проверена на соответствие. Такая проверка может быть выполнена приемлемой организацией первой, второй или третьей стороны.

Примечание — Эти требования основываются на методологии, известной как цикл «Plan — Do — Check — Act» (PDCA). Цикл PDCA можно описать следующим образом:

- планирование (plan) — определение целей и порядка действий, необходимых для достижения результатов, соответствующих политике организации в области безопасности;
- осуществление (do) — реализация запланированных процессов;
- проверка (check) — мониторинг и измерение процессов в сравнении с политикой, целями, нормативными и иными регламентирующими безопасность требованиями и сообщений о результатах;
- действие (act) — проведение мероприятий, направленных на постоянное улучшение работы системы менеджмента безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система менеджмента безопасности цепи поставок

ТРЕБОВАНИЯ

Security management system for the supply chain.
Requirements

Дата введения — 2010—05—01

1 Область применения

Настоящий 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;

c) 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.

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.*

Издание официальное

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.

3.10 **высшее руководство** (top management): Лицо или группа лиц, руководящих и контролирующих работу организации на высшем уровне.

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

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

4 Элементы системы менеджмента безопасности

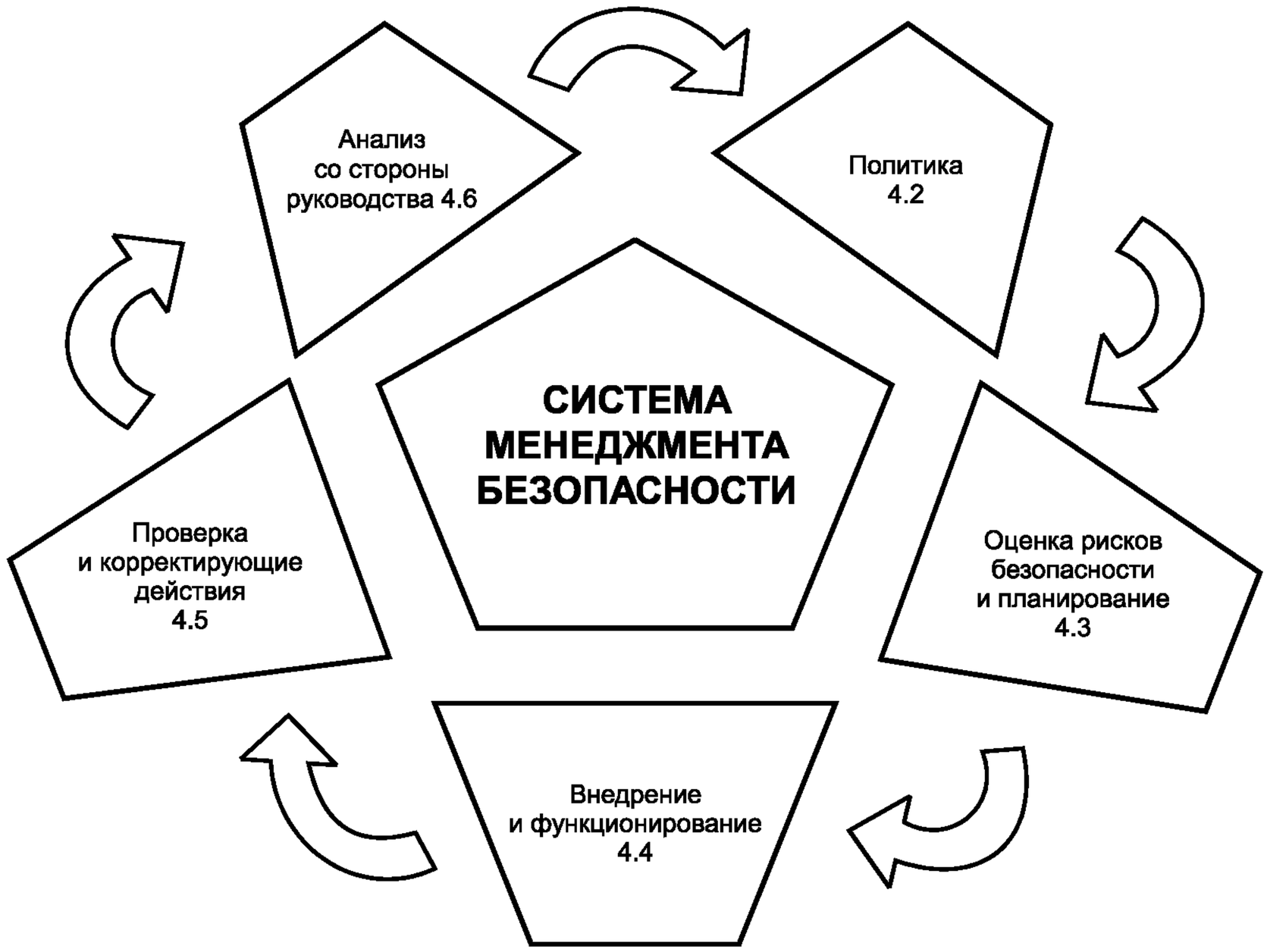

Рисунок 2 — Элементы системы менеджмента безопасности

4.1 Общие требования

Элементы менеджмента безопасности приведены на рисунке 2.

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.

4.2 Политика в области менеджмента безопасности

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 выбирать 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.

4.3 Оценка рисков безопасности и планирование

4.3.1 Оценка рисков безопасности

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 определять результативность и своевременность их выполнения (см. 4.5.1).

4.3.2 Законодательные, нормативные и прочие требования к обеспечению безопасности

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.

4.3.3 Цели в области менеджмента безопасности

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.

4.3.4 Задачи в области менеджмента безопасности

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.

4.3.5 Программы в области менеджмента безопасности

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:

a) 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.

4.4 Внедрение и функционирование

4.4.1 Структура, полномочия и ответственность в менеджменте безопасности

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.

4.4.2 Компетентность, подготовка и осведомленность

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;

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

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

4.4.3 Связь

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.

4.4.4 Документация

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.

4.4.5 Управление документами и данными

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.

4.4.6 Управление операциями

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.

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

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.

4.5 Проверка и корректирующие действия

4.5.1 Мониторинг и измерение функционирования безопасности

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.

4.5.2 Оценка системы

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.

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

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.

4.5.4 Управление записями

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.

4.5.5 Аудит

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, независимый от тех лиц, которые несут непосредственную ответственность за проверяемую деятельность.

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

4.6 Анализ со стороны руководства и постоянное улучшение

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.

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
(обязательное)

Сведения о соответствии ссылочных национальных и межгосударственных 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.		

УДК 656.614.3.004:006.354 ОКС 13.310 47.020.99 Т 51

Ключевые слова: менеджмент безопасности, цепь поставки, оценка рисков безопасности, угрозы, риски

Редактор *Р.Г. Говердовская*
Технический редактор *В.Н. Прусакова*
Корректор *М.С. Кабашова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 09.07.2010. Подписано в печать 26.07.2010. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 2,32. Уч.-изд. л. 1,80. Тираж 171 экз. Зак. 605.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.