ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53662— 2009 (ИСО 28001:2006)

Система менеджмента безопасности цепи поставок

НАИЛУЧШИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Оценки и планы

ISO 28001:2006
Security management systems for the supply chain — Best practices for implementing supply chain security — Assessments and plans
(MOD)

Издание официальное

БЗ 5—2009/222

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 от 15 декабря 2009 г. № 1027-ст

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 1027-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО 28001:2006 «Системы менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности цепи поставок. Оценки и планы». (ISO 28001:2006 «Security management systems for the supply chain — Best practices for implementing supply chain security — Assessments and plans») 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 (раздел 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 D

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 Основные положения . . . 4
4.1 Паспорт участка цепи поставок . . . 4
4.2 Деловые партнеры . . . 4
4.3 Свидетельства о соответствии, принятые в международной практике . . . 4
4.4 Деловые партнеры, освобождаемые от предъявления Декларации об охране . . . 5
4.5 Анализ состоятельности обеспечения безопасности деловых партнеров . . . 5
5 Процесс обеспечения безопасности и охраны цепи поставок . . . 5
5.1 Общие положения . . . 5
5.2 Определение масштабов оценки уязвимости (охраны) . . . 5
5.3 Проведение оценки уязвимости (охраны) . . . 5
5.4 Разработка Плана обеспечения безопасности (охраны) цепи поставок . . . 6
5.5 Реализация Плана обеспечения безопасности (охраны) цепи поставок . . . 6
5.6 Документирование и мониторинг процессов обеспечения безопасности и охраны цепи поставок . . . 6
5.7 Меры, принимаемые после реализации акта незаконного вмешательства . . . 7
5.8 Защита информации по обеспечению безопасности и охраны . . . 7
Приложение А (справочное) Процесс обеспечения безопасности и охраны цепи поставок . . . 8
Приложение В (справочное) Методика проведения оценки рисков и выработки контрмер . . . 14
Приложение С (справочное) Руководство по оказанию помощи и сертификации . . . 20
Приложение D (обязательное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте . . . 21
Библиография . . . 21

Введение

Акты незаконного вмешательства, направленные против цепи поставок, создают угрозу торговым отношениям и экономической стабильности страны. Население, товары, объекты транспортной инфраструктуры, включая транспортные средства, должны защищаться от актов незаконного вмешательства и их потенциальных воздействий. Такая защищенность способствует развитию экономики и общества в целом.

Высокодинамические международные цепи поставок включают в себя множество организаций и деловых партнеров. Принимая во внимание всю сложность существующих цепей поставок, настоящий стандарт позволяет применять требования в отношении обеспечения безопасности и охраны для отдельных организаций, согласуясь с характерными особенностями, деловыми обязанностями и функциями во всей цепи поставок.

Стандарт — выбор для организаций в применении и документировании разумного уровня обеспечения безопасности и охраны в пределах цепи поставок и их узловых элементов, а также в принятии обоснованных решений по предотвращению угроз и уменьшению рисков.

Стандарт мультимодален и призван взаимодействовать с Рамочными стандартами безопасности и облегчения мировой торговли [1] Всемирной таможенной организации. Он не является попыткой замены или вытеснения существующих требований в области таможенного законодательства.

Требования настоящего стандарта применяются на добровольной основе. Стандарт помогает организациям в установлении адекватного уровня обеспечения безопасности и охраны в пределах контролируемого организацией участка цепи поставок. Стандарт может использоваться органами по сертификации при проведении аудитов на соответствие существующего уровня обеспечения безопасности и охраны и выдаче необходимых документов организациям, которые заявляют о своем соответствии требованиям настоящего стандарта. Клиенты, деловые партнеры, а также федеральные органы исполнительной власти могут потребовать от организации подтверждения соответствия их системы менеджмента обеспечения безопасности и охраны требованиям настоящего стандарта. При проведении аудитов третьей стороной следует принимать во внимание аккредитацию органов по сертификации, упомянутую в приложении С.

Результатом применения настоящего стандарта является следующее:

- Паспорт участка цепи поставок, определяющий пределы цепи поставок, охватываемые Планом обеспечения безопасности (охраны) цепи поставок;
- Отчет об оценке уязвимости (охраны) как документ, содержащий перечень уязвимых мест цепи поставок с определением сценариев угроз и описанием ожидаемых воздействий по каждому виду потенциальной угрозы;
- План обеспечения безопасности (охраны), описывающий мероприятия по управлению угрозами безопасности, выявленными в ходе проведения оценки уязвимости (охраны);
- программы подготовки, описывающие порядок проведения учений и тренировок персонала, ответственного за охрану (службы охраны), по выполнению своих обязанностей в области обеспечения безопасности и охраны.

Для проведения оценки уязвимости (охраны), необходимой для разработки Плана обеспечения безопасности (охраны), организация, использующая настоящий стандарт, должна:

- определить существующие угрозы обеспечения безопасности;
- определить наиболее вероятные развития событий в случаях реализации выявленных оценкой уязвимости (охраны) угроз.

Такие определения проводятся в ходе анализа существующего состояния обеспечения безопасности и охраны цепи поставок на основе экспертного заключения об уязвимости цепи поставок по каждому виду угрозы.

В случае обнаружения неприемлемых уязвимых мест в цепи поставок организация должна разработать дополнительные процедуры или внести соответствующие эксплуатационные изменения для снижения вероятности и/или последствий на случай реализации угрозы. Такие дополнения или изменения, принимаемые организацией, называются контрмерами. Контрмеры, принимаемые в целях снижения уровня угроз до приемлемого, должны включаться в План обеспечения безопасности (охраны) цепи поставок с учетом их приоритетности.

Приложения А и В демонстрируют примеры процессов риск-менеджмента по обеспечению безопасности и охраны людей, собственности и функционирования цепи поставок. Они помогают как в макроподходе к сложным цепям поставок, так и при более детальном их рассмотрении.

Приложения А и В преследуют также следующие цели:

- содействие пониманию методик разработки и внедрения, которыми могут воспользоваться организации;
- содействие пониманию руководством процесса риск-менеджмента для обеспечения постоянного улучшения;
- помощь организациям в управлении ресурсами при принятии мер по существующим или возникающим рискам обеспечения безопасности;
- описание возможных способов проведения оценки рисков и снижения угроз безопасности в цепи поставок, начинающейся от источников сырья и заканчивающейся доставкой продукции или услуг конечному пользователю.

Для случаев, когда организации принимают на себя обязательства в отношении настоящего стандарта, приложение С содержит рекомендации по сертификации систем менеджмента безопасности на соответствие требованиям ГОСТ Р 53662—2009.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система менеджмента безопасности цепи поставок

НАИЛУЧШИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Оценки и планы

Security management systems for the supply chain.
Best practices for implementing supply chain security. Assessments and plans

Дата введения — 2010—07—01

1 Область применения

В настоящем стандарте приведены рекомендации и требования для организаций — участников цепи поставок по:

- разработке и внедрению процессов обеспечения безопасности и охраны цепи поставок;
- документированному установлению минимального уровня охраны для всей цепи поставок или ее части;
- содействию в достижении соответствия критериям, предъявляемым к Уполномоченному экономическому оператору, сформулированным в Рамочных стандартах безопасности и облегчения мировой торговли [1] Всемирной таможенной организации, и существующим законодательным и нормативным актам, регламентирующим обеспечение безопасности и охраны цепи поставок.

Примечание — Только *федеральный орган исполнительной власти по контролю и надзору в области таможенного дела* может присвоить организации статус Уполномоченного экономического оператора при условии ее соответствия требованиям в области обеспечения безопасности и охраны цепи поставок и наличия соответствующих подтверждающих документов.

В дополнение настоящий стандарт устанавливает требования к документации, по которой возможно проводить оценку соответствия.

Организация, принявшая на себя ответственность по настоящему стандарту, должна:

- определить участки цепи поставок, на которых организация будет обеспечивать безопасность и охрану (см. 4.1);
- провести там оценку уязвимости (охраны) и разработать адекватные контрмеры;
- разработать и внедрить План обеспечения безопасности (охраны) цепи поставок;
- подготовить персонал, ответственный за охрану (службы охраны), в соответствии с его должностными обязанностями.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие документы:

ГОСТ Р ИСО 9001—2008 Системы менеджмента качества. Требования

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

ГОСТ Р 53660—2009 Суда и морские технологии. Оценка охраны и разработка планов охраны портовых средств

Международная конвенция по охране человеческой жизни на море 1974 года, с поправками, Международной морской организации.

Издание официальное

3 Термины и определения

Для целей настоящего стандарта применяются следующие термины и определения:

3.1 **уполномоченные должностные лица** (appropriate law enforcement and other government officials): Должностные лица органов исполнительной власти и подведомственных им организаций, наделенные соответствующими полномочиями по решению вопросов в отношении цепи поставок или отдельных ее участков.

3.2 **активы** (asset(s)): Предприятие, технологическое оборудование, здания, наземные, водные и воздушные транспортные средства и другие элементы инфраструктуры, а также относящиеся к ним системы, которые имеют отличительную и измеримую деловую функцию или услугу.

Примечание — Это определение включает в себя любую информационную систему, являющуюся частью обеспечения безопасности и охраны и применения менеджмента безопасности.

3.3 **Уполномоченный экономический оператор** (authorized economic operator): Участник внешнеэкономической деятельности, чья деятельность получила одобрение федерального органа исполнительной власти по контролю и надзору в области таможенного дела, как соответствующая нормам Всемирной таможенной организации или стандартам обеспечения безопасности и охраны цепи поставок.

Примечание 1 — Уполномоченный экономический оператор — термин, установленный Всемирной таможенной организацией в Рамочных стандартах безопасности и облегчения мировой торговли [1].

Примечание 2 — Термин «Уполномоченный экономический оператор» включает, в частности, производителей, импортеров, экспортеров, брокеров, перевозчиков, консолидаторов, посредников, операторов портов, терминалов, интеграционных операторов, складских операторов, дистрибьюторов.

3.4 **деловой партнер** (business partner): Подрядчик или поставщик, с которым организация заключает контракт о содействии в выполнении ее функции как организация — участник цепи поставок.

3.5 **грузовая транспортная единица** (cargo transport unit): Автомобильное, морское, речное, воздушное грузовое транспортное средство, грузовой вагон, контейнер, цистерна.

3.6 **последствие** (consequence): Возможная потеря жизни или здоровья, экономические или финансовые потери, в том числе происшедшие в результате нарушения деятельности транспортных систем, при реализации акта незаконного вмешательства в цепи поставок или использования цепи поставок в качестве оружия.

3.7 **транспортное средство** (conveyance): Физический инструмент торговли, с помощью которого производится перемещение товаров.

Примечание — Грузовая транспортная единица, оборудование для обработки груза, грузовой автомобиль, судно, самолет, железнодорожный вагон.

3.8 **контрмера** (countermeasure): Действие, предпринятое для снижения вероятности реализации угроз безопасности, направленное против достижения их целей или уменьшения возможных последствий.

3.9 **фаза контроля** (custody): Период времени, в течение которого организация — участник цепи поставок непосредственно контролирует производство, обработку и перемещение товаров, а также всю информацию о процессах, происходящих в цепи поставок.

3.10 **фаза постконтроля** (downstream): Период времени после выхода товаров из фазы контроля организации — участника цепи поставок.

3.11 **товары** (goods): Предметы, являющиеся объектом контракта, заключающегося на их производство, обработку и перемещение в цепи поставок в целях удовлетворения потребностей потребителя.

3.12 **международные цепи поставок** (international supply chain): Цепи поставок, которые осуществляются с пересечением государственных границ.

Примечание — Все участки такой цепи поставок считаются международными с момента заключения контракта потребителем, который включает в себя проведение таможенного контроля в стране назначения. Если международные договоры или региональные соглашения не содержат требований о таможенной очистке товаров, тогда окончанием цепи поставок является точка ввоза товара в страну назначения.

3.13 **вероятность** (likelihood): Степень возможности развития сценария угрозы безопасности, которая может привести к реализации акта незаконного вмешательства.

Примечание — Вероятность оценивается с учетом внедренных процессов противодействия акту незаконного вмешательства, в котором используется рассматриваемый сценарий угрозы, и имеет количественное выражение.

3.14 **система менеджмента** (management system): Структура организации для управления ее процессами или действиями, посредством которых вкладываемые ресурсы преобразуются в продукт или услугу, отвечающую целям организации.

Примечание — Настоящий стандарт не имеет целью требовать наличие определенной системы менеджмента и/или создания отдельной системы менеджмента безопасности. Примерами систем менеджмента являются ГОСТ Р ИСО 9001 (Системы менеджмента качества. Требования), ГОСТ Р ИСО 14001 (Системы экологического менеджмента. Требования и руководство по применению), ГОСТ Р 53663 (Системы менеджмента безопасности цепи поставок. Требования) и Международный кодекс по управлению безопасной эксплуатацией судов и предотвращению загрязнения (ISM Code) [2] Международной морской организации.

3.15 **организация — участник цепи поставок** (organization in the supply chain): Любое юридическое лицо, которое:

- заключает контракт на поставку, изготовление, обработку, перемещение, выгрузку товаров в цепи поставок, которая в какой-то момент пересекает государственную границу;
- осуществляет перемещение товаров любым принятым в международной цепи поставок способом вне зависимости от того, пересекает его участок цепи поставок государственную границу или нет; или
- предоставляет, формирует или управляет информацией о поставках, используемой в практике деловых отношений, в том числе с таможенными органами.

3.16 **риск-менеджмент** (risk management): Процесс принятия решений по управлению, основанный на анализе возможных угроз, их последствий, а также возможностей или вероятности успеха.

Примечание — Процесс риск-менеджмента обычно начинается с оптимизации распределения ресурсов организации, необходимых для обеспечения работ в существующих условиях.

3.17 **область деятельности** (scope of service): Функция(и) и место ее(их) реализации организацией — участником цепи поставок.

3.18 **Декларация об охране** (security declaration): Документально оформленные обязательства делового партнера, в которых определены меры обеспечения безопасности и охраны, внедренные этим партнером, включающие, как минимум, меры защиты товаров, транспортных средств и связанной с этим информации, а также подтверждение и демонстрация этих мер.

Примечание — Декларация об охране используется организацией — участником цепи поставок для оценки адекватности мер охраны, относящихся к безопасности товаров в целом.

3.19 **План обеспечения безопасности (охраны)** (security plan): Запланированные мероприятия для обеспечения адекватного менеджмента безопасности и охраны.

Примечание 1 — Назначение плана — гарантировать принятие мер по защите организации от актов незаконного вмешательства.

Примечание 2 — План может комбинироваться с другими оперативными планами.

3.20 **обеспечение безопасности и охраны** (security): Противодействие преднамеренным действиям, направленным на нанесение вреда или ущерба цепи поставок или посредством цепи поставок.

3.21 **акт незаконного вмешательства** (security incident): Любое действие или обстоятельство, представляющее угрозу безопасности цели (см. 3.26).

3.22 **персонал, ответственный за безопасность (служба охраны)** (security personnel): Персонал организации — участника цепи поставок, имеющий обязанности в области обеспечения безопасности и охраны.

Примечание — Персонал службы охраны может создаваться организацией или привлекаться на договорной основе.

3.23 **конфиденциальная информация; конфиденциальные материалы** (security sensitive information; security sensitive materials): Информация или материалы о процессе обеспечения безопасности и охраны цепи поставок, которые содержат сведения, касающиеся вопросов обеспечения безопасности и охраны, обработки товаров или распоряжений органов исполнительной власти, не предназначенные для широкого доступа и являющиеся объектом заинтересованности инициаторов актов незаконного вмешательства.

3.24 **менеджмент безопасности** (security management): Систематизированная и скоординированная деятельность, с помощью которой организация — участник цепи поставок управляет своими рисками и связанными с ними потенциальными угрозами и воздействиями.

3.25 **цепь поставок** (supply chain): Взаимосвязанный набор ресурсов и процессов, который начинается с оформления контракта на поставку, продолжается процессом получения сырья, производством, обработкой и заканчивается передачей товаров и относящихся к ним услуг конечному пользователю.

Примечание — Цепь поставок может включать в себя продавцов, промышленные предприятия, логистические центры, внутренние центры распределения, дистрибьюторов, оптовых продавцов и других юридических лиц, участвующих в производстве, обработке и доставке товаров и относящихся к ним услуг.

3.26 **цель** (target): Персонал, транспортные средства, товары, активы, процессы производства и обработки, системы управления или документооборота в рамках организации — участника цепи поставок.

3.27 **сценарий угрозы** (threat scenario): Описание способа реализации потенциального акта незаконного вмешательства.

3.28 **фаза предконтроля** (upstream): Период времени до входа товаров в фазу контроля организации — участника цепи поставок.

3.29 **Всемирная таможенная организация (ВТО)** (World Customs Organization (WCO)): Независимый межправительственный орган, задачей которого является повышение эффективности таможенных администраций.

Примечание — ВТО — всемирная межправительственная организация в области таможенного дела.

4 Основные положения

4.1 Паспорт участка цепи поставок

Для обеспечения взаимодействия с деловыми партнерами, операторами цепи поставок, таможенными органами и другими заинтересованными лицами организация — участник цепи поставок должна составить Паспорт участка цепи поставок с описанием управляемого ею участка цепи поставок, который должен соответствовать настоящему стандарту. В Паспорт должны быть включены следующие данные:

- сведения об организации,
- область деятельности;
- наименование и контактные данные всех вовлеченных в область деятельности организации — участника цепи поставок деловых партнеров;
- дата проведения последней оценки уязвимости (охраны) и срок ее действия.

Паспорт должен быть подписан должностным лицом организации — участника цепи поставок, обладающим необходимыми полномочиями.

Организация — участник цепи поставок может расширить перечень сведений, содержащихся в Паспорте, путем включения в него данных о других участках цепи поставок.

4.2 Деловые партнеры

Если организация — участник цепи поставок взаимодействует с деловыми партнерами на своем участке цепи поставок, то согласно разделам 4.3 и 4.4 она может запросить у таких партнеров Декларацию об охране. Организация — участник цепи поставок на основе предоставленной Декларации об охране и собственной оценки уязвимости (охраны) может потребовать от деловых партнеров проведения дополнительных мер обеспечения безопасности и охраны.

4.3 Свидетельства о соответствии, принятые в международной практике

Транспортные и иные компании при наличии международных свидетельств (сертификатов) о соответствии, выдаваемых во исполнение международных договоров и соглашений, регламентирующих вопросы обеспечения безопасности и охраны объектов транспортной инфраструктуры, обладают положительным опытом, процедурами и планами обеспечения безопасности и охраны, отвечающими применимым требованиям настоящего стандарта, и не требуют проведения дополнительных аудитов по подтверждению их соответствия. Для судоходных компаний, судов и операторов портовых средств такие одобрения выдаются в соответствии с требованиями глав XI-2/4 и XI-2/10 Международной конвенции по охране человеческой жизни на море 1974 года Международной морской организации.

Для признания транспортной или иной компании в качестве Уполномоченного экономического оператора, упомянутого в разделе 1 настоящего стандарта, *федеральные органы исполнительной власти по контролю и надзору в области таможенного дела* могут потребовать от них в дополнение к

существующим международным свидетельствам (сертификатам) о соответствии внедрить дополнительные меры по обеспечению безопасности и охраны.

4.4 Деловые партнеры, освобождаемые от предъявления Декларации об охране

Деловые партнеры, которые продемонстрировали организации — участнику цепи поставок, что они:

1) прошли проверку и подтвердили свое соответствие настоящему стандарту или стандарту ИСО 20858, или

2) отвечают требованиям раздела 4.3, или

3) имеют статус Уполномоченного экономического оператора, присвоенного в соответствии с Рамочными стандартами безопасности и облегчения мировой торговли [5] Всемирной таможенной организации, должны быть перечислены в Паспорте участка цепи поставок.

В отношении таких деловых партнеров не требуется проведения дополнительных проверочных мероприятий.

4.5 Анализ состоятельности обеспечения безопасности деловых партнеров

Организация — участник цепи поставок должна анализировать процессы и средства своих деловых партнеров, за исключением партнеров, которые отвечают требованиям раздела 4.3 или 4.4, с тем чтобы убедиться в объективности представленных ими Деклараций об охране и их состоятельности. Проведение такого анализа и его частота должны учитываться при проведении анализа рисков организации в отношении своих деловых партнеров. Результаты такого анализа должны сохраняться.

Примечание — Организация — участник цепи поставок, заявляющая о своем соответствии, в том числе на участках цепи поставок, контролируемых деловыми партнерами, но требующая подтверждения соответствия настоящему стандарту, в дальнейшем для облегчения прочтения будет именоваться «организация», если не потребуется именовать ее иначе.

5 Процесс обеспечения безопасности и охраны цепи поставок

5.1 Общие положения

Организации — участники цепи поставок, принявшие на себя обязательства по настоящему стандарту, должны обеспечивать управление безопасностью и охраной на подконтрольных им участках цепи поставок и иметь действующую систему менеджмента для обеспечения этих целей. Стандарт требует проработки и внедрения положительного опыта и/или процессов в области обеспечения безопасности и охраны для снижения рисков воздействия на цепь поставок, могущих привести к актам незаконного вмешательства.

Организация — участник цепи поставок, заявляющая о своем соответствии настоящему стандарту, должна иметь План обеспечения безопасности (охраны). План, основываясь на выводах оценки уязвимости (охраны), документально отображает внедренные процедуры, меры и контрмеры по обеспечению безопасности и охраны в отношении участков цепи поставок, указанных в Паспорте участка цепи поставок.

5.2 Определение масштабов оценки уязвимости (охраны)

Масштабы оценки уязвимости (охраны) должны охватывать всю деятельность организации, указанную в Паспорте участка цепи поставок (см. 4.1). Оценка уязвимости (охраны) и пересмотр Плана обеспечения безопасности (охраны) должны проводиться периодически. Результаты оценок охраны должны оформляться документально и сохраняться.

Оценка уязвимости (охраны) должна охватывать информационные ресурсы и документацию, имеющие отношение к обработке и передвижению товаров, во время их нахождения в фазе контроля организации — участника цепи поставок. Существующие мероприятия по обеспечению безопасности и охраны (см. 4.3, 4.4) должны оцениваться во всех потенциально уязвимых местах и для каждого делового партнера.

5.3 Проведение оценки уязвимости (охраны)

5.3.1 Персонал, проводящий оценку

Специалист или группа специалистов, проводящих оценку уязвимости (охраны), должны обладать навыками и знаниями, по меньшей мере, в следующих областях:

- технологии риск-менеджмента, применимые ко всем аспектам цепи поставок с момента принятия товаров в фазу контроля организации — участника цепи поставок до момента их выхода из указанной фазы контроля;

- применение соответствующих мер по недопущению несанкционированного разглашения или доступа к конфиденциальным материалам;

- действия и процедуры, применимые при производстве, обработке и доставке товаров и их документальном оформлении;
- меры по обеспечению безопасности и охраны в отношении партий товара, транспортных средств, персонала, помещений, а также информационных систем рассматриваемого участка цепи поставки;
- понимание угроз безопасности и методологий их уменьшения;
- понимание настоящего стандарта.

Персональные данные лиц, проводящих оценку уязвимости (охраны), включая сведения об их квалификации, должны быть задокументированы.

5.3.2 Процесс оценки

Организация — участник цепи поставок должна разработать, внедрить и поддерживать в рабочем состоянии процедуру по определению существующих контрмер, направленных на снижение угроз безопасности. Организация — участник цепи поставок должна перечислить применимые сценарии угроз, включая угрозы, определяемые уполномоченными должностными лицами. Если оценка охраны проводилась без участия уполномоченных должностных лиц, это должно быть отражено в Отчете об оценке уязвимости (охраны).

По каждому сценарию угроз организация — участник цепи поставок должна оценить существующие контрмеры и определить последствия и вероятность реализации каждой угрозы, а также оценить любые потребности в принятии дополнительных мер. Если меры оцениваются как неадекватные, то следует применить дополнительные меры для уменьшения угроз до приемлемого уровня. Такой процесс должен повторяться для каждого сценария угрозы.

Организация — участник цепи поставок должна анализировать Декларации об охране каждого делового партнера (см. 4.2), используя профессиональные навыки и знания, требования законодательных и иных нормативных правовых актов. Для определения объективности предоставляемых Деклараций также следует получать и использовать любую другую доступную информацию.

Организация — участник цепи поставок должна учитывать сведения и сроки действия каждой Декларации об охране при проведении оценки уязвимости (охраны) и при определении общей уязвимости части цепи поставок, внесенной в Паспорт участка цепи поставок.

Деловые партнеры, соответствующие разделам 4.3 и 4.4, не нуждаются в проведении дальнейшей оценки охраны.

Следующая информация должна оформляться документально:
- все рассмотренные сценарии угроз;
- методики, используемые при оценке этих угроз;
- все определенные контрмеры с учетом их приоритетности.

5.4 Разработка Плана обеспечения безопасности (охраны) цепи поставок

Организация — участник цепи поставок должна разработать и поддерживать в рабочем состоянии План обеспечения безопасности (охраны) участка цепи поставок, внесенного в Паспорт участка цепи поставок. План может быть разделен на приложения, в которых описываются меры по обеспечению безопасности и охраны для различных частей цепи поставок, включая меры в отношении деловых партнеров (см. 4.3 и 4.4), принимаемые в соответствии с их Декларациями об охране. В План также должен быть включен порядок контроля Деклараций об охране и периодичность их анализа.

При разработке Плана обеспечения безопасности (охраны) организация — участник цепи поставок должна рассмотреть и проанализировать руководства, приведенные в приложениях А и В.

5.5 Реализация Плана обеспечения безопасности (охраны) цепи поставок

Для реализации процессов обеспечения безопасности и охраны цепи поставок организация — участник цепи поставок должна разработать и внедрить у себя систему менеджмента.

5.6 Документирование и мониторинг процессов обеспечения безопасности и охраны цепи поставок

5.6.1 Общие положения

Организация — участник цепи поставок должна разработать и поддерживать в рабочем состоянии процедуры по документированию, мониторингу и измерению функционирования вышеупомянутой системы менеджмента, проводить аудиты системы менеджмента в запланированные промежутки времени для определения того, что система результативно внедрена и поддерживается в рабочем состоянии. Результаты проведенных аудитов должны оформляться документально и сохраняться.

5.6.2 Постоянное улучшение

Организация — участник цепи поставок должна оценивать возможности по улучшению мер обеспечения безопасности и охраны как способа усиления безопасности собственного участка цепи поставок.

5.7 Меры, принимаемые после реализации акта незаконного вмешательства

Организация — участник цепи поставок должна проводить анализ Плана обеспечения безопасности (охраны) после реализации акта незаконного вмешательства, который затронул любой участок международной цепи поставок, контролируемый организацией. В процессе данного анализа должно определяться следующее:

- причины совершения акта незаконного вмешательства;
- эффективность мер и процедур по восстановлению безопасности;
- меры по предотвращению повторения акта незаконного вмешательства и достижению необходимого уровня обеспечения безопасности и охраны.

В случае реализации акта незаконного вмешательства организация — участник цепи поставок при необходимости должна реализовывать процедуру доклада органам исполнительной власти или иным заинтересованным лицам в соответствии с требованиями Плана обеспечения безопасности (охраны) или обязательствами по контракту.

Организация — участник цепи поставок должна сохранять сведения в отношении реализации мероприятий, предусмотренных настоящим пунктом, в течение срока, установленного нормативными актами.

5.8 Защита информации по обеспечению безопасности и охраны

Планы, мероприятия, процессы, процедуры и записи организации, относящиеся к обеспечению безопасности и охраны, считаются конфиденциальной информацией и должны быть защищены от несанкционированного доступа или разглашения. Доступ к такой информации предоставляется исключительно лицам, которым она необходима для выполнения своих должностных обязанностей. Помимо уполномоченных должностных лиц доступ к такой информации предоставляется в следующих случаях:

- лицу требуется доступ к конфиденциальной информации по обеспечению безопасности и охраны для выполнения обязанностей, которые предусмотрены Планом обеспечения безопасности (охраны);
- лицо проходит подготовку по действиям, которые предусмотрены Планом обеспечения безопасности (охраны);
- лицу необходима информация для контроля других лиц, осуществляющих действия, предусмотренные Планом обеспечения безопасности (охраны);
- лицо действует от имени стороны, которой согласно контрактным обязательствам организация — участник цепи поставок предоставила доступ к своей конфиденциальной информации с оговоренными сроками и условиями такого доступа.

Примечание — Если организация — участник цепи поставок сертифицирована по системе менеджмента безопасности цепи поставок органом по сертификации, аккредитованным для работ по сертификации на соответствие требованиям настоящего стандарта, то такой доступ к конфиденциальной информации организации, оговоренный в обязательствах по контракту, может не считаться необходимым и в любом случае будет зависеть от согласия самой организации. Факт того, что конфиденциальная информация защищена от несанкционированного доступа или разглашения, не препятствует организации демонстрировать своим деловым партнерам или другим заинтересованным лицам меры по обеспечению безопасности и охраны, а также свою систему менеджмента безопасности цепи поставок.

Приложение А
(справочное)

Процесс обеспечения безопасности и охраны цепи поставок

А.1 Общие положения

Настоящее приложение содержит руководство по разработке процессов обеспечения безопасности и охраны цепи поставок, которые могут быть реализованы организацией, в которой внедрена и действует система менеджмента. На рисунке А.1 представлено графическое описание этих процессов.

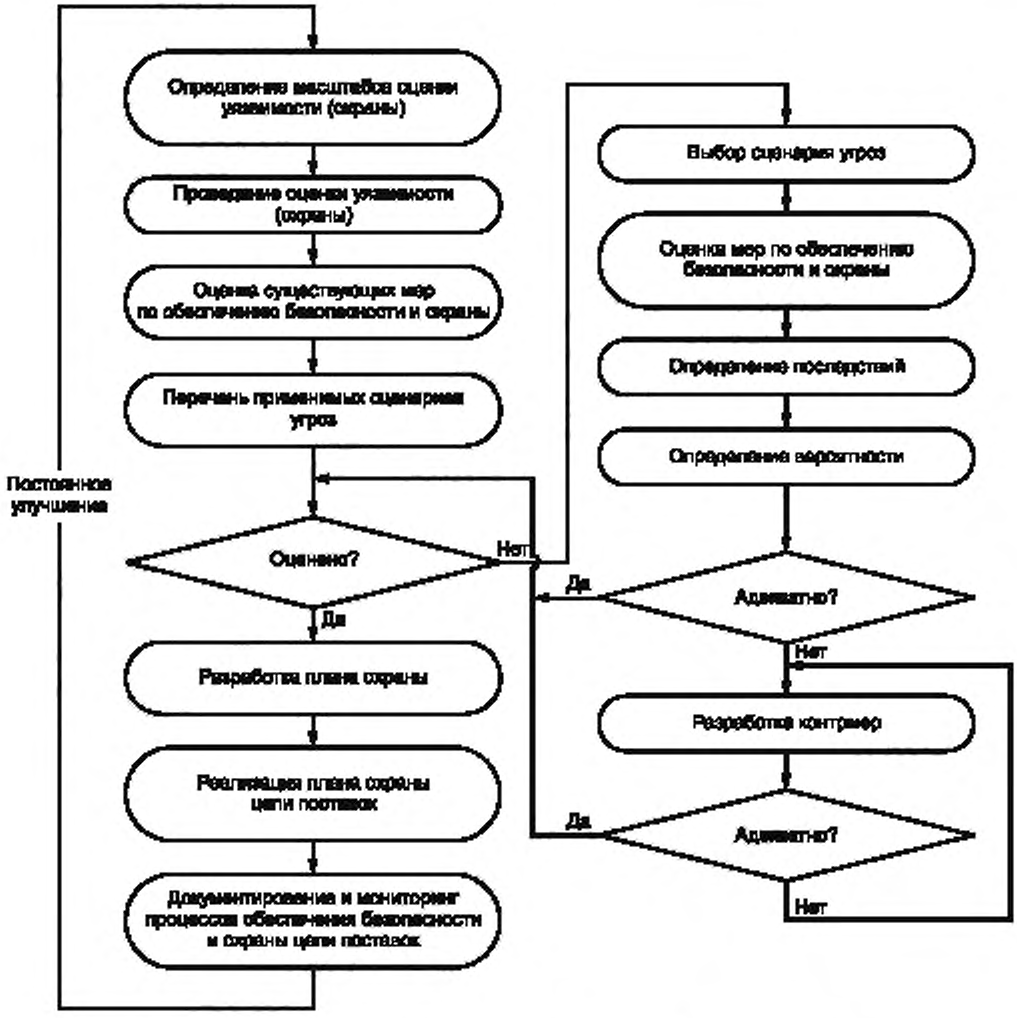

Рисунок А.1 — Схема разработки процессов обеспечения безопасности и охраны

А.2 Определение масштабов оценки уязвимости (охраны)

Оценка уязвимости (охраны) является попыткой идентификации рисков, распространяющихся на тот участок цепи поставок, который организация — участник цепи поставок согласно своему Паспорту участка цепи поставок

желает привести в соответствие с настоящим стандартом. Для выполнения этой оценки необходимо установить пределы оцениваемого участка цепи поставок.

А.3 Проведение оценки уязвимости (охраны)

А.3.1 Общие положения

Проводимая квалифицированным персоналом оценка существующих мер по обеспечению безопасности и охраны должна проводиться для всех уязвимых мест, которые включают, но не ограничиваются следующим:

- места производства и обработки товаров до их размещения на грузовой транспортной единице или транспортном средстве;
- места складирования и сбора товаров, подготовленных к транспортированию;
- места конечного перемещения товаров;
- места погрузки и выгрузки на транспортные средства;
- места смены товаром фаз контроля,
- места сбора и обработки документации или информации, имеющей отношение к партиям перевозимых товаров, где она является доступной;
- внутренние маршруты перемещения товаров,
- транспортные средства, используемые при различных способах транспортирования;
- другое.

А.3.2 Опросный лист анализа функционирования

Пример системного подхода к анализу существующих мер по обеспечению безопасности и охраны представлен в приведенном ниже Опросном листе анализа функционирования.

Пункты Опросного листа анализа функционирования, касающиеся деловых партнеров, которые подтвердили организации, что они:

- прошли проверку и подтвердили свое соответствие настоящему стандарту или стандарту ИСО 20858, или
- отвечают требованиям раздела 4.3, или
- имеют статус Уполномоченного экономического оператора, присвоенный в соответствии с Рамочными стандартами безопасности и облегчения мировой торговли [1] Всемирной таможенной организации, должны содержать комментарий, который дает объяснение, каким образом рассматривался тот или иной фактор, например, в соответствии с настоящим стандартом, ИСО 20858 или Международным кодексом по охране судов и портовых средств [3].

А.3.3 Анализ функционирования

При проведении оценки уязвимости (охраны) организации — участника цепи поставки должен быть рассмотрен и заполнен Опросный лист анализа функционирования, приведенный в таблице А.1. Опросный лист может быть изменен с учетом особенностей деятельности и структуры организации — участника цепи поставок. В Опросном листе анализа функционирования следует использовать графу «Да», если указанный фактор уже внедрен организацией — участником цепи поставок. Если фактор не внедрен или внедрен частично, следует использовать графу «Нет» и добавить пояснение в графу «Комментарий». В данной графе можно описать другие используемые альтернативные меры или отметить, что риск является незначительным. Если фактор неприменим, следует вписать «НП» (не применяется) в графе «Комментарий». Пункты Опросного листа, которые неприменимы в силу законодательных или нормативных требований, должны быть отмечены в графе «Комментарий» как запрещенные.

Таблица А.1 — Опросный лист анализа функционирования

Фактор анализа	Да	Нет	Комментарий
Менеджмент безопасности цепи поставок			
Внедрена ли в организации система менеджмента, касающаяся обеспечения безопасности и охраны цепи поставок?			
Назначен ли в организации представитель руководства по безопасности, ответственный за обеспечение безопасности и охраны цепи поставок?			
План обеспечения безопасности (охраны)			
Имеется ли в организации действующий План обеспечения безопасности (охраны)?			
Отражены ли в Плане конечные цели организации в части обеспечения безопасности и охраны фаз предконтроля и постконтроля деловыми партнерами?			
Внедрены ли в организации мероприятия по управлению в кризисных ситуациях, сохранности устойчивого бизнеса и планы восстановления безопасности?			

Продолжение таблицы А.1

Фактор анализа	Да	Нет	Комментарий
Обеспечение безопасности активов			
Приняты ли в организации меры по обеспечению: - физической защиты зданий и сооружений; - мониторинга и контроля внешнего и внутреннего периметров; - управления доступом на территории, запрещенные к несанкционированному нахождению возле перевозочных средств, складских площадок и помещений, грузового оборудования и устройств контроля и выдачи идентификационных документов персоналу и посетителям с использованием контрольно-пропускных устройств?			
Используются ли новейшие технологии для усиления защиты активов, такие как средства обнаружения несанкционированных проникновений в зоны ограниченного доступа, средства теле- и видеонаблюдения с возможностью хранения записанной информации в целях проведения расследований возможных актов незаконного вмешательства?			
Имеется ли порядок связи с персоналом, ответственным за безопасность (службы охраны), или органами исполнительной власти в случае возникновения нарушений, связанных с обеспечением безопасности и охраны?			
Внедрены ли процедуры по ограничению, предотвращению и оповещению о несанкционированном доступе в зоны обработки, складирования товаров и месторасположения транспортных средств?			
Существует ли идентификация лиц, которые получают и отправляют товары?			
Персонал, ответственный за безопасность (службы охраны)			
Проводится ли аттестация при приеме на работу, а также периодическая аттестация персонала, ответственного за безопасность (службы охраны)?			
Проводится ли подготовка персонала, ответственного за безопасность (службы охраны), для обеспечения более качественного исполнения своих обязанностей в области обеспечения безопасности и охраны (например, по обеспечению целостности товаров, выявлению потенциальных внутренних угроз, управлению контролем доступа)?			
Осведомлен ли персонал о процедурах, действующих в организации, в отношении докладов о выявленных подозрительных случаях?			
Включает ли система управления доступом возможность немедленного изъятия/аннулирования у увольняющегося персонала идентификационных карт или пропусков, выданных организацией для передвижения по зонам ограниченного доступа и для работ с информационными системами?			
Информационная безопасность			
Гарантируют ли применимые организацией процедуры то, что вся информация как в бумажном, так и в электронном виде, касающаяся процессов, связанных с товарами, является четкой, своевременной, точной и защищена от искажений и потерь или внесения ошибочных данных?			
Снабжает ли организация отгружаемые или получаемые товары соответствующей сопроводительной документацией?			
Осуществляет ли организация контроль точности и своевременности получаемой от своих деловых партнеров информации о товарах?			
Защищаются ли соответствующие данные с использованием систем сохранности, не затрагивая операционные системы обработки основных данных (обеспечиваются ли процессы обновления данных)?			
Обеспечен ли весь персонал уникальным идентификатором (ID пользователя) для персонального использования, с тем чтобы получить возможность отслеживания его действий?			
Используется ли эффективная система управления паролями, позволяющая аутентифицировать пользователя и требующая от него периодической смены пароля?			

Окончание таблицы А.1

Фактор анализа	Да	Нет	Комментарий
Имеется ли защита от несанкционированного доступа к информации и от неправильного ее использования?			
Обеспечение безопасности и охрана товаров и транспортных средств			
Внедрены ли процедуры по ограничению, выявлению и оповещению о несанкционированном доступе для всех зон обработки товаров и закрытых грузовых транспортных единиц?			
Обработка товаров контролируется квалифицированным персоналом?			
Внедрены ли процедуры оповещения органов исполнительной власти в случае выявления или подозрения на незаконные действия?			
Внедрены ли процедуры, обеспечивающие целостность товаров при их передаче другой организации — участнику цепи поставок?			
Существует ли порядок отслеживания уровня угроз на всем протяжении маршрутов передвижения товаров?			
Снабжены ли операторы транспортных средств необходимыми правилами, руководствами и инструкциями в области обеспечения безопасности и охраны?			
Закрытые грузовые транспортные единицы			
(Рамочные стандарты безопасности и облегчения мировой торговли [1] включают в себя Программу обеспечения целостности пломб, изложенную в дополнении к приложению 1, где указаны процедуры по установке и проверке пломб, обеспечивающих высокую степень безопасности, и/или других устройств для обнаружения вмешательства. Перед заполнением данной формы необходимо ознакомиться с упомянутым приложением к Рамочным стандартам.)			
При применении закрытых грузовых транспортных единиц используются ли процедуры по установке и регистрации механических пломб, обеспечивающих высокую степень безопасности, предписанных в стандарте ИСО 17712 [4], и/или других устройств для обнаружения вмешательства?			
При применении опломбированных закрытых грузовых транспортных единиц внедрена ли процедура проверки целостности пломб и обнаружения расхождений в их нумерации при смене транспортным средством фаз контроля?			
Непосредственно перед применением закрытых грузовых транспортных единиц проводится ли их проверка на предмет наличия зараженности?			
При применении закрытых грузовых транспортных единиц внедрена ли документально оформленная процедура по проверке непосредственно перед заполнением их физической целостности, включая надежность запирающих механизмов?			
Рекомендуется процесс осмотра, состоящий из семи пунктов: - передняя стенка; - левая стенка; - правая стенка; - пол; - потолок/крыша; - внутренний/внешний запирающий механизм; - тележка/шасси			

А.3.4 Сценарии угроз

В ходе проведения оценки уязвимости (охраны) рассматриваются сценарии угроз, приведенные в таблице А.2. При оценке уязвимости (охраны) также рассматривают другие сценарии угроз, которые могут быть предложены уполномоченными должностными лицами, руководством организации или экспертами в области обеспечения безопасности и охраны, проводящими оценку уязвимости (охраны).

Таблица А.2 — Сценарии угроз цепи поставок

Сценарии угроз	Возможные последствия
1 Проникновение и/или установление контроля над активом (включая транспортные средства) в пределах цепи поставок	Нанесение повреждений/разрушений актива (включая транспортные средства); использование актива в качестве средства нанесения повреждений/разрушений; акции протеста населения, повлекшие за собой экономические потери; захват заложников/убийство людей
2 Использование цепи поставок для незаконного перемещения товаров и пассажиров	Нелегальное перемещение запрещенных предметов, в том числе оружия; нелегальное перемещение людей, в том числе террористов
3 Информационное вмешательство	Получение местного или удаленного доступа к информационным/документальным системам в целях нарушения деятельности цепи поставок или облегчения незаконной деятельности
4 Целостность товаров	Подделка, подмена и/или кража в террористических целях
5 Несанкционированное использование	Использование деятельности международной цепи поставок для реализации террористических актов, включая использование транспортного средства в качестве оружия
6 Другое	

А.4 Разработка Плана обеспечения безопасности (охраны)

А.4.1 Общие положения

План обеспечения безопасности (охраны) и/или приложения к нему могут включаться в оперативные планы или процедуры организации и не требовать оформления как отдельного документа. Для случаев, когда План является неотъемлемой частью других планов или процедур, организация должна поддерживать в рабочем состоянии ссылочную таблицу для подтверждения того, что все требования по обеспечению безопасности и охраны были соблюдены.

План обеспечения безопасности (охраны) может быть разделен на приложения, содержащие описание обеспечения безопасности и охраны для отдельных участков цепи поставок, включая соответствующие меры, предпринимаемые деловыми партнерами в соответствии с их Декларациями об охране (где применимо). План/приложения должны также содержать порядок контроля Деклараций об охране и периодичность их анализа. План обеспечения безопасности (охраны)/приложения должны включать в себя описание, как минимум.

- участка цепи поставок;
- должностных обязанностей всего персонала, ответственного за безопасность (службы охраны);
- структуры менеджмента безопасности, включая персональные данные представителя руководства по безопасности;
- данных по связи, которыми должен пользоваться персонал, ответственный за безопасность (службы охраны) для оповещения органов исполнительной власти об актах незаконного вмешательства;
- навыков и знаний, которыми должен обладать персонал, ответственный за безопасность (службы охраны);
- программы подготовки в области обеспечения безопасности и охраны;
- процессов повышения квалификации персонала, ответственного за безопасность, (службы охраны) в целях поддержания навыков и знаний для выполнения своих должностных обязанностей;
- порядка проведения тренировок по Плану обеспечения безопасности (охраны). Для выполнения этого требования организация должна принимать участие в учениях, проводимых органами исполнительной власти, а также проводить собственные тренировки с персоналом, ответственным за обеспечение безопасности (службы охраны),
- процессов, отвечающих, как минимум, требованиям органов исполнительной власти, применимых в случае возникновения непредвиденных ситуаций или при снижении уровня безопасности (охраны).

План обеспечения безопасности (охраны) должен содержать процедуры, которые, как минимум:

- обеспечивают получение информации о партиях товаров до их принятия организацией для дальнейшего транспортирования;
- обеспечивают четкое соответствие получаемых к обработке товаров информации, указанной в сопроводительной товарной документации. Получаемый штучный товар должен сверяться на соответствие с информацией в контракте на поставку;
- обеспечивают установление личности водителей, осуществляющих перевозку товаров, до получения или отправки этих товаров;
- обеспечивают установление личности всех лиц, находящихся на транспортном средстве, помимо водителя;

- обеспечивают принятие решений и проведение расследований в случае обнаружения недостач, излишков или других существенных несоответствий, а в случае выявления подозрительных или незаконных действий — оповещение соответствующих органов исполнительной власти;
- описывают все контрмеры, внедренные на контролируемом участке цепи поставок;
- описывают все меры и процедуры по восстановлению безопасности, которые должны быть внедрены на контролируемом участке цепи поставок, в случае реализации акта незаконного вмешательства;
- описывают все меры и процедуры, реализуемые при смене товаром фаз контроля организации,
- описывают процедуры по предоставлению уполномоченным лицам дополнительной информации об обрабатываемых товарах. Процедуры также должны включать в себя объемы и порядок запроса по представлению такой информации;
- описывают процедуры, указанные в разделе А.4.3.

А.4.2 Документация

Организация — участник цепи поставок должна хранить в защищенном месте следующие обновляемые документы:

- Паспорт участка цепи поставок;
- завершенную оценку уязвимости (охраны);
- персональные данные и данные о квалификации лиц, проводивших оценку уязвимости (охраны),
- перечень всех рассмотренных контрмер;
- Декларации об охране;
- План обеспечения безопасности (охраны) и приложения к нему;
- записи о результатах проведенных учений и тренировок с указанием тематик, задействованного персонала и дат проведения;
- другие документы, предписанные требованиями или высшим руководством.

А.4.3 Связь

Организация — участник цепи поставок, где это возможно, должна установить контакты с соответствующими органами исполнительной власти для обеспечения следующих целей:

- установления процедур для обнаружения незаконных действий с товарами или при возникновении подозрений на такие действия, а также чрезвычайных ситуаций или угроз в отношении международной цепи поставок. Такие процедуры должны содержать подробную информацию о способах связи с органами исполнительной власти и быть включены в План обеспечения безопасности (охраны) участка цепи поставок организации,
- участия в совещаниях и семинарах, проводимых соответствующими органами исполнительной власти, по вопросам таможенного регулирования перемещаемых организацией товаров и обеспечения их безопасности и охраны,
- открытого диалога с уполномоченными должностными лицами и соответствующими органами исполнительной власти о четком понимании гарантий эффективности Плана обеспечения безопасности (охраны) участка цепи поставок организации.

Если уполномоченные должностные лица соответствующих органов исполнительной власти не поддерживают свое участие в таком диалоге, организации следует документировать такие попытки с объяснением причин их неучастия.

А.5 Реализация Плана обеспечения безопасности (охраны)

Внедрение нового или пересмотренного Плана обеспечения безопасности (охраны) проводится оперативными методами с применением действующей в организации системы менеджмента, с тем чтобы гарантировать наличие достаточных ресурсов управления другими операциями, относящимися к обеспечению безопасности и охране, и проведения мониторинга эффективности функционирования Плана.

А.6 Документирование и мониторинг процессов обеспечения безопасности и охраны

Организация должна разработать и поддерживать в рабочем состоянии процедуры по осуществлению мониторинга и измерению функционирования собственной системы менеджмента безопасности, с тем чтобы гарантировать ее постоянную пригодность, применимость и результативность. При определении ключевых параметров мониторинга и измерений организация должна учитывать все угрозы и риски, а также их потенциальные последствия.

А.7 Постоянное улучшение

Руководство организации в ходе управления своей частью цепи поставок должно постоянно анализировать систему менеджмента ее безопасности, с тем чтобы определить потребность в ее совершенствовании.

Приложение В
(справочное)

Методика проведения оценки рисков и выработки контрмер

В.1 Общие положения

Настоящее приложение содержит методику, которую могут применять организации — участники цепи поставок для проведения оценки рисков реализации акта незаконного вмешательства, которые могут нанести ущерб деятельности организации, определения контрмер, соответствующих масштабам деятельности и размерам организации. В методике использована такая последовательность:

- составить перечень области деятельности организации,
- определить существующие меры управления обеспечением безопасности и охраны,
- определить сценарии угроз;
- определить последствия по каждому случаю реализации сценария угрозы;
- определить вероятность реализации акта незаконного вмешательства при существующем уровне безопасности (охраны),
- определить адекватность мер по обеспечению безопасности и охраны,
- при необходимости разработать дополнительные меры по обеспечению безопасности и охраны.

На рисунке В.1 представлено графическое описание процесса проведения оценки рисков и выработки контрметр.

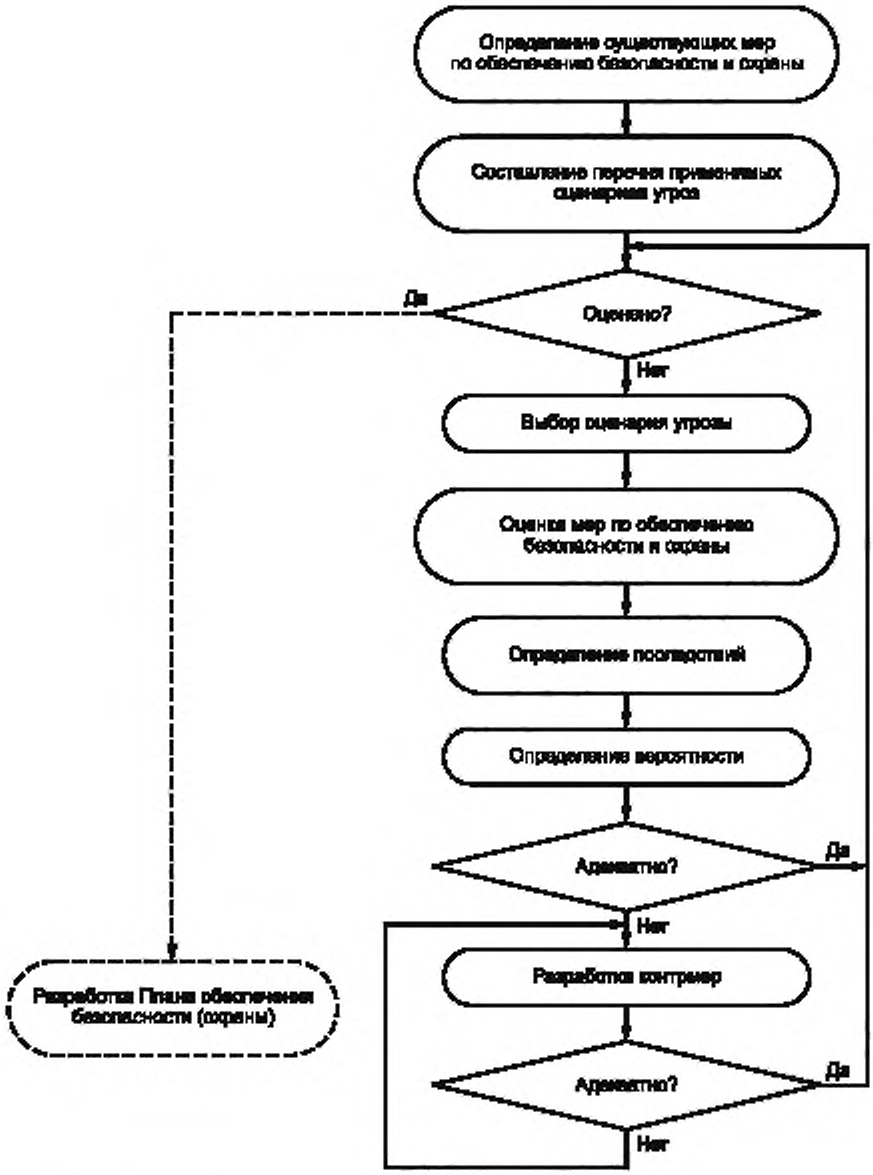

Рисунок В.1 — Схема процесса проведения оценки рисков и выработки контрмер

В.2 Первый шаг — рассмотрение сценариев угроз

При проведении оценки уязвимости (охраны) следует учитывать, как минимум, сценарии угроз, приведенные в таблице В.1. Также следует учитывать другие сценарии, установленные органами исполнительной власти, руководством цепи поставок или уполномоченными лицами, проводящими оценку уязвимости (охраны).

Таблица В.1 — Сценарии угроз цепи поставок

Примерные сценарии угроз	Возможные последствия
1 Незаконное проникновение и/или установление контроля над активом (включая транспортные средства)	Повреждение/разрушение актива; использование актива в качестве средства нанесения повреждений/разрушений; акции протеста населения, повлекшие за собой экономические потери; захват заложников/убийство людей
2 Использование цепи поставок для незаконного перемещения товаров	Нелегальное перемещение запрещенных предметов, в том числе оружия; нелегальное перемещение людей, в том числе террористов
3 Информационное вмешательство	Получение местного или удаленного доступа к информационным/документальным системам цепи поставок в целях нанесения ущерба или обеспечения проведения незаконных действий
4 Целостность товара	Подделка, подмена и/или кража в террористических целях
5 Несанкционированное использование	Использование деятельности международной цепи поставок для реализации террористических актов, включая использование транспортного средства в качестве оружия
6 Другое	

При проведении оценки уязвимости (охраны) следует учитывать:

- состояние контроля доступа:
  - к сооружениям организации — участника цепи поставок, включая окрестности,
  - транспортным средствам,
  - информации,
  - прочему;
- условия эксплуатации и технические характеристики транспортных средств:
  - при нормальной эксплуатации,
  - в местах технического обслуживания,
  - при соответствующих заменах запчастей, например из-за поломок,
  - при ротации транспортных средств,
  - при нахождении в местах стоянки,
  - при возможном использовании транспортных средств в качестве оружия,
  - прочее;
- условия обработки товаров:
  - при погрузке,
  - производстве,
  - хранении (включая промежуточное хранение),
  - перемещении,
  - выгрузке,
  - компоновке/раскомпоновке,
  - прочее;
- условия перемещения товаров:
  - по воздуху,
  - автодорогам,
  - железной дороге,
  - внутренним водным путям,
  - морю,
  - прочее;
- возможность выявления/предотвращения несанкционированных проникновений при поставке товаров;
- условия проведения инспекционных проверок (например, транспортных средств).
- характеристики персонала:
  - уровень компетентности, подготовки и понимания,
  - надежность,
  - другое;
- наличие деловых партнеров;
- состояние внутренней/внешней связи:
  - для обмена информацией,

- использования в чрезвычайных ситуациях,
- другое,

- состояние обработки данных о товарах и/или маршрутах его перемещения:
  - степень защищенности данных,
  - степень достоверности данных,
  - прочее,
- наличие внешней информации:
  - официальной, полученной от органов исполнительной власти,
  - касающейся отраслевых особенностей,
  - о ранее происшедших чрезвычайных ситуациях и актах незаконного вмешательства,
  - о возможностях и времени реагирования на чрезвычайные ситуации и акты незаконного вмешательства,
  - прочее.

В.3 Второй шаг — классификация последствий

При оценке последствий должны учитываться потенциальные человеческие и экономические потери. Оцениваемые последствия по каждому акту незаконного вмешательства должны классифицироваться как высокие, средние или низкие (см. таблицу В.2). В процессе проведения оценки уязвимости (охраны) могут использоваться численные значения последствий, которые впоследствии должны быть переведены в качественные.

Обоснование классификации последствий по каждому акту незаконного вмешательства должно быть документально оформлено.

Отнесение величин последствий к «высоким», «средним» или «низким» требует особого внимания. Использование чрезмерно низких показателей этих величин может привести к учету контрмер по значительно большему количеству сценариев угроз, чем это необходимо. Однако использование чрезмерно высоких показателей величин может привести к пренебрежению контрмерами по таким сценариям угроз, последствия от которых могут оказаться для организации и органов исполнительной власти недопустимыми.

Высокая степень последствий может быть определена как последствия, которые были бы неприемлемы во всех, но маловероятных ситуациях.

Средняя степень последствий может быть определена как последствия, которые были бы неприемлемы с высокой вероятностью ситуации.

Низкая степень последствий может быть определена как последствия, которые обычно являются приемлемыми.

Приемлемость не следует путать с желательностью или согласием. Приемлемость может рассматриваться как характеристика объемов возможного ущерба, которые организация или орган исполнительной власти по возможности готовы принять при определенных условиях. Организация или орган исполнительной власти могут установить объемы возможного ущерба, которые могут быть нежелательными, но все же приемлемыми.

Таблица В.2 — Классификация последствий

Степень	Последствия
Высокая	Наличие жертв и пострадавших в значительном масштабе и/или Воздействие на экономику — крупные повреждения активов и/или инфраструктуры, исключающие их дальнейшую деятельность, и/или Воздействие на экологию — полное поражение различных элементов экосистемы на обширной территории
Средняя	Наличие жертв и пострадавших в небольшом масштабе и/или Воздействие на экономику — повреждение активов и/или инфраструктуры, допускающее их функционирование после ремонта, и/или Воздействие на экологию — долговременный ущерб части экосистемы
Низкая	Наличие пострадавших и/или Воздействие на экономику — минимальные повреждения активов и/или инфраструктуры и систем, и/или Воздействие на экологию — некоторый ущерб окружающей среде

В.4 Третий шаг — классификация вероятности акта незаконного вмешательства

Статус физических и организационных мер по обеспечению безопасности и охраны в цепи поставок, зафиксированный в Опросном листе анализа функционирования и других предусмотренных документах, должен учитываться при классификации потенциальных актов незаконного вмешательства. Физические меры по обеспечению безопасности и охраны включают в себя меры по оснащению объекта средствами, которые препятствуют или выявляют несанкционированный доступ к цели. Организационные меры по обеспечению безопасности и охраны включают в себя действия персонала и процедуры, которые препятствуют или выявляют несанкционированный доступ к цели. Вероятность по каждому акту незаконного вмешательства в отношении отдельных активов должна классифицироваться как высокая, средняя и низкая.

Высокая вероятность определяется в случаях, когда проведенные мероприятия по обеспечению безопасности и охраны предполагают низкую защищенность от реализации акта незаконного вмешательства. Если при проведении оценки использовались численные значения, то результаты должны быть переведены в качественные значения.

Средняя вероятность определяется в случаях, когда проведенные мероприятия по обеспечению безопасности и охраны предполагают умеренную защищенность от реализации акта незаконного вмешательства.

Низкая вероятность определяется в случаях, когда проведенные мероприятия по обеспечению безопасности и охраны предполагают надежную защищенность от реализации акта незаконного вмешательства.

Обоснование классификации вероятности по каждому акту незаконного вмешательства должно быть документально оформлено.

В.5 Четвертый шаг — учет показателей акта незаконного вмешательства

Схема учета показателей акта незаконного вмешательства в качестве примера приведена в таблице В.3, которую возможно использовать при определении необходимости в разработке контрмер для отдельных актов незаконного вмешательства.

Таблица В.3 — Схема учета показателей акта незаконного вмешательства

Классификация вероятности				
высокая			средняя	низкая
Классификация последствий	Высокие	Контрмеры	Контрмеры	Учитывать
	Средние	Контрмеры	Контрмеры или учитывать, соответственно	Документировать
	Низкие	Учитывать	Документировать	Документировать

Идентификация и разработка контрмер для актов незаконного вмешательства требуется для тех из них, которые одновременно имеют высокие показатели вероятности и последствий, а также для актов со средним показателем вероятности и высоким показателем последствий. Для остальных актов незаконного вмешательства идентификация и разработка контрмер не требуется, за исключением случаев, если это не рекомендовано лицами, проводящими оценку уязвимости (охраны). Персонал, проводящий оценку уязвимости (охраны), обязан перечислить все акты незаконного вмешательства, в отношении которых требуется принятие контрмер.

Примечание — Соответствующие уполномоченные должностные лица могут устанавливать контрмеры для определенных сценариев угроз с чрезвычайно высокими показателями последствий вне зависимости от их вероятности, как соответствующие национальной политике. Разработанные для таких сценариев контрмеры должны оцениваться *органами исполнительной власти* на эффективность.

В.6 Пятый шаг — разработка контрмер

Если разработка контрмер необходима или она проводится по рекомендации лиц, проводящих оценку уязвимости (охраны), то следует уделять внимание вопросам уменьшения последствий и/или вероятности реализации сценариев угроз. Целью будет снижение вероятности реализации сценариев угроз или уменьшение убытков, которые могут произойти в случае их реализации до уровня, при котором разработка дополнительных контрмер больше не требуется.

Контрмеры могут применяться при следующих действиях.

- исправление: могут применяться организационные и/или физические меры;
- перемещение: перевод рисков может быть в рамках субподряда, физического перехода по месту или времени;
- прекращение: возможно, что из-за уровня риска по решению организации ее деятельность может быть приостановлена.

В определенных условиях организация вынуждена согласиться с риском (см. примечание ниже) ввиду того, что требуемые контрмеры нерезультативны или для их реализации у организации недостаточно полномочий, а также в силу других непреодолимых факторов.

Примечание — Допускается ситуация в имеющемся виде, поскольку организация не может предпринять каких-либо действий. Такие ситуации должны документироваться и периодически пересматриваться.

В.7 Шестой шаг — внедрение контрмер

Новые контрмеры представляют собой переход к организационным методам, которые должны внедряться в рамках существующей системы менеджмента, для того чтобы обеспечить наличие достаточных ресурсов, управляющее воздействие на другие операции и поддержку этого перехода руководством организации.

В.8 Седьмой шаг — оценка контрмер

Используя методы, изложенные в настоящем стандарте, каждая контрмера должна оцениваться на результативность по уменьшению вероятности и/или последствий до тех пор, пока степень риска не потребует отказаться от разработки дополнительных контрмер. Такая контрмера считается результативной и должна быть внесена в Отчет об оценке уязвимости (охраны).

В.9 Восьмой шаг — повторение процесса

Когда контрмеры будут разработаны и оценены на результативность, следует продолжить процесс по следующему сценарию угроз, пока перечень сценариев не будет исчерпан.

В.10 Непрерывность процесса

Процесс оценки непрерывен. Как показано на рисунке В.1, мониторинг обеспечения безопасности и охраны должен осуществляться постоянно, для того чтобы обеспечить гарантированную реализацию запланированных мер по обеспечению безопасности и охраны.

Приложение С
(справочное)

Руководство по оказанию помощи и сертификации

С.1 Общие положения

Организации, желающие внедрить настоящий стандарт, не обязаны пользоваться услугами консалтинговых организаций. В случае, если организация принимает решение о том, что ей нужен совет или помощь в проведении оценки уязвимости (охраны), в разработке Плана обеспечения безопасности (охраны) или в выполнении необходимых требований, она может воспользоваться услугами консалтинговой организации. При этом организация — соискатель консалтинговых услуг должна убедиться в компетентности привлекаемой консалтинговой организации, например, путем изучения рекомендаций этой консалтинговой организации или отзывов о выполненных ею ранее работах. Консалтинговые организации не могут участвовать в проведении сертификации организаций, которым они оказывали консалтинговые услуги.

С.2 Демонстрация соответствия стандарту ГОСТ Р 53662—2009 посредством аудита

Настоящий стандарт — это подробное изложение требований, способствующих организациям, принявшим на себя добровольную ответственность по их внедрению, установить и демонстрировать адекватный уровень обеспечения безопасности и охраны на контролируемых ими участках цепи поставок. Таким образом, настоящий стандарт служит основанием для определения, проверки или демонстрации существующего уровня обеспечения безопасности и охраны в пределах цепи поставок организации посредством аудита. Аудит проводится первой, второй или третьей стороной или органом исполнительной власти, который решит использовать соответствие организации требованиям настоящего стандарта в качестве основания для ее принятия в контролируемые ими программы обеспечения безопасности и охраны цепи поставок.

Виды аудита:

- аудит, проводимый первой стороной, — определение соответствия, выполняемое организацией самостоятельно,
- аудит, проводимый второй стороной, — проведение оценки соответствия организации согласованным критериям, которая осуществляется другой организацией, учреждением или органом, заинтересованным в деятельности организации — участника цепи поставок,
- аудит, проводимый третьей стороной, — проведение оценки соответствия согласованным критериям, которая выполняется уполномоченным органом по сертификации, независимым от всех сторон.

Сертификация организаций проводится органом по сертификации, уполномоченным компетентным органом исполнительной власти по техническому регулированию и метрологии.

Органы исполнительной власти, решившие использовать соответствие организации требованиям настоящего стандарта в качестве основания для ее принятия в контролируемые ими программы обеспечения безопасности и охраны цепи поставок, могут сертифицировать организацию самостоятельно или с привлечением признанных ими уполномоченных органов по сертификации.

С.3 Сертификация по ГОСТ Р 53662—2009 органами по сертификации третьей стороны

Если демонстрация соответствия осуществляется посредством аудита, проводимого третьей стороной, тогда организация, добивающаяся сертификации, должна выбрать такой орган по сертификации третьей стороны, *который признан компетентным органом исполнительной власти по техническому регулированию и метрологии.*

Приложение D
(обязательное)

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

Таблица D.1

Обозначение ссылочного национального, межгосударственного 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 53663—2009	MOD	ИСО 28000:2005 «Система менеджмента безопасности цепи поставок. Требования»
ГОСТ Р 53660—2009	MOD	ИСО 20858:2004 «Суда и морские технологии. Оценка охраны и разработка планов охраны портовых средств»
Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: - IDT — идентичные стандарты; - MOD — модифицированные стандарты.		

Библиография

[1] Рамочные стандарты безопасности и облегчения мировой торговли. Всемирная таможенная организация
[2] Международный кодекс по управлению безопасной эксплуатацией судов и предотвращению загрязнения (ISM Code), Международная морская организация
[3] Международный кодекс по охране судов и портовых средств (ISPS Code), Международная морская организация
[4] ISO/PAS 17712 Freight containers — Mechanical seals (Грузовые контейнеры. Механические затворы)

УДК 656.614.3.004:006.354 ОКС 13.310, 47.020.99 Т 51

Ключевые слова: уполномоченный экономический оператор, международная цепь поставок, риск-менеджмент, план обеспечения безопасности

Редактор *А.Д. Чайка*
Технический редактор *В.Н. Прусакова*
Корректор *Т.И. Кононенко*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 15.10.2010. Подписано в печать 10.11.2010. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 3,26. Уч.-изд. л. 2,80. Тираж 141 экз. Зак. 893.

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