ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28001— 2019

Системы менеджмента безопасности цепи поставок

НАИЛУЧШИЕ ПРАКТИКИ ОСУЩЕСТВЛЕНИЯ БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК, ОЦЕНКИ И ПЛАНОВ БЕЗОПАСНОСТИ

Требования и руководство по применению

(ISO 28001:2007, IDT)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Ассоциацией по сертификации «Русский Регистр» (Ассоциация Русский Регистр) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 010 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 23 декабря 2019 г. № 1433-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28001:2007 «Системы менеджмента безопасности цепи поставок. Наилучшие практики осуществления безопасности цепи поставок, оценки и планов безопасности. Требования и руководство по применению» (ISO 28001:2007 «Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance», IDT).

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

5 ВЗАМЕН ГОСТ Р 53662—2009 (ИСО 28001:2006)

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

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

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Основные положения 4
4.1 Заявление о применении 4
4.2 Бизнес-партнеры 4
4.3 Международно признанные сертификаты или одобрения 4
4.4 Бизнес-партнеры, освобожденные от предоставления декларации по безопасности 5
4.5 Анализ безопасности бизнес-партнеров 5
5 Процесс безопасности цепи поставок 5
5.1 Общие положения 5
5.2 Идентификация области оценки безопасности 5
5.3 Проведение оценки безопасности 6
5.4 Разработка плана обеспечения безопасности цепи поставок 6
5.5 Выполнение плана обеспечения безопасности цепи поставок 6
5.6 Документация и мониторинг процесса обеспечения безопасности цепи поставок 7
5.7 Меры, которые необходимо проводить после инцидента в области безопасности 7
5.8 Защитные меры по обеспечению безопасности информации 7
Приложение А (справочное) Процесс обеспечения безопасности цепи поставок 8
Приложение В (справочное) Методология оценки риска в области безопасности и разработка контрмер 15
Приложение С (справочное) Руководство по получению консультаций и сертификации 21
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 22
Библиография 23

Введение

Инциденты, связанные с нарушением безопасности международных цепей поставок, представляют собой угрозу международной торговле и экономическому росту государств, занятых в сфере торговли. Люди, грузы, инфраструктуры и оборудование, в том числе средства транспортировки, должны быть защищены от инцидентов, связанных с нарушением безопасности и их возможными разрушительными последствиями. Такая защита выгодна как экономике государств, так и обществу в целом.

Международные цепи поставок являются весьма динамичными и объединяют множество организаций и деловых партнеров. Настоящий стандарт признает всю сложность этой проблемы. Настоящий стандарт разработан с учетом того, чтобы отдельные организации могли применять его требования с учетом конкретной бизнес-модели своей организации, ее ролью и функцией в международной цепи поставок.

Настоящий стандарт обеспечивает возможность установить и документировать разумный уровень безопасности в рамках международных цепей поставок и их частей, что позволит организациям принимать более взвешенные с точки зрения риска решения в отношении их безопасности.

Настоящий стандарт является мультимодальным и предназначен для того, чтобы наряду и в дополнение к рамочным стандартам Всемирной таможенной организации обеспечить безопасность и облегчить мировую торговлю (основное). Его назначение не сводится к тому, чтобы охватить, заменить или отменить отдельные программы таможенных организаций, касающиеся безопасности цепи поставок и их требований по сертификации и валидации.

Использование настоящего стандарта должно способствовать установлению надлежащего уровня безопасности организации в рамках той (тех) части(ей) международной цепи поставок, которые она контролирует. Настоящий стандарт является также основой для определения или подтверждения уровня безопасности, существующего в рамках цепи(ей) поставок таких организаций, внутренними или внешними аудиторами или теми государственными учреждениями, которые выбирают использование такого соответствия настоящему стандарту и в качестве основы для принятия программ безопасности в своих цепях поставок. Клиенты, деловые партнеры, правительственные и другие организации могут обратиться с просьбой к организации, заявляющей о своем соответствии настоящему стандарту, пройти аудит или проверку для подтверждения такого соответствия. Государственные учреждения могут взаимно договориться о принятии оценок соответствия, выполненных другими правительственными организациями. В случае необходимости проведения аудита третьей стороной организация должна рассмотреть возможность привлечения стороннего органа по сертификации, аккредитованного компетентным органом, являющимся членом Международного форума по аккредитации (см. приложение С).

В задачу настоящего стандарта не входит дублирование государственных требований и рамочных стандартов безопасности цепи поставок Всемирной таможенной организации (ВТО). Организации, которые уже имеют сертификацию или валидацию взаимно признанными правительственными органами, отвечают требованиям настоящего стандарта.

Выходными данными настоящего стандарта должны быть:

- Заявление об области распространения, которое определяет границы цепи поставок, охватываемые планом обеспечения безопасности;
- Оценка безопасности, которая документирует уязвимость цепи поставок к определенным сценариям угрозы безопасности. А также описывает последствия, которые целесообразно предвидеть по каждому сценарию потенциальных угроз безопасности;
- План обеспечения безопасности, который описывает меры безопасности вместо управления сценариями угроз безопасности, выявленных при оценке безопасности;
- Учебные программы, определяющие уровень подготовки сотрудников службы безопасности, отвечающего за безопасность, для выполнения своих служебных обязанностей.

Для проведения оценки безопасности, необходимой для подготовки плана обеспечения безопасности, организация, использующая настоящий стандарт, должна идентифицировать предполагаемые угрозы (сценарии угроз безопасности), определить вероятные действия людей по каждому из сценариев угроз безопасности, выявленных при оценке безопасности, при возникновении инцидента безопасности.

Такого рода определение проводится путем анализа текущего состояния безопасности цепи поставок. Основываясь на выводах этого анализа выносится профессиональное заключение об уязвимости той или иной цепи по каждому из сценариев угрозы безопасности.

Если цепочка поставок по сценарию является недопустимо уязвимой в обеспечении угрозы безопасности, организация должна разработать дополнительные процедуры или функциональные оперативные изменения для снижения вероятности, последствий или того и другого. Эти изменения называются контрмерами. Контрмеры, исходя из системы приоритетов, должны быть включены в план обеспечения безопасности для снижения существующей угрозы до приемлемого уровня.

Приложения А и В являются наглядными примерами менеджмента риска, основанного на процессах безопасности и направленного на защиту людей, имущества и миссии международной цепи. Они облегчают макроподход в отношении комплексных цепей поставок и/или более дискретный подход к их частям.

Эти приложения также предназначены для портовых средств и других средств инфраструктуры или предприятия для того, чтобы:

- облегчить понимание, принятие и внедрение методологий, которые могут быть созданы самими организациями;
- служить руководством для основной линии по постоянному улучшению менеджмента безопасности;
- оказывать помощь организациям в управлении ресурсами для решения существующих и возникающих рисков безопасности;
- описать возможные способы оценки рисков и смягчения последствий угроз безопасности в цепи поставок, начиная с размещения сырья и хранения до изготовления и транспортировки готовой продукции к месту продажи.

В приложении С даны указания в отношении консультаций и сертификации по настоящему стандарту, если применяющая его организация выберет эту опцию.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системы менеджмента безопасности цепи поставок

НАИЛУЧШИЕ ПРАКТИКИ ОСУЩЕСТВЛЕНИЯ БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК, ОЦЕНКИ И ПЛАНОВ БЕЗОПАСНОСТИ

Требования и руководство по применению

Security management systems for the supply chain. Best practices for implementing supply chain security, assessments and plans. Requirements and guidance

Дата введения — 2020—07—01

1 Область применения

В настоящем стандарте приводятся требования и руководство для организаций, принимающих участие в международных цепочках поставок для того, чтобы:

- разработать и внедрить процессы безопасности цепи поставок;
- установить и документировать минимальный уровень безопасности в рамках цепи поставки(ок) или в какой-либо из ее частей;
- содействовать в достижении соответствия критериям, предъявляемым к уполномоченному экономическому оператору (УЭО), сформулированным в рамочных стандартах безопасности и облегчения мировой торговли Всемирной таможенной организации, и существующим законодательным и нормативным актам, регламентирующим обеспечение безопасности в цепи поставок;
- помочь в отношении определения соответствия критериям, установленным для уполномоченного экономического оператора (УЭО), изложенным в рамочных стандартах Всемирной таможенной организации, и национальным программам по безопасности 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.

Пользователи настоящего стандарта должны:

- определить часть международной цепи, в пределах которой они установили безопасность (см. 4.1);
- провести оценки уровня безопасности на эту часть цепи поставок и разработать адекватные контрмеры;
- разработать и внедрить план обеспечения безопасности цепи поставок;
- подготовить сотрудников службы безопасности в соответствии с их должностными обязанностями.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая любые изменения).

Издание официальное

ISO 20858:2007, Ships and marine technology — Maritime port facility security assessments and security plan development (Суда и морские технологии. Оценка безопасности оборудования морских портов и разработка плана обеспечения безопасности)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

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 **актив(ы)** (asset(s)): Заводы, машинное оборудование, имущество, здания, подвижной состав, суда, воздушные суда, транспортные средства и другие элементы инфраструктуры или завода и связанные с ними системы, которые имеют особую и поддающуюся количественной оценке бизнес-функцию или услугу.

Примечание — Это определение включает в себя любую информационную систему, которая является неотъемлемой частью обеспечения безопасности 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 цепи поставок.

Примечания

1 Уполномоченный экономический оператор — термин, определенный в рамочных стандартах Всемирной таможенной организации.

2 К уполномоченным экономическим операторам относятся в частности производители, импортеры, экспортеры, брокеры, перевозчики, консолидаторы, посредники, порты, аэропорты, операторы терминалов, интегрированные операторы, склады и дистрибьюторы.

3.4 **деловой партнер** (business partner): Те подрядчики, поставщики или провайдеры услуг, с которыми организация заключает договор об оказании помощи для выполнения своей функции в цепи поставок (3.15).

3.5 **грузовая транспортная единица** (cargo transport unit): Автотранспортное средство, железнодорожный грузовой вагон, грузовой контейнер, автоцистерна, железнодорожные цистерны или передвижные цистерны.

3.6 **последствия** (consequence): Гибель людей, экономический ущерб или ущерб имуществу, в том числе разрушение транспортных систем (которые можно предвидеть) в результате нападения на организацию в цепи поставок или использования цепи поставок в качестве оружия.

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

Пример — Ящик, палета, грузовая транспортная единица, погрузочно-разгрузочное оборудование, грузовой автомобиль, судно, самолет и железнодорожный вагон.

3.8 **контрмеры** (countermeasures): Меры, предпринимаемые для снижения вероятности сценария угрозы безопасности в достижении его цели или предпринимаемые для уменьшения вероятных последствий сценария угрозы безопасности.

3.9 **фаза контроля** (custody): Период времени, когда организация в цепочке поставок непосредственно сама контролирует изготовление, обработку, погрузку и перемещение грузов и связанную с ним товаросопроводительную документацию цепи поставок.

3.10 **фаза постконтроля** (downstream): Погрузочно-разгрузочные работы, процессы и перемещение, когда товары в цепи поставок находятся вне сферы контроля этой организации.

3.11 **товары** (goods): Те изделия или материалы, которые после размещения заказа на поставку, должны быть изготовлены, обработаны, отгружены или перевезены в рамках цепи поставок для использования или их потребления покупателем.

3.12 **международная цепь поставок** (international supply chain): Цепь поставок, которая в какой-то момент пересекает международную или экономическую границу.

Примечания

1 Все части этой цепи считаются международными, начиная с размещения заказа на поставку по заключенному контракту до момента прохода таможенного контроля в стране назначения или в сфере экономики.

2 Если таможенная очистка груза из определенных стран или сфер экономики исключена из договоров или региональных соглашений, то конечным пунктом международной цепи поставок является порт страны назначения или сфера экономики, где товар, при отсутствии таможенных соглашений или договоров, должен будет пройти таможенную очистку.

3.13 **вероятность** (likelihood): Мера возможности превращения сценария угрозы безопасности в инцидент безопасности.

Примечание — Оценка вероятности выполняется, исходя из существующей устойчивости процессов безопасности в отличие от инцидента, связанного со сценарием угрозы безопасности, который рассматривается и выражается в качественном или количественном отношении.

3.14 **система менеджмента** (management system): Система организации для управления процессами или деятельностью, которая преобразует входные данные по ресурсам в продукцию или услугу, отвечающую целям организации.

Примечание — Цель настоящего стандарта не сводится к конкретизации систем менеджмента, т.е. стандарт не требует создания отдельной системы обеспечения безопасности. Примерами систем менеджмента являются ИСО 9001 (Система менеджмента качества), ИСО 14001 (Система экологического менеджмента), ИСО 28000 (Спецификация на системы менеджмента безопасности цепи поставок) и Международный кодекс по управлению безопасностью (МКУБ) Международной морской организации.

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

- производит, перемещает, обрабатывает, осуществляет погрузку, консолидацию, разгрузку или получение товара путем размещения заказа на покупку, который пересекает международную или экономическую границу;
- осуществляет транспортировку грузов в международной цепи поставок любым способом независимо от того, пересекает ли груз национальную (или экономическую) границы, или
- обеспечивает, управляет или осуществляет формирование, распределение или движение сопроводительной документации, используемой как таможенными органами, так и в бизнесе.

3.16 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в области риска.

3.17 **объем услуг** (scope of service): Совокупность операций, которые выполняет организация в цепи поставок, и места, где она эти операции выполняет.

3.18 **декларация безопасности** (security declaration): Документально оформленное обязательство бизнес-партнера, где определены меры безопасности, осуществляемые этим бизнес-партнером и включающие, как минимум, способы защиты товаров и реальных инструментов международной торговли, связанной с ними информации, а также способы демонстрации и проверки мер безопасности.

Примечание — Она (декларация безопасности) должна использоваться организацией в цепи поставок для оценки адекватности мер по обеспечению безопасности грузов.

3.19 **план обеспечения безопасности** (security plan): Документ, содержащий запланированные мероприятия для обеспечения адекватного менеджмента безопасности.

Примечания

1 План составляется для обеспечения реализации тех мер, которые защищают организацию от инцидентов, нарушающих безопасность.

2 Такой план может быть включен в состав других оперативных планов.

3.20 **безопасность** (security): Устойчивость к умышленным действиям, направленным на причинение вреда или ущерба цепи или цепью поставок.

Примечание — Люди могут быть/не быть работниками данной организации.

3.21 **инцидент в сфере безопасности** (security incident): Любое действие или обстоятельство, которое порождает последствия (3.6).

3.22 **сотрудники службы безопасности** (security personnel): Те люди в организации цепи поставок, на которых возложены функции по обеспечению безопасности.

Примечание — Люди могут быть/не быть работниками данной организации.

3.23 **конфиденциальная информация/конфиденциальные материалы** (security sensitive information, security sensitive materials): Информация или материалы, подготовленные или включенные в процесс обеспечения безопасности цепи поставок и содержащие сведения о процессах, связанных с безопасностью, грузах, или правительственные директивы, которые не будут легкодоступны общественности и которые могут быть полезными тому, кто захочет спровоцировать инцидент безопасности.

3.24 **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, производственное оборудование, логистических провайдеров, внутренние распределительные центры, дистрибьюторов, оптовиков и другие организации, участвующие в производстве, обработке, транспортировке и доставке грузов и связанных с ними услуг.

3.25 **объект атаки** (target): Персонал, транспортные средства, товары, материальные активы, производственные процессы и транспортировка, системы контроля или документооборота, существующие в рамках организации, задействованные в цепи поставок.

3.26 **сценарий угрозы безопасности** (security threat scenario): Способ, посредством которого может произойти потенциальный инцидент в сфере безопасности.

3.27 **фаза предконтроля** (upstream): Транспортировка, процессы и перемещение товаров, имеющие место до того, как организация принимает товар под свой контроль в цепи поставок.

3.28 **Всемирная таможенная организация (ВТО)** (World customs organization (WCO)): независимый межправительственный орган, чья миссия заключается в повышении результативности и эффективности таможенного администрирования.

Примечание — ВТО — единственная в мире межправительственная организация, компетентная в таможенных вопросах.

4 Основные положения

4.1 Заявление о применении

Организация должна описать в заявлении о применении ту часть международной цепи поставок, которая по ее утверждению соответствует настоящему стандарту. Заявление о применении должно, как минимум, включать следующую информацию:

a) подробное описание организации;

b) объем услуг;

c) фамилии и контактную информацию по всем бизнес-партнерам в рамках определенного объема услуг;

d) дату выполнения оценки безопасности и срок действия этой оценки и

e) подпись лица, уполномоченного подписать документ от имени этой организации.

Организации в цепи поставок могут распространить заявление о применении на другие части цепи, например, включая пункт конечного назначения.

4.2 Бизнес-партнеры

Если в рамках цепи поставок, описанных в заявлении о применении, организация пользуется услугами партнеров по бизнесу, то в соответствии с положениями 4.3 и 4.4 она должна потребовать от них предоставить декларацию по (обеспечению) безопасности.

Организация должна рассмотреть эту декларацию по безопасности при выполнении своей оценки безопасности и при необходимости потребовать принятия конкретных контрмер.

4.3 Международно признанные сертификаты или одобрения

Транспортные компании и владельцы транспортных средств, являющиеся держателями международно признанных сертификатов или одобрений, выданных во исполнение обязательных международных конвенций, регулирующих безопасность в различных транспортных секторах, должны иметь инструкции по безопасности, планы и процессы, которые отвечают применимым требованиям настоящего

стандарта и не требуют проведения аудита для подтверждения их соответствия. Судоходным компаниям, владельцам судов и портового оборудования, свидетельства или одобрения должны выдаваться в соответствии с СОЛАС XI-2 / 4 либо с СОЛАС XI-2/10.

Согласно разделу 1 настоящего стандарта национальные таможенные органы могут потребовать от транспортных компаний и владельцев транспортных средств помимо наличия международно признанных сертификатов по безопасности или одобрений дополнительных мер по безопасности как условия для назначения компании УЭО.

4.4 Бизнес-партнеры, освобожденные от предоставления декларации по безопасности

Бизнес-партнеры, которые доказали организации, что они:

a) подтвердили соответствие настоящему стандарту или ИСО 20858;

b) подпадают под требования 4.3 или

c) были назначены в качестве УЭО-А национальным таможенным управлением в соответствии с ее программой безопасности цепи поставок, отвечающей требованиям рамочных стандартов безопасности ВТО (WCO SAFE Framework), должны быть указаны в заявлении о применении. В таких случаях у организации нет необходимости выполнять дополнительную оценку безопасности таких бизнес-партнеров или требовать от них предоставления декларации о безопасности.

4.5 Анализ безопасности бизнес-партнеров

За исключением бизнес-партнеров, перечисленных в 4.3 или 4.4, организация в цепи поставок должна проводить анализ процессов и оборудования своих партнеров для выяснения обоснованности представленных ими деклараций по безопасности. Объем и периодичность анализа должны определяться на основе анализа существующих рисков. Результаты проведенных анализов должны храниться в организации.

Примечание — В последующих пунктах в целях удобства восприятия организация, заявляющая о своем соответствии, включая те части ее поставок, которые находятся в ведении деловых партнеров, независимо от того, соответствует это или нет настоящему стандарту, именуется как «организация», если не требуется иное для однозначного понимания этого.

5 Процесс безопасности цепи поставок

5.1 Общие положения

Необходимо, чтобы организации, участвующие в международных цепях поставок и принявшие к действию настоящий стандарт, не только управляли безопасностью своей части цепочки, но также и имели на местах систему менеджмента для ее обеспечения. Настоящий стандарт требует наличия безопасных практик и/или процессов для обеспечения безопасности и их осуществления, в целях снижения риска в международной цепи поставок от той деятельности, которая может привести к инциденту безопасности.

Организации в цепи поставок, заявляющие о своем соответствии настоящему стандарту, должны иметь план обеспечения безопасности, основанный на результатах оценки безопасности и содержащий документально оформленные существующие меры безопасности и процедуры, а также по мере необходимости контрмеры, если это применимо к той части международной цепи поставок, которая включена в заявление о применении.

5.2 Идентификация области оценки безопасности

Область оценки безопасности должна включать все виды деятельности, выполняемые организацией, указанные в заявлении о применении (см. 4.1). Эта оценка должна проводиться с определенной периодичностью, а план обеспечения безопасности должен пересматриваться по мере необходимости. Результаты оценки должны быть документально оформлены и находиться на хранении в организации.

Оценка безопасности должна также охватывать информационные системы, документы и сети, относящиеся к погрузочно-разгрузочным работам и перемещению грузов во время нахождения их в этой организации. Существующие мероприятия безопасности должны с учетом 4.3 и 4.4 подлежать оценке на всех площадках и для бизнес-партнеров, где имеется вероятность уязвимости безопасности.

5.3 Проведение оценки безопасности

5.3.1 Оценка персонала

Лицо или группа лиц, выполняющих оценку безопасности, должны в совокупности обладать практическим опытом и знаниями, которые должны включать, но не ограничиваться только этим, следующее:

- методы оценки риска, применимые ко всем аспектам международной цепи поставок, с момента приема груза организацией под свой контроль до момента, когда груз выходит из-под контроля организации или покидает международную цепь поставок;
- использование соответствующих мер для недопущения несанкционированного вскрытия или доступа к материалам особой важности с точки зрения безопасности;
- операции и процедуры, применяемые при производстве, обработке, погрузочно-разгрузочных операциях, перевозке и/или связанные с документацией на товары, в зависимости от обстоятельств;
- понимание методики угрозы безопасности и методики подавления;
- соблюдение настоящего стандарта.

Имя (имена) лиц или членов группы, выполняющих оценку, а также их квалификация, должны быть документированы.

5.3.2 Процесс оценки

Организация должна установить, осуществлять и поддерживать процедуру(ы) по идентификации существующих контрмер для снижения угроз безопасности. Организация должна иметь перечень применяемых сценариев угроз безопасности, включая и те, которые одобряются соответствующими государственными органами. Если государственные органы не участвовали в проведении оценки, то это должно быть отражено документально.

Для каждого сценария угрозы безопасности организация должна оценить существующие контрмеры и определить вероятность и последствия, соответствующие каждому из сценариев, а также оценить необходимость дополнительных контрмер для снижения рисков безопасности до приемлемого уровня.

В соответствии с 4.2 организация должна проанализировать каждую из представленных бизнес-партнерами деклараций по безопасности и дать профессиональную оценку знаний объекта(ов) и/или требований регулирующего органа. При определении применимости декларации по безопасности организация также может получать и использовать любую другую доступную ей информацию.

При выполнении оценки безопасности и определении общей уязвимости цепи, описанной в заявлении о применении, организация должна проанализировать детали и пригодность каждой декларации.

Не следует подвергать дальнейшей оценке бизнес-партнеров, подпадающих под положения 4.3 или 4.4.

В процессе оценки должна быть документирована следующая информация:

a) все рассмотренные сценарии угроз безопасности;

b) процессы, использованные при оценке тех угроз, а также

c) все идентифицированные контрмеры и приоритеты.

5.4 Разработка плана обеспечения безопасности цепи поставок

Организации должны разработать и поддерживать план обеспечения безопасности для всей части цепи, описанной в своих заявлениях о применении. Такой план может быть разбит на приложения, в которых приводится описание безопасности каждого конкретного участка цепи поставок, включая меры безопасности бизнес-партнеров организации, подпадающие под положения 4.3 или 4.4, которые они должны поддерживать в соответствии со своими декларациями по безопасности. План/приложения должны также содержать информацию о том, каким образом организация будет контролировать и осуществлять периодический пересмотр этих деклараций по безопасности.

При разработке своих планов обеспечения безопасности организации должны анализировать и руководствоваться рекомендациями (указаниями), приведенными в справочных приложениях А и В.

5.5 Выполнение плана обеспечения безопасности цепи поставок

Организация должна разработать систему менеджмента, позволяющую внедрить ее специальные процессы обеспечения безопасности цепи поставок.

5.6 Документация и мониторинг процесса обеспечения безопасности цепи поставок

5.6.1 Общие положения

Организация должна разработать и поддерживать процедуры по документированию, мониторингу и измерению выполнения своей системы менеджмента, упомянутой выше. Организация должна периодически проводить плановые аудиты системы менеджмента для обеспечения уверенности, что система должным образом разработана и поддерживается. Результаты аудитов должны быть документированы и храниться в организации.

5.6.2 Постоянное улучшение

Организация должна выполнять оценку возможностей улучшения своих мероприятий по обеспечению безопасности как одного из средств повышения безопасности своей части цепи поставок.

5.7 Меры, которые необходимо проводить после инцидента в области безопасности

После любого инцидента, имеющего отношение к любой из частей международной цепи поставок, контролируемых организацией, данная организация должна провести анализ своего плана по обеспечению безопасности. Этот анализ должен:

a) определить причину инцидента и необходимое корректирующее действие;

b) определить результативность мер и процедур по обеспечению исправления положения в плане безопасности и

c) рассмотреть сделанные выводы, повторно оценить эти части цепи поставок в соответствии с 5.3.2.

В случае нарушения безопасности организация должна, в случае необходимости, руководствоваться существующими процедурами отчетности для таможенных и/или соответствующих правоохранительных органов, а также положениями, изложенными в плане по безопасности и в контрактных обязательствах.

Организация должна сохранять партию товара и другие необходимые данные цепи поставок в течение срока, предписанного действующими законами и нормативными актами.

5.8 Защитные меры по обеспечению безопасности информации

Планы по обеспечению безопасности, меры, процессы, процедуры и записи организации должны рассматриваться в качестве информации особой важности с точки зрения обеспечения безопасности и защиты от несанкционированного доступа или разглашения. Такая информация должна быть доступна только тем лицам, которым «необходимо знать». Кроме соответствующих правоохранительных должностных лиц или их номинантов, лицом, которому «необходимо знать», может быть:

a) лицо, которому необходим доступ к конкретной конфиденциальной информации по безопасности для проведения деятельности, включенной в план обеспечения безопасности;

b) лицо, проходящее подготовку для выполнения видов деятельности, приведенных в плане обеспечения безопасности;

c) лицо, осуществляющее контроль за деятельностью других лиц, осуществляющих ее в соответствии с планом обеспечения безопасности, или

d) лицо-участник либо действующее от имени участника, которому в соответствии с условиями контракта с данной организацией был предоставлен доступ к конфиденциальной информации, контролируемой организацией в соответствии с согласованными правилами и условиями.

Примечание — Если организация сертифицирована по ИСО 28001 третьей стороной — органом по сертификации, аккредитованным компетентным органом по аккредитации, или была сертифицирована или признана соответствующей требованиям ИСО 28001 взаимно признанными государственными органами, то согласованный договором доступ к конфиденциальной информации этой организации не может расцениваться в качестве обязательного и в любом случае будет зависеть от согласия организации. Тот факт, что ее особой важности информация по безопасности защищена от несанкционированного доступа или раскрытия, не освобождает организацию от инструктирования своих бизнес-партнеров и других лиц о механизмах и системах, связанных с безопасностью цепи поставок.

Приложение А
(справочное)

Процесс обеспечения безопасности цепи поставок

А.1 Общие положения

Настоящее приложение представляет собой руководство по разработке процесса обеспечения безопасности цепи поставок, которое может быть внедрено в организации, имеющей систему менеджмента. Рисунок А.1 представляет графическое описание такого процесса.

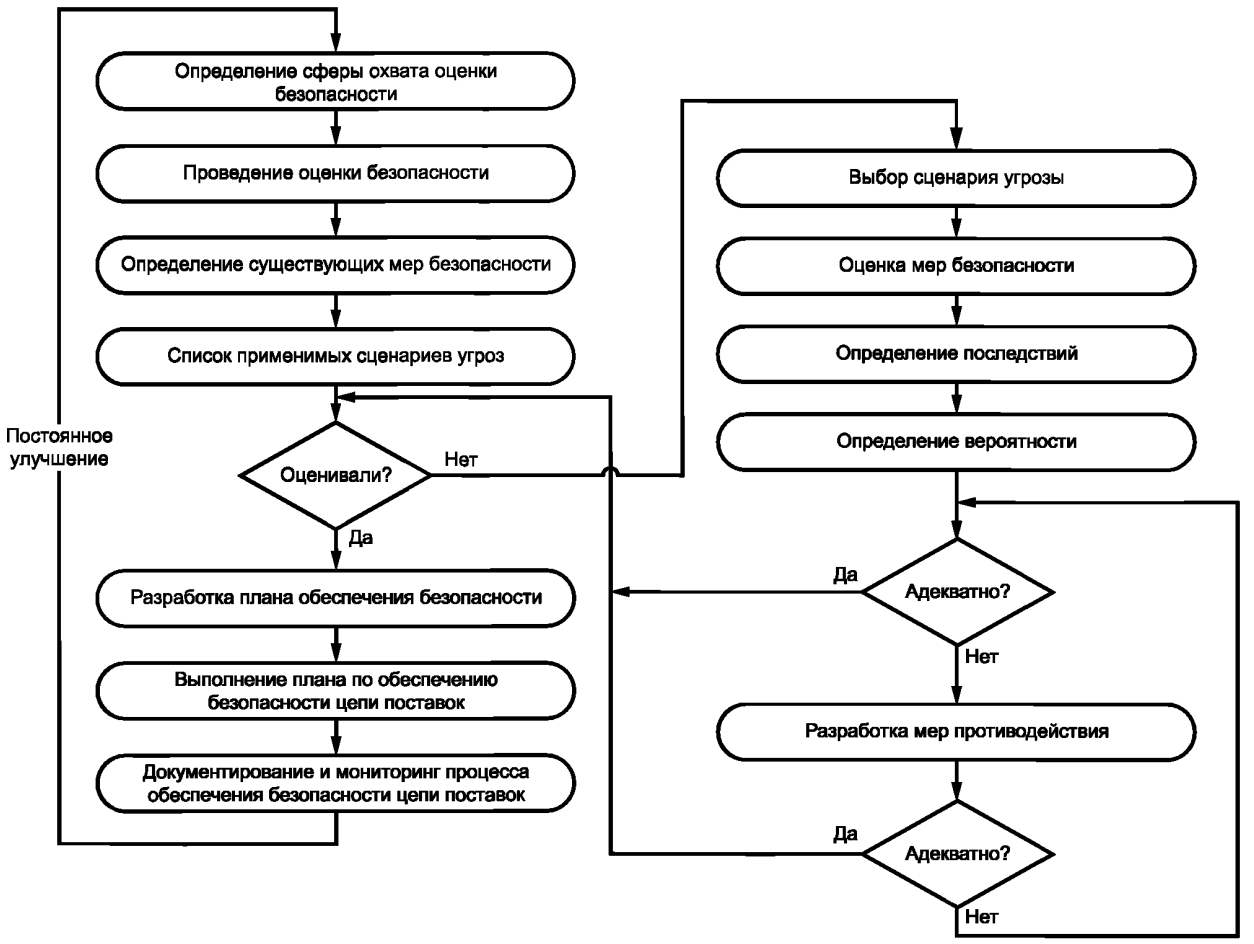


Рисунок А.1 — Графическое описание процесса безопасности цепи поставок

А.2 Модель зрелости

Оценка безопасности представляет собой попытку выявить риски, связанные с безопасностью части цепи поставок организации в соответствии с ее заявлением о применении, желанием привести ее в соответствие с настоящим стандартом. Для выполнения такой оценки необходимо установить границы области применения (как физические, так и виртуальные).

А.3 Подробная самооценка элементов

А.3.1 Общие положения

С помощью квалифицированного персонала следует выполнить оценку мероприятий обеспечения безопасности во всех местах, где существует потенциальная уязвимость, которые должны включать, но не ограничиваться следующим:

- места производства товаров, их обработки или погрузочных работ до помещения их на транспортную единицу, укладки на поддоны для транспортировки или подготовки к их отгрузке иным образом;
- места хранения подготовленных к отправке товаров или складирования товара до его транспортировки;
- места перевозки грузов;
- места погрузки/выгрузки на/с транспортного средства;
- места смены ответственности по контролю за грузом;
- места, где документация или информация, касающаяся перевозимых товаров, обрабатывается, подготавливается или становится доступной;
- направления транспортных маршрутов внутри страны и различные виды перевозочных средств, используемых при транспортировке;
- иные.

А.3.2 Опросный лист анализа функционирования

Рассматриваемый опросный лист анализа функционирования представляет собой пример системного подхода к анализу существующих мероприятий по обеспечению безопасности.

Следует, чтобы те части анализа, которые относятся к бизнес-партнерам, доказавшим данной организации, что они:

a) подтвердили соответствие настоящему стандарту или ИСО 20858;

b) подпадают под положения 4.3 или

c) были назначены в качестве УЭО в соответствии с программой национального таможенного агентства по безопасности цепи поставок, которая по определению должна соответствовать рамочным стандартам ВТО по безопасности, содержали ссылку на то, как этот фактор был учтен, например соответствует настоящему стандарту, ИСО 20858 или Кодексу ОСПС.

А.3.3 Анализ функционирования

Ниже, в таблице А.1, приводится опросный лист анализа функционирования, который можно заполнить и учитывать при выполнении оценки уровня безопасности для организации в цепи поставки. Этот перечень не является всеобъемлющим и может быть адаптирован с учетом оценки риска и бизнес-модели организации. Если приведенный показатель уже выполняется в организации в цепи поставок, тогда подлежит проверке блок «Да». Если не выполняется или выполняется частично, то проверке подлежит блок «Нет» и, где применимо, в колонке «Комментарии» следует привести объяснение, описывающее применение других альтернативных мер или ссылку на то, что вероятность риска очень низкая. Если показатель не применяется или находится вне области распространения Заявления о применении организации, тогда в разделе «Комментарии» должна быть сделана пометка «Не применяется» (NA). Пункты перечня, которые не могут быть выполнены в силу применяемых законов/нормативных документов, следует пометить в колонке «Комментарии» как запрещенные.

Таблица А.1 — Опросный лист анализа функционирования

Фактор анализа	Да	Нет	Комментарии
Управление безопасностью цепи поставок			
Имеет ли организация систему менеджмента, которая занимается вопросами безопасности цепи поставок?			
Есть ли в организации лицо, отвечающее за безопасность цепи поставок?			
План обеспечения безопасности			
Имеет ли организация(и) текущии(е) план(ы) по обеспечению безопасности?			
Обращен ли данный план к ожиданиям организации в части безопасности и ожиданиям бизнес-партнеров по восходящему и нисходящему потокам?			
Имеет ли организация антикризисное управление, целостность бизнеса и план восстановления безопасности?			
Безопасность (активов)			
Располагает ли организация на местах мерами, направленными на: - физическую безопасность зданий; - мониторинг и контроль внешних и внутренних периметров;			

Продолжение таблицы А.1

Фактор анализа	Да	Нет	Комментарии
- наличие приборов контроля, препятствующих несанкционированному доступу к оборудованию, транспортным средствам, эстакадам под загрузку — разгрузку, погрузочным и грузовым отсекам, а также административного контроля за выдачей удостоверения личности (работнику, посетителю, продавцу и т.д.) и других средств контроля?			
Существуют ли технологии оперативной безопасности, которые значительно усиливают защиту имущества? Например, обнаружение проникновения или система камер записи видеонаблюдения / слежения, которые охватывают зоны, имеющие важное значение для функционирования цепи поставок, причем записи хранятся довольно длительный период времени, позволяющий их использовать при расследовании в случае инцидента			
Существуют ли на местах протоколы о контактах сотрудников внутренней службы безопасности или внешних правоохранительных органов в случае нарушения безопасности?			
Существуют ли процедуры, позволяющие ограничить, обнаружить и сообщить о несанкционированном доступе ко всем складским помещениям и транспортным средствам?			
Удостоверяется личность лиц, доставляющих или получающих груз до его погрузки-выгрузки?			
Обязанности сотрудников службы безопасности			
Есть ли в организации процедуры оценки добросовестности работников до их трудоустройства и периодической оценки их отношения к своим обязанностям, связанным с безопасностью?			
Проводит ли организация соответствующую подготовку для оказания помощи работникам при выполнении ими своих функций по обеспечению безопасности, например сохранность целостности груза, выявление потенциальной внутренней угрозы для безопасности, защита и контроль доступа?			
Ставит ли компания в известность своих работников о наличии процедур для передачи ими информации о подозрительных инцидентах?			
Регистрируется ли системой контроля доступа немедленное изъятие у работника компании просроченного удостоверения личности, а также доступ к конфиденциальной информации и к информационным системам?			
Информационная безопасность			
Существуют ли процедуры для обеспечения того, чтобы вся используемая информация по обработке груза как в электронном, так и в рукописном виде была отчетливой, своевременной, точной и защищенной от исправления, утери или внесения неверных данных?			
Проводит ли организация сверку документов на отгрузку или на получение груза с соответствующей товаросопроводительной документацией?			
Обеспечивает ли организация точность и своевременность передачи информации на груз, полученной от деловых партнеров?			

Продолжение таблицы А.1

Фактор анализа	Да	Нет	Комментарии
Защищены ли соответствующие данные за счет использования систем хранения данных, не зависящие от работы основной системы обработки данных (есть ли на местах резервное дублирование данных)?			
Все ли пользователи имеют уникальный идентификатор (идентификатор пользователя), необходимый для личного и единственного использования, с помощью которого можно проследить за их деятельностью?			
Эффективна ли система управления паролями, используемыми для аутентификации пользователей, и должны ли пользователи, как минимум, раз в год менять свои пароли?			
Есть ли защита от несанкционированного доступа и злоупотребления информацией?			
Безопасность товаров и их транспортировки			
Существуют ли процедуры, позволяющие ограничить, обнаружить и сообщить о несанкционированном доступе к местам транспортировки, местам проведения погрузки-выгрузки и хранению грузов в закрытых транспортных средствах?			
Квалифицированные ли лица назначаются для контроля грузовых операций?			
Существуют ли процедуры для уведомления соответствующих правоохранительных органов в тех случаях, когда организацией обнаруживаются или предполагаются какие-то нарушения или нелегальная деятельность?			
Существуют ли в организации процедуры по обеспечению целостности товара / груза, когда эти товары / грузы передаются другой организации (транспортные услуги, центр по консолидации, использование смешанных видов транспорта и т.п.) в цепи поставок?			
Существуют ли на местах процессы для отслеживания изменений уровня угрозы по ходу транспортных маршрутов?			
Существуют ли правила безопасности, процедуры и руководящие указания, предназначенные для транспортных диспетчеров (например, недопущение опасных маршрутов)?			
Закрытые грузовые транспортные единицы			
Рамочные стандарты безопасности ВТО включают в себя «Программу целостности пломбы», описанную в дополнении к приложению 1, которое устанавливает процедуры, касающиеся установки и проверки пломб повышенной секретности и/или других устройств для препятствия доступа. Персоналу, заполняющему эту форму, следует ознакомиться с данным дополнением рамочных стандартов			
Если используются закрытые грузовые транспортные единицы, то имеются ли на местах документально оформленные процедуры для установки и регистрации механических пломб высокого уровня секретности, отвечающие требованиям ИСО/PAS 17712 и/или другие устройства для пломбирования, выдаваемые стороне, производящей загрузку грузовой транспортной единицы?			

Окончание таблицы А.1

Фактор анализа	Да	Нет	Комментарии
Если используются закрытые грузовые транспортные единицы, то имеются ли на местах документально оформленные процедуры проверки на наличие признаков вскрытия пломб при смене транспорта при отгрузки?			
Если используются закрытые грузовые транспортные единицы, то проводится ли стороной, производящей загрузку, его проверка на чистоту непосредственно перед загрузкой?			
Если используются закрытые грузовые транспортные единицы, то имеются ли на местах документально оформленные процедуры по проведению проверки стороной, производящей загрузку непосредственно перед их заполнением, физической целостности, в том числе надежности запорных механизмов транспортной единицы? Рекомендуется проводить инспекцию по семи пунктам: - передняя стенка; - левая сторона; - правая сторона; - пол; - потолок/крыша; - внутри/снаружи перекрытия; - наружная часть/шасси			

А.3.4 Сценарии угроз безопасности

При выполнении оценки безопасности необходимо рассмотреть сценарии угрозы безопасности, не ограничиваясь только теми, которые перечислены в таблице А.2. Оценка безопасности должна также учитывать и другие сценарии, которые могут быть определены государственными органами, руководством организации или профессионалом(ами) в области безопасности, занимающимися выполнением оценки.

Таблица А.2 — Сценарии угроз безопасности

Сценарии и угрозы безопасности	Возможные последствия
1 Вмешательство и/или взятие под контроль собственности (включая транспорт) в рамках цепи поставок	Порча/уничтожение собственности (в том числе транспорта) в рамках цепи поставок. Порча/уничтожение вне целевого использования собственности или товаров. Причина — гражданские волнения или беспорядки экономического характера. Захват заложников/убийство людей
2 Использование цепи поставок, как средства борьбы с контрабандой	Незаконный ввоз оружия в страну или вывоз из страны/экономика. Терроризм в стране или за пределами страны/экономика
3 Фальсификация информации	Получение локального или удаленного доступа к системам информации/документации цепи поставок для нарушения операций или содействия незаконной деятельности
4 Целостность груза	Саботаж и/или хищение в террористических целях
5 Несанкционированный доступ	Проведение операций в международной цепи поставок для содействия террористическим инцидентам, в том числе использование способа транспортировки в качестве оружия
6 Прочее	

А.4 Использование инструментов для самооценки

А.4.1 Общие положения

План обеспечения безопасности и/или приложения необязательно должен представлять собой самостоятельные документы, они могут быть включены в оперативные планы или процедуры. Если план обеспечения безопасности включен в другие планы организации, то в этом случае, чтобы убедиться в соблюдении всех требований плана обеспечения безопасности, в них должна быть включена и таблица с перекрестными ссылками.

План может быть разделен на приложения, каждое из которых описывает безопасность конкретного участка цепи поставок, включая те меры безопасности, за безопасность которых должны нести ответственность их бизнес-партнеры в соответствии с их декларациями (если применимо). Этот план/приложения должны также содержать четкие указания на то, каким образом организация будет осуществлять мониторинг или периодический пересмотр их деклараций по безопасности. План обеспечения безопасности/приложения должны включать, но не ограничиваться, описанием следующего:

- участка цепи поставок, рассматриваемой данным планом или приложением;
- должностных обязанностей, связанных с обеспечением безопасности для всех сотрудников службы безопасности;
- структуры менеджмента безопасности, включая персональные данные лица, назначенного в качестве менеджера по безопасности;
- внутренней и внешней контактной информации по чрезвычайным ситуациям, которая должна использоваться персоналом в отчетности по инцидентам, связанным с безопасностью;
- навыков и знаний, которыми должны обладать сотрудники службы безопасности;
- учебных программ по безопасности;
- процесса аттестации лиц, назначенных для выполнения установленных обязанностей по обеспечению безопасности, способствующего овладению необходимыми навыками и знаниями для выполнения своих функциональных обязанностей;
- как реализуются элементы плана обеспечения безопасности. Для удовлетворения этих требований могут быть использованы: участие в запуске государственной программы по подготовке в области безопасности или обучение персонала организации;
- процессов, отвечающих, как минимум, требованиям безопасности, введенным правительством на непредвиденные обстоятельства или для повышения уровня безопасности.

План обеспечения безопасности должен содержать процедуры, включающие, но не ограничивающиеся только мерами, которые, как минимум:

- обеспечивают получение информации об отгрузке товаров до того, как перевозимые грузы принимаются организацией для их дальнейшей транспортировки;
- обеспечивают, что полученные организацией товары/грузы для их консолидации/деконсолидации, сверены с информацией на товары/грузы, указанные в судовых документах/списке. Отправка товарных/грузовых единиц должна быть сверена с приказом на поставку или с распоряжением о выдаче товара/или части груза по коносаменту со склада;
- обеспечивают надлежащую идентификацию водителей, доставляющих или получающих товары/грузы до получения ими или отгрузки товаров или грузовых единиц;
- обеспечивают надлежащую идентификацию не только непосредственно водителей транспортных средств, но и их пассажиров;
- обеспечивают, что любые недостачи/излишки, а также другие существенные расхождения или отклонения от норм устранены и/или должным образом расследуются, а соответствующие правоохранительные органы уведомлены об обнаружении незаконной или подозрительной деятельности (в зависимости от обстоятельств);
- описывают любые контрмеры и процедуры, которые были осуществлены в этой части цепи;
- описывают любые контрмеры и процедуры, которые были осуществлены в этой части цепи поставок для восстановления ее безопасности в случае инцидента;
- описывают процедуры по предоставлению уполномоченному персоналу дополнительной информации о перевозимых товарах. Она должна включать способ определения пользователем законности запроса о предоставлении дополнительной информации и как/какая информация должна быть предоставлена;
- описывают процедуры, установленные в соответствии с А.4.3.

А.4.2 Документация

Организация должна хранить в безопасном месте самые последние версии следующей документации:

- заявлений о применении;
- выполненную оценку безопасности;
- имена и данные по квалификации персонала, выполнявшего оценку безопасности;
- перечень всех рассмотренных контрмер;
- декларации безопасности;
- план обеспечения безопасности и при необходимости приложения;
- записи о проведенных учебных тренировках с указанием тематик, задействованного персонала и дат проведения;
- другая информация, предусмотренная нормативными документами и руководством.

А.4.3 Связь

Организации следует установить, по мере целесообразности, контакт с соответствующими правоохранительными и другими государственными должностными лицами в следующих целях:

- установление процедур, которым надлежит следовать в случае фальсификации или подозрения на фальсификацию товара/груза или в чрезвычайных ситуациях, а также в случае получения угроз, касающихся международной цепи поставок. Эти процедуры должны, если это предусмотрено, включать конкретные телефонные номера, по которым следует звонить в соответствующие правительственные учреждения. Эти процедуры должны быть включены в план обеспечения безопасности цепи поставок;
- участие (при необходимости) в консультациях, проводимых соответствующими государственными должностными лицами на национальном и местном уровнях, для обсуждения вопросов, представляющих взаимный интерес, в том числе таможенных правил и процедур, а также требований по обеспечению безопасности помещений и груза;
- реагирование на государственные информационно-пропагандистские усилия и внесение своего вклада в диалог, обеспечивающий понимание того, что план обеспечения безопасности организации остается актуальным и эффективным.

Если соответствующие правоохранительные и другие государственные должностные лица не хотят участвовать в таком диалоге, организации следует документировать свою попытку(и) и констатировать, что соответствующие правоохранительные и другие правительственные чиновники не принимали участия в диалоге.

А.5 Реализация плана обеспечения безопасности

Внедрение нового или пересмотренного плана обеспечения безопасности представляет собой изменение в оперативной практике и должно осуществляться в соответствии с системой менеджмента организации для обеспечения того, что в наличии есть надлежащие ресурсы, влияние на другие операции является управляемым, а результативность плана контролируется и оценивается.

А.6 Документация и мониторинг процесса обеспечения безопасности

Организации следует установить и поддерживать процедуры по мониторингу и оценке деятельности своей системы менеджмента безопасности в целях обеспечения ее продолжающей стабильности, адекватности и результативности. При определении частоты измерения и мониторинга ключевых параметров эффективности организации следует рассмотреть угрозы и риски, связанные с безопасностью, в том числе механизмы потенциального ухудшения и их последствия.

А.7 Постоянное улучшение

Руководству организации при оперативном управлении своей части цепи поставок следует провести анализ системы менеджмента безопасности для оценки возможностей ее улучшения и необходимости внесения в нее изменений.

Приложение В
(справочное)

Методология оценки риска в области безопасности и разработка контрмер

В.1 Общие положения

В данном приложении приводится методология, которая может быть использована организациями в международных цепях поставок для проведения оценки риска их деятельности, которая может пострадать от инцидентов, связанных с нарушением безопасности, а также для определения соответствующих контрмер, эффективных для данного типа и размера деятельности в цепи поставок. В методологии необходимо использовать такую последовательность действий:

a) перечислить все виды деятельности, приведенные в области применения;
b) определить элементы управления безопасностью на местах, существующие на данный момент;
c) идентифицировать сценарии угрозы безопасности;
d) определить последствия, если сценарий угрозы безопасности был закончен;
e) определить, какова вероятность данного происшествия с учетом существующего уровня безопасности;
f) определить, адекватны ли существующие меры контроля безопасности;
g) если нет, то разработать дополнительные меры безопасности.

Рисунок В.1 является графическим представлением данного процесса.

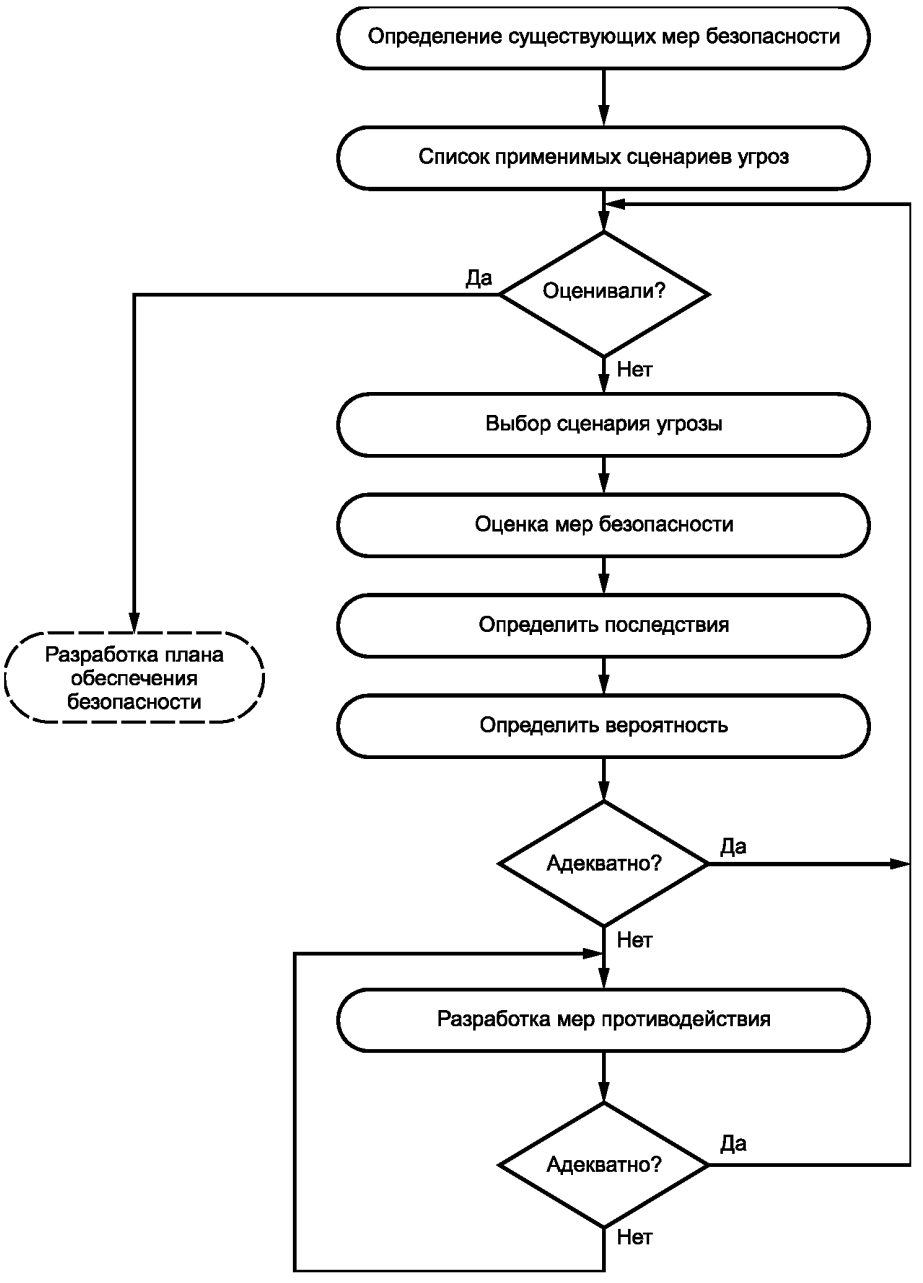


Рисунок В.1 — Графическое представление методологии оценки рисков в области безопасности

В.2 Шаг первый — рассмотрение сценариев угроз безопасности

При выполнении оценки безопасности следует, как минимум, рассмотреть сценарии угрозы безопасности, перечисленные в таблице В.1, а также другие сценарии, выявленные государственными органами, руководством цепи поставок или профессионалами в области безопасности, выполняющими такие оценки.

Таблица В.1 — Сценарии угроз безопасности цепи поставок

Примеры сценариев угроз безопасности	Примеры использования (возможные последствия)
1 Вмешательство и/или взятие под контроль собственности (включая транспорт) в рамках цепи поставок	Порча/уничтожение собственности Порча/уничтожение вне целевого использования собственности или товаров Причина — акции протеста населения или беспорядки экономического характера Захват заложников/убийство людей
2 Использование цепи поставок как средства организации контрабанды	Незаконный ввоз оружия в страну или вывоз из страны Терроризм в стране или за пределами страны
3 Фальсификация информации	Получение локального или удаленного доступа к системам информации/документации цепи поставок с целью нарушения деятельности или содействия незаконной деятельности
4 Целостность груза	Подкуп, саботаж и/или хищение в террористических целях
5 Несанкционированное использование	Проведение операций в международной цепи поставок для содействия террористическим актам (например, использование транспортных средств в качестве оружия)
6 Прочее	

При проведении оценки необходимо рассмотреть следующее:

1) контроль доступа:
   - в помещения организации в цепи поставок, включая прилегающую территорию;
   - на транспортные средства (автомобильный, железнодорожный, воздушный, баржи, суда и т.п.);
   - к информации;
   - другое;

2) транспортные средства (грузовые автомобили, железнодорожный транспорт, баржи, самолеты, корабли и т.д.), с учетом:
   - нормальной эксплуатации;
   - помещения — мастерские для технического обслуживания (например, площадка для проведения работ);
   - вынужденные изменения, к примеру в связи с неисправностью;
   - смена назначения;
   - транспортные средства, находящиеся в неподвижном состоянии;
   - использование транспортного средства в качестве оружия;
   - другое;

3) погрузочно-разгрузочные работы:
   - погрузка;
   - хранение (в том числе промежуточное хранение);
   - передача;
   - выгрузка;
   - деконсолидация/консолидация;
   - другое;

4) перевозка грузов:
   - воздушным транспортом;
   - автомобильным транспортом;
   - железнодорожным транспортом;
   - внутренними судоходными путями;
   - морскими судами;
   - другое;

5) обнаружение (несанкционированного) доступа/предотвращение применительно к партии товара;

6) в ходе инспекций, например осмотр транспортных средств;

7) работники:
- уровень компетентности, профессиональной подготовки и информированности;
- добросовестность;
- другое;

8) использование бизнес-партнеров;

9) связь внутренняя/внешняя:
- обмен информацией;
- чрезвычайные ситуации;
- другое;

10) обработка или переработка информации о грузах или транспортных маршрутов:
- защита данных;
- обеспечение данных;
- другое;

11) внешняя информация:
- правовая;
- заказы со стороны властей;
- отраслевая практика;
- происшествия и инциденты;
- возможность первой реакции и время реагирования;
- другое.

В.3 Второй шаг — классификация последствий

При проведении оценки последствий следует учитывать возможность людских и экономических потерь. Последствия каждого инцидента в сфере безопасности, оцениваемые в цепи поставок, должны классифицироваться как высокие, средние или низкие (см. таблицу В.2). До тех пор, пока результаты не будут преобразованы в качественную систему, в процессе оценки можно пользоваться числовой системой.

Обоснование при классификации последствий каждого инцидента в области безопасности должно быть документировано.

При классификации последствий и указании их числовых значений («высокое», «среднее» и «низкое») следует проявлять осторожность. Использование чрезмерно низких пороговых значений может привести к необходимости рассмотрения контрмер по большему количеству сценариев угрозы безопасности, чем это на самом деле необходимо. Однако при использовании слишком высоких пороговых значений можно пропустить контрмеры по целостности сценариев угрозы безопасности; последствия для этой организации или правительства, под чьим руководством она действует, будут недопустимыми.

«Высокая» классификационная категория последствия может рассматриваться как последствие, которое было бы неприемлемым во всех ситуациях, но с низкой вероятностью.

«Средняя» классификационная категория последствия может рассматриваться как последствие, которое было бы неприемлемым с высокой вероятностью ситуации.

«Низкая» классификационная категория последствия может, как правило, рассматриваться как приемлемое последствие.

Не следует путать приемлемость с желательностью или одобрением. Приемлемость скорее может быть расценена как согласие с размером возможного ущерба, на который организация или правительство, в рамках которого она работает, готова согласиться при определенных условиях, связанных с вероятностью. Организация или правительство может определить, что вероятность определенного уровня ущерба может быть хоть и нежелательной, но приемлемой.

Таблица В.2 — Классификация последствий

Определение категории	Последствие
Высокая	«Смерть и увечье» — гибель людей в определенных масштабах и/или «Экономическое воздействие» — серьезный ущерб активам и/или инфраструктуре, препятствующий дальнейшим операциям, и/или «Воздействие на окружающую среду» — полное уничтожение нескольких аспектов экосистемы на большой площади
Средняя	«Смерть и увечье» — например, гибель людей и/или «Экономическое воздействие» — например, повреждение имущества и/или инфраструктуры, требующие ремонта, и/или «Воздействие на окружающую среду» — например, нанесение вреда части экосистемы на длительный срок

Окончание таблицы В.2

Определение категории	Последствие
Низкая	«Смерть и увечье» — травмы, но без гибели людей и/или «Экономическое воздействие» — минимальное повреждение имущества и/или инфраструктуры и систем, и/или «Воздействие на окружающую среду» — например, нанесение незначительного экологического ущерба

В.4 Шаг третий — классификация по степени вероятности инцидентов в области безопасности

При классификации потенциальных инцидентов в области безопасности должны быть приняты во внимание статус физических и оперативных мер по обеспечению безопасности цепи поставок, документированный в перечне для проведения анализа эффективности безопасности, а также представленный в других документах. Физические меры по безопасности включают в себя объекты, которые препятствуют или обнаруживают несанкционированный доступ к объектам атаки. Оперативные меры по обеспечению безопасности включают людей и процедуры, которые препятствуют или обнаруживают несанкционированный доступ к объекту атаки. Вероятность каждого инцидента в области безопасности, происходящего на отдельном объекте, должны быть классифицированы как высокая, средняя и низкая.

Категория высокой степени вероятности должна присваиваться тогда, когда меры безопасности на местах предполагают незначительную устойчивость к инциденту по безопасности. Если в процессе оценки используется числовая система, то числовые результаты должны быть преобразованы в эту качественную систему.

Категория средней степени вероятности должна присваиваться тогда, когда меры безопасности на местах предполагают умеренную устойчивость к возникновению инцидента в области безопасности.

Категория низкой степени вероятности должна присваиваться тогда, когда меры безопасности на местах предполагают достаточную устойчивость к возникновению инцидента в области безопасности.

Основание для классификации по степени вероятности, присваиваемой каждому инциденту в области безопасности, должно быть документировано.

В.5 Шаг четвертый — шкала для инцидента в области безопасности

В таблице В.3 приведена шкала балльности для инцидента в области безопасности, представляющая собой пример, который может быть использован для определения необходимости контрмер для конкретных инцидентов в области безопасности.

Таблица В.3 — Шкала балльности инцидента в области безопасности

Классификация/ последствия	Классификация по (степени) вероятности		
	Высокая	Средняя	Низкая
Высокая	Контрмеры	Контрмеры	Рассмотреть
Средняя	Контрмеры	Контрмеры или рассматривать как соответствующую	Документировать
Низкая	Рассмотреть	Задокументировать	Документировать

Идентификация контрмер необходима для инцидентов в области безопасности, которые имеют высокий балл в обеих графах — вероятность и последствия, а также средний балл — в графе вероятность и высокий балл — в графе последствия. Для других инцидентов по безопасности контрмеры не требуются, если только они не считаются целесообразными с точки зрения оценщика. Лицу, выполняющему оценку безопасности, следует включать в список каждый из инцидентов безопасности для рассмотрения контрмер.

Примечание — Соответствующие правоохранительные и другие государственные должностные лица могут устанавливать контрмеры для некоторых сценариев, имеющих чрезвычайно высокий балл, которые должны быть приняты вне зависимости от вероятности, как вопрос национальной политики. Контрмеры, разработанные в результате этого исключения, должны быть рассмотрены правительством с точки зрения их эффективности.

В.6 Шаг пятый — разработка контрмер

Если разработка контрмер необходима или, по мнению лица, производящего оценку, считается желательной, то следует рассмотреть сценарии последствий и/или вероятности угрозы безопасности для смягчения их последствий. Целью этих мер является снижение вероятности сценария угрозы безопасности в будущем или уменьшение ущерба, который может быть вызван этими сценариями до уровня, при котором дополнительные контрмеры больше не потребуются.

Контрмеры могут быть представлены следующими видами деятельности:

- Исправление: организационные и/или физические меры.
- Передача: передача рисков может осуществляться путем заключения контрактов с субподрядчиками, физической передачи на другие площадки, переноса на другое время и т.д.
- Завершение: вполне возможно, что из-за уровня риска организация примет решение не продолжать деятельность.

При определенных обстоятельствах организация может согласиться с риском (см. примечание) из-за нереальности выполнения необходимых контрмер, отсутствия полномочий для их введения или других непреодолимых факторов.

Примечание — Допущение ситуации означает, что организацией не могут быть предприняты никакие действия. Такие виды деятельности и оценки должны быть документированы и подвергаться периодическому анализу.

В.7 Шаг шестой — осуществление контрмер

Новые контрмеры представляют собой изменение оперативной практики и могут быть приняты в соответствии с системой менеджмента организации для обеспечения того, что имеются достаточные ресурсы; влияние на другие операции контролируется, а данное изменение пользуется поддержкой руководства.

В.8 Шаг седьмой — оценка контрмер

При использовании способов, указанных в настоящем стандарте, следует оценивать результативность каждой из контрмер по снижению вероятности или последствиям (или их комбинацию) до тех пор, пока угроза безопасности больше не будет требовать рассмотрения вопроса о применении дополнительных контрмер. Достижение результативности контрмеры расценивается как достижение поставленной цели, что и следует отражать в отчете по оценке безопасности.

В.9 Шаг восьмой — повторение этого процесса

После того, как контрмеры были разработаны и оценены как результативные, следует продолжить процесс по следующему сценарию угрозы безопасности до тех пор, пока список сценариев не будет исчерпан.

В.10 Продолжение процесса

Процесс оценки носит непрерывный характер. Как видно из рисунка В.1, контроль безопасности должен выполняться непрерывно для обеспечения планомерного выполнения мер по обеспечению безопасности, процесс же оценки следует выполнять по мере необходимости.

Приложение С
(справочное)

Руководство по получению консультаций и сертификации

С.1 Общие положения

Организации, намеревающиеся внедрить ИСО 28001, не обязаны получать услуги внешнего (стороннего) консультанта. Если организация решает, что ей нужна консультация или помощь в проведении оценки уровня безопасности, разработке планов обеспечения безопасности и выполнении необходимых требований, она может прибегнуть к услугам внешнего консалтинга. Однако организация, заинтересованная в консультации, сама несет ответственность за проверку и подтверждение компетенции консультантов, предлагающих консалтинговые услуги, например путем поиска положительных отзывов, ссылок или путем анализа выполненной работы. Консультанты, которые предоставляют услуги этой организации, не могут участвовать в аудитах этой организации, проводимых третьей стороной.

С.2 Демонстрация соответствия стандарту ИСО 28001 при аудите

ИСО 28001 является подробным изложением требований, предназначенных для того, чтобы помочь организациям, которые решают добровольно внедрить требования, создать и продемонстрировать соответствующий уровень безопасности в рамках той части (частей) международной цепи поставки(ок), которые находятся под их контролем. Поэтому он служит основой для определения, подтверждения или демонстрации уровня безопасности, существующей в рамках цепи поставки(ок) организаций посредством процесса проверки (аудита) первой, второй или третьей стороной, или любым правительственным учреждением, которое решает использовать соответствие настоящему стандарту в качестве основы для включения в свои программы цепи безопасности поставок.

Типы аудита:

- Аудит первой стороны представляет собой определение соответствия самой организацией.
- Аудит второй стороны представляет собой определение или проверку соответствия организации критериям, согласованным с другой организацией, учреждением или органом, который заинтересован в участии организации в цепи поставок.
- Аудит третьей стороны представляет собой определение или проверку соответствия согласованным критериям организацией независимой от всех сторон.

Валидация и сертификация правительством или государственным органом.

Государственные органы, заинтересованные в соответствии требованиям настоящего стандарта и использовании его в качестве основы в своих программах цепи безопасности, возможно пожелают сами сертифицировать и подтвердить свое соответствие или, чтобы избежать дублирования, могут рассчитывать на проведение аудитов другими сторонами. ВТО устанавливает руководящие принципы для таможенных администраций в отношении требований к валидации и сертификации для национальных таможенных программ безопасности цепи согласно рамочным стандартам безопасности ВТО, а также для взаимного признания таких программ.

С.3 Сертификация по ГОСТ Р ИСО 28001 органами по сертификации третьей стороны

Если соответствие устанавливается аудитом третьей стороны, то организации, желающей пройти сертификацию, следует рассмотреть вопрос о выборе органа по сертификации третьей стороны, аккредитованного компетентным органом по аккредитации, как, например, таким, который является членом Международного форума по аккредитации (МАФ (IAF)), и подчиняются Многосторонним соглашениям о признании МФА (Multilateral Recognition Arrangement (MLA)). Такие аккредитационные органы соответствуют международно признанным правилам, кодексам практики и протоколам аудитов, таким как ИСО 17021 и ИСО 19011.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 20858:2007	—	*

* Соответствующий национальный стандарт отсутствует. До его приятия рекомендуется использовать перевод на русский язык данного международного стандарта. Официальный перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

Библиография

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

[2] ISO 14001:2004, Environmental management systems — Requirements with guidance for use (Система экологического менеджмента. Требования и руководство по применению)

[3] ISO17021:2006, Conformity assessment — Requirements for bodies providing audit and certification of management systems (Оценка соответствия. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента)

[4] ISO /PAS 17712:2006, Freight containers — Mechanical seals (Грузовые контейнеры. Устройства пломбировочные механические)

[5] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing (Руководящие указания по аудиту систем менеджмента)

[6] ISO 20858:2004, Ships and marine technology — Maritime port facility security assessments and security plan development (Судовые и морские технологии. Оценка безопасности оборудования морских портов. Разработка плана обеспечения безопасности)

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

[8] ISO 28003:2007, Security management systems for the supply chain — Requirements for bodies. providing audit and certification of supply chain security management systems (Системы менеджмента безопасности цепи поставок. Требования к органам, осуществляющим аудит и сертификацию цепи поставок)

[9] International Safety Management (ISM) Code, International Maritime Organization (Международный кодекс по управлению безопасностью (МКУБ))

[10] SAFE Framework of Standards — Appendix to Annex 1, World Customs Organization (Рамочные стандарты по безопасности. Дополнение к Приложению 1, ВТО)

УДК 656.61:006.354 ОКС 03.100.01

Ключевые слова: система менеджмента, безопасность цепи поставок, оценка цепи поставок, план обеспечения безопасности цепи поставок, оценка соответствия, цепь поставок

БЗ 2—2020/42

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 06.02.2020. Подписано в печать 10.02.2020. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,16.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru