ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28004-3— 2018

СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководящие указания по внедрению ИСО 28000

Часть 3

Дополнительное специальное руководство по внедрению ИСО 28000 в организациях среднего и малого бизнеса (за исключением морских портов)

[ISO 28004-3:2014, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports), IDT]

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации оборонной продукции и технологий» (ФГУП «Рособоронстандарт») на основе официального перевода на русский язык англоязычной версии указанного в пункте 4 стандарта, который выполнен ФГУП «Стандартинформ»

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 27 июля 2018 г. № 435-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28004-3:2014 «Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ИСО 28000. Часть 3. Дополнительное специальное руководство по принятию ИСО 28000 для использования в операциях среднего и малого бизнеса (кроме морских портов)» [ISO 28004-3:2014 «Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)», IDT].

Международный стандарт разработан Техническим комитетом ISO/TC 8 «Суда и морские технологии».

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые элементы настоящего стандарта могут являться объектами патентных прав

*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, 2014 — Все права сохраняются
© Стандартинформ, оформление, 2018

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 Дополнительные указания 1
4 Документация 11
5 Руководство для организаций среднего и малого бизнеса в части получения консультаций и сертификации 12
5.1 Общие положения 12
5.2 Демонстрация соответствия ИСО 28000 посредством аудита 12
5.3 Сертификация ИСО 28000 независимыми органами по сертификации. 12
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 13
Библиография 14

Введение

ИСО 28000:2007, а также руководство по его внедрению, изложенное в стандартах серии ИСО 28004, разработаны в связи с возникшей потребностью в наличии идентифицируемых критериев оценки (процедуры валидации) системы менеджмента цепи поставок, по отношению к которым системы менеджмента безопасности в целях установления соответствия требованиям ИСО 28000 и стандартов серии ИСО 28004 могут быть оценены и сертифицированы. Руководство, изложенное в стандартах серии ИСО 28004, имеет универсальный характер и предназначено для организаций различного типа, планирующих внедрить ИСО 28000. Организации, представляющие малый бизнес, могут испытывать трудности в определении мер, необходимых для реализации каждого требования, установленного в ИСО 28000. Целью настоящего стандарта является предоставление руководства для организаций среднего и малого бизнеса (за исключением морских портов), а также обеспечение их необходимой информацией для определения области валидации и мер верификации, необходимых для соответствия требованиям безопасности, изложенным в ИСО 28000 и стандартах серии ИСО 28004.

В целях определения эффективности имеющихся методов и систем обеспечения безопасности в ИСО 28000 установлены требования к причастным сторонам относительно оценки планов и процедур менеджмента обеспечения безопасности посредством периодических пересмотров, проверок, составления отчетов после происшествий, а также соответствующего обучения. Для обеспечения непрерывности безопасности цепи поставок важно, чтобы причастные стороны гарантировали транспортной отрасли наличие установленных мер по обеспечению безопасности и защите целостности цепи поставок при нахождении грузов под их прямым контролем. Неспособность одной из причастных сторон осуществить меры по защите цепи поставок от глобальных угроз и эксплуатационных рисков влечет за собой нарушение целостности системы и, как следствие, отсутствие гарантий относительно безопасного транспортирования дорогостоящих грузов.

Причастные стороны, представляющие средний и малый бизнес, являются неотъемлемой частью системы транспортирования поставок, в связи с чем в их отношении установлены требования по проведению проверок возможностей с последующим подтверждением для транспортной отрасли их соответствия действующему законодательству, нормативным и правовым актам, наилучшим практикам отрасли, а также их собственной политике и целям в области безопасности, основанным на идентифицируемых угрозах и рисках, связанных с функционированием. Настоящий стандарт устанавливает руководство и критерии для оценки качества планов менеджмента безопасности для защиты целостности цепи поставок, разработанных в соответствии с ИСО 28000 организациями среднего и малого бизнеса (за исключением морских портов). Требования, изложенные в настоящем стандарте, приведены в виде дополнений к отдельным положениям стандартов серии ИСО 28004 и не противоречат им.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Руководящие указания по внедрению ИСО 28000

Часть 3
Дополнительное специальное руководство по внедрению ИСО 28000 в организациях среднего и малого бизнеса (за исключением морских портов)

Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 3. Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

Дата введения — 2019—06—01

1 Область применения

Настоящий стандарт содержит руководство по внедрению ИСО 28000 для организаций среднего и малого бизнеса (за исключением морских портов). Руководство, изложенное в настоящем стандарте, дополняет основное руководство, изложенное в ИСО 28004-1, не противоречит ему, а также требованиям ИСО 28000.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные нормативные документы. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных — последнее издание (включая все изменения к нему):

ИСО 28000:2007, Specification for security management systems for the supply chain (Системы менеджмента безопасности цепи поставок. Технические условия)

ИСО 28004-1:2007, Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles (Системы менеджмента безопасности цепи поставок. Руководство по внедрению ИСО 28000. Часть 1. Основные принципы)

3 Дополнительные указания

ИСО 28000 разработан для применения организациями, заинтересованными в обеспечении наилучшей защиты цепей поставок или услуг, предоставляемых операторам цепи поставок. Основные положения стандартов серии ИСО 28004 представляют собой руководство для организаций любых размеров, планирующих внедрить ИСО 28000. Поскольку стандарты серии ИСО 28004 содержат руководство для широкого круга организаций, их положения для организаций среднего и малого размера могут быть более трудоемкими, чем это необходимо. Целью настоящего стандарта является адаптация положений указанного выше руководства для его использования небольшими организациями. В случае выявления необходимости предоставления более подробной информации организации, применяющие настоящий стандарт, должны руководствоваться требованиями стандартов серии ИСО 28004. Конкретные методы приведены в настоящем стандарте для наглядности и могут быть заменены на аналогичные методы.

Организациям, внедряющим ИСО 28000, необходимо:

- установить цель — обеспечение безопасности цепи поставок;
- оценить текущее состояние безопасности цепи поставок;
- разработать планы, включающие существующие процессы и процедуры цепи поставок, а также любые дополнительные процессы/процедуры или системы, необходимые для обеспечения соответствия установленным целям безопасности цепи поставок;

Издание официальное

- подготовить персонал к выполнению их функций и обязанностей согласно плану обеспечения безопасности цепи поставок;
- обеспечить установку и поддержание в надлежащем состоянии любых систем или оборудования, обозначенных в плане обеспечения безопасности цепи поставок;
- приступить к выполнению плана обеспечения безопасности цепи поставок;
- проводить мониторинг результатов выполнения плана обеспечения безопасности цепи поставок;
- проводить периодический пересмотр состояния безопасности цепи поставок в целях обнаружения изменений в условиях поставок, включая новые угрозы;
- проводить периодическую проверку планов (тренировки) организации и расследовать все инциденты в области обеспечения безопасности цепи поставок;
- обновлять цели, планы и осуществлять подготовку персонала на основе данных контроля выполнения, пересмотра, тренировок или расследований.

Пользователи серии стандартов ИСО 28004, которые ранее не работали со стандартами в сфере менеджмента, должны обратить внимание на термины «намерение», «входные данные» и «выходные данные», которые использованы в отношении каждого требования, рассматриваемого в настоящем стандарте. «Намерение» применено как заголовок раздела, в котором объясняется, что необходимо организации для выполнения работы. «Входные данные» — это раздел, в котором объяснено, что необходимо анализировать или рассматривать. «Выходные данные» — это раздел, в котором объяснено, какие цели имеет организация или какие действия ей следует предпринять относительно конкретного требования.

Шаг 1. Подготовительная работа

До начала процесса внедрения ИСО 28000 организация может рассмотреть вопрос о включении в систему менеджмента безопасности цепи поставок (в пределах области применения) всей организации или ее отдельных структурных подразделений. При принятии соответствующего решения отсутствуют ограничения в рассматриваемых аспектах, тем не менее рекомендуется принимать во внимание следующую информацию:

- существующие цели организации;
- потребности или ожидания потребителей;
- интересы государства, если система менеджмента принимается с учетом государственной политики или программы;
- наличие/отсутствие осведомленности о системах менеджмента ИСО.

В пределах планируемой области применения систему менеджмента безопасности следует распространить на все области и функции, связанные с цепью поставок. В целях упрощения определения заданных областей и функций организация должна проанализировать в том числе следующую информацию:

- места производства, оформления или обработки грузов до погрузки на транспорт, укладки на паллеты или иной подготовки для отправки;
- места отправки, хранения или сбора грузов до их транспортирования;
- места перевозки грузов;
- места погрузки или разгрузки грузов после их транспортирования;
- места смены контроля над грузами;
- места обработки, создания и доступа к документации или информации об отправляемых грузах;
- транспортные маршруты и средства перевозки при различных способах транспортирования;
- прочее.

Шаг 2. Установление «Политики в области менеджмента безопасности» (раздел 4.2 ИСО 28000 и ИСО 28004-1)

После определения области применения необходимо установить Политику в области менеджмента безопасности. Установление Политики в области менеджмента безопасности является одной из важнейших задач, так как вся система менеджмента безопасности цепи поставок будет строиться в соответствии с ее положениями, а при проведении сертификации Политика станет критерием оценки всех целей, действий и планов.

В процессе разработки Политики в области менеджмента безопасности рекомендуется обеспечить проведение оценки существующих условий, которая позволит определить как действующие внутренние условия организации, так и потребности в необходимых ресурсах.

Политика в области менеджмента безопасности должна быть одобрена высшим руководством организации. Политика должна быть понятной, четко сформулированной и устанавливать общие/основные

цели в области менеджмента безопасности организации. В ней должны быть отражены все известные угрозы безопасности, изложены обоснованные ожидания организации по эффективному преодолению угроз с помощью применения подходов превентивного менеджмента. Кроме того, Политика должна соответствовать размеру и структуре организации и включать обязательство постоянного улучшения. Для иллюстрации приведено следующее заявление о Политике.

Пример — BETA TRUCKING LTD — НАША ПОЛИТИКА В ОБЛАСТИ БЕЗОПАСНОСТИ:

- поддержка показателя утери/повреждения груза, по крайней мере на X % ниже, чем средний показатель отрасли;

- соблюдение требований нормативных и правовых актов в части транспортирования/безопасности, действующих для данной продукции;

- соответствие или превосходство практик по безопасности, установленных Всемирной таможенной организацией для уполномоченного экономического оператора.

Примечание — Данную политику используют в том случае, если в рамках цепи поставок перемещаются импортируемые или экспортируемые грузы;

- расследование всех заявлений об утратах и инцидентов в области обеспечения безопасности с последующим проведением соответствующих корректировок;

- постоянное улучшение безопасности и эксплуатационной эффективности цепи поставок, при необходимости осуществляя необходимые изменения;

- сотрудничество в полном объеме с правительственными уполномоченными органами в случае обнаружения или возникновения подозрения в контрабанде;

- предоставление информации о Политике всему персоналу и сторонним организациям (в необходимом объеме). Организации могут ограничить доступ к тем элементам Политики, которые сочтут конфиденциальными (например, порядок взаимодействия с полицией или таможней при обнаружении контрабанды). Организации могут использовать свои заявления о Политике в рекламных целях;

- заявление о Политике должно быть документально оформлено и обновляться в результате пересмотров в соответствии с ИСО 28000, раздел 4.4.4. При пересмотре заявления о Политике все предыдущие издания должны быть заменены.

Шаг 3. Выполнение «оценки безопасности» (пункт 4.3.1 ИСО 28000, подраздел 4.3 ИСО 28004-1)

Организации, внедряющие ИСО 28000, должны выполнить оценку безопасности цепей поставок и услуг по их сопровождению, находящихся в области применения, установленной руководством организации. Оценка безопасности определяет общую безопасность системы методом сравнения существующих процессов и мер безопасности с перечнем известных сценариев угроз (рисков), тем самым подтверждая, что контроль риска осуществляется надлежащим образом. В целом, риск считают контролируемым в том случае, если правдоподобность появления событий, вызывающих средние или значительные последствия в результате срывов в цепи поставок, низкая.

С высокой долей ответственности следует управлять большими, сложными или многосоставными цепями поставок, так как каждая часть цепи поставок является критичной для обеспечения низкого уровня правдоподобности возникновения опасных для организации ситуаций. В случае выполнения отдельных оценок для каждой цепи поставок, входящих в комплекс, истинный уровень правдоподобности срыва поставок не всегда очевиден.

Необходимо документально оформлять все аспекты оценки безопасности, в том числе:

- персонал, задействованный в проведении оценки, и его квалификацию;
- описание используемой методологии, включая определения всех терминов и цифровых/буквенных символов, используемых в методологии для описания вероятности, правдоподобности появления событий, последствий, критичности или эффективности;
- сценарии угроз, использованные при выполнении оценки;
- описание области применения;
- составление перечня существующих планов или процедур, пересмотренных в процессе оценки;
- предположения (при их наличии);
- необходимые пояснения, фотографии, диаграммы или другие описания для подтверждения результатов оценки;
- аспекты, связанные с цепью поставок, требующей обеспечения дополнительных мер безопасности (необходимых контрмер);
- дату завершения выполнения оценки.

В стандартах серии ИСО 28000 подробно не установлены требования к квалификации персонала, проводящего оценку. Основываясь на требованиях, установленных в ИСО 28000, организации могут использовать приведенные ниже общие указания для формирования экспертной группы по проведению оценки.

Лицо или группа лиц, проводящие оценку безопасности, должны обладать в том числе следующими навыками и знаниями:

- методами оценки рисков, применимых ко всем аспектам цепи поставок внутри области применения;
- опытом применения соответствующих мер, обеспечивающих отсутствие неправомочного раскрытия или доступа к конфиденциальным данным по безопасности;
- операций и процедур, относящихся к обработке, оформлению, перемещению и/или документальному оформлению грузов (при необходимости);
- мер по безопасности, связанных с консигнацией, перевозками, персоналом, помещениями и информационными системами в соответствующей части цепи поставок;
- пониманием угроз безопасности и методологий уменьшения негативных последствий;
- применимой законодательной базы, нормативных и правовых актов, а также правовой политики соответствующих органов управления;
- требований ИСО 28000 и стандартов серии ИСО 28004.

Оценка безопасности сложных цепей поставок, охватывающих многочисленные операционные среды, требует от персонала, участвующего в ее выполнении, более высокого уровня квалификации.

Шаг 4. Идентификация угроз безопасности (сценариев угроз)

При проведении оценки безопасности нельзя рассмотреть все возможные сценарии угроз, поэтому экспертной группе необходимо осуществить разработку обоснованного перечня сценариев угроз и документально оформить конкретные сценарии, используемые при проведении оценки. При разработке перечня сценариев угроз экспертная группа может, при необходимости, получить входные данные из многочисленных источников, включая документы организации, информацию компетентных лиц внутри цепи поставок, сведения, предоставленные промышленными объединениями, страховыми компаниями и уполномоченными государственными органами. Несмотря на отсутствие данного требования в ИСО 28000 сценарии угроз могут включать в себя несчастные случаи и события природного характера. Для иллюстрации приведен следующий перечень сценариев угроз.

Таблица 1 — Сценарии угроз

Сценарии угроз	Реализация
1) Проникновение и/или установление контроля над активом (включая транспортные средства) в пределах цепи поставок	Повреждение/разрушение актива (включая транспортные средства). Повреждение/разрушение внешней цели с использованием активов или грузов. Нарушение гражданского или экономического равновесия. Захват заложников/убийство людей
2) Использование цепи поставок в целях контрабанды	Незаконное перемещение оружия/грузов/валюты в цепи поставок
3) Фальсификация информации	Получение местного или удаленного доступа к информационным/документальным системам в целях нарушения функционирования или содействия незаконной деятельности
4) Целостность груза	Фальсификация, повреждение и/или кража грузов или транспортных средств в цепи поставок
5) Запугивание персонала в целях разрешения осуществления незаконных действий	Давление на сотрудников цепи поставок со стороны криминальных элементов, чтобы способствовать незаконной деятельности в цепи поставок

Шаг 5. Последствия

После определения и документального оформления области применения и сценариев угроз экспертная группа должна документально оформить ожидаемые последствия реализации каждого из сценариев. Несмотря на наличие множества методов определения или классификации таких последствий приведенный ниже метод является довольно простым и эффективным для применения во многих ситуациях.

Примечание — Пользователь настоящего стандарта вправе использовать и другие методы.

Оценка последствий должна учитывать возможность гибели и травмирования людей и варианты экономического ущерба. Последствия каждого случая по нарушению безопасности, выявленного

в цепи поставок, следует классифицировать как «высокие», «средние» или «низкие» (таблица 2). В процессе оценки может быть использована числовая система до момента преобразования численных результатов в качественные показатели.

Обоснования классификации последствий для каждого инцидента в области обеспечения безопасности должны быть документально оформлены.

Установление высоких, средних или низких значений последствий требует особого внимания. Использование чрезмерно низких пороговых значений может приводить к использованию возможных контрмер для большего количества сценариев угроз безопасности, чем требуется в действительности. Однако при использовании чрезмерно высоких пороговых значений вероятен риск упущения возможности применения контрмер по отношению к сценариям угроз безопасности, имеющим недопустимые для организации последствия, классифицируемые как:

- высокие — это последствия, неприемлемые в ситуациях с низким уровнем правдоподобности их появления.
- средние — это последствия, неприемлемые в ситуациях с высоким уровнем правдоподобности их появления.
- низкие — это, как правило, приемлемые последствия.

Приемлемость не следует путать с желательностью или одобрением. Приемлемость может быть рассмотрена как характеристика размеров возможного ущерба, которые организация или орган исполнительной власти готовы принять при определенных условиях, связанных с вероятностью. Организация или орган исполнительной власти могут установить размеры возможного ущерба, которые могут быть нежелательными, но все же приемлемыми.

Таблица 2 — Классификация последствий

Степень	Последствие
Высокая	**Гибель и травмирование** — большое количество погибших и раненых **и/или** **Экономическое воздействие** — серьезное повреждение активов и/или инфраструктуры, препятствующее дальнейшему функционированию **и/или** **Воздействие на окружающую среду** — полное разрушение многочисленных элементов экосистемы на обширной территории
Средняя	**Гибель и травмирование** — небольшое количество погибших и раненых **и/или** **Экономическое воздействие**, например повреждение активов и/или инфраструктуры, которые в результате нуждаются в восстановлении **и/или** **Воздействие на окружающую среду**, например,повреждение части экосистемы в течение долгого промежутка времени
Низкая	**Гибель и травмирование** — наличие пострадавших **и/или** **Экономическое воздействие** — минимальное повреждение активов и/или инфраструктуры и систем **и/или** **Воздействие на окружающую среду** — некоторые повреждения окружающей среды

Шаг 6. Анализ существующих условий

После определения и документирования последствий экспертная группа должна проводить анализ всех функций, процессов (включая информационные системы), планов и мер в соответствии с установленной областью применения. Этот анализ должен быть тщательно задокументирован таким образом, чтобы осведомленные лица, не участвующие в проведении анализа, могли понять выводы, сделанные экспертной группой.

В процессе оценки рассматривается следующее.

1) Контроль доступа:

- к помещениям организации в цепи поставок, включая близлежащие окрестности;
- транспортным средствам (автомобильному транспорту, железнодорожному транспорту, воздушному транспорту, баржам, судам и т. д.);

- информации;
- прочему.

2) Транспортные средства (грузовые автомобили, железнодорожный транспорт, баржи, самолеты, суда и т. д.), принимая во внимание:
- нормальный режим эксплуатации;
- мастерские технического обслуживания;
- изменения, вызванные, к примеру, поломками;
- смену транспортных средств;
- транспортные средства во время стоянки;
- использование транспортных средств в качестве оружия;
- прочее.

3) Обработка:
- погрузка;
- изготовление;
- хранение (включая промежуточное хранение);
- перемещение;
- выгрузка;
- раскомпоновка/компоновка;
- прочее.

4) Транспортировка грузов:
- по воздуху;
- автомобильным дорогам;
- железным дорогам;
- внутренним водным путям;
- океанским маршрутам;
- прочее.

5) Обнаружение/предотвращение несанкционированных проникновений при поставке грузов.

6) Процесс инспектирования, например инспектирование автотранспортных средств.

7) Персонал:
- уровень компетентности, подготовки и понимания;
- надежность;
- прочее.

8) Привлечение деловых партнеров.

9) Внутренний/внешний обмен информацией:
- обмен информацией;
- чрезвычайные ситуации;
- прочее.

10) Управление или обработка информации о грузах или транспортных маршрутах:
- защита информации;
- достоверность информации;
- прочее.

11) Внешняя информация:
- правовая;
- постановления органов власти;
- отраслевые особенности;
- несчастные случаи и происшествия;
- возможность применения мер неотложного реагирования и скорость реакции;
- прочее.

Рекомендуется использовать опросные листы. Приведенный ниже опросный лист анализа функционирования (таблица 3) может быть полезен для организации — участника цепи поставок при проведении оценки безопасности. Форма опросного листа может быть изменена с учетом модели бизнеса организации и возможных результатов проведения оценки рисков. Если указанные факторы уже реализованы организацией, следует использовать графу «Да». Если фактор не реализован или реализован частично, следует использовать графу «Нет» и по возможности добавить в графу комментариев описание других альтернативных мер или сведения о низком уровне риска. Если фактор не соответствует или выходит за рамки деятельности организации, в графе комментариев следует сделать отметку

«Не применимо» (НП). Пункты опросного листа, которые не могут быть реализованы из-за действующей законодательной базы или нормативных и правовых актов, должны быть отмечены как запрещенные в графе комментариев.

Таблица 3 — Опросный лист анализа функционирования

Фактор	Да	Нет	Комментарии
Менеджмент безопасности цепи поставок			
• Имеет ли организация систему менеджмента, которая рассматривает безопасность цепи поставок?			
• Имеет ли организация назначенное лицо, ответственное за безопасность цепи поставок?			
План обеспечения безопасности			
• Имеет ли организация действующий план обеспечения безопасности?			
• Отражены ли в плане ожидания организации в части обеспечения безопасности деловыми партнерами фазы предконтроля и постконтроля?			
• Использует ли организация подходы кризисного менеджмента, имеется ли целостность бизнеса и план восстановления безопасности?			
Защита активов			
• Имеет ли организация готовые меры, которые рассматривают: - физическую защиту зданий; - мониторинг и контроль внешнего и внутреннего периметров; - реализацию контроля доступа, которая запрещает несанкционированный доступ к сооружениям, средствам транспортирования, погрузочным платформам и грузовым площадкам, а также административный контроль идентификации (персонал, посетители, поставщики и т. д.) и другие средства контроля доступа?			
• Имеются ли рабочие технологии по обеспечению безопасности, которые значительно усиливают защиту активов? Например, средства обнаружения или записывающие камеры CCTV/DVS теле- и видеонаблюдения для зон ограниченного доступа с возможностью хранения информации, которые можно использовать при расследованиях инцидентов в области обеспечения безопасности.			
• Имеются ли готовые протоколы для установления контактов с внутренним персоналом в области обеспечения безопасности или внешними правоохранительными органами в случае нарушения безопасности?			
• Имеются ли процедуры для ограничения, выявления и фиксации несанкционированного доступа ко всем зонам размещения грузов и транспортных средств?			
• Устанавливается ли личность персонала, доставляющего или получающего грузы, до момента их получения или выпуска?			
Персонал, ответственный за безопасность			
• Имеет ли организация процедуры для оценки надежности персонала до его найма, а также периодической оценки выполнения им своих обязанностей по обеспечению безопасности?			
• Проводит ли организация обучение персонала, помогающее сотрудникам в выполнении обязанностей по обеспечению безопасности, таких как сохранение целостности груза, определение потенциальных внутренних угроз безопасности и контроль защиты доступа?			
• Обязывает ли организация сотрудников, знающих процедуры компании, регистрировать подозрительные происшествия?			
• Включает ли система контроля доступа немедленное изъятие у увольняющегося сотрудника идентификационных карт или пропусков в зоны ограниченного доступа и к информационным системам?			

Продолжение таблицы 3

Фактор	Да	Нет	Комментарии
Информационная безопасность			
• Используются ли процедуры, гарантирующие, что вся информация, которую используют для грузообработки как в электронном, так и в бумажном виде, является достоверной, точной и защищенной от искажений, потерь или внесения ошибочных данных?			
• Снабжает ли организация соответствующей товаросопроводительной документацией груз при его отправке или получении?			
• Обеспечивает ли организация тщательное и своевременное документирование информации о грузе, полученной от деловых партнеров?			
• Существует ли защита данных, использующая системы хранения данных, на которые не влияют действия системы обработки данных (имеется ли готовый процесс резервного копирования данных)?			
• Имеют ли все пользователи уникальный идентификатор (ID пользователя) для персонального использования в целях получения возможности контроля их действий?			
• Используется ли эффективная система менеджмента паролей для аутентификации пользователей и требуется ли от пользователей смена паролей, по крайней мере ежегодно?			
• Существует ли защита от несанкционированного доступа и неправильного использования информации?			
Безопасность грузов и транспортных средств			
• Имеются ли процедуры по ограничению, обнаружению и оповещению о несанкционированном доступе для всех зон обработки грузов и закрытых грузовых транспортных единиц?			
• Назначены ли квалифицированные лица для надзора за операциями с грузами?			
• Есть ли процедуры для уведомления соответствующих правоохранительных органов в тех случаях, когда организация обнаруживает или подозревает неправомерные или незаконные действия?			
• Есть ли процедуры для обеспечения целостности товаров/грузов, когда их доставляют в другую организацию (поставщик транспортных услуг, центр сбора и т. д.) в цепи поставок?			
• Есть ли готовые процессы, чтобы проследить изменения уровней угроз на всем протяжении транспортных маршрутов?			
• Существуют ли правила, процедуры или руководства по обеспечению безопасности для операторов перевозок (например, обход опасных маршрутов)?			
Закрытые грузовые транспортные единицы			
(Система рамочных стандартов Всемирной таможенной организации WCO SAFE Framework [1] включает Программу обеспечения целостности пломб, изложенную в Дополнении к приложению 1, которая определяет процедуры по установке и верификации силовых пломбировочных устройств наивысшей степени надежности и/или других средств обнаружения проникновений. Персонал, заполняющий соответствующую форму, должен ознакомиться с этим документом).			
• Если используется закрытая грузовая транспортная единица, то имеются ли документированные процедуры по установке и регистрации механических пломб с высокой степенью безопасности, соответствующих [2] и/или других средств обнаружения проникновений?			
• Если используется закрытая грузовая транспортная единица, то имеются ли документированные процедуры для проверки нарушений пломб, когда меняется контроль перевозки в течение маршрута, и для рассмотрения выявленных несоответствий?			

Окончание таблицы 3

Фактор	Да	Нет	Комментарии
• Непосредственно перед применением закрытых грузовых транспортных единиц проводится ли их проверка в части наличия загрязнения?			
• Если используются закрытые транспортные единицы, то имеются ли у формирующей их организации документированные процедуры для проверки физической целостности единиц непосредственно перед их заполнением, включая надежность запирающих механизмов? Рекомендуется процесс проверки, состоящий из семи пунктов: - передняя стенка - левая стенка - правая стенка - пол - потолок/крыша - внутренний/внешний запирающий механизм - тележка/шасси			

Шаг 7. Оценка правдоподобности появления события

Примечание — Уровень правдоподобности появления события устанавливается в зависимости от степени простоты или затрудненности при развитии сценария угрозы безопасности до момента возникновения самого инцидента в области обеспечения безопасности. Правдоподобность не является вероятностью, что произойдет инцидент в области обеспечения безопасности. Если экспертная группа оценивает угрозу наступления событий природного характера или несчастных случаев, то учитывает вероятность согласно архивным данным.

Экспертная группа должна определить уровень правдоподобности для каждого сценария возникновения угрозы после или в течение обзора существующих условий. При наличии нескольких участков экспертная группа может рассматривать каждый из них отдельно. При этом в процессе классификации потенциальных инцидентов в области обеспечения безопасности следует принимать во внимание состояние мер по обеспечению физической и эксплуатационной безопасности в цепи поставок, отраженных в документах (возможно с использованием опросного листа анализа функционирования). Меры по обеспечению физической безопасности включают размещение объектов, препятствующих несанкционированному доступу к определенной цели или обеспечивающих его фактическое обнаружение. Меры по обеспечению эксплуатационной безопасности включают процедуры, осуществляемые персоналом, препятствующие несанкционированному доступу к определенной цели или обеспечивающие его фактическое обнаружение. Уровень правдоподобности появления каждого инцидента в области обеспечения безопасности для конкретного актива должен быть классифицирован как высокий, средний и низкий.

Высокий уровень правдоподобности появления события определяют в тех случаях, когда меры по обеспечению безопасности предусматривают низкую степень защиты от актов незаконного вмешательства в цепь поставок. Если для оценки используют количественные величины, результаты должны быть преобразованы в качественные показатели.

Средний уровень правдоподобности появления события определяют в тех случаях, когда меры по обеспечению безопасности предусматривают умеренную степень защиты от реализации актов незаконного вмешательства.

Низкий уровень правдоподобности появления события определяют в тех случаях, когда меры по обеспечению безопасности предусматривают надежную степень защиты от актов незаконного вмешательства.

Обоснование классификации уровней правдоподобности для каждого инцидента в области обеспечения безопасности должно быть документально оформлено.

Шаг 8. Оценка сценария угрозы

Рассматривая перечень сценариев угроз, приписанные им последствия и уровни правдоподобности появления каждого из них, экспертная группа должна определить необходимость принятия дополнительных мер по контролю риска возникновения всех сценариев реализации угрозы. Использование карты оценки угроз является одним из методов такого определения. В таблице 4 представлен пример такой карты для определения контрмер в случае конкретного акта незаконного вмешательства.

Таблица 4 — Карта оценки угроз

		Уровень правдоподобности появления события		
		Высокий	Средний	Низкий
Классификация последствий	Высокие	Разработка контрмер	Разработка контрмер	Учет
	Средние	Разработка контрмер	Разработка контрмер или учет при необходимости	Документирование
	Низкие	Учет	Документирование	Документирование

Определение контрмер необходимо для тех сценариев угроз, правдоподобность появления и последствия которых оценивают как высокие, а также как средние и высокие. Для других сценариев угроз контрмеры не являются необходимыми, за исключением случаев, рекомендованных экспертами. Персонал, оценивающий безопасность, должен включить в составляемый перечень каждый сценарий угрозы, который требует применения соответствующих контрмер.

Шаг 9. Разработка контрмер

Если требуется разработка контрмер или данная работа рекомендуема экспертами, то должны быть рассмотрены последствия и/или уровни правдоподобности сценария угрозы безопасности. Целью этой работы является уменьшение правдоподобности реализации сценариев угроз или уменьшение ущерба от их реализации до уровня, при котором дополнительные контрмеры больше не требуются.

Контрмеры могут представлять собой следующие действия:

- **обработка**: обработка может состоять из организационных и/или физических мер;
- **передача риска:** перевод рисков может быть осуществлен в рамках субподрядного договора, физической передачи товара и т. д.;
- **прекращение деятельности** (связанной с конкретным риском): при определении уровня риска организация может принять решение не продолжать данный вид деятельности.

В определенных ситуациях организация может быть вынуждена допустить (см. ниже) риск из-за невозможности принятия необходимых контрмер, отсутствия полномочий для осуществления необходимых контрмер или других непреодолимых обстоятельств. Допустить подобного рода ситуацию означает, что организация не может предпринять никаких мер. Такие ситуации и оценки должны документировать и периодически пересматривать.

Шаг 10. Внедрение контрмер

Применение новых контрмер означает изменение методов функционирования, которые должны быть установлены в существующей системе менеджмента организации для обеспечения наличия достаточных ресурсов, а также управляемости воздействий на другие функции и поддержку этих изменений руководством организации.

Шаг 11. Оценка контрмер

В соответствии с методологией, установленной в стандартах серии ИСО 28004, каждая контрмера должна быть оценена на предмет эффективности уменьшения правдоподобности появления событий или последствий (или их комбинации) до тех пор, пока риск в области безопасности более не требует рассмотрения дополнительных контрмер. Такая контрмера считается результативной и должна быть отражена в отчете по оценке безопасности.

Шаг 12. Повторение процесса

После того как контрмеры разработаны и оценены как результативные, следует продолжить процесс оценки для следующего сценария угрозы, пока перечень сценариев не будет исчерпан.

Шаг 13. Непрерывность процесса

Процесс оценки безопасности является непрерывным, необходимо осуществлять постоянный мониторинг безопасности в целях выполнения мер по обеспечению безопасности и осуществления соответствующего процесса оценки.

Шаг 14. Разработка плана обеспечения безопасности

Необходимо отражать в соответствующих документах порядок работы систем менеджмента, функции и обязанности задействованного персонала, а также дополнительные аспекты, рассмотренные ниже. Данная информация должна содержаться в производственных планах организации, в отдельных документах и/или в качестве приложений к ним. В целях обобщения данная часть документации будет называться планом обеспечения безопасности. План обеспечения безопасности должен включать в том числе описание следующих аспектов:

- участка цепи поставок, включенного в план;
- обязанностей всего персонала, задействованного в области обеспечения безопасности;
- структуры менеджмента безопасности, включая персональные данные лица, назначенного менеджером по безопасности, а также роль высшего руководства;
- внутренней и внешней контактной информации для обеспечения аварийной безопасности, подлежащей использованию персоналом в отчетах по инцидентам в области обеспечения безопасности;
- навыков и знаний, которыми должен владеть персонал, имеющий обязанности по обеспечению безопасности;
- программ подготовки по обеспечению безопасности;
- процесса повышения квалификации персонала, направленного на овладение навыками и знаниями, необходимыми для обеспечения требований безопасности;
- процесса отработки на учениях элементов плана обеспечения безопасности. В целях соответствия указанным требованиям персонал может принимать участие в проводимых органами исполнительной власти тренировках или соответствующих занятиях по обеспечению безопасности;
- процессов, обеспечивающих соответствие требованиям органов исполнительной власти в части непредвиденных обстоятельств или в отношении повышения уровня безопасности;
- процесса контроля системы менеджмента безопасности цепи поставок.

План обеспечения безопасности должен содержать процедуры, включающие мероприятия по реализации процессов и мер, которые экспертная группа оценила и сочла приемлемыми для обеспечения безопасности цепи поставок, а также дополнительных необходимых контрмер, определенных по результатам оценки безопасности цепи поставок. Они могут включать:

- обеспечение получения информации о партии товаров до момента их принятия организацией для последующего транспортирования;
- обеспечение безошибочного согласования полученных для укрупнения/разукрупнения товаров/грузов с информацией в товарных/грузовых декларациях/перечнях. Отправка товарных/грузовых единиц должна быть верифицирована по заказам на покупку или доставку;
- обеспечение достоверной идентификации водителей транспортных средств, доставляющих или получающих товары/грузы, до того, как товарные или грузовые единицы будут получены или отправлены;
- обеспечение достоверной идентификации помимо водителей пассажиров транспортных средств, доставляющих или получающих товары/грузы;
- гарантии того, что все недостачи, излишки и другие существенные несоответствия урегулированы и/или надлежащим образом расследованы, а в случае обнаружения незаконных или подозрительных действий уведомлены соответствующие правоохранительные органы;
- описание любых контрмер, предпринятых в этом участке цепи поставок;
- описание любых мер и процедур, которые предприняты в этой части цепи поставок для восстановления безопасности в случае ее нарушения;
- описание любых мер и процедур, которые предприняты при передаче другой организации контроля над товарами/грузами;
- описание процедур с целью предоставления уполномоченному персоналу дополнительной информации об отправляемых товарах. Они должны отражать то, как именно пользователь будет определять законность запроса дополнительной информации и какая информация предоставляется.

4 Документация

Организация должна обеспечить защиту доступа к следующей информации:

- положения об области применения;
- сведения о завершенной оценке безопасности;
- персональные данные и данные о квалификации лиц, проводящих оценку;
- перечень всех рассмотренных контрмер;
- план обеспечения безопасности и, при необходимости, приложения к нему;
- отчеты о проведенных учебных тренировках и занятиях, посетившем их персонале, предмете занятий и дате(ах) проведения;
- прочие аспекты, предписанные нормативными и правовыми актами или системой менеджмента;
- результаты мониторинга системы менеджмента и внесенные в процессе его проведения изменения.

5 Руководство для организаций среднего и малого бизнеса в части получения консультаций и сертификации

5.1 Общие положения

Организации, которые планируют внедрить ИСО 28000, не обязаны пользоваться услугами сторонних консультантов. Если тем не менее понадобятся консультации или помощь при выполнении оценок, разработке планов обеспечения безопасности или внедрении необходимых требований, сотрудники организации могут обратиться к сторонним консультационным службам. Однако при этом необходимо проверить и подтвердить компетенцию предлагающих услуги консультантов, например посредством получения рекомендаций, отзывов о выполненных работах или путем наведения справок. Персонал, консультирующий организацию, не должен участвовать в аудитах организации, проводимых третьей стороной.

5.2 Демонстрация соответствия ИСО 28000 посредством аудита

Требования, установленные в ИСО 28000, помогают организациям, добровольно их внедряющим, установить и продемонстрировать соответствующий уровень безопасности на контролируемых ими участках международной цепи поставок. ИСО 28000 служит основой для определения, валидации или демонстрации существующего уровня безопасности цепи поставок организации посредством проведения аудита первой, второй или третьей стороной, а также любым органом исполнительной власти, который выбирает в качестве основания для принятия в свои программы безопасности цепи поставок соответствие настоящему стандарту.

Виды аудита:

- аудит, проводимый первой стороной, заключается в определении соответствия, выполняемом организацией самостоятельно;
- аудит, проводимый второй стороной, заключается в определении соответствия организации согласованным критериям или верификации, которое осуществляет независимая организация, учреждение или лицо, которое заинтересовано в деятельности организации — участника цепи поставок;
- аудит, проводимый третьей стороной, заключается в определении соответствия организации согласованным критериям или верификации, которое осуществляет независимая организация.

5.3 Сертификация ИСО 28000 независимыми органами по сертификации

Если демонстрации соответствия включает аудит, проводимый третьей стороной, то организация, претендующая на получение сертификата, должна выбирать сторонний орган по сертификации, аккредитованный в установленном порядке, соответствующий международным правилам, руководствам, а также правилам проведения аудита, изложенным в международных стандартах [1] и [3].

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 28000:2007	—	*
ISO 28004-1:2007	—	*

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

Библиография

[1] ISO/IEC 17021 Conformity assessment — Requirements for bodies providing audit and certification of management systems (Оценка соответствия. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента)

[2] ISO 17712 Freight containers — Mechanical seals (Контейнеры грузовые. Механические уплотнения)

[3] ISO 19011 Guidelines for auditing management systems (Руководящие указания по аудиту систем менеджмента)

[4] WCO (2012), SAFE framework of standards to secure and facilitate global trade

УДК 656.614.3.004:006.354 ОКС 03.100.01

Ключевые слова: менеджмент безопасности, цепь поставок, угрозы, менеджмент риска, организации среднего бизнеса, организации малого бизнеса

БЗ 6—2018/74

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 30.07.2018. Подписано в печать 09.08.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 123001 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru