МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO 28004-3

Первое издание
2014-02-01

Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000.

Часть 3:

Дополнительное специальное руководство по принятию ISO 28000 для использования в операциях среднего и малого бизнеса (кроме 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)

Ответственность за подготовку русской версии несёт GOST R (Российская Федерация) в соответствии со статьёй 18.1 Устава ISO

Ссылочный номер
ISO 28004-3:2014(R)

ДОКУМЕНТ ЗАЩИЩЕН АВТОРСКИМ ПРАВОМ

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Опубликовано в Швейцарии

Содержание

Страница

Предисловие ... **iv**

Введение ... **v**

1 Область применения ... **1**

2 Нормативные ссылки ... **1**

3 Дополнительное руководство ... **1**

4 Документация ... **14**

5 Руководство для среднего и малого бизнеса, получающего консультацию и сертификацию ... **15**

5.1 Общие положения ... 15

5.2 Демонстрация соответствия стандарту ISO 28000 посредством аудита ... 15

5.3 Сертификация по ISO 28000 сторонними органами сертификации ... 15

Библиография ... **16**

Предисловие

Международная организация по стандартизации (ISO) является всемирной федерацией национальных организаций по стандартизации (комитетов-членов ISO). Разработка международных стандартов обычно осуществляется техническими комитетами ISO. Каждый комитет-член, заинтересованный в деятельности, для которой был создан технический комитет, имеет право быть представленным в этом комитете. Международные правительственные и неправительственные организации, имеющие связи с ISO, также принимают участие в работах. Что касается стандартизации в области электротехники, ISO работает в тесном сотрудничестве с Международной электротехнической комиссией (IEC).

Процедуры, используемые для разработки настоящего документа и предназначенные для его дальнейшего поддержания, указаны в Части 1 Директив ISO/IEC. В особенности следует отметить, что для различных типов документов ISO необходимы разные критерии для утверждения. Настоящий документ был разработан в соответствии с редакционными правилами Части 2 Директив ISO/IEC. (см. www.iso.org/directives).

Обращается внимание на возможность патентования некоторых элементов данного международного стандарта. ISO не несет ответственности за идентификацию какого-либо или всех таких патентных прав. Детали любых патентных прав, идентифицированных при разработке документа, должны содержаться в Введении и/или в перечне полученных патентов ISO. (см. www.iso.org/patents).

Любое фирменное наименование в настоящем документе является информацией, предоставляемой для удобства пользователей, и не носит рекомендательный характер.

Для объяснения смысла специальных терминов и выражений ISO, связанных с оценкой соответствия, а также для информации о приверженности ISO принципам WTO Соглашения по техническим барьерам в торговле (TBT) следует использовать следующий указатель URL: Foreword - Supplementary information

За настоящий документ несет ответственность Технический комитет ISO/TC 8, *Суда и морские технологии.*

Настоящее первое издание ISO 28004-3 отменяет и замещает ISO/PAS 28004-3:2012.

ISO 28004 состоит из следующих частей под общим названием *Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000*:

— *Часть 1: Общие принципы*

— *Часть 2: Руководящие указания по принятию ISO 28000 для использования в работе средних и малых морских портов*

— *Часть 3: Дополнительное специальное руководство по принятию ISO 28000 для использования в операциях среднего и малого бизнеса (кроме морских портов)*

— *Часть 4: Дополнительное специальное руководство по внедрению ISO 28000, когда соответствие ISO 28001 является предметом менеджмента*

Введение

ISO 28000:2007 и руководство, содержащееся в ISO 28004, были разработаны в ответ на необходимость иметь идентифицируемые критерии оценки системы менеджмента цепи поставок (процесс валидации), по которым системы менеджмента безопасности можно будет оценить и сертифицировать на соответствие ISO 28000 и ISO 28004. Руководство, в настоящее время содержащееся в ISO 28004, предназначено для того, чтобы помочь организациям, принимающим ISO 28000. Поскольку типов организаций, которые могут использовать ISO 28000, множество, руководство, предоставляемое в ISO 28004, универсально по своей сущности. В результате некоторые более мелкие организации испытывали трудности в определении мер, необходимых для рассмотрения каждого из требований, установленных в ISO 28000. Поэтому целью настоящей части ISO 28004 является обеспечение руководства и расширение информации, которую можно будет использовать среднему и малому бизнесу (кроме морских портов), чтобы помочь им в определении области валидации и мер верификации, необходимых для соответствия требованиям по безопасности, определенных в ISO 28000 и ISO 28004.

ISO 28000 требует, чтобы заинтересованные организации оценивали возможности своих планов и процедур менеджмента обеспечения безопасности посредством периодических пересмотров, проверок, отчетов после происшествия и обучения, чтобы определить эффективность имеющихся методов и систем обеспечения безопасности. Для полной непрерывной сквозной безопасности цепи поставок важно, чтобы заинтересованные организации гарантировали транспортной отрасли то, что у них есть достаточно готовых мер безопасности для защиты целостности цепи поставок при нахождении грузов под их прямым контролем. Ошибка одной из заинтересованных организаций в защите цепи поставок от любых глобальных угроз и эксплуатационных рисков может серьезно повлиять на целостность системы и разрушить доверие тех, кто полагается на безопасную транспортировку своих дорогостоящих грузов.

Заинтересованные организации среднего и малого бизнеса являются составной частью системы поставок и от них будут требовать проведения проверок их операционных возможностей и подтверждения для транспортной отрасли, что возможности отвечают соответствующему законодательству и нормативным документам, лучшим практикам отрасли, а также их собственной политике и целям безопасности, основанным на выявленных угрозах и рисках для их функционирования. Информация, содержащаяся в настоящей части ISO 28004, обеспечивает руководство и критерии для оценки качества планов менеджмента безопасности, разработанных организациями среднего и малого бизнеса (кроме морских портов) в соответствии с ISO 28000 для защиты целостности цепи поставок. Более подробная информация представлена как усиливающая, но не изменяющая общее руководство, определенное в ISO 28004. Кроме ряда внесенных дополнений никаких изменений в ISO 28004 произведено не было.

Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000.

Часть 3.
Дополнительное специальное руководство по принятию ISO 28000 для использования в операциях среднего и малого бизнеса (кроме морских портов)

1 Область применения

Настоящая часть ISO 28004 разработана, чтобы дополнить ISO 28004-1 специальным руководством для среднего и малого бизнеса (кроме морских портов) по использованию ISO 28000. Дополнительное руководство в настоящей части ISO 28004, усиливая общие руководящие указания, представленные в основных разделах ISO 28004-1, не противоречит им и не исправляет ISO 28000.

2 Нормативные ссылки

Следующие документы, полностью или частично являются ссылочными в данном документе и обязательными при его применении. При датированных ссылках применяется только приведенное издание документа. При недатированных ссылках необходимо использовать самое последнее издание нормативного ссылочного документа (включая любые изменения).

ISO 28000:2007, *Системы менеджмента безопасности цепи поставок. Технические условия*

ISO 28004-1:2007, *Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000. Часть 1: Общие принципы*

3 Дополнительное руководство

ISO 28000 разработан для принятия организациями, заинтересованными в лучшей защите их цепей поставок или услуг, предоставляемых для операторов цепи поставок. Основная часть ISO 28004 разработана для предоставления руководства организациям любых размеров, желающих принять ISO 28000. Поскольку ISO 28004 содержит руководящие указания для широкого круга организаций, он может оказаться более сложным, чем это необходимо для организаций более малого размера. Целью настоящей части ISO 28004 является упрощение руководства для использования небольшими организациями. Организации, использующие настоящую часть ISO 28004 должны справляться с основным стандартом ISO 28004, если по конкретным вопросам требуется больше информации, чем предоставлено в настоящей части ISO 28004. Руководство, приведенное в настоящей части ISO 28004, не изменяет ISO 28000 или основной стандарт ISO 28004. Если в настоящей части ISO 28004 обсуждаются специальные методологии, то они приведены для иллюстративных целей (чтобы объяснить, что необходимо выполнить), и другие методологии могли бы быть замещены.

Организациям, принимающим ISO 28000, будет необходимо:

— установить, какие из их целей имеют отношение к обеспечению безопасности цепи поставок;

— оценить текущее состояние безопасности цепи поставок;

— разработать планы, которые будут включать существующие процессы и процедуры цепи поставок и любые дополнительные процессы/процедуры или системы, которые были определены как необходимые для соответствия установленным целям безопасности цепи поставок;

— подготовить персонал к выполнению их функций и обязанностей, как это определено в плане по обеспечению безопасности цепи поставок;

— установить/поддерживать любые системы или оборудование, обозначенное в плане по обеспечению безопасности цепи поставок;

— начать выполнение плана по обеспечению безопасности цепи поставок;

— контролировать результаты выполнения плана по обеспечению безопасности цепи поставок;

— периодически переоценивать состояние безопасности цепи поставок, чтобы обнаружить изменения, включая новые угрозы;

— периодически проверять планы (тренировки) организации и расследовать любые инциденты в области безопасности цепи поставок;

— обновлять цели, планы и подготовку персонала на основе данных контроля выполнения, переоценок, тренировок или расследований.

Пользователи ISO 28004, которые ранее не работали со стандартами менеджмента, должны обратить внимание на использование слов ‘намерение’, ‘исходные данные’, и ‘результаты’, которые используются в отношении каждого требования, рассматриваемого в настоящей части ISO 28004. Намерение используется как заголовок раздела, в котором объясняется, что необходимо организации для выполнения работы. Исходные данные – это раздел, в котором объясняется, что необходимо анализировать или рассматривать. Результаты – это раздел, в котором объясняется, какие цели имеет организация или какие действия ей следует предпринять относительно конкретного требования.

Шаг 1 – Подготовительная работа

До начала процесса принятия ISO 28000 организация может рассмотреть, хочет ли она включить в систему менеджмента безопасности цепи поставок (в пределах области применения) всю организация или отдельные ее части. Организация не ограничена в вопросах, которые она должна рассматривать при принятии решения, однако, она может принимать во внимание некоторые из следующих аспектов:

— Свои корпоративные цели.

— Потребности или ожидания потребителей;

— Интересы правительства, если система менеджмента принимается с учетом правительственной политики или программы;

— Свою осведомленность или недостаток осведомленности о системах менеджмента ISO.

В пределах планируемой области применения система менеджмента безопасности должна распространяться на все области и функции, связанные с цепью поставок. Чтобы облегчить определение этих областей и функций, организация должна рассмотреть, не ограничиваясь этим, следующее.

— Где грузы производились, оформлялись или обрабатывались до погрузки на транспорт, укладки на паллеты или иной подготовки для отправки;

— Где грузы, предназначенные для отправки, хранятся или собираются до транспортировки;

— Куда грузы перевозятся;

— Куда грузы погружаются или разгружаются после транспортировки;

— Где меняется контроль над грузом;

— Где документация или информация относительно отправляемых грузов обрабатывается, создается или оказывается в зоне доступа;

— Транспортные маршруты и средства перевозки при различных способах транспортировки;

— Прочее.

Шаг 2 – Установление 'Политики менеджмента безопасности' (Раздел 4.2 ISO 28000 и ISO 28004-1)

После того, как будет предварительно определена область применения, следующим шагом будет установление политики менеджмента безопасности. Политика менеджмента безопасности очень, поскольку вся система менеджмента безопасности цепи поставок будет строиться в соответствии с ней и, если требуется сертификация, то политика будет критерием оценки всех целей, действий и планов.

Хотя может казаться, что политика менеджмента безопасности должна быть установлена первым делом, а оценка существующих условий будет ею определяться, между ними существует синергия, поскольку становятся ясными действующие внутренние условия и выясняются потребности в ресурсах.

Политика менеджмента безопасности должна содержаться в указании, которое одобрено вышестоящим менеджментом. Политика должна быть содержательной и четко устанавливать общие/основные цели менеджмента безопасности организации. Они должны отражать известные угрозы безопасности и предоставлять обоснованные ожидания, что организация будет способна лучше справиться со своими угрозами, чем организация, которая не приняла подход упреждающего менеджмента. Она также должна соответствовать размеру и характеру организации и включать обязательство постоянного улучшения. Для иллюстрации приводится следующее постановление о политике.

BETA TRUCKING LTD – НАША ПОЛИТИКА БЕЗОПАСНОСТИ

— Поддерживать показатель утери/повреждения груза, по крайней мере, на X% ниже, чем средний в промышленности для обслуживаемых рынков;

— Соблюдать все правительственные нормативные документы по транспортировке/безопасности, применяемые на обслуживаемых рынках;

— Соответствовать или превосходить практики по безопасности, установленные Всемирной таможенной организацией для Уполномоченного экономического оператора (замечание: эта политика может быть использована, если цепь поставок перемещает импортируемые или экспортируемые грузы);

— Расследовать все заявления об утратах и инциденты по безопасности и производить корректировки.

— Постоянно добиваться улучшения безопасности и эксплуатационной эффективности цепи поставок, при возможности производя изменения.

— Комплексно взаимодействовать с правительственными уполномоченными органами, если обнаружена или заподозрена незаконная контрабанда.

— Постановление о политике должно быть известно всему соответствующему персоналу и сторонним организациям до необходимой степени. Если некоторые моменты политики должны быть конфиденциальными (например, взаимодействие с полицией или таможней при обнаружении контрабанды), организация может ограничить их распространение. Организации могут использовать свои постановления о политике в рекламных целях.

— Постановление о политике должно быть документировано и обновляться при пересмотрах, как требуется в ISO 28000, раздел 4.4.4. При пересмотре постановления о политике все предыдущие издания должны быть заменены.

Шаг 3 – Выполнение ‘оценки безопасности’ (ISO 28000, раздел 4.3.1, ISO 28004-1, раздел 4.3)

Организации, принимающие ISO 28000, должны выполнять оценку безопасности цепей поставок и своих вспомогательных служб, находящихся в области применения, установленной менеджментом. Оценка определяет общую безопасность системы методом сравнения существующей безопасности, процессов функционирования и мер с перечнем известных сценариев угроз (рисков), чтобы определить, управляется ли риск надлежащим образом. Риск считается контролируемым, если вероятность средних или значительных последствий срывов в цепи поставок сведена к ситуации с низкой вероятностью.

Следует с осторожностью управлять большими сложными или множественными цепями поставок, когда каждая критична для организации в отношении маловероятных ситуаций. Если отдельные оценки выполняются для каждой цепи поставок, то истинная величина вероятности нарушения может не быть очевидной.

Важно, чтобы все аспекты оценки безопасности были документированы, включая:

— занятый персонал и его квалификацию для проведения оценки;

— описание используемой методологии, включая определения любых терминов или цифровых/буквенных символов, используемых в методологии для описания вероятности, правдоподобия, последствий, критичности или эффективности;

— сценарии угроз, которые были использованы при выполнении оценки;

— описание области применения;

— составление перечня существующих планов или процедур, которые были пересмотрены в процессе оценки;

— сделанные предположения (если это имеет место);

— достаточные пояснения, фотографии, диаграммы или другие описания для подтверждения результатов оценки;

— аспекты цепи поставок, которая требует дополнительных мер по безопасности (необходимые меры противодействия);

— дату завершения выполнения оценки.

Ни ISO 28000, ни основная часть ISO 28004-1 не определяют подробно квалификацию, требуемую от персонала, проводящего оценку. Однако, на основе ожидаемых результатов организации, применяющие ISO 28000, могут использовать следующее общее руководство для формирования своей экспертной группой.

Лицо или группа, проводящая оценку безопасности, должны вместе иметь навыки и знания, которые включают, не ограничиваясь этим, следующее:

— Техника оценки рисков, применимая ко всем аспектам цепи поставок внутри области применения;

— Применение соответствующих мер, чтобы избежать неправомочного раскрытия или доступ к секретным материалам по безопасности;

— Операции и процедуры, включаемые в обработку, оформление, перемещение и/или документирование грузов при необходимости;

— Меры по безопасности, связанные с консигнацией, перевозками, персоналом, помещениями и информационными системами в соответствующей части цепи поставок.

— Понимание угроз безопасности и методологий смягчения.

— Знание применяемых законов, нормативных документов, правовой политики и вовлеченных правительственных агентств.

— Понимание ISO 28000 и ISO 28004.

Цепи поставок, которые являются более сложными или охватывают многочисленные операционные среды, будут требовать более квалицированных работников для выполнения оценок, чем для простых цепей поставок.

Шаг 4 – Определение угроз безопасности (сценариев угроз)

Никакая оценка безопасности не может рассмотреть все сценарии угроз, поэтому важно, чтобы экспертная группа разработала обоснованный перечень сценариев угроз и документировала те, которые были использованы в процессе выполнения оценки. При разработке перечня сценариев угроз экспертная группа может при желании получить исходные данные из многочисленных источников, включая корпоративные документы, хорошо информированных людей внутри цепи поставок, промышленные объединения, страховые компании и соответствующие правительственные органы. Хотя ISO 28000 не требует, сценарии угроз могут включать несчастные случаи и действия природы. Для иллюстрации приводится 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 качестве способов контрабанды	Перемещение незаконного оружия/грузов/валюты в цепи поставок
3) Фальсификация информации	Получение местного или удаленного доступа к информационным/документальным системам в целях нарушения функционирования или облегчения незаконной деятельности.
4) Целостность груза	Фальсификация, повреждение и/или кража грузов или транспортных средств в цепи поставок
5) Запугивание работников для разрешения незаконных действий	Давление на сотрудников цепи поставок со стороны криминальных элементов, чтобы способствовать незаконной деятельности в цепи поставок.

Шаг 5 – Последствия

После того, как область применения и сценарии угроз были определены и задокументированы, экспертная группа должна будет документировать ожидаемые последствия каждого сценария угрозы. Хотя существует много методов определения или классификации последствий, приведенный ниже метод является довольно простым и эффективным во многих ситуациях (Примечание: могут использоваться другие методологии).

Оценка последствий должна предусматривать потенциальные потери погибшими и экономические потери. Последствия каждого инцидента по безопасности, выявленного в цепи поставок, должны классифицироваться как высокие, средние или низкие (см. Таблицу 2). В процессе оценки может быть