ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28004-2— 2019

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

Часть 2

РУКОВОДСТВО ПО ВНЕДРЕНИЮ ИСО 28000 В МОРСКИХ ПОРТАХ, ОТНОСЯЩИХСЯ К СРЕДНЕМУ И МАЛОМУ БИЗНЕСУ

(ISO 28004-2:2014, IDT)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Международный менеджмент, качество, сертификация» (АНО «ММКС») совместно с Обществом с ограниченной ответственностью «Палекс» и Ассоциацией по сертификации «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. № 1437-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28004-2:2014 «Системы менеджмента безопасности для цепи поставок. Руководство по внедрению ИСО 28000. Часть 2. Руководство по применению ИСО 28000 для использования операторами морских портов малого и среднего размера» (ISO 28004-2:2014 «Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations», IDT)

5 ВВЕДЕН ВПЕРВЫЕ

*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, 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 Обзор 1
2.1 Цель 1
2.2 Предпосылки 1
2.3 ИСО 28000, пункт 4.3.1 — требования к оценке риска, угрожающего безопасности 2
2.4 Требования к оценке риска 3
3 Области риска цепи поставок морского порта 6
3.1 Общие положения 6
3.2 Аварии. Портовые операции 6
3.3 Риски преступной деятельности 8
3.4 Риски возникновения пожара 9
3.5 Финансовые риски заинтересованных сторон 11
3.6 Риски, связанные с трудовыми отношениями 12
3.7 Риски механических поломок оборудования 13
3.8 Политические и государственные риски 14
3.9 Риски, связанные с терроризмом 16
3.10 Погодные риски 17
4 Оценочные критерии плана управления безопасностью порта и процесс присвоения рейтинга . . . 19
4.1 Общие положения 19
4.2 Процесс оценки плана управления безопасностью и процедуры 19
4.3 Критерии для оценки соответствия 19
4.4 Использование ИСО 20858 для процедур оценки и определения безопасности 20
4.5 Рейтинговая система оценки плана управления безопасностью 21
Библиография 23

Введение

Настоящий стандарт подготовлен на основе ИСО 28004-2:2014. Настоящая часть серии стандартов ИСО 28004 является руководством и способствует информированию средних и малых морских портов, желающих внедрить ИСО 28000. Дополнительная информация предназначена для улучшения, но не изменения общего руководства, в настоящее время определенного в ИСО 28004.

Никаких изменений в ИСО 28004-2 не внесено, кроме дополнений справочного характера.

Настоящий стандарт обеспечивает взаимосвязь с другими стандартами ИСО и соответствующими техническими спецификациями.

Существует несколько установленных и ожидающих рассмотрения соответствующих стандартов ИСО, которые вместе с этой частью ИСО 28004 предоставляют дополнительные указания и инструкции для операторов морских портов для составления их планов мер по обеспечению управления безопасностью и оценки способности этих мер защищать целостность цепи поставок грузов, находящихся под их непосредственным контролем. Стандарты ИСО 20858, ИСО 28001, ИСО 28002, ИСО 28003, включая серию стандартов ИСО 28004, упоминаются в ИСО 28004-2 и предназначены для предоставления операторам конкретных указаний. Соответствие этих стандартов ИСО 28000 представлено в таблице 1.

Таблица 1 — Соответствующие стандарты ИСО

Стандарт ИСО	Техническое описание
ИСО 28004 -1	Предоставляет руководство для органов по сертификации по оценке соответствия организации требованиям ИСО 28000
ИСО 20858	Предоставляет интерпретацию профессионального Международного кодекса по охране судов и портовых средств (IMO ISPS) и руководство по оценке плана управления безопасностью порта и установленным операционным процедурам
ИСО 28001	Содержит требования по безопасности, отвечающие основным требованиям безопасности Программы уполномоченных экономических операторов Всемирной таможенной организации (ВТамО)
ИСО 28002	Предоставляет руководство по разработке мер повышения устойчивости цепи поставок организации
ИСО 28003	Предоставляет руководство для органов по сертификации по оценке соответствия организации требованиям ИСО 28000

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Системы менеджмента безопасности цепи поставок.
Руководящие указания по внедрению ИСО 28000**

Часть 2

РУКОВОДСТВО ПО ВНЕДРЕНИЮ ИСО 28000 В МОРСКИХ ПОРТАХ, ОТНОСЯЩИХСЯ К СРЕДНЕМУ И МАЛОМУ БИЗНЕСУ

Security management systems for the supply chain. Guidelines for the implementation of ISO 28000.
Part 2. Guidelines for adopting ISO 28000 for use in medium and small seaport operations

Дата введения — 2020—07—01

1 Область применения

В настоящем стандарте определены возможные риски и угрозы в цепи поставок, процедуры для проведения оценки риска/угроз и критерии оценки соответствия и результативности документированных планов управления безопасностью в соответствии с ИСО 28000 и руководящими принципами внедрения серии стандартов ИСО 28004. Результатом этих усилий станет система оценки уровня доверия, основанная на качестве системы менеджмента безопасности, реализуемой морским портом для обеспечения безопасности и непрерывности деятельности цепи поставок грузов, обрабатываемых морским портом. Рейтинговую систему следует использовать в качестве средства определения измеримого уровня достоверности того, что операции по безопасности морского порта соответствуют требованиям ИСО 28000 для защиты целостности цепи поставок.

Организации, выбирающие сертификацию третьей стороной, могут дополнительно продемонстрировать, что они вносят значительный вклад в безопасность цепи поставок.

2 Обзор

2.1 Цель

Целью настоящего стандарта является предоставление руководства по внедрению ИСО 28000 средним и малым портам. Это руководство содержит критерии самооценки, которые могут быть использованы этими портами при внедрении ИСО 28000. Хотя критерии самооценки не приведут к сертификации третьей стороной, их можно использовать для определения жизнеспособности плана управления безопасностью заинтересованной стороны порта для обеспечения целостности цепи поставок в соответствии с положениями и рекомендациями по безопасности, указанными в ИСО 28000 и серии стандартов ИСО 28004. Цель состоит в том, чтобы разработать рейтинговую шкалу оценки риска, которую можно использовать для оценки способности плана управления безопасностью порта обеспечивать непрерывную защиту и непрерывную работу цепи поставок груза, получаемого, хранящегося и передаваемого морским портом. Использование этих критериев самооценки позволит определить, соответствует ли морской порт каждому требованию ИСО 28000 с достаточной степенью детализации.

2.2 Предпосылки

Международный кодекс безопасности судов и портовых средств (ISPS) требует, чтобы каждый морской портовый комплекс разработал комплексный план управления безопасностью портового ком-

Издание официальное

плекса с грузом, находящимся под его непосредственным контролем. План управления безопасностью порта должен учитывать те приложения, системы безопасности и оперативные меры, которые предназначены для защиты персонала, портовых сооружений, судов у причала, грузовых транспортных единиц (включая железнодорожные и наземные) в пределах физических возможностей портового комплекса от риска инцидента безопасности (ИСО 20858 предоставляет четкие рекомендации по выполнению этих требований). Стандарт ИСО 28000 и серия стандартов ИСО 28004 устанавливают руководящие принципы для защиты глобальной цепи поставок на очень высоком уровне, но не предоставляют достаточно конкретных деталей, которые позволили бы обеспечить последовательный уровень реализации для охвата всех положений и программ безопасности для больших, средних и малых морских портов, которые являются неотъемлемыми частями инфраструктуры безопасности глобальной цепи поставок. Чтобы обеспечить долгосрочную и последовательную безопасность цепи поставок, необходимо, чтобы каждая из заинтересованных сторон в этой интегрированной глобальной сети была оценена и несла ответственность за содействие обеспечению безопасности и бесперебойной доставке груза.

Средние и малые морские порты являются неотъемлемой частью инфраструктуры доставки в цепи поставок, особенно с учетом того, что данные порты, как правило, являются первыми точками входа для большинства товаров, которые отправляются и распределяются по местным и международным направлениям. Данные средние и малые порты являются портами подачи товаров, отправляемых в более крупные мегапорты, для консолидации и распределения грузов для дальних перевозок в другие мегапорты и по всему миру. Следовательно, крайне важно, чтобы в средних и малых морских портах были соблюдены и поддерживались проверенные меры безопасности, которые могут обеспечить защиту и дальнейшее безопасное прохождение товаров, перевозимых через их портовые сооружения.

В то время как ИСО 28000 и серия стандартов ИСО 28004 предоставляют общие обзоры ожидаемых требований для обеспечения безопасности цепи поставок, существуют ограниченные инструкции, измеримые требования и критерии приемлемости, которые позволяют предприятию создавать и реализовывать план управления безопасностью, что обеспечит соблюдение установленных норм в ИСО 28000. Поэтому настоящий стандарт предназначен для предоставления методов, процедур, руководящих принципов и критериев приемлемости, которые будут использоваться для определения уровня соответствия требованиям безопасности серии стандартов ИСО 28004.

2.3 ИСО 28000, пункт 4.3.1 — требования к оценке риска, угрожающего безопасности

ИСО 28000, пункт 4.3.3: «При установлении и пересмотре своих целей организация должна учитывать нормативно-законодательные и другие требования по безопасности». Кодекс ISPS, принятый каждым государством-членом, устанавливает такие требования к оценке риска безопасности. Следовательно, согласно пункту 4.3.1 ИСО 28000 заинтересованная сторона морского порта и управляющая организация должны установить и поддерживать процедуру для постоянной идентификации угроз и оценки рисков безопасности, связанных с менеджментом риска для безопасности, а также для выявления и реализации необходимых мероприятий управленческого контроля для защиты цепи поставок. Методы идентификации угроз, оценки риска и менеджмента риска, включая контроль, должны соответствовать характеру и масштабам операций морского порта. Эта оценка должна учитывать вероятность возникновения события и все его последствия для заинтересованной стороны морского порта, угрозы для непрерывности деятельности, безопасности цепи поставок, необходимость восстановления после бедствия. В частности, оценка риска должна предусматривать минимум следующее:

a) угрозы и риски для деятельности, включающей управление безопасностью, человеческий фактор и другие действия, которые оказывают влияние на результаты деятельности организации, условия или безопасность;

b) события природного характера (штормы, наводнения, сильные ветры и т. д.), которые могут сделать мероприятия и оборудование неэффективными;

c) факторы, находящиеся вне контроля организации, такие как сбои в поставляемом извне оборудовании и услугах, изменения в местной и международной политике и правилах безопасности, а также политические изменения, влияющие на владение и эксплуатацию морского порта;

d) угрозы и риски заинтересованных сторон, такие как несоблюдение нормативных требований, финансовые ограничения или изменения в правах собственности, которые влияют на деятельность порта и безопасность цепи поставок;

e) проектирование, установка, проверка и техническое обслуживание оборудования для обеспечения безопасности, включая установку новых систем и обучение персонала эксплуатации, ремонту и техническому обслуживанию;

f) сбои критической информации, систем управления данными и связи, используемых для управления и защиты цепи поставок.

Организации, являющиеся заинтересованными сторонами морского порта, ответственные за обеспечение защиты безопасности товаров цепи поставок, должны обеспечить наличие результатов этих оценок и соответствующих мер безопасности для обеспечения целостности цепи поставок. План управления безопасностью морского порта должен содержать положения и процедуры для выполнения целей системы безопасности, эксплуатационных требований, оценки риска, минимизации последствий, непрерывности деятельности и этапов восстановления после бедствия. В частности, план должен учитывать следующее:

- определение требований к проектированию, спецификации, установке и эксплуатации охранных устройств и систем;
- идентификацию кадрового ресурса безопасности, уровней квалификации и обучения, необходимых для эксплуатации и обслуживания устройств и систем безопасности (ИСО 28000, пункт 4.4.2);
- определение общей оценки угроз и рисков в организации и структуре менеджмента для минимизации выявленных рисков;
- обеспечение непрерывности функционирования и этапы восстановления после бедствия, которые будут реализованы для восстановления систем безопасности для защиты цепи поставок и восстановления морского порта до полного рабочего состояния.

Организация должна документировать и поддерживать вышеуказанную информацию в актуальном состоянии. Организация должна иметь персонал, обученный пониманию и применению планов и процедур управления безопасностью и операций, указанных в плане. Методология организации по идентификации угрозы, оценке риска и минимизации последствий должна:

- быть четко определенной в отношении ее области применения, ролей и обязанностей заинтересованных сторон, ожидаемого характера и сроков риска и угроз, чтобы обеспечить проактивность действий, а не реагирование;
- идентифицировать и контролировать сбор информации от источников для документирования существующих и определения будущих угроз безопасности и рисков, связанных с цепью поставок;
- предусмотреть классификацию угроз и рисков и идентификацию шагов по минимизации последствий для тех рисков и угроз, которые следует либо избегать, либо устранять или которыми следует управлять;
- обеспечивать мониторинг действий для обеспечения результативности и своевременности их внедрения (ИСО 28000, пункт 4.5.1) для обеспечения бесперебойной защиты цепи поставок.

План управления безопасностью морского порта должен быть запланированной частью процедуры непрерывного совершенствования для поддержания в актуальном состоянии персонала и систем морского порта с выявленными угрозами, рисками и эксплуатационной безопасностью, необходимыми для сохранения цепи поставок.

Процессы идентификации угроз, оценки рисков, менеджмента риска и их результаты должны быть основой для разработки и внедрения комплексной системы безопасности цепи поставок. Важно, чтобы связи между процессами идентификации угроз, оценкой рисков, менеджментом риска и другими элементами системы менеджмента безопасности были четко установлены, постоянно отслеживались и обновлялись для отражения любых изменений в оценке угроз и рисков портовых операций для обеспечения безопасности цепи поставок.

2.4 Требования к оценке риска

2.4.1 Общие положения

Процессы идентификации угроз, оценки рисков и минимизации рисков являются ключевыми инструментами управления, контроля и устранения рисков для обеспечения безопасности и непрерывной работы цепи поставок. План управления безопасностью морского порта должен охватывать каждую из этих областей и обеспечивать конкретные роли и обязанности для каждой из заинтересованных сторон, участвующих в защите цепи поставок.

2.4.2 Рассмотрение оценки риска средних и малых портов

Цель документа — оценка риска для цепи поставок, характеристики шагов, которые должны предприниматься для минимизации и предотвращения серьезных нарушений в цепи поставок грузов, перевозимых через морские порты среднего и малого размеров. Эти морские порты обычно являются начальной точкой входа для большого сегмента товаров, отправляемых в крупные и международные

мегапорты. Грузы поступают в порты из мест, расположенных выше по цепи поставок, через железнодорожные, автомобильные и другие транспортные средства, которые либо перевозят, либо собирают груз, хранящийся в местах расположения портов. Поэтому цель состоит в том, чтобы определить и оценить способность портовых операций защищать груз и поддерживать ожидаемые темпы доставки товаров по мере прохождения товаров через морской порт.

Входные данные — это информация о сборке, обработке, хранении, погрузке/разгрузке груза и окончательные требования к исходящей перевозке, а также план операций в порту и планы управления безопасностью, которые функционируют в соответствии с планом непрерывности деятельности (COOP), разрабатываемым с учетом выявленного и предполагаемого рисков, связанных с количеством, потоком и типом груза, обрабатываемого портом. Для каждого выявленного риска и/или угрозы потоку товаров через порт должен быть разработан план по предотвращению или минимизации воздействия рисков, включающий перечень работ и официальные планы аварийного восстановления для обеспечения кооперации порта и потока товаров. Данные планы, которые разрабатываются и поддерживаются портами и соответствующими заинтересованными сторонами, в дальнейшем пройдут оценку и им будет присвоен номер сертификата/уровня доверия, который можно использовать для измерения уровня соответствия стандарту ИСО 28000 и серии стандартов ИСО 28004 по обеспечению безопасности цепи поставок.

Основным результатом этого документа будет набор руководящих принципов для оценки соответствия плана управления безопасностью морского порта требованиям серии стандартов ИСО 28004. Руководство будет охватывать идентификацию угроз, оценку рисков и менеджмент риска для операций морского порта, а также документированные процедуры и практики, применяемые заинтересованными сторонами морского порта для предотвращения, обнаружения нарушений, реагирования на них и приведения порта в нормальное рабочее состояние для обеспечения безопасности и непрерывности деятельности цепи поставок.

2.4.3 Намерение

Намерение состоит в том, чтобы создать и задокументировать набор процедур для определения способности средних и малых портов соответствовать требованиям безопасности цепи поставок, указанным в ИСО 28000 и серии стандартов ИСО 28004, для идентифицированных угроз и оценки рисков для операций в морском порту. Процессы идентификации угроз безопасности, оценки рисков и менеджмент риска являются ключевыми инструментами в управлении и снижении рисков безопасности для подробных инструкций деятельности в цепи поставок. Угрозы и риски для безопасности могут значительно различаться в инфраструктуре цепи поставок от незначительных инцидентов до полномасштабных нарушений безопасности грузов. Цель состоит в том, чтобы (a) идентифицировать и охарактеризовать те угрозы и риски, которые характерны для небольших морских портов, и определить возможное воздействие на операции по безопасности порта; (b) оценить процессы минимизации последствий угроз в морском порту и меры по их предупреждению, разработанные в ответ на эти угрозы/риски; (c) оценить способность морского порта поддерживать целостность цепи поставок для товаров, транспортируемых через его объекты. План управления безопасностью морского порта будет затем оценен для определения способности морского порта обеспечивать безопасность цепи поставок от выявленных угроз и рисков для их деятельности.

2.4.4 Процесс

Процессы идентификации угроз безопасности, оценка риска и менеджмент риска в значительной степени варьируются в разных отраслях — от простой оценки до сложного количественного анализа с обширной документацией. Поэтому организации и учреждения, являющиеся заинтересованными сторонами морского порта, должны поддерживать комплексный план управления безопасностью, учитывающий эти угрозы и риски для их деятельности.

Заинтересованная сторона, организации и агентства, ответственные за безопасность цепи поставок, а также сами порты обязаны создавать и поддерживать план управления безопасностью, который идентифицирует все вероятные угрозы и риски безопасности для операций портов, создает стратегии минимизации последствий и процедуры восстановления для обеспечения целостности цепи поставок. Каждая операция в морском порту будет оцениваться по качеству и возможностям реализованного плана управления безопасностью для полной защиты цепи поставок от выявленных угроз и рисков, которые она контролирует или на которые оказывает влияние. Для измерения возможностей обеспечения безопасности морского порта должны быть использованы такие показатели результативности деятельности (KPI), которые позволяют установить, что:

- политика и цели по безопасности достигаются;
- все идентифицированные угрозы и риски цепи поставок управляются, контролируются и/или снижаются, так как соответствующие меры были приняты и были эффективны;
- персонал службы безопасности хорошо осведомлен и обучен методам защиты, обнаружения, минимизации последствий и процедурам восстановления, необходимым для защиты цепи поставок;
- разработан план непрерывности деятельности/операций (COOP) и восстановления после инцидента с адекватными положениями для быстрого восстановления оборудования и систем безопасности порта, предназначенных для защиты цепи поставок;
- на местах реализован процесс постоянного улучшения для того, чтобы учиться на любых нарушениях системы менеджмента безопасности, включая инциденты и почти-ошибки;
- регулярно проводятся учения и подготовка по безопасности для того, чтобы гарантировать, что заинтересованные стороны/персонал осведомлены о своих назначенных ролях и обязанностях по безопасности и реагированию на инциденты безопасности.

Показатели результативности (KPI) для управления угрозами и рисками цепи поставок включают вероятность их возникновения, уязвимость систем безопасности, ожидаемое воздействие на безопасность операций порта и шаги по восстановлению для обеспечения непрерывности защиты безопасности.

Оценка показателей результативности будет отражать способность плана устранять или снижать практически достижимый минимальный риск безопасности, уменьшая либо вероятность возникновения, либо потенциальную серьезность воздействия инцидентов, связанных с безопасностью.

2.4.5 Ожидаемые выходы

Для операций средних и малых морских портов существует минимум девять областей универсальных рисков и угроз, которые могут привести к серьезным нарушениям в цепи поставок для перевозимого, обрабатываемого, хранящегося и передаваемого груза организациями, заинтересованными сторонами морского порта и ответственными за обеспечение целостности груза в порту. Данные области включают в себя следующее:

- аварии, которые происходят на портовых объектах, с участием персонала, с оборудованием, с разливами грузов и жидкостей;
- преступная деятельность, такая как кража, вандализм и контрабанда;
- пожар в зданиях, на оборудовании порта, на борту судов и в прилегающих к порту районах;
- финансовые проблемы с заинтересованными сторонами портовых операций и перевозок;
- волнения рабочего персонала, включая забастовки; нехватку персонала и профессиональной подготовки;
- поломки механизмов/оборудования, которые выводят из строя основные опорные элементы (краны, оборудование связи, погрузчики) на длительные периоды времени;
- политические волнения, связанные с правительственными ограничениями, новой политикой и нормативными актами, которые оказывают воздействие на портовые операции;
- террористические акты, которые включают физические атаки/нарушения портовых операций и/или нарушения грузопотока из-за обнаружения контрабанды, что вынуждает порт закрываться до удаления контрабанды и наведения порядка в порту для возобновления нормальной работы;
- проблемы, связанные с погодой, такие как природные явления (сильные штормы, ветер, жара, холод, лед, снег и наводнения), которые могут нарушить работу и сделать меры безопасности неэффективными и оборудование непригодным в течение периода от нескольких часов до нескольких дней/недель.

Каждая из этих девяти областей, указанных выше, представляет уровень риска для непрерывных операций в морском порту, который может повлиять на безопасность цепи поставок. После определения входных параметров, которые позволяют оценить характер и уровень риска для операций морского порта для каждой из этих областей угроз и риска, эти входные данные становятся основой для разработки стратегий минимизации последствий, чтобы свести к минимуму причины их возникновения и сформулировать планы восстановления, когда они происходят. Для каждой из указанных областей в последующих пунктах рассматриваются стратегии оценки риска, стратегии минимизации последствий и рекомендации по восстановлению после бедствия.

2.4.6 Ожидаемый выход/результат

Целью данного руководства является установление принципов, по которым организация может определить, подходят ли процессы идентификации угроз, оценки риска и менеджмента риска и достаточны ли они для защиты целостности цепи поставок или нет. Процесс сертификации позволит

операторам морских портов и заинтересованным сторонам цепи поставок оценить вероятность того, что их товары и операции будут надежно защищены и обработаны своевременно в соответствии с разработанной политикой безопасности, процедурами и графиками доставки, согласованными между заинтересованными в транспортировании сторонами и их конечными пользователями-получателями. План управления безопасностью морского порта, содержащий информацию о внедренных мерах безопасности, будет оценен, и ему будет присвоен доверительный уровень (в баллах), указывающий на его оцениваемое качество и способность гарантировать целостность цепи поставок.

2.4.7 Процесс сертификации

Чтобы гарантировать последовательность и завершение заслуживающего доверия процесса оценки, процесс сертификации должна проводить компетентная независимая организация. Сам процесс будет состоять из перечня оценочных баллов и критериев, охватывающих области угроз и рисков для безопасности цепи поставок, которые определены в плане управления безопасностью морского порта. Цель состоит в том, чтобы иметь полностью обученный персонал и/или представителей опытных независимых организаций, обладающих необходимыми техническими знаниями для анализа и оценки установленных планов управления безопасностью. ИСО 20858 содержит конкретные рекомендации по определению компетентности и технических знаний, необходимых персоналу для проведения оценки безопасности морских портовых средств в соответствии с требованиями ИСО 28000. Кроме того, ИСО 20858 предоставляет конкретные руководящие указания и требования к документации для оценки регистрации качества плана управления безопасностью порта. Оценка и сертификация независимой квалифицированной третьей стороной предусматривается для выполнения следующих действий:

- подтверждения для сообщества пользователей того, что морской порт соответствует намеченным целям и стандартам, указанным в ИСО 28000 и серии стандартов ИСО 28004, для обеспечения целостности цепи поставок;
- создания повторяемого процесса, который можно использовать в качестве стандартизированной основы для измерения и сравнения планов управления безопасностью морских портов с отраслевыми стандартами.

Оценка будет основываться на способности порта отвечать критериям сертификации в соответствии с выявленным риском, процедурой минимизации последствий и планами восстановления, связанными с уровнем операций в морском порту, грузопотоками, типом груза, географическим положением и системами безопасности заинтересованных сторон, структурой деятельности для обеспечения безопасности цепи поставок. Результатом процесса оценки будет присвоение показателя оценки качества, который определяет, какого уровня доверия (от 1 до 5, при этом 5 является самым высоким) заслуживает план управления безопасностью морского порта и насколько он может защитить поставки от идентифицированных рисков и угроз для операций морского порта.

3 Области риска цепи поставок морского порта

3.1 Общие положения

Далее повторно рассматриваются девять областей риска морского порта, включая идентификацию типов связанных рисков, оценку риска, шаги по минимизации последствий для снижения риска, рекомендации по восстановлению для возобновления систем защиты портовых операций до их нормального рабочего состояния. В зависимости от темпа операций, организационной структуры заинтересованных сторон, потока товаров через морской порт, географического положения, правительственных и политических соображений каждый морской порт будет иметь различные уровни угроз и рисков для своих портовых операций по обеспечению безопасности и бесперебойности транспортных услуг для цепи поставок. Те из них, которые относятся к каждому морскому порту, должны быть учтены в плане управления безопасностью и актуализированы в случае появления новых угроз, рисков и/или изменений в рабочем состоянии морского порта.

3.2 Аварии. Портовые операции

3.2.1 Природа риска

Происшествия могут быть чисто случайными по своему характеру и/или могут быть отнесены к категории происшествий, которые происходят ожидаемо и которые можно было бы предотвратить с использованием более эффективного надзора за управлением, обучением персонала и оперативными процедурами. Безопасность цепи поставок должна быть основана на постоянном наблюдении и охране

груза во время его нахождения в порту сотрудниками службы безопасности с использованием охранных систем и оборудования. Любое происшествие, которое нарушает контроль за грузом и безопасность груза, должно быть устранено с использованием конкретных планов, чтобы свести к минимуму случаи возникновения угрозы, предотвратить происшествия, где это возможно, и выполнить шаги по восстановлению, чтобы обеспечить безопасность в цепи поставок.

Тяжелая техника, погрузочные краны, транспортные средства для перевозки грузов, рельсы и устройства для разгрузки грузов — все это создает проблемы безопасности для персонала морского порта, который эксплуатирует эти системы и контролирует безопасность грузов в цепи поставок в порту. Промышленные аварии с участием персонала, с оборудованием, с грузами и/или с разливами жидкостей/химикатов могут нарушать целостность цепи поставок, если меры безопасности и операции в морском порту нарушаются в течение любого значительного промежутка времени.

3.2.2 Оценка риска

Должна быть проведена оценка вероятности возникновения и тяжести последствий идентифицированного риска. В зависимости от природы происшествия должна быть определена вероятность возникновения и ожидаемое воздействие на безопасность и непрерывность деятельности/операций. Оценка должна быть связана с конкретным воздействием на безопасность (потеря ключей, системы мониторинга и защиты) и на ожидаемые уязвимые места в случае нарушения защиты. Все случаи (даже те, которые имеют ограниченное воздействие на безопасность и портовые операции) должны быть оценены. Должна быть проведена оценка каждого происшествия с целью определения уровня риска в отношении цепи поставок на основе способности операторов морского порта быстро восстанавливать и верифицировать работу систем безопасности и на основе того, что целостность цепи поставок не затронута. Любой инцидент, оцененный как имеющий высокий риск для операций по обеспечению безопасности цепи поставок, должен выявлять конкретные уязвимые места, которые могут быть подвержены этому инциденту.

Аварии, в которых участвуют ключевые сотрудники службы безопасности, должны быть немедленно идентифицированы с положениями о замене персонала на тех, кто обучен выполнять необходимые задачи и обязанности. План управления безопасностью должен устранять эти уязвимые места и создавать шаги по минимизации последствий, чтобы избежать (если возможно) или запланировать шаги по восстановлению для обеспечения постоянной защиты цепи поставок.

3.2.3 Стратегии минимизации последствий

Операторы порта и заинтересованные стороны должны определить типы аварий, произошедших в портах, и количественно оценить их конкретное воздействие на портовые операции. Промышленные аварии с участием персонала, с оборудованием, с грузами и с разливами жидкостей/химикатов могут быть количественно оценены с использованием накопленных данных, характеризующих частоту, серьезность воздействия на операции и принятые превентивные меры для минимизации их повторения. Должны быть приняты превентивные меры безопасности, которые предупреждают персонал и напоминают ему о проблемах безопасности и процедурах их предотвращения.

План управления безопасностью должен учитывать конкретные процедуры, шаги, которые необходимо будет выполнить, чтобы предотвратить в дальнейшем последствия и привести систему в рабочее состояние после каждого события. Планы по минимизации последствий в зависимости от характера и ожидаемого воздействия для каждого из оцениваемых рисков должны быть достаточно подробными, чтобы заинтересованные стороны могли предпринять конкретные шаги по защите цепи поставок и привести морской порт в рабочее состояние.

3.2.4 Руководство по восстановлению

План управления безопасностью должен предусматривать конкретные шаги, которые можно рассчитать и оценить, чтобы определить способность морского порта обеспечивать безопасность цепи поставок и возобновлять нормальную работу. По авариям, которые затрагивают ключевой персонал службы безопасности и/или оборудование и операционные системы безопасности, должны быть оформлены документы, содержащие процедуры восстановления, которые определяют конкретные шаги по замене персонала, оборудования и систем безопасности. Резервный и/или заменяющий персонал должен быть обучен всем аспектам безопасности цепи поставок, включая процедуры физической защиты, проверки и обнаружения, а также использованию защитных устройств и автоматизированных систем. При авариях, останавливающих портовые операции, следует учитывать процедуры, которые будут применяться для защиты груза, находящегося в пути или хранящегося в порту, до восстановления нормальной работы порта.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

3.3 Риски преступной деятельности

3.3.1 Природа риска

Преступная деятельность в морском порту и деятельность, связанная с отгрузкой и прибытием товаров, отправляемых в морской порт, или получением груза из источника фазы предконтроля, может привести к немедленному прекращению всех перевозок в морском порту. Преступная деятельность может потребовать закрытия и/или изоляции зон оперативной поддержки до тех пор, пока она не будет расследована правоохранительными органами. Кроме того, кража важных предметов оборудования и компонентов может оказывать воздействие на операции до тех пор, пока запасные детали не будут приобретены и введены в эксплуатацию. В зависимости от характера и серьезности проблемы задержки могут быть измерены в днях, если операции порта из-за нее сокращены. Если преступная деятельность связана с персоналом порта, то заинтересованные стороны оператора порта должны будут принять специальные меры для восстановления целостности операций порта и восстановления утраченного доверия со стороны сообщества цепи поставок.

3.3.2 Оценка риска

Криминогенными (по определению) являются теневые виды деятельности, которые скрыты и трудны для выявления. Они могут иметь множество форм: от кражи товаров и услуг, контрабанды наркотиков, оружия, людей, товаров до взяточничества и мошенничества. Все эти действия направлены на нарушение безопасности и целостности цепи поставок. Потеря товаров, транспортирование контрабанды, мошенничество и подкуп персонала, используемого для обеспечения операций по безопасности порта, включая цепь поставок, могут воздействовать на целостность цепи поставок и подрывать репутацию морского порта и заинтересованных сторон. Вероятность возникновения и серьезность идентифицированного риска для операций необходимо будет оценить. В зависимости от характера преступной деятельности необходимо будет определить вероятность возникновения и ожидаемое воздействие на непрерывность операций. Все случаи, даже те, которые имеют ограниченное воздействие на операции безопасности порта, должны быть оценены. Если деятельность включает в себя замену критически значимого защитного оборудования и/или критически значимого персонала, то оценка должна включать наличие и закупку конкретного предмета оборудования, его установку и тестирование, а также наличие квалифицированного и обученного персонала, способного при необходимости восстановить системы до полного рабочего состояния.

Незаконный ввоз контрабандных товаров создает особый набор обстоятельств, когда они обнаружены/выявлены сотрудниками службы безопасности порта. Обнаружение незаконных наркотических средств, оружия, опасных материалов и/или людей потребует вмешательства правоохранительных органов, конфискации и хранения запрещенного груза. Каждое событие потенциально может остановить поток грузов и оказать влияние на непрерывность операций. План управления безопасностью должен учитывать эти нарушения. Процедуры безопасности должны быть скорректированы или улучшены, чтобы предотвратить будущие инциденты. Криминальная кража или взлом компьютеров и компьютерных файлов должны быть конкретно рассмотрены и должна быть сделана оценка воздействия и времени, необходимого для восстановления потерянных данных. План управления безопасностью должен содержать специальные положения для защиты важных файлов данных, включая планы управления безопасностью портов, которые в случае утери или компрометации могут поставить под угрозу цепь поставок и операции порта.

Преступление в форме хищения или хакерской атаки на компьютеры и компьютерные файлы должно быть предметом особого рассмотрения для оценки воздействия и времени, необходимого для восстановления потерянных данных. План управления безопасностью должен иметь специальные положения для защиты важных файлов данных, включая планы управления безопасностью портов, которые в случае утери или разглашения могут поставить под угрозу цепь поставок и операции порта.

3.3.3 Стратегии минимизации последствий

При выявлении преступной деятельности в плане должны быть определены конкретные шаги, которым будет следовать каждая заинтересованная организация и каждое ведомство для прекращения, задержания и оценки ущерба/потерь для груза в цепи поставок. Планы по минимизации последствий должны быть достаточно подробными, чтобы заинтересованные стороны могли предпринять конкрет-

ные шаги по защите цепи поставок и привести морской порт в рабочее состояние в зависимости от характера и ожидаемого воздействия для каждого из оцениваемых рисков.

Предупреждение, выявление и задержание преступников потребует координации действий между местными правоохранительными органами и заинтересованными сторонами порта, ответственными за обеспечение защиты безопасности операций морского порта. План управления безопасностью должен учитывать конкретные процессы и процедуры для предотвращения, мониторинга, обнаружения, расследования типов выявленных областей криминального риска на основе накопленных данных и исследовательских данных, собранных местными и международными правоохранительными органами. Разработка планов периодических и выборочных проверок грузов наряду с автоматизированным сканированием и использованием оборудования обнаружения поможет в выявлении контрабандных грузов и сдерживании будущей преступной деятельности. Кража товаров, ввозимых и хранящихся в порту, может быть сведена к минимуму — введением ограничения на доступ в порт и проведением проверок безопасности, инспекций и положительной идентификации всего персонала и транспортных средств, въезжающих/находящихся внутри порта. План должен охватывать активное и пассивное контрольное оборудование (камеры, охранники, карты доступа/считыватели), которое можно использовать для обеспечения безопасности цепи поставок груза 24/7.

Если установлено, что преступная деятельность связана с идентифицируемым источником на фазе предконтроля, то дополнительные инспекции безопасности должны быть направлены на эти источники, и/или должны быть введены ограничения, накладываемые на груз из указанных идентифицированных источников доставки.

Подозрительный источник доставки должен требовать дополнительных проверок и договоренностей с правоохранительными органами для оказания помощи в идентификации, проверке и конфискации контрабандного груза и в задержании лиц, причастных к преступной деятельности.

Для контроля и снижения риска участия в преступной деятельности персонала морских портов в плане должны быть предусмотрены подробные процедуры найма и проверки персонала. Эти процедуры должны включать мероприятия для проверки данных, обучение этике для всего персонала и периодические проверки. Руководство также должно иметь процедуру безопасности для ограничения доступа к портовым средствам с использованием контрольных точек безопасности, требующих положительной идентификации для всего персонала и посетителей, заходящих на объекты.

3.3.4 Руководство по восстановлению

План управления безопасностью должен предусматривать конкретные шаги, которые можно рассчитать и оценить, чтобы определить способность морского порта обеспечивать безопасность цепи поставок и возобновить нормальную работу. Роли и обязанности каждого участника должны быть четко указаны наряду с конкретными действиями, которые следует выполнять в ответ на каждую выявленную преступную деятельность. Для каждого фактического события процессы оценки безопасности и предупреждения в морском порту должны оцениваться, чтобы определить, насколько хорошо реализованные системы и/или процедуры были способны обнаруживать преступную деятельность и реагировать на нее. Если в отчетах после действий выявлены слабые места, необходимо внести коррективы, чтобы устранить любые выявленные недостатки в плане защиты безопасности цепи поставок.

Если обнаруживается, что системы и/или процедуры являются несовершенными, то необходимо усовершенствовать системы и процедуры безопасности, чтобы уменьшить или исключить возможность возникновения недостатков в будущем. В тех случаях, когда персонал морского порта был причастен к преступной деятельности, необходимо будет улучшить процедуры найма и проверки персонала, а также ввести в действие политику, обеспечивающую дополнительный надзор для предотвращения подобных случаев в будущем.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту и на основании критериев оценки ему присваивается доверительный уровень.

3.4 Риски возникновения пожара

3.4.1 Природа риска

Пожар в морском порту может привести к серьезным нарушениям, если он разрушит важные здания, системы безопасности, основное оборудование, транспортное оборудование и охраняемый груз. Кроме того, пожары на судах, пришвартованных в порту, а также пожары в прилегающих районах могут привести к задержкам с доставкой товаров в морской порт. Воздействие крупного пожара в морском

порту может привести к отключению оборудования на длительный период времени, особенно если системы безопасности и обработки грузов вышли из строя. Повреждение крайне важных физических и автоматизированных систем защиты (заборы, камеры охраны, системы камер, компьютеры и компьютерные системы, системы связи) потребует приведения этих систем в рабочее состояние до возобновления нормальной работы морского порта. План управления безопасностью должен учитывать области потенциального риска возникновения пожара и иметь планы и процедуры плана непрерывности деятельности/операций (COOP) и аварийного восстановления после бедствия, чтобы обеспечить безопасность груза в цепи поставок порта. Особое внимание должно быть уделено обеспечению того, чтобы ни одна из важных систем безопасности не была нарушена каким-либо пожаром, а также защите груза от возможного вмешательства со стороны учреждений за пределами порта, реагирующих на пожар.

Стратегии предупреждения пожаров и минимизации последствий, в том числе возможности морского порта по тушению пожаров для быстрого устранения огня, а также планы восстановления после бедствия будут оказывать влияние на безопасность порта и возможности обработки грузов заинтересованными сторонами порта. Должна быть проведена оценка плана управления безопасностью морского порта, чтобы определить, являются ли профилактические меры, обучение персонала и шаги по восстановлению достаточными и эффективными для обеспечения целостности цепи поставок для груза, находящегося под непосредственным контролем морского порта во время пожара.

3.4.2 Оценка риска

Необходимо оценивать вероятность возникновения и серьезность последствий идентифицированного риска для портовых операций. В зависимости от характера пожара и степени ущерба, нанесенного эксплуатационным возможностям морского порта, необходимо будет определить ожидаемое воздействие на непрерывность операций. Оценка должна учитывать ожидаемое время задержки и необходимые процедуры восстановления, чтобы вернуть портовые операции в нормальное рабочее состояние. Все инциденты в виде пожаров, даже те, которые оказывают ограниченное воздействие на портовые операции, должны быть оценены. Если инциденты связаны с восстановлением объектов и/или заменой важного оборудования для защиты безопасности, тогда оценка должна включать наличие и закупку требуемых изделий, установку и тестирование (при необходимости) для восстановления системы до полного рабочего состояния. Отдельное решение должно быть разработано по утрате компьютеров и компьютерных файлов, которые поддерживают управление, контроль и связь между местными, региональными и международными органами безопасности. Должна быть проведена оценка воздействия и времени, необходимого для восстановления этих данных и доступа к связи.

Предполагаемая продолжительность простоя, вызываемого каждым случаем, должна быть определена с точки зрения часов, дней и недель. Ожидаемая продолжительность простоя в результате инцидента будет основным фактором для разработки стратегий минимизации последствий и процедур восстановления, которые должны быть учтены заинтересованной стороной в плане управления безопасностью порта для обеспечения непрерывности операций.

3.4.3 Стратегии минимизации последствий

План управления безопасностью должен учитывать конкретные процессы, которые будут реализованы для предотвращения, защиты целостности цепи поставок и максимально быстрого восстановления системы до рабочего состояния после каждого происшествия. Все время, в том числе во время реагирования на инцидент, цепь поставок груза должна быть защищена. Должны быть разработаны планы перемещения любого груза на пути пожара, переключения на резервные системы для любых систем безопасности, затронутых пожаром, и назначения/переназначения любого дополнительного персонала для физического мониторинга и обеспечения доступа к цепи поставок и критическим системам защиты во время инцидента. Планы минимизации последствий должны быть достаточно подробными, чтобы описывать конкретные роли, обязанности и шаги, которые должны быть предприняты заинтересованными сторонами для реализации процедуры предупреждения и реагирования на инцидент. В плане должны быть учтены ожидаемые задержки и время простоя систем безопасности, которые влияют на работу морского порта, а также какие процедуры будут реализованы морским портом для обеспечения безопасности цепи поставок в течение этого временного периода.

3.4.4 Руководство по восстановлению

План управления безопасностью должен предусматривать конкретные шаги, которые можно рассчитать и оценить, чтобы определить способность морского порта обеспечить безопасность цепи поставок и возобновить нормальную работу. Если портовое сооружение будет выведено из эксплуатации в течение длительного периода времени, то необходимо будет разработать обходной план, чтобы

перенаправить обычный поток на фазы предконтроля и постконтроля по цепи поставок в другие места. Для любых поврежденных систем должен быть предусмотрен процесс проверки и сертификации, который подтверждает правильность работы заменяющих систем. План управления безопасностью должен предусматривать альтернативные системы защиты для замены любых автоматизированных систем защиты, которые вышли из строя и не могут обеспечить безопасность груза в цепи поставок. В плане должны быть рассмотрены системы ручного управления, дополнительные охранники, места временного безопасного хранения с должным образом обученным персоналом как временная коррекция для поддержки постоянного потока товаров через порт до тех пор, пока автоматизированные системы и обычные операции не будут восстановлены.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

3.5 Финансовые риски заинтересованных сторон

3.5.1 Природа риска

Финансовое благополучие заинтересованных сторон, участвующих в операциях в морских портах, необходимо отслеживать и оценивать на основе их способности выполнять свои конкретные функции и обязанности по защите целостности цепи поставок и поддержке операций порта. Финансовая нагрузка на заинтересованную сторону порта может оказать воздействие на ряд областей, включая наличие достаточного количества обученного персонала, техническое обслуживание и обеспечение запасными частями, а также контроль и защиту безопасности. Бюджетные ограничения могут повлиять на качество и результативность мер безопасности, необходимых для защиты цепи поставок, а также необходимых мер для поддержания уровня услуг для обеспечения бесперебойной непрерывной работы цепи поставок. Заинтересованная сторона морского порта должна быть в состоянии противостоять растущему перечню рисков и угроз для цепи поставок. Это может потребовать приобретения дополнительного оборудования для обеспечения безопасности и дополнительного персонала для минимизации этих угроз и рисков. В дополнение, непредвиденные расходы из-за случайных событий, таких как несчастные случаи, пожары, разрушительные штормы, криминальная и террористическая деятельность, могут серьезно повлиять на финансовые возможности заинтересованных сторон в сфере осуществления операций цепи поставок.

Финансовое воздействие в результате реагирования на новые угрозы и риски, а также случайные события следует учитывать в плане управления безопасностью. При выявлении потенциальных недостатков, которые могут воздействовать на защиту безопасности цепи поставок, план управления безопасностью должен учитывать мероприятия по минимизации последствий, которые необходимо предпринять заинтересованными сторонами для изменения операций порта в целях защиты груза, находящегося под их непосредственным контролем.

3.5.2 Оценка риска

План управления безопасностью морского порта должен содержать процедуры для мониторинга и оценки финансового состояния каждой из заинтересованных сторон, занимающихся обеспечением безопасности, обработкой и транспортированием грузов в цепи поставок, входящих и выходящих из порта. Их конкретные роли и обязанности должны быть оценены для выявления отдельных точек сбоя, которые могут повлиять на безопасность и доставку товаров, если они не в состоянии предоставить необходимые услуги для обеспечения целостности цепи поставок и портовых операций.

Необходимо определить любую точку, где возможны ошибки/нарушения, и провести оценку ожидаемого воздействия на безопасность и портовые операции. Бюджетные ограничения необходимо проанализировать, чтобы определить их воздействие на текущие и будущие операции, а также необходимо предпринять для поддержания требуемого уровня безопасности и эксплуатационной готовности морского порта. Особое внимание необходимо уделить операциям на фазе предконтроля, где финансовые проблемы могут воздействовать на способность заинтересованных сторон осуществлять надлежащие меры безопасности и надзор, определенные в ИСО 28000.

3.5.3 Стратегии минимизации последствий

План управления безопасностью должен обеспечивать возможность общей и стоимостной оценок, если потенциальные финансовые проблемы могут оказать воздействие на операции в морском порту. Для этих единичных критических точек ошибок/нарушений должны быть созданы альтернативы, обеспечивающие непрерывность требуемой работы служб безопасности цепи поставок, служб безопас-

ности и эксплуатации порта. Для обеспечения наличия средств, необходимых для поддержания оперативных потребностей цепи поставок, стратегии минимизации последствий должны включать в себя план, содержащий целесообразный процесс финансового планирования и прогнозирования бюджета с запланированными периодами проведения финансового анализа. Если в критических областях поддержки обнаружен дефицит, то необходимо предпринять конкретные шаги возможных обходов и/или сокращения услуг, которые не влияют на целостность цепи поставок.

Финансовые проблемы заинтересованных сторон на фазе предконтроля, которые оказывают влияние на безопасность доставки груза в морской порт, следует решать в том случае, если для этого потребуется дополнительный источник ресурсов для защиты целостности груза, входящего в порт. Если стоимость дополнительных источников ресурсов превышает ожидаемую отдачу от инвестиций по обработке груза, придется рассмотреть вопрос об отказе от груза до тех пор, пока не будут даны гарантии того, что процедура обработки груза будет выполнена в соответствии с ИСО 28000 и серией стандартов ИСО 28004.

3.5.4 Руководство по восстановлению

План управления безопасностью должен предусматривать конкретные шаги, которые можно рассчитать и оценить, чтобы определить способность морского порта обеспечивать безопасность цепи поставок и возобновлять нормальную работу. Если заинтересованная сторона порта не в состоянии адекватно выполнить свою роль и свои обязанности по поддержке цепи поставок, то в плане должны быть рассмотрены альтернативные шаги для обеспечения безопасности и рабочего состояния морского порта. План управления безопасностью должен содержать проверенный оперативный бюджет, который определяет необходимые источники финансовых ресурсов для обеспечения непрерывности операций цепи поставок и темпов операций для поддержки ожидаемого потока товаров через морской порт.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

3.6 Риски, связанные с трудовыми отношениями

3.6.1 Природа рисков

Безопасность цепи поставок во многом зависит от качества и количества персонала, предназначенного для обеспечения безопасности груза в порту. Сотрудники службы безопасности должны быть полностью подготовлены для выполнения конкретных задач по безопасности в соответствии с ролями и обязанностями, определенными им в плане управления безопасностью цепи поставок. Любой риск, который вызывает нехватку обученного персонала для мониторинга, эксплуатации и реализации процедуры безопасности морского порта, подвергнет риску цепь поставок. Необходимо определить проблемы, связанные с трудовыми ресурсами, которые могут повлиять на нормальную работу порта, и установить процедуры для обеспечения непрерывной работы систем безопасности морского порта. Перерыв в работе, вызванный волнениями рабочего персонала (забастовка, замедление работы), нехваткой персонала для поддержки операций и/или наличием плохо обученного персонала, может поставить под угрозу процедуру безопасности, разработанную для защиты потока товаров через порт. Персонал порта должен быть хорошо осведомлен, проинформирован о существующей процедуре и полностью обучен процедурам предупреждения бедствий и восстановления после бедствий. Кроме того, должны быть разработаны планы на случай непредвиденных обстоятельств, чтобы обеспечить доступ к дополнительным источникам кадровых ресурсов для удовлетворения потребности в кадрах для проведения критически значимых операций в порту и защиты цепи поставок.

3.6.2 Оценка риска

Защита цепи поставок и непрерывная работа порта будут зависеть от качества и достаточного количества обученного персонала для поддержки операций порта. Должны быть определены проблемы, связанные с трудовыми ресурсами, включая забастовки, и проведена оценка с точки зрения их воздействия на управление и реализацию процедуры обеспечения безопасности порта. Для каждой важной должности персонала, которая может повлиять на операции порта и безопасность, должна быть проведена оценка уязвимости системы при условии, что эти источники человеческих ресурсов недоступны. Должна быть идентифицирована возможная утрата ключевого персонала по любой причине (забастовка, болезнь, увольнение), а планы и процедуры на случай непредвиденных обстоятельств — подвергнуты оценке, чтобы определить их способность обеспечивать непрерывность работы порта и его безопасность. Оценка должна учитывать ожидаемое время задержки, воздействие на защиту без-

опасности цепи поставок и требуемую процедуру восстановления для возвращения портовых операций в нормальное рабочее состояние.

3.6.3 Стратегия минимизации последствий

Для обеспечения бесперебойной работы порта планы управления безопасностью и планы эксплуатации порта должны включать достаточное количество обученного персонала для выполнения обычных и любых непредвиденных операций, вызванных утратой ключевого персонала. Должна существовать специальная процедура, чтобы обеспечить подготовку временного и любого замещающего персонала для поддержки нехватки персонала, вызванной проблемами с трудовыми ресурсами, которые могут нарушить трафик и безопасность цепи поставок. План управления безопасностью должен предусматривать подготовку ключевого персонала для выполнения нескольких функций и обязанностей, чтобы иметь в наличии достаточное количество квалифицированного персонала для сведения к минимуму проблем, связных с трудовыми ресурсами, и возможных нарушений, которые могут быть вызваны нехваткой источников кадровых ресурсов. План должен иметь резервные руководства для критических ситуаций, чтобы в случае возникновения нехватки персонала в этих областях трафик и безопасность цепи поставок не подвергались непредвиденным последствиям.

3.6.4 Руководство по восстановлению

План управления безопасностью должен предусматривать конкретные шаги, которые можно рассчитать и оценить, чтобы определить способность морского порта обеспечивать безопасность цепи поставок и возобновлять нормальную работу. Нехватка персонала и/или плохо обученный персонал могут поставить под угрозу целостность операций цепи поставок. Поэтому в плане должны быть предусмотрены условия для набора дополнительно обученного персонала в относительно короткие сроки. Заинтересованная сторона порта должна быть в состоянии обеспечить наличие контингента из обученного и квалифицированного персонала для каждой из ключевых должностей, которые могут повлиять на деятельность, если она останется вакантной. Кроме того, в плане должны быть рассмотрены процедуры обучения и набора ключевых замещающих сотрудников, назначенных в контингент резервного персонала.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

3.7 Риски механических поломок оборудования

3.7.1 Природа рисков

Механическая поломка основных предметов оборудования может замедлить и/или остановить работу. Отказ системы безопасности порта и защиты груза отразится на целостности цепи поставок груза. Если критически значимое оборудование не будет работать в течение какого-либо длительного периода времени, то это повлияет на безопасность груза и непрерывность операций. Отказ оборудования и систем более широкого спектра может привести к сокращению и/или остановке запланированного потока товаров через порт, если резервные системы не будут подключены к сети для поддержки нормального потока операций.

Отказ оборудования может произойти в любом эксплуатационном оборудовании порта — от погрузочного крана, грузовых транспортных средств до компьютерных систем и систем контроля и защиты безопасности морского порта и цепи поставок. Отказ систем обнаружения, таких как видеонаблюдение, оборудование для внутриполостного сканирования и программное обеспечение систем слежения за базами данных, приведет к замедлению или остановке движения груза через порт. Риск для цепи поставок будет высоким, если из-за отказа этих систем груз в цепи поставок останется незащищенным в течение значительного периода времени.

3.7.2 Оценка риска

Сбои или поломки систем защиты и безопасности портов и цепи поставок могут поставить под угрозу безопасность грузов в цепи поставок. Если резервные или альтернативные системы защиты не могут быть быстро задействованы, то обработку и перемещение груза следует прекратить до тех пор, пока системы защиты не будут введены в действие. Целостность цепи поставок зависит от постоянно и непрерывно действующей гарантии защиты, которая обеспечивает сквозную защиту груза во время его транспортирования до конечного пункта назначения. Если меры безопасности вышли из строя, то риск для цепи поставок можно считать высоким в любое время. При выходе систем защиты безопасности из строя перемещение груза должно быть остановлено и должны быть внедрены дополнительные систе-

мы физической безопасности для защиты груза до тех пор, пока системы безопасности порта не будут возвращены в оперативный режим работы. План управления безопасностью порта должен учитывать эти непредвиденные обстоятельства и предоставлять систему отчетности, которая документирует перерыв в защите и шаги, предпринятые для подтверждения того, что в течение этого периода не было никаких нарушений безопасности.

3.7.3 Стратегии минимизации последствий

Чтобы обеспечить постоянную защиту груза в цепи поставок, должны быть предусмотрены планы обеспечения дополнительной физической защиты, работающие в ручном режиме, пока все автоматизированные системы защиты, на которые повлияло нарушение, не будут восстановлены в рабочее состояние. Если оборудование/системы отключены от сети в течение какого-либо длительного периода, то должны быть предусмотрены меры по прекращению движения груза до тех пор, пока не будут созданы резервные системы и предприняты операционные шаги для защиты цепи поставок и подтверждения того, что груз не находился под угрозой, пока системы не работали. Стратегии минимизации последствий должны учитывать планы профилактического технического обслуживания, чтобы оборудование и системы работали в полную силу, а планы действий в чрезвычайных ситуациях должны обеспечивать альтернативные операции при неожиданных сбоях оборудования/системы.

План профилактического обслуживания должен быть ключевым элементом стратегии минимизации последствий. При определении того, как минимизировать воздействие отказов оборудования/систем на непрерывность деятельности, необходимо учитывать установленный план профилактического технического обслуживания и знание среднего времени между отказами (MTBF) и средним временем ремонта (MTTR). Для того чтобы избежать непредвиденных поломок, оборудование и системы, достигшие ожидаемого времени обслуживания MTBF, должны пройти техническое обслуживание либо их необходимо заменить. Время ремонта оборудования MTTR будет определять ожидаемое время простоя и то, какие стратегии восстановления должны быть в наличии, чтобы восстановить работоспособность систем. Согласование графиков технического обслуживания с запланированным временем простоя между требованиями по обработке грузов позволит ограничить нарушение потока движения в порту.

3.7.4 Руководство по восстановлению

План управления безопасностью должен предусматривать конкретные шаги, которые можно рассчитать и оценить, чтобы определить способность морского порта обеспечивать безопасность цепи поставок и возобновлять нормальную работу. Если системы безопасности порта находятся в автономном режиме и не могут обеспечить защиту груза, должны быть разработаны планы по остановке операций порта до восстановления системы. Резервные системы и оборудование должны быть легко доступными, а персонал должен быть обучен их внедрению после обнаружения отказа системы. В тех случаях, когда эти автоматизированные системы требуют длительного времени для ремонта, влияющего на непрерывность операций, процедуры и руководства должны быть рассмотрены в плане восстановления безопасности для защиты цепочки поставок до тех пор, пока все системы безопасности не будут работать. Для любых заменяемых и/или ремонтируемых систем безопасности портов должен быть предусмотрен процесс проверки и сертификации, который подтверждает, что заменяющие системы работают должным образом, предоставляя необходимые услуги защиты безопасности.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

3.8 Политические и государственные риски

3.8.1 Природа рисков

Политические проблемы, изменения в руководстве и политике местных органов власти могут оказывать непосредственное воздействие на портовые операции, заинтересованные стороны и на то, как в порту реализуются меры безопасности. Постановления Правительства могут повлиять на управление портов, на работу портов и на то, какие органы будут уполномочены защищать цепи поставок. Эти изменения могут повлиять на ограничения владения портом, потребовать изменений в таможенных и инспекционных процедурах и ограничить финансирование для безопасности порта и поддержки правоохранительных органов. План управления безопасностью порта должен отражать определенные роли и обязанности для каждой из заинтересованных сторон, которые управляют операциями порта и обеспечивают защиту безопасности цепи поставок. Изменения и/или ограничения, обусловленные политическими решениями в структуре организационной отчетности и критических ролях и обязанностях заинтересованных сторон, могут повлиять на непрерывность операций и безопасность цепи поставок.

План управления безопасностью должен учитывать те изменения, которые вводят международные правительства и руководящие органы (ЕС, ВТО, США, НАТО), непосредственно влияющие на операции по цепи поставок, и требования защиты безопасности. В связи с растущей обеспокоенностью по поводу террористической и криминальной деятельности во всем мире международные правительства, организации, грузоотправители и конечные пользователи требуют усовершенствованных процедур обнаружения и предотвращения проникновения из транспортных систем в запрещенные зоны портов материалов, связанных с оружием массового уничтожения, и наркотиков. Должны быть проанализированы политические изменения, которые могут повлиять на способность операторов порта обеспечивать бесперебойную защиту цепи поставок.

3.8.2 Оценка риска

Следует проводить анализ политических и нормативных актов, затрагивающих заинтересованные стороны и агентства, уполномоченные поддерживать портовые операции и защищать цепь поставок. Должна быть проведена оценка для определения уровня риска, связанная с вынужденными изменениями. Для каждого выявленного изменения в местных и международных правительственных правилах должна быть проведена оценка способности заинтересованных сторон порта внедрять изменения и минимизировать любые риски, связанные с этими изменениями. Изменения в правилах защиты цепи поставок могут серьезно повлиять на защиту цепи поставок и могут увеличить операционные риски, если изменения не будут реализованы должным образом. Принятые правительством правила, требующие дополнительных мер безопасности, могут влиять на непрерывность операций и источники ресурсов (персонал, оборудование, финансирование), необходимые для защиты цепи поставок. Новые правила (такие, как усиленное сканирование груза) на предмет контрабанды и оружия массового уничтожения (ОМУ) могут потребовать дополнительного оборудования для обнаружения, средств и обученного персонала по использованию и обслуживанию оборудования.

Для каждого идентифицированного изменения необходимо провести оценку возможностей заинтересованной стороны для реализации изменения. Те изменения, которые определены как относящиеся к среднему или высокому риску, потребуют, чтобы план управления безопасностью порта учитывал конкретные шаги по минимизации последствий для снижения риска, связанного с обязательным изменением.

3.8.3 Стратегии минимизации последствий

План управления безопасностью должен ссылаться на конкретные процессы, которые должны быть реализованы, если происходят изменения в политической и/или правительственной сфере и нормативных актах, которые влияют на деятельность по защите безопасности цепи поставок. Если государственная политика создает риски для операций в портах и/или для безопасности цепи поставок, план управления безопасностью должен учитывать вероятные шаги, которые должна предпринять заинтересованная сторона для реализации изменений и минимизации риска для системы. В плане управления безопасностью должны быть учтены конкретные политики, которые меняют роли и обязанности заинтересованных сторон, с указанием чрезвычайных мер, обеспечивающих непрерывную защиту безопасности цепи поставок. Стратегические изменения, которые затрагивают кадровое обеспечение либо для замены, либо для принятия новых обязанностей, должны включать элементы обучения, которые должны быть учтены в плане управления безопасностью. Риск для системы будет представлять собой необходимую кривую обучения, связанную с любыми изменениями политики, которые влияют на существующие положения о безопасности, реализуемые в морском порту. Введение новых требований должно быть проверено, подтверждено и проконтролировано, чтобы гарантировать, что они работают по мере необходимости, не добавляют дополнительного риска системе и обеспечивают любую дополнительную безопасность, как это предусмотрено изменением.

Если политические изменения и изменения в директивах/программах влияют на штат сотрудников в плане его замены или принятия новых обязанностей, то в плане управления безопасностью необходимо учесть элементы обучения. При политических изменениях, оказывающих влияние на существующую систему безопасности в порту, риск, возникающий для системы, потребует реализации функции обучения.

Чтобы убедиться, что внедрение новых требований не вносит дополнительного риска для системы и обеспечивает дополнительную безопасность, предусмотренную изменением, оно должно быть проверено, пройти валидацию и мониторинг.

3.8.4 Руководство по восстановлению

План управления безопасностью морского порта должен предусматривать конкретные шаги для реализации любых необходимых изменений государственной политики, которые влияют на безопас-

ность операций морского порта и цепь поставок. Этапы восстановления должны включать любые изменения в управлении, в штатном расписании и/или во внедрении и эксплуатации новых процедур безопасности, правил и оборудования. План управления безопасностью должен предусматривать конкретные шаги, которые можно рассчитать и оценить, чтобы определить способность морского порта обеспечивать безопасность цепи поставок и возобновлять нормальную работу после внесения любых изменений. Для любых новых политик и/или систем защиты безопасности порта должен быть предусмотрен процесс инспекции и сертификации, который проверяет правильность работы этих политик и систем, обеспечивающих необходимые услуги защиты безопасности.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

3.9 Риски, связанные с терроризмом

3.9.1 Природа рисков

Террористические атаки — это всемирная глобальная террористическая угроза, которая реализуется во многих формах, и ни одно место не застраховано от этих атак. Случайный характер атак трудно предвидеть и часто очень трудно обнаружить. Террористическая деятельность предназначена для срыва и уничтожения операций, включая физический ущерб объектам, людям, угрозу кибератак, которые могут нарушить работу компьютеров, коммуникаций и сетей безопасности. Повреждения портовых сооружений могут включать оборудование, погрузочные краны, портовые сооружения, грузы и суда, заходящие в порты. Вторичной угрозой является обнаружение опасного груза, содержащего оружие массового уничтожения (ОМУ) и другие материалы для изготовления бомб, которые потребуют закрытия порта до тех пор, пока эти материалы не будут безопасно удалены. Любой из этих примеров может серьезно повлиять на работу порта и иметь долгосрочный эффект в будущих операциях, если портовые средства будут повреждены.

3.9.2 Оценка риска

Террористическая деятельность может привести к закрытию порта на неопределенный срок и нарушению целостности цепи поставок. Малые и средние морские порты могут иметь ограниченные ресурсы для обнаружения и защиты операций порта от целенаправленной террористической деятельности. Меньшие порты фидерного типа особенно уязвимы к проблемам с опасным грузом, который обычно входит в цепь поставок в этих фидерных портах от местного наземного и железнодорожного грузового транспорта. В то время как вероятность целевой террористической деятельности в малых портах имеет низкий показатель, любой инцидент может привести к закрытию порта и созданию достаточной потери трафика через порт. Трафик может не возвратиться к исходному состоянию после восстановления операций порта, если сообщество пользователей будет рассматривать порт, как порт с потенциальным риском будущих операций.

Защита цепи поставок и непрерывности деятельности порта будут зависеть от качества и необходимого количества компетентного персонала, обученного мониторингу и обнаружению возможной угрозы для цепи поставок и операций порта. Оценка риска должна учитывать возможность возникновения, наличие места для мониторинга и обнаружения возможной террористической угрозы, а также конкретные роли и обязанности, которые будут выполняться каждой заинтересованной стороной или организацией при обнаружении и/или возникновении угрозы в морском порту.

Особое внимание должно быть уделено растущей угрозе кибератак на системы передачи информации и данных, защищающих цепь поставок. Для обнаружения и предотвращения кибератак должны быть установлены компьютерные и сетевые системы обнаружения взломов систем безопасности, предотвращения утечки данных, предотвращения кражи информации о планах защиты безопасности, повреждения файлов критических данных и/или фальсификации данных о доставке, чтобы скрыть опасные грузы. Должна быть проведена детальная оценка качества и возможностей, установленных компьютерных и сетевых систем защиты, чтобы определить уязвимость систем по отношению к возможным кибератакам.

3.9.3 Стратегии минимизации последствий

Стратегии минимизации последствий должны учитывать необходимость определения и защиты критически значимых объектов морского порта и систем безопасности, а также планируемые меры по предупреждению (после обнаружения) любой террористической деятельности. Шаги раннего обнаружения и предупреждения являются лучшей защитой от случайных и хорошо спланированных террори-

стических актов. Терроризм — это глобальная проблема, и заинтересованным сторонам порта необходимо установить связи с глобальными, региональными и местными правоохранительными органами и спецслужбами, чтобы получать информационные оповещения о любой известной террористической деятельности, которая сосредоточена в их областях.

Террористическая деятельность (по определению) будет скрытой операцией, которая потребует от портов передавать информацию в спецслужбы для раннего предупреждения и оповещения о любой потенциальной деятельности, направленной на цепь поставок и операции морского порта. План управления безопасностью требует устанавливать связи с правоохранительными органами и спецслужбами и тщательно внедрять документированные процедуры обнаружения и реагирования на потенциальный террористический акт. В частности, план управления безопасностью должен включать следующие шаги по минимизации последствий:

- установление связей со спецслужбами и правоохранительными органами, которые отслеживают террористическую деятельность;
- внедрение документированной процедуры по реагированию в случае выявления потенциальной угрозы;
- использование технологического оборудования и систем для мониторинга портовых сооружений и выявления возможной террористической деятельности;
- использование инспекционного оборудования и оборудования для сканирования груза с целью обнаружения ОМУ и опасных материалов, спрятанных в грузе, перевозимом через порт;
- внедрение документированной процедуры действий при обнаружении опасного груза для его задержания, изоляции и утилизации, чтобы быстро вернуть порт в нормальное состояние;
- непрерывное обучение для повышения осведомленности персонала о проблемах наблюдения и обнаружения потенциальных террористических угроз;
- процедура обеспечения безопасного доступа в порт с позитивной идентификацией персонала и посетителей и защиты от несанкционированного движения легковых и грузовых автомобилей, пытающихся проникнуть в портовые сооружения.

Кроме того, в плане должны быть конкретно указаны роли и обязанности каждой из заинтересованных сторон при мониторинге, обнаружении, обмене данными и реагировании на возможные угрозы. Должны быть предусмотрены условия для периодических учебных сессий для проверки готовности заинтересованных сторон, безопасности систем обнаружения и шагов реагирования на инцидент.

3.9.4 Руководство по восстановлению

Должно быть сделано все, чтобы обнаружить и предотвратить террористический акт. Восстановление может быть экстенсивным, если основные элементы порта повреждены. Кроме того, грузоотправители потеряют доверие к порту, если угроза террористической деятельности высока. Если любой инцидент фактически произойдет, то после возвращения порта в нормальное рабочее состояние потребуется значительный объем усилий в области маркетинга для восстановления уровня доверия и целостности услуг, предлагаемых портом для защиты цепи поставок.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 и серией стандартов ИСО 28004 по его способности обеспечивать непрерывность операций в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

3.10 Погодные риски

3.10.1 Природа рисков

Экстремальные погодные условия могут повлиять на способность операторов порта безопасно загружать и разгружать суда, перемещать грузы вокруг морского порта и обеспечивать безопасность грузов, если охранные системы зависят от погодных условий (потеря мощности, плохая видимость и заблокированный доступ к защищаемым районам). Прогнозы погоды для операций в морских портах обычно обеспечивают достаточное заблаговременное предупреждение, что позволяет предпринять превентивные меры для сведения к минимуму воздействия сильных штормов и/или неблагоприятных погодных условий, которые могут привести к остановке работы порта. Исходя из географического положения и погодных условий в исторической ретроспективе ожидается, что в течение года в морском порту будут происходить некоторые задержки в работе, вызванные дождем, снегом, льдом, сильными ветрами и в некоторых случаях наводнениями. Эти условия в дополнение к чрезвычайно низким и высоким температурам будут в некоторой степени влиять на поток перевозок в морском порту, а также на способность морского порта обеспечивать безопасность грузов, если системы безопасности будут выведены из строя из-за погодных условий.

План управления безопасностью должен иметь хорошо проработанные документированные планы действий в экстремальных погодных условиях, способных поставить под угрозу безопасность груза, обрабатываемого портом. Погодные условия, которые приводят к остановке работы порта и повреждению критически значимого оборудования, систем безопасности и средств, следует учитывать с использованием накопленных данных о вероятности возникновения экстремальных погодных условий и о том, какие шаги были предприняты в прошлом для восстановления нормального режима работы порта.

3.10.2 Оценка риска

Экстремальные погодные условия могут разрушить портовые сооружения и замедлить перемещение грузов в морском порту. Если на обеспечение безопасности порта оказывают влияние погодные условия, целостность цепи поставок может быть нарушена, если альтернативные планы защиты грузов в цепи поставок не внедрены надлежащим образом. Сильные штормы (дождь, ветер, снег), вызывающие наводнения, морские волнения и повреждения в линиях электропередачи в зданиях и в портовом оборудовании (в результате сильного ветра), замедляют и/или приостанавливают операции в порту. Для защиты груза в порту и поддержания способности персонала управлять мерами безопасности груза в цепи поставок должна быть проведена оценка индивидуального потенциального риска экстремально холодной погоды, приводящей к сезонной ледовой блокировке и температурам замерзания, влияющим на оборудование и персонал.

Каждый из этих возможных рисков имеет вероятность возникновения, основанную на накопленных данных о погодных условиях для каждого географического порта. Несмотря на некоторую степень предсказуемости, планы управления безопасностью должны учитывать и оценивать те факторы риска, которые делают порт неспособным поддерживать позитивный контроль безопасности и защиту цепи поставок. В частности, необходимо оценить риск, связанный с потерей мощности и любым ущербом программным системам, критическим системам защиты портов и системам мониторинга безопасности, а также составить планы минимизации последствий для минимизации риска, угрожающего целостности цепи поставок.

3.10.3 Стратегия минимизации последствий

План управления безопасностью должен ссылаться на конкретные процессы, которые должны быть реализованы, чтобы предотвратить серьезные задержки, защитить целостность цепи поставок и как можно быстрее восстановить систему до рабочего состояния после каждого происшествия. Правильный прогноз погоды должен обеспечить достаточное предварительное уведомление об угрозе сложных погодных условий, которые могут нарушить работу порта. Поэтому (как часть плана управления) должны быть предусмотрены меры для мониторинга погодных условий и предоставления оповещений заинтересованным сторонам, когда погодные условия могут нарушить обслуживание. Используя погодные данные в исторической ретроспективе и их воздействие на портовые операции, в плане следует учитывать ожидаемые задержки в течение определенного периода года, которые могут быть отнесены к каждому погодному состоянию, и данные о том, какие операции в порту и процедуры безопасности были реализованы для минимизации воздействия на цепь поставок.

Для таких условий, как сезонное похолодание и обледенение, которые влияют на портовые операции и системы безопасности, план должен учитывать альтернативные пути для обеспечения непрерывности операций и защиты цепи поставок. В плане управления безопасностью (в зависимости от серьезных изменений ожидаемой погоды) заранее должны учитываться определенные планы, процедуры и процессы, а персонал должен быть обучен шагам, которые необходимо предпринять для защиты цепи поставок. Планы по минимизации последствий должны быть достаточно подробными и содержать конкретные роли, обязанности и мероприятия, которые должны быть приняты заинтересованной стороной для реализации процедуры предупреждения в ответ на ожидаемые погодные условия.

3.10.4 Руководство по восстановлению

Погодные условия, влияющие на цепь поставок и деятельность портов, достаточно предсказуемы, и, как правило, предупреждение предоставляется достаточно заблаговременно, чтобы принять превентивные меры для защиты цепи поставок. Исторические данные о суровых погодных условиях, этапах предупреждения и процедурах восстановления должны быть задокументированы и проанализированы, чтобы определить наилучшие этапы восстановления для обеспечения непрерывности портовых операций. Во всех случаях критические системы, которые могут повлиять на работу портов и безопасность цепи поставок, должны иметь определенные резервные системы/оборудование и обученный персонал для выполнения шагов восстановления. Восстановление может быть экстенсивным, если основные элементы порта и системы безопасности повреждены и выведены из строя в течение длительных периодов времени.

Качество плана восстановления следует оценивать в соответствии с ИСО 28000 по его способности обеспечивать непрерывность операций по безопасности цепи поставок в морском порту, и на основании критериев оценки ему присваивается доверительный уровень.

4 Оценочные критерии плана управления безопасностью порта и процесс присвоения рейтинга

4.1 Общие положения

Процесс анализа и оценки обеспечения безопасности в плане управления безопасностью порта основывается на определении его соответствия международным стандартам ИСО и способности внедренной системы безопасности эффективно обеспечивать сохранность груза в цепи поставок. Для обеспечения соответствия требованиям безопасности ИСО 28000 планы управления безопасностью организаций заинтересованных сторон средних и малых портов следует периодически анализировать для определения их дееспособности и эффективности в защите цепи поставок от идентифицированных угроз и рисков в отношении операторов портов. Периодический анализ должен включать проверку процедур обеспечения безопасности порта для обнаружения, защиты и реагирования на инциденты или чрезвычайные ситуации, вызванные нарушениями безопасности и угрозами. Проверки можно проводить как внутренними силами, так и независимыми группами обученных специалистов по безопасности. Оценки следует проводить по набору показателей результативности деятельности по управлению (KPI), эксплуатации, снижения рисков и восстановления, чтобы установить уровень уверенности в том, что планы управления безопасностью морского порта достаточны для обеспечения целостности цепи поставок для всех грузов, обрабатываемых морским портом.

ИСО 20858 предусматривает конкретные дополнительные указания и утвержденный чек-лист оценки возможностей и полноты плана управления безопасностью порта по устранению угроз и рисков для целостности цепи поставок. Настоящий стандарт вместе с соответствующими положениями ИСО 20858 предоставляет набор расширенных инструкций и руководств, которые можно использовать для оценки и определения того, соответствуют ли реализованные планы требованиям ИСО 28000 и серии стандартов ИСО 28004 и достаточны ли они для защиты цепи поставок грузов, находящихся под контролем порта.

4.2 Процесс оценки плана управления безопасностью и процедуры

Заинтересованная сторона среднего и малого морского порта должна разработать и поддерживать комплексный план управления безопасностью и документы, включающие процедуры для обеспечения целостности цепи поставок. План управления следует периодически проверять и оценивать для того, чтобы внедренные процедуры безопасности были достаточными для защиты цепи поставок от идентифицированных угроз и рисков для операций морского порта. Планы защиты безопасности следует оценивать по набору показателей результативности (KPI), чтобы определить полноту, качество и эффективность разработанного плана заинтересованной стороны морского порта в соответствии с требованиями, указанными в ИСО 28000. Оценка также будет включать соответствие следующим документам:

- WCO SAFE «Рамочные стандарты по безопасности»;
- «Таможенно-торговое партнерство США против терроризма» (C-TPAT);
- Правила уполномоченного экономического оператора (AEO).

4.3 Критерии для оценки соответствия

Следующие установленные показатели результативности деятельности (KPI) в качестве критериев следует использовать для измерения качества и эффективности плана управления безопасностью для защиты целостности цепи поставок от идентифицированных угроз и рисков для операций морского порта. Показатели результативности деятельности включают эксплуатационную готовность (планы действий, готовность персонала и возможности систем) порта к обнаружению, защите и реагированию на типы угроз/риска, определенные в девяти возможных типах инцидентов. В частности, критерии оценки позволяют оценить качество оперативных планов, готовность персонала и эффективность автоматизированных систем безопасности для защиты груза, находящегося в порту и под непосредственным контролем организации морского порта. Планы управления безопасностью должны быть оценены для каждой из девяти областей риска, чтобы определить, насколько правильно и точно разработан план,

идентифицированы и учтены угрозы, риски, меры по минимизации последствий и этапы восстановления для защиты цепи поставок.

Оценка показателей и тщательный анализ плана управления безопасностью направлены на следующее:

- актуальны ли методы предупреждения проблем с безопасностью, возможности персонала, планы обеспечения непрерывности COOP и проектный анализ DR в отношении выявленных угроз и рисков для операций морского порта?
- выявили ли заинтересованные стороны и уполномоченные организации все возможные угрозы и риски для операций, охватывающих девять областей риска?
- являются ли выявленные угрозы и риски актуальными в отношении меняющихся глобальных угроз и рисков для цепи поставок?
- доскональность плана по устранению каждого из выявленных потенциальных рисков и угроз для морского порта, включая список инцидентов и чрезвычайных ситуаций, которые произошли в морском порту в исторической ретроспективе;
- идентификацию ответственного(ых) лица (лиц) и вертикали управления для реагирования на конкретные угрозы, риски, чрезвычайные ситуации и инциденты;
- верификацию работы оборудования для обеспечения безопасности и верификацию планов обслуживания для обеспечения непрерывности услуг;
- наличие необходимой информации во время чрезвычайной ситуации, например чертежи компоновки предприятия, данные о безопасности и особые процедуры реагирования для защиты цепи поставок груза;
- планы и процедуры реагирования, которые должны выполняться внутренними и внешними заинтересованными сторонами и любым внешним персоналом, находящимся на территории, включая процедуры эвакуации;
- оценку эффективности работы сотрудников службы безопасности морского порта по процедурам распознавания, защиты и реализации плана управления безопасностью для защиты цепи поставок, включая ответственность, полномочия и обязанности персонала с конкретными ролями в ходе чрезвычайной ситуации (например, сотрудники охраны, пожарные, сотрудники скорой помощи, специалисты по радиологической утечке/токсическому загрязнению);
- доскональность процедуры, описывающей, как меры безопасности и условия безопасности восстанавливаются в краткосрочной и среднесрочной перспективе, проверяются и сертифицируются для правильной работы;
- идентификацию, расположение и защиту материального обеспечения, записей, данных и оборудования, а также какие действия необходимы для защиты критических предметов во время чрезвычайной ситуации;
- определение, есть ли в наличии на местах определенные процедуры, роли и обязанности для взаимодействия со службами экстренной помощи и службами быстрого реагирования;
- эффективность процедур обмена информацией с заинтересованными сторонами, организациями и учреждениями, принимающими решения сообщать, давать и получать необходимые разрешения и рекомендации для реагирования на чрезвычайные ситуации;
- полноту планов восстановления после инцидента для возобновления операций порта с конкретными пошаговыми процедурами восстановления, требованиями к ресурсам и расчетными временными рамками для восстановления систем безопасности порта до полного рабочего состояния.

В дополнение, план управления безопасностью оценивается на предмет участия внешних уполномоченных организаций в планировании и реагировании на чрезвычайные ситуации, чтобы убедиться, что их роли и обязанности четко задокументированы и адекватны для поддержки диапазона угроз и рисков работы морского порта.

4.4 Использование ИСО 20858 для процедур оценки и определения безопасности

ИСО 20858 предоставляет руководство и инструкции по определению, которые могут быть использованы операторами порта для оценки способности их плана управления безопасностью порта защищать целостность цепи поставок. В ИСО 20858 (раздел 4) содержится руководство по подтверждению необходимых знаний, которые требуются персоналу для оценки планов управления безопасностью, чек-листа для оценки планов и сценариев возможных угроз и инцидентов безопасности, которые могут повлиять на работу порта. В частности, в ИСО 20858 (подраздел 4.3) приведена подробная

таблица, содержащая более чем 128 факторов оценки состояния безопасности портов, которые можно использовать для оценки соответствия, возможностей, эффективности и готовности планов управления безопасностью порта к защите груза, находящегося под непосредственным контролем порта. В ИСО 20858 (подраздел 4.4) приведен список возможных сценариев угроз и сценариев безопасности, относящихся к элементам девяти областей риска (см. 2.4.5). Для всего, что находится под непосредственным управлением портов, как указано в ИСО 20858 (подраздел 4.2), и для настоящего стандарта следует включить следующее:

- все средства портов, морские, железнодорожные и наземные операции, которые проводятся в пределах физических границ портового сооружения;
- судоходные, наземные и железнодорожные транспортные каналы, используемые для приближения к объектам порта;
- области, непосредственно связанные с портовыми сооружениями, которые находятся за пределами установленного периметра безопасности;
- услуги по поставке, хранению и складированию грузов, используемые для укладки или обработки груза до/во время/после морской перевозки в пределах портовой инфраструктуры;
- средства для проверки, мониторинга, контроля, доступа к данным и документации по грузу для морских, железнодорожных и наземных перевозок обрабатываются, охраняются и доступны в пределах портовой инфраструктуры.

Область применения данной оценки распространяется на все портовые эксплуатационные и инфраструктурные объекты, погрузочные доки, зоны хранения, автоматизированные и физические системы контроля и защиты, а также железнодорожные, наземные и судовые транспортные системы.

4.5 Рейтинговая система оценки плана управления безопасностью

План управления безопасностью средних и малых морских портов должен пройти оценку для определения уровня его соответствия требованиям обеспечения безопасности, указанным в ИСО 28000. Процесс оценки направлен на качество плана управления безопасностью морского порта и обеспечение защиты цепи поставок груза от выявленных операционных рисков и угроз для морского порта. Критерии оценки для определения способности планов защитить безопасность и непрерывную работу цепи поставок представлены в таблице 2. Пятиуровневая рейтинговая система начинается с уровня 1 «Неприемлемый» и заканчивается уровнем 5 «Исключительный». Номер рейтинга присваивается для обозначения оцененной уязвимости и вероятности того, что план управления безопасностью достаточен для защиты целостности цепи поставок.

Таблица 2 — Критерии оценки для плана управления безопасностью

Уровень 1	**Неприемлемый** Высокая вероятность, что план системы управления порта не предоставляет адекватные условия для обеспечения бесперебойного потока грузов через морской порт. В плане не учтены все выявленные зоны риска и угрозы, которые оказывают влияние на цепь поставок грузов, поступающих в порт, уязвимые для сбоев и нарушений безопасности. План управления безопасностью не имеет достаточной детализации для определения шагов по предупреждению, минимизации последствий и восстановлению после бедствий, необходимых для защиты цепи поставок и обеспечения непрерывности деятельности (операций)
Уровень 2	**Предельный** Средняя или высокая вероятность того, что непрерывность деятельности (операций) и безопасность цепи поставок могут быть нарушены для идентифицированных областей риска и угроз, положений о предупреждении и восстановлении, которые отражены в плане управления безопасностью порта. План управления безопасностью охватывает некоторые, но не все выявленные области риска и угроз. План показывает взаимную компенсацию силы и слабости с акцентом на слабость, которая потенциально может включать непрерывность и безопасность цепи поставок. В плане недостаточно подробно рассматриваются этапы предупреждения, минимизации последствий и восстановления после бедствия для защиты цепи поставок и обеспечения непрерывности деятельности/операций

Окончание таблицы 2

Уровень 3	**Приемлемый** Низкая или средняя вероятность того, что непрерывность деятельности/операций и безопасность цепи поставок могут быть нарушены выявленными зонами риска и угроз на основе положений о предупреждении и восстановлении, рассмотренных в порту и отраженных в плане управления безопасностью. Управление безопасностью охватывает все идентифицированные области риска и угроз и включает документированные процедуры предупреждения, минимизации последствий и восстановления после бедствия, которые имеют больше преимуществ, которые могут оказать воздействие на безопасность и поток товаров через морской порт, чем недостатков
Уровень 4	**Выдающийся** Средняя или высокая вероятность того, что непрерывная работа и безопасность цепи поставок могут быть поставлены под угрозу в выявленных областях риска и угроз на основе положений о предотвращении и восстановлении, указанных в плане управления безопасностью порта. Управление безопасностью охватывает все идентифицированные области риска безопасности и имеет шаги по предотвращению, смягчению последствий и аварийному восстановлению, которые демонстрируют больше преимуществ (сильных сторон), чем недостатков (слабых сторон), которые могут повлиять на безопасность и поток товаров через морской порт
Уровень 5	**Исключительный** Средняя или высокая вероятность того, что непрерывность деятельности/операций и безопасность цепочки поставок могут быть поставлены под угрозу в выявленных областях риска и угроз на основе положений о предотвращении и восстановлении, указанных в плане управления безопасностью порта. Управление безопасностью охватывает все выявленные зоны риска для безопасности и имеет шаги по предотвращению, минимизации последствий и восстановлению после бедствий, которые демонстрируют больше преимуществ (сильных сторон), чем недостатков (слабых сторон), которые могут повлиять на безопасность и поток товаров через морской порт

Библиография

[1] ISO 20858, Ships and marine technology — Maritime port facility security assessments and security plan development (Суда и морские технологии. Оценка охраны и разработка планов охраны портовых средств)[1)]

[2] ISO 28000, Specification for security management systems for the supply chain (Система менеджмента безопасности цепи поставок)[2)]

[3] ISO 28001, Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance (Система менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности цепи поставок. Оценки и планы)[3)]

[4] ISO 28002, Security management systems for the supply chain — Development of Resilience in the supply chain — Requirements with guidance for use (Системы менеджмента безопасности для цепи поставок. Развитие устойчивости в цепи поставок. Требования и руководство по применению)[4)]

[5] ISO 28003, Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems (Системы менеджмента безопасности для цепи поставок. Требования к органам, проводящим аудит и сертификацию системы менеджмента безопасности цепи поставок)[4)]

[6] ISO 28004-1, 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 ISO 28000. Часть 1. Основные принципы)[4)]

[1)] В Российской Федерации действует ГОСТ Р 53660—2009 (ИСО 20858:2004) «Суда и морские технологии. Оценка охраны и разработка планов охраны портовых средств».

[2)] В Российской Федерации действует ГОСТ Р 53663—2009 (ИСО 28000:2005) «Система менеджмента безопасности цепи поставок. Требования».

[3)] В Российской Федерации действует ГОСТ Р 53662—2009 (ИСО 28001:2005) «Система менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности цепи поставок. Оценки и планы».

[4)] Официальный перевод этого стандарта находится в Федеральном информационном фонде стандартов.

УДК 656.614.3.004:006.354 ОКС 03.100.01

Ключевые слова: система менеджмента, безопасность, цепь поставок, руководство, внедрение, применение, использование, оператор, морской порт, средний и малый порты

БЗ 5—2020

Редактор *Л.И. Нахимова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 26.03.2020. Подписано в печать 05.05.2020. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,93.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11
gost.e-ecolog.ru gost.e-ecolog.ru
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