МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO 28004

Первое издание
2007-10-15

Системы менеджмента безопасности цепи поставок. Руководство по внедрению ISO 28000

Security management systems for the supply chain – Guidelines for the implementation of ISO 28000

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

Ссылочный номер
ISO 28004:2007(R)

Отказ от ответственности при работе в PDF

Настоящий файл PDF может содержать интегрированные шрифты. В соответствии с условиями лицензирования, принятыми фирмой Adobe, этот файл можно распечатать или вывести на экран, но его нельзя изменить, пока не будет получена лицензия на загрузку интегрированных шрифтов в компьютер, на котором ведется редактирование. В случае загрузки настоящего файла заинтересованные стороны принимают на себя ответственность за соблюдение лицензионных условий фирмы Adobe. Центральный секретариат ISO не несет никакой ответственности в этом отношении.

Adobe – торговый знак фирмы Adobe Systems Incorporated.

Подробности, относящиеся к программным продуктам, использованным для создания настоящего файла PDF, можно найти в рубрике General Info файла; параметры создания PDF были оптимизированы для печати. Были приняты во внимание все меры предосторожности с тем, чтобы обеспечить пригодность настоящего файла для использования комитетами-членами ISO. В редких случаях возникновения проблемы, связанной со сказанным выше, просьба проинформировать Центральный секретариат по адресу, приведенному ниже.

ДОКУМЕНТ ЗАЩИЩЕН АВТОРСКИМ ПРАВОМ

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

Опубликовано в Швейцарии

Содержание

Страница

Предисловие

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

Проекты международных стандартов разрабатываются в соответствии с правилами, установленными в Директивах ISO/IEC, Часть 2.

Основная задача технических комитетов заключается в подготовке международных стандартов. Проекты международных стандартов, принятые техническими комитетами, рассылаются комитетам-членам на голосование. Их опубликование в качестве международных стандартов требует одобрения не менее 75 % комитетов-членов, принимающих участие в голосовании.

Следует иметь в виду, что некоторые элементы настоящего документа могут быть объектом патентного права. ISO не может нести ответственность за идентификацию какого-либо одного или всех патентных прав.

ISO 28004 был подготовлен Техническим комитетом ISO/TC 8, *Суда и морские технологии,* в сотрудничестве с другими техническими комитетами, ответственными за конкретные элементы цепи поставок.

Настоящее первое издание ISO 28004 прекращает действие и замещает ISO/PAS 28004:2006, который был технически пересмотрен.

Введение

ISO 28000:2007, *Системы менеджмента безопасности цепи поставок. Технические условия* и настоящий международный стандарт были разработаны в ответ на потребность в стандарте по системе менеджмента цепи поставок, позволяющего организациям оценить и сертифицировать их системы менеджмента безопасности, а также как руководство по внедрению такого стандарта.

ISO 28000 совместим со стандартами по системам менеджмента ISO 9001:2000 (менеджмент качества) и ISO 14001:2004 (экологический менеджмент). Эти стандарты облегчают объединение систем менеджмента качества, экологического менеджмента и менеджмента цепи поставок, если организации ставят перед собой такую задачу.

В начале каждого раздела/подраздела настоящего международного стандарта приводится текст в рамках, устанавливающий полные требования, взятые из международного стандарта ISO 28000, после которого следуют соответствующие руководящие указания. Нумерация разделов настоящего международного стандарта соответствует нумерации разделов международного стандарта ISO 28000.

Настоящий международный стандарт должен пересматриваться или в него должны вноситься поправки, если это признано необходимым. Пересмотр настоящего документа должен проводиться при пересмотре ISO 28000.

Настоящий международный стандарт не ставит своей целью включение всех положений контракта между операторами цепи поставок, поставщиками и заинтересованными сторонами. Пользователи несут ответственность за его правильное применение.

Соответствие настоящему международному стандарту само по себе не освобождает от правовых обязательств.

Системы менеджмента безопасности цепи поставок. Руководство по внедрению ISO 28000

1 Область применения

Настоящий международный стандарт содержит общие рекомендации по применению ISO 28000:2007, *Системы менеджмента безопасности цепи поставок. Технические условия.*

В нем разъясняются основополагающие принципы ISO 28000 и описываются цели, типичные входные данные, процессы и типичные результаты для каждого требования ISO 28000. Это поможет пониманию и внедрению ISO 28000.

В настоящем документе не вводятся дополнительные требования по сравнению с требованиями, установленными в международном стандарте ISO 28000, а также не устанавливаются обязательные подходы к внедрению ISO 28000.

ISO 28000

1 Область применения

Настоящий международный стандарт устанавливает требования к системе менеджмента безопасности, включая аспекты, являющиеся критическими для обеспечения безопасности цепи поставок. Эти аспекты включают, но не ограничиваются этим, финансирование, обработку, управление информацией, а также средства для упаковки, хранения и перемещения грузов от одного вида транспорта к другому и от одного места положения к другому. Менеджмент безопасности связан со многими другими аспектами управления бизнесом. Эти другие аспекты должны рассматриваться непосредственно там и тогда, где и когда они оказывают влияние на менеджмент безопасности, включая транспортировку этих товаров в цепи поставок.

Настоящий международный стандарт применим к организациям всех размеров, начиная от небольших организаций и кончая многонациональными, занимающимся изготовлением, предоставлением услуг, хранением или транспортировкой на любом этапе производства или цепи поставок, которые хотят:

a) разработать, внедрить, поддерживать и совершенствовать систему менеджмента безопасности;

b) обеспечить соответствие проводимой политике в области менеджмента безопасности;

c) демонстрировать такое соответствие другим;

d) добиться сертификации/регистрации системы менеджмента безопасности аккредитованным органом сертификации третьей стороны; или

e) самостоятельно определять или декларировать соответствие настоящему международному стандарту.

Существуют законодательные и регулирующие нормы, отраженные в некоторых требованиях настоящего международного стандарта.

Настоящий международный стандарт не требует дублирующих доказательств соответствия.

Организации, выбирающие сертификацию третьей стороной, в дальнейшем могут подтвердить, что они внесли существенный вклад в безопасность цепи поставок.

2 Нормативные ссылки

Нормативные ссылки отсутствуют. Данный раздел включен для сохранения нумерации разделов, аналогичной нумерации ISO 28000.

3 Термины и определения

ISO 28000

3 Термины и определения

3.1
средства
facility
предприятие, машины, имущество, здания, транспортные средства, суда, оборудование портов и другие объекты инфраструктуры или предприятия и связанные системы, которые выполняют определенные и количественно оцениваемые деловые функции или услуги

ПРИМЕЧАНИЕ Данное определение включает системную программу, которая является необходимой для достижения безопасности и применения менеджмента безопасности.

3.2
безопасность
security
противодействие умышленным несанкционированным действиям, наносящим повреждения или ущерб цепи поставок или со стороны цепи поставок

3.3
менеджмент безопасности
security management
систематические и координированные действия и инструкции, посредством которых организация оптимально управляет своими рисками и связанными возможными угрозами и воздействиями

3.4
цели менеджмента безопасности
security management objective
конкретные результаты или достижения, необходимые для обеспечения безопасности, для соответствия политике в области менеджмента безопасности

ПРИМЕЧАНИЕ Важно, чтобы такие результаты были непосредственно или косвенно связаны с продукцией, доставкой или услугами, предоставляемыми бизнесом потребителям или конечным пользователям.

3.5
политика в области обеспечения безопасности
security management police
общие намерения и направление деятельности организации, относящиеся к обеспечению безопасности, и основа для управления процессами и действиями, связанными с обеспечением безопасности, вытекающими из политики организации и обязательных требований и согласующихся с ними

3.6
программы менеджмента безопасности
security management programmes
средства, с помощью которых достигается цель менеджмента безопасности

3.7
задача менеджмента безопасности
security management target
конкретный уровень исполнения, необходимый для достижения цели менеджмента безопасности

3.8
заинтересованная сторона
stakeholder
лицо или экономический субъект, имеющие законный интерес к работе, достижениям или результатам деятельности организации

ПРИМЕЧАНИЕ Примеры включают потребителей, акционеров, финансистов, страховщиков, сотрудников регулятивных органов, органы, учрежденные статутом, наемных сотрудников, подрядчиков, поставщиков, трудовые организации или общества.

3.9
цепь поставок
supply chain
связанный набор ресурсов и процессов, который начинается с получения сырья и продолжается до поставки продукции или услуг разными видами транспорта конечному потребителю

ПРИМЕЧАНИЕ Цепь поставок может включать поставщиков, производственные мощности, логистов, внутренние центры распределения, дистрибьюторов, оптовиков и другие организации, связанные с конечным потребителем.

3.9.1
последующие действия
downstream
относятся к действиям, процессам и перемещениям грузов в цепи поставок после того, как они выходят из-под прямого оперативного контроля организации, включая страхование, финансирование, управление данными, а также упаковку, хранение и транспортировку грузов, но не ограничиваясь этим

3.9.2
предшествующие действия
upstream
относятся к действиям, процессам и перемещениям грузов в цепи поставок перед тем, как они попадают под прямой оперативный контроль организации, включая страхование, финансирование, управление данными, а также упаковку, хранение и транспортировку грузов, но не ограничиваясь этим

3.10
высшее руководство
top management
лицо или группа лиц, руководящих организацией и контролирующих ее на высшем уровне

ПРИМЕЧАНИЕ Высшее руководство, особенно, крупной многонациональной организации, персонально может не заниматься деятельностью, описанной в настоящем стандарте, но реализовывать ее через свои распоряжения.

3.11
постоянное совершенствование
continual improvement
постоянный процесс совершенствования системы менеджмента безопасности для улучшения общих характеристик безопасности в соответствии с политикой организации в этой области

Для целей настоящего документа используются термины и определения, установленные в ISO 28000, а также следующие термины и определения.

3.1
риск
risk
правдоподобие реализации угрозы безопасности и её последствия

3.2
подтверждение надежности при приеме на работу, связанную с секретностью
security cleared
процесс проверки надежности лиц для получения доступа к секретным материалам по безопасности

3.3
угроза
threat
любое возможное преднамеренное действие или серия действий с возможным нанесением ущерба заинтересованным сторонам, средствам, операциям, цепи поставок, обществу, экономике или непрерывности и целостности бизнеса

4 Элементы системы менеджмента безопасности

Рисунок 1 – Элементы системы менеджмента безопасности

4.1 Общие требования

a) Требования ISO 28000

Организация должна разработать, документально оформить, внедрить, поддерживать и постоянно совершенствовать эффективную систему менеджмента безопасности для идентификации угроз безопасности, оценки рисков, а также для контроля и смягчения их последствий. Организация должна постоянно повышать свою эффективность в соответствии с требованиями, установленными в Разделе 4. Организация должна определить область применения системы менеджмента безопасности. Если организация привлекает стороннюю организацию для выполнения какого-либо процесса, влияющего на соответствие этим требованиям, то она должна обеспечить управление такими процессами. Необходимое управление и ответственность за такие процессы, выполняемые сторонней организацией, должны идентифицироваться в системе менеджмента безопасности.

b) Цель

Организация должна разработать и поддерживать систему менеджмента, соответствующую всем требованиям документа ISO 28000. Это может помочь организации отвечать всем правилам, требованиям и законам, касающимся обеспечения безопасности.

Уровень детализации и сложности системы менеджмента безопасности, объем документации и её ресурсы зависят от размеров и сложности организации, а также от характера её деятельности.

Организация обладает свободой и гибкостью при определении своих границ и может внедрить документ ISO 28000 во всей организации, или в конкретных рабочих подразделениях, или для конкретной деятельности.

При определении границ и области применения системы менеджмента безопасности следует принимать меры предосторожности. Организации не должны пытаться ограничить свои области применения с тем, чтобы исключить оценку тех операций или деятельности, которые необходимы для работы организации в полном объеме или тех, которые могут влиять на безопасность сотрудников и других заинтересованных сторон.

Если ISO 28000 внедряется для конкретного рабочего подразделения или для конкретной деятельности, политика и процедуры в области обеспечения безопасности, разработанные другими подразделениями организации, могут быть использованы отдельным рабочим подразделением или для конкретной деятельности для помощи в выполнении требований указанного документа. Это может потребовать небольшого пересмотра политики и процедур в области обеспечения безопасности или внесения в них поправок, для того, чтобы они могли быть применены в отдельном рабочем подразделении или для конкретной деятельности.

c) Типичные входные данные

Все требования, предъявляемые к входным данным, установлены в ISO 28000.

d) Типичный результат

Типичным результатом является эффективно внедренная и поддерживаемая система менеджмента безопасности, помогающая организации в постоянном поиске усовершенствований.

4.2 Политика в области менеджмента безопасности

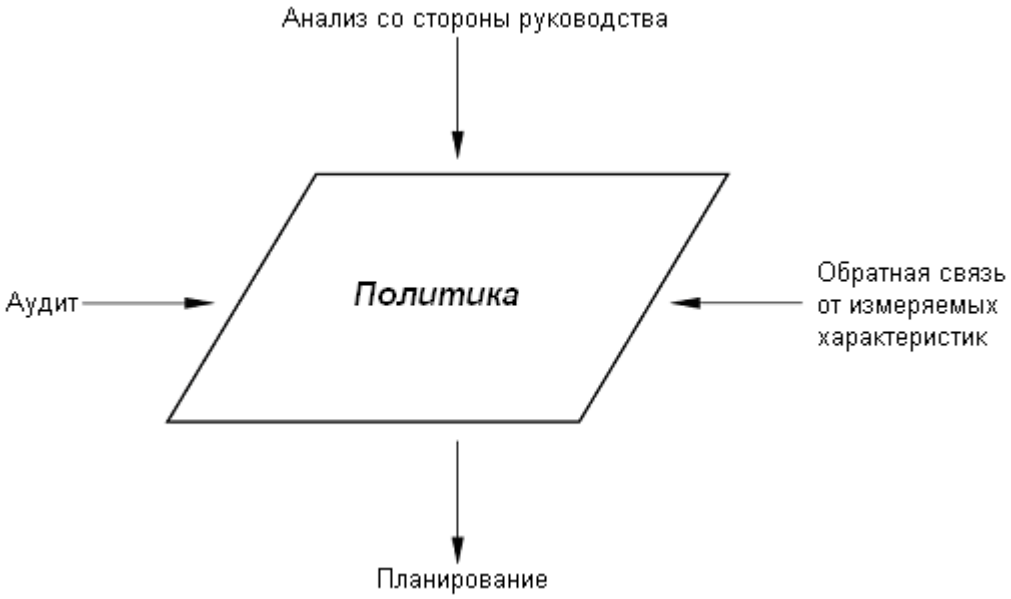

Рисунок 2 Политика в области менеджмента безопасности

a) Требование ISO 28000

Высшее руководство организации должно утверждать общую политику в области менеджмента безопасности.

Политика должна:

a) согласовываться с политикой организации в других областях;

b) создавать основу, позволяющую выполнить конкретные цели, задачи и программы в области менеджмента безопасности;

c) согласовываться с общей организационной структурой менеджмента угроз и рисков безопасности;

d) соответствовать угрозам для организации, а также характеру и масштабу её деятельности;

e) четко определять общие/основные цели менеджмента безопасности;

f) включать обязательство по постоянному совершенствованию менеджмента безопасности;

g) включать обязательство по обеспечению соответствия действующему законодательству, обязательным и законным требованиям, а также другим требованиям, под которыми организация ставит свою подпись;

h) быть одобрена высшим руководством;

i) документально оформляться, внедряться и поддерживаться

j) сообщаться всем вовлеченным сотрудникам и третьим сторонам, включая подрядчиков и посетителей, с тем, чтобы эти лица соблюдали свои обязательства, связанные с менеджментом безопасности;

k) быть доступной для заинтересованных сторон, если это необходимо;

l) предусматривать её пересмотр в случае приобретения других организаций, или слияния с ними, или других изменений в сфере деятельности организации, которые могут повлиять на целостность или соответствие системы менеджмента безопасности.

ПРИМЕЧАНИЕ Организации могут выбрать детальную политику в области менеджмента безопасности для внутреннего пользования, которая содержит достаточную информацию и указания по управлению системой менеджмента безопасности (части которой могут быть конфиденциальными), и имеет сводный (не конфиденциальный) вариант, содержащий основные цели, для распространения среди заинтересованных лиц и организаций.

b) Цель

Политика в области обеспечения безопасности является кратким изложением обязательств высшего руководства в этой области. Она устанавливает общие направления и принципы действия для организации. Указанная политика также устанавливает ответственность за обеспечение безопасности и характеристики безопасности, требуемые по всей организации.

Документально оформленная политика в области обеспечения безопасности должна разрабатываться и утверждаться высшим руководством организации.

c) Типичные входные данные

При разработке политики в области обеспечения безопасности руководство должно рассмотреть

следующие позиции, особенно в связи с цепью поставок организации:

- политика и цели, соответствующие деятельности организации в целом;
- исторические и текущие характеристики безопасности организации;
- потребности заинтересованных сторон;
- возможности и потребности постоянного совершенствования;
- необходимые ресурсы;
- участие сотрудников;
- участие подрядчиков, заинтересованных сторон и другого персонала, не работающего в организации.

d) Процесс

При разработке и утверждении политики в области обеспечения безопасности высшее руководство должно принимать во внимание вопросы, перечисленные ниже.

Эффективно сформулированная и представленная политика в области обеспечения безопасности должна:

1) соответствовать характеру и масштабу рисков организации, связанных с безопасностью;

Идентификация угроз, оценка рисков и управление рисками являются основой успешно функционирующей системы менеджмента безопасности и должны отражаться в политике организации в области безопасности.

Политика в области безопасности должна соответствовать представлению о будущем организации. Она должна быть реалистичной и не должна ни преувеличивать риски, с которыми сталкивается организация, ни преуменьшать их.

2) включать обязательство постоянного совершенствования;

Глобальные угрозы безопасности увеличивают давление на организацию в отношении снижения рисков происшествий в цепи поставок. В дополнение к необходимости соответствия правовым, национальным и регулирующим обязательствам и другим правилам и руководству таких организаций как например, Всемирная таможенная организация (WCO), организация должна поставить своей целью эффективное и результативное улучшение характеристик безопасности и совершенствование своей системы менеджмента безопасности, с тем, чтобы отвечать потребностям меняющейся мировой торговли, бизнеса и регулирования.

Планируемое улучшение характеристик должно отражаться в целях безопасности (см. 4.3.2) и осуществляться через программу менеджмента безопасности (см. 4.3.5), хотя положение о политике в этой области может включать широкую сферу деятельности.

3) включать обязательство, как минимум, соответствовать текущим применимым правилам в области безопасности, а также другим требованиям, под которыми стоит подпись организации;

Организации должны соответствовать применяемым обязательным требованиям в области безопасности. Обязательство в отношении политики в области безопасности является публичным подтверждением организации, что она должна соответствовать законодательству (не превышать его) или другим требованиям, либо предписанным законом, либо принятым добровольным подписанием, например, рамочным стандартам Всемирной таможенной организации.

ПРИМЕЧАНИЕ “Другие требования” могут означать, например, корпоративную или групповую политику, собственные стандарты организации, или технические требования или своды инструкций, под которыми стоит подпись организации.

4) документально оформляться, внедряться и поддерживаться;

Планирование и подготовка являются основой для успешного внедрения. Часто положения политики в области безопасности и цели безопасности являются нереалистичными, поскольку существуют неадекватные и несоответствующие ресурсы для их реализации. Перед тем, как делать какие-либо публичные заявления, организация должна гарантировать, что имеются в наличии любые необходимые финансы, практический опыт и ресурсы и что все цели безопасности реально достижимы в рамках этой политики.

Для того, чтобы политика в области безопасности была эффективной, она должна документально оформляться и периодически пересматриваться в отношении продолжающейся адекватности, а в случае необходимости исправляться и изменяться.

5) сообщаться всем сотрудникам с тем, чтобы они были осведомлены о своих персональных обязательствах в отношении безопасности;

Участие и обязательства сотрудников являются необходимыми для успешного обеспечения безопасности.

Сотрудники должны быть осведомлены о влиянии менеджмента безопасности на качество среды, в которой они работают, и должны поощряться за внесение ими вклада в менеджмент безопасности.

Маловероятно, что сотрудники (на всех уровнях, включая руководство) смогут внести эффективный вклад в менеджмент безопасности, если они не понимают политику организации и свои обязанности, а также не обладают соответствующей компетентностью для решения поставленных задач.

Это требует от организации ясного доведения политики и целей безопасности до своих сотрудников, чтобы они могли иметь основу для определения своего собственного вклада в обеспечение безопасности.

6) быть доступной для заинтересованных сторон;

Любое лицо или группа лиц (работающих в организации или вне организации), связанных с безопасностью организации или испытывающих ее влияние, должны быть особенно заинтересованы в заявлении о политике организации в области безопасности. Поэтому должен существовать процесс информирования их об этой политике. В случае необходимости такой процесс должен обеспечивать получение заинтересованными сторонами указанной информации.

7) должна периодически пересматриваться, чтобы обеспечить сохранение ее значимости и соответствия для организации.

Изменения неизбежны, правила и законодательство развиваются, а ожидания заинтересованных сторон возрастают. Поэтому политика организации в области безопасности и система менеджмента нуждаются в регулярном пересмотре для обеспечения постоянного соответствия и эффективности.

Если вносятся изменения, то о них необходимо сообщить по возможности как можно скорее.

e) Типичный результат

Типичным результатом является всесторонняя, лаконичная и понятная политика в области безопасности, которая сообщается во всей организации, а также, при необходимости, заинтересованным сторонам.