
**Системы менеджмента безопасности
цепи поставок. Наилучшие методы
обеспечения безопасности в цепи
поставок, оценки и планы. Требования
и руководящие указания**

iTeh STA *Security management systems for the supply chain – Best practices for
(standards.itih.ai) implementing supply chain security, assessments and plans –
Requirements and guidance*

ISO 28001:2007

<https://standards.itih.ai/catalog/standards/sist/a3764b6d-5ec3-49eb-825e-715f88045fb6/iso-28001-2007>

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



Ссылочный номер
ISO 28001:2007(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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 28001:2007

<https://standards.iteh.ai/catalog/standards/sist/a3764b6d-5ec3-49eb-825e-715f88045fb6/iso-28001-2007>



ДОКУМЕНТ ЗАЩИЩЕН АВТОРСКИМ ПРАВОМ

© ISO 2007

Все права сохраняются. Если не указано иное, никакую часть настоящей публикации нельзя копировать или использовать в какой-либо форме или каким-либо электронным или механическим способом, включая фотокопии и микрофильмы, без предварительного письменного согласия ISO по адресу, указанному ниже, или членом ISO в стране регистрации пребывания.

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

Опубликовано в Швейцарии

Содержание

Страница

Предисловие	iv
Введение	v
1 Область применения	1
2 Нормативные ссылки	1
3 Термины и определения	2
4 Область применения	6
4.1 Заявление о применении	6
4.2 Партнеры по бизнесу	6
4.3 Международные сертификаты одобрения	7
4.4 Партнеры по бизнесу, освобождаемые от декларации безопасности	7
4.5 Проверки системы безопасности партнеров по бизнесу	7
5 Процесс обеспечения безопасности цепи поставок	7
5.1 Общие положения	7
5.2 Определение области оценки безопасности	8
5.3 Проведение оценки безопасности	8
5.4 Разработка плана обеспечения безопасности цепи поставок	9
5.5 Выполнение плана обеспечения безопасности цепи поставок	9
5.6 Документация и мониторинг процесса безопасности цепи поставок	9
5.7 Действия, необходимые после происшествий с нарушением безопасности	10
5.8 Защита секретной информации	10
Приложение А (информативное) Процесс обеспечения безопасности цепи поставок	12
A.1 Общие положения	12
A.2 Определение области применения оценки безопасности	13
A.3 Проведение оценки безопасности	13
A.4 Разработка плана обеспечения безопасности	17
A.5 Выполнение плана обеспечения безопасности	19
A.6 Документация и мониторинг процесса обеспечения безопасности	19
A.7 Постоянное совершенствование	19
Приложение В (информативное) Методология для оценки риска для безопасности, и разработки контрмер	20
V.1 Общие положения	20
V.2 Шаг первый – Рассмотрение сценариев угроз	21
V.3 Шаг второй – Классификация последствий	24
V.4 Шаг третий – Классификация вероятности происшествий, связанных нарушением безопасности	25
V.5 Шаг четвертый – Градация происшествий, связанных с недостаточным обеспечением безопасности	26
V.6 Шаг пятый – Разработка контрмер	26
V.7 Шаг шестой – Осуществление контрмер	27
V.8 Шаг седьмой – Оценка контрмер	27
V.9 Шаг восьмой – Повторение процесса	27
V.10 Продолжение процесса	27
Приложение С (информативное) Руководство по получению консультаций и сертификации	28
C.1 Общие положения	28
C.2 Подтверждение соответствия стандарту ISO 28001 путем проведения аудита	28
C.3 Сертификация на ISO 28001 органами сертификации третьей стороны	28
Библиография	29

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 28001 был подготовлен Техническим комитетом ISO/TC 8, *Суда и морские технологии*, в сотрудничестве с другими техническими комитетами, ответственными за специфические элементы безопасности цепи поставок.

Первое издание ISO 28001 отменяет и заменяет ISO/PAS 28001, который был технически пересмотрен.

iteh STANDARD PREVIEW
(standards.iteh.ai)

[ISO 28001:2007](https://standards.iteh.ai/catalog/standards/sist/a3764b6d-5ec3-49eb-825e-715f88045fb6/iso-28001-2007)

<https://standards.iteh.ai/catalog/standards/sist/a3764b6d-5ec3-49eb-825e-715f88045fb6/iso-28001-2007>

Введение

Происшествия, связанные с недостаточным обеспечением безопасности в международных цепях поставок, представляют угрозу международной торговле и экономическому росту стран, занимающихся торговлей. Люди, товары, инфраструктура и оборудование, включая транспортные средства, нуждаются в защите от происшествий связанных с безопасностью и их разрушительного воздействия. Такая защита приносит пользу экономике и обществу в целом.

Международные цепи поставок являются весьма динамичными и включают множество организаций и партнеров по бизнесу. Настоящий международный стандарт учитывает эту сложность. Он позволяет отдельным организациям, работающим в цепи поставок, устанавливать свои требования в соответствии с конкретной бизнес моделью организации и её ролью и функцией в международной цепи поставок.

Настоящий международный стандарт позволяет организациям определить и документально оформить приемлемые уровни безопасности международных цепей поставок и их компонентов. Они дают возможность таким организациям на основе анализа рисков принимать более аргументированные решения по обеспечению безопасности в рассматриваемых международных цепях поставок.

Настоящий международный стандарт является комбинированным и предназначается для того, чтобы совместно с рамочными стандартами Всемирной таможенной организации (WCO) и в дополнение к ним обеспечить безопасность всемирной торговли и облегчить её. Он не стремится заменить или отменить программы обеспечения безопасности цепей поставок отдельных агентств и их требования к сертификации и валидации.

Настоящий международный стандарт поможет организациям в определении адекватных уровней безопасности той части (тех частей) международной цепи поставок, которой (которыми) они управляют. Он также является основой для определения или валидации уровня существующей безопасности в такой цепи (цепях) поставок организации внутренними или внешними аудиторами или теми правительственными агентствами, которые выбраны для проверки соответствия этому документу, как основание для приема в их программы обеспечения безопасности цепи поставок. Клиенты, партнеры по бизнесу, правительственные агентства и другие органы могут попросить организации, которые объявили о соответствии настоящему международному стандарту, провести аудит или валидацию для подтверждения такого соответствия. Правительственные агентства могут прийти к взаимному соглашению о признании валидаций, проведенных другими правительственными агентствами. Если аудит организации проводится третьей стороной, то организация должна рассмотреть возможность привлечения органа сертификации третьей стороны, аккредитованного компетентным органом, который является членом Международного форума аккредитования (IAF) (см. Приложение С).

Целью настоящего международного стандарта не является дублирование правительственных требований и стандартов, касающихся обеспечения безопасности цепи поставок в соответствии с рамочными стандартами WCO. Организации, которые уже были сертифицированы или валидированы взаимно признаваемыми правительствами, считаются соответствующими настоящему стандарту.

Результаты, полученные в настоящем документе, являются следующими.

Объявление области действия, определяющей границы цепи поставок, охватываемые планом обеспечения безопасности.

Оценка безопасности, которая документально обосновывает уязвимость цепи поставок для определения планов обеспечения безопасности, а также описывает последствия каждой из возможных сценариев угроз.

План обеспечения безопасности, который приводит меры по обеспечению безопасности,

ISO 28001:2007(R)

предпринимаемые на месте, по борьбе с угрозами безопасности, идентифицированными при проведении оценки безопасности.

Программа обучения, устанавливающая, как персонал службы безопасности должен обучаться, чтобы успешно выполнять свои обязанности.

Для оценки безопасности, необходимой для разработки плана обеспечения безопасности, организация, использующая настоящий международный стандарт должна

- идентифицировать возможные угрозы (сценарии угроз безопасности);
- определить, может ли персонал реагировать должным образом на сценарии угроз, установленных в результате оценки безопасности.

Такое определение производится путем анализа текущего состояния безопасности в цепи поставок. Основываясь на данных, полученных в результате проведения такого анализа, выносится профессиональное суждение о том, в какой мере цепь поставок остается уязвимой при реализации каждого плана действий по обеспечению безопасности.

Если считается, что цепь поставок остается неприемлемо уязвимой при сценарии возникновения угроз, организация должна разработать дополнительные процедуры или ввести оперативные изменения для снижения вероятности инцидентов и их последствий или обоих. Такие действия называются контрмерами. Основываясь на системе приоритетов, контрмеры должны вводиться в план действий по обеспечению безопасности для снижения угроз до приемлемого уровня.

Приложения А и В являются иллюстративными примерами управления рисками, основанного на процессах обеспечения безопасности, для защиты людей, активов и задач международной цепи поставок. Они облегчают применение как общего подхода для комплексных цепей поставок, так и/или более детальных методов для частей цепей поставок.

Указанные приложения также

- облегчают понимание, принятие и внедрение методологий, которые могут быть модифицированы организациями;
- содержат руководящие указания по основам менеджмента безопасности для постоянного совершенствования;
- помогают организациям управлять ресурсами и направлять их на существующие и возникающие риски для безопасности;
- описывают возможные средства для оценки рисков и ослабления угроз безопасности в цепи поставок, связанных с распределением сырья во время хранения, изготовлением и транспортировкой готовых изделий на рынок.

В Приложение С даются указания по получению рекомендаций и сертификации по этому международному стандарту, если организация, использующая его, выбирает к исполнению этот вариант.

Системы менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности в цепи поставок, оценки и планы. Требования и руководящие указания

1 Область применения

Настоящий документ включает требования и руководящие указания для организаций, работающих в международных цепях поставок, касающиеся

- разработки и внедрения процессов обеспечения безопасности в цепях поставок;
- определения и документирования минимального уровня безопасности в цепи (цепях) поставок или в сегменте цепи поставок;
- соответствия применяемым критериям уполномоченных экономических операторов, установленных далее в рамочных стандартах Всемирной таможенной организации, и соответствующим национальным программам по обеспечению безопасности цепи поставок.

ПРИМЕЧАНИЕ Только национальное таможенное управление может определять организации в качестве уполномоченных экономических операторов в соответствии с программой обеспечения безопасности в цепи поставок и требованиями, предъявляемыми к сертификации и валидации.

Кроме того, настоящий документ устанавливает требования к документации, которые позволяют провести верификацию.

Пользователи настоящего международного стандарта должны

- определить часть международной цепи поставок, для которой они установили систему обеспечения безопасности (см. 4.1);
- проводить оценку системы обеспечения безопасности этой части цепи поставок и разработать адекватные контрмеры;
- разработать и внедрить план обеспечения безопасности цепи поставок;
- обучить персонал, обеспечивающий безопасность, его служебным обязанностям.

2 Нормативные ссылки

Следующие ссылочные документы являются обязательными при применении данного документа. Для жестких ссылок применяется только цитированное издание документа. Для плавающих ссылок необходимо использовать самое последнее издание нормативного ссылочного документа (включая любые изменения).

ISO 20858:–¹, *Суда и морские технологии. Оценки безопасности оборудования морских портов и разработка плана обеспечения безопасности*

International Convention for the Safety of Life at Sea (SOLAS), 1974 с внесенными изменениями, International Maritime Organization

3 Термины и определения

В настоящем документе используются следующие термины и определения.

3.1 соответствующие правоохранительные органы и другие правительственные чиновники
appropriate law enforcement and other government officials
государственный и правоприменяющий персонал, под юрисдикцией которого находится международная цепь поставок или её часть

3.2 актив (активы)
asset(s)
предприятие, механизмы, собственность, здания, автомобили, суда, самолеты, транспортные средства и другие элементы инфраструктуры или предприятий и связанные системы, выполняющие отдельные количественно оцениваемые бизнес-функции или услуги

ПРИМЕЧАНИЕ Это определение включает информационную систему, необходимую для обеспечения безопасности и осуществления менеджмента безопасности.

3.3 уполномоченный экономический оператор
authorized economic operator
сторона, участвующая в международном движении товаров и выполняющая какую-либо функцию, утвержденная национальной таможенной администрацией или действующая по её поручению, в соответствии с рамочными стандартами Всемирной таможенной организации или равноценными стандартами по безопасности цепи поставок

ПРИМЕЧАНИЕ 1 Термин "Уполномоченный экономический оператор" определен в рамочных стандартах Всемирной таможенной организации.

ПРИМЕЧАНИЕ 2 В частности, Уполномоченными экономическими операторами могут быть изготовители, импортеры, экспортеры, брокеры, перевозчики, объединители, посредники, порты, аэропорты, операторы терминалов, интегрированные операторы, товарные склады и дистрибьюторы.

3.4 партнер по бизнесу
business partner
подрядчик, поставщик или организация, занимающаяся предоставлением услуг, с которыми организация заключает контракты с целью получения помощи при выполнении её функций, как **организации, работающей в цепи поставок (3.15)**

3.5 грузовые транспортные средства
cargo transport unit
грузовой автомобиль, железнодорожный грузовой вагон, грузовой контейнер, автоцистерна, железнодорожная цистерна или передвижная цистерна

¹ Будет опубликован. Пересмотр ISO/PAS 20858:2004.

3.6**последствие
consequence**

возможные потери в людях, ущерб, причиненный собственности, или экономический ущерб, включая разрушение транспортных систем, вызванные атакой на организацию, работающую в цепи поставок, или вследствие использования цепи поставок как оружия

3.7**средство транспортировки
conveyance**

физические средства международной торговли, используемые для перевозки товаров из одного места в другое

ПРИМЕРЫ Коробка, поддон, грузовое транспортное средство, оборудование для погрузки и разгрузки грузов, грузовик, судно, самолет и железнодорожный вагон.

3.8**контрмеры
countermeasures**

действия, предпринимаемые для снижения вероятности сценария угроз безопасности, которые могут возникать при выполнении поставленных целей, или для сокращения возможных последствий

3.9**охрана
custody**

промежуток времени, в течение которого организация, работающая в цепи поставок, непосредственно контролирует изготовление, обработку, погрузочно-разгрузочные работы и транспортировку товаров, а также информацию, связанную с их доставкой в цепи поставок

3.10**последующие действия
downstream**

такие действия как погрузочно-разгрузочные работы, обработка и движение товаров после того, как они выходят из-под контроля организации в цепи поставок

3.11**товары
goods**

изделия, которые после размещения заказа на покупку изготавливаются, обрабатываются, погружаются-разгружаются и транспортируются в цепи поставок для использования и потребления покупателем

3.12**международная цепь поставок
international supply chain**

цепь поставок, которая в определенном месте пересекает международную или экономическую границу

ПРИМЕЧАНИЕ 1 Все части указанной цепи считаются международными с момента заключения заказа до момента когда товары проходят таможенный контроль в стране или экономической зоне назначения.

ПРИМЕЧАНИЕ 2 Если договоры или региональные соглашения исключают таможенную очистку товаров из установленных стран или экономических зон, окончанием международной цепи поставок является порт страны или экономической зоны назначения, где товары должны проходить таможенную очистку, если соглашения или договоры не были заключены на месте.

3.13

вероятность likelihood

легкость или трудности, с которыми сценарий угроз безопасности может развиваться с переходом в происшествие, связанное с недостаточным обеспечением безопасности

ПРИМЕЧАНИЕ Вероятность оценивается на основе противодействия процесса обеспечения безопасности происшествию, включая проверку сценария угроз и либо количественную, либо качественную оценку.

3.14

система менеджмента management system

структура организации для управления её процессами или действиями, которые превращают привлекаемые ресурсы в изделия или услуги в соответствии с целями организации

ПРИМЕЧАНИЕ Целью настоящего документа не является создание специальной системы менеджмента и/или отдельной системы менеджмента безопасности. Примерами систем менеджмента являются ISO 9001 (Системы менеджмента качества), ISO 14001 (Системы экологического менеджмента), ISO 28000 (Системы менеджмента безопасности цепи поставок), и система Международного менеджмента безопасности (ISM) Международной морской организации.

3.15

организация, участвующая в цепи поставок organization in the supply chain

любая организация, которая

- изготавливает, перегружает, обрабатывает, загружает, объединяет, отгружает или принимает товары после размещения заказа на поставку, которые в определенном месте пересекают международную или экономическую границу;
- транспортирует товары любым способом в международной цепи поставок независимо от того, пересекает ли её сегмент цепи поставок национальную (или экономическую) границу; или
- обеспечивает, управляет или предоставляет, распределяет или передает информацию по поставкам, используемую таможенными агентствами или в практике деловых отношений.

3.16

менеджмент рисков risk management

процесс принятия решений по менеджменту, основанных на анализе возможных угроз, их последствий, вероятности их успеха

ПРИМЕЧАНИЕ Процесс менеджмента рисков обычно инициируется для оптимизации распределения ресурсов организации, необходимых для работы в конкретной обстановке.

3.17

область применения услуг scope of service

функция (функции), которую (которые) выполняет организация, участвующая в цепи поставок, а также где она выполняет эту функцию (эти функции)

3.18

декларация безопасности security declaration

документированные обязательства партнера по бизнесу, определяющие меры по обеспечению безопасности, осуществляемые им, включая, как минимум, защиту товаров и физических средств международной торговли, защиту соответствующей информации, а также демонстрацию и проверку мер по обеспечению безопасности

ПРИМЕЧАНИЕ Эта декларация может использоваться организацией, участвующей в цепи поставок, для оценивания адекватности мер по обеспечению безопасности, касающихся безопасности товаров.

3.19

план обеспечения безопасности security plan

планируемые мероприятия, обеспечивающие адекватный менеджмент безопасности

ПРИМЕЧАНИЕ 1 Данный план должен обеспечивать применение мер, защищающих организацию от происшествий, связанных с недостаточным обеспечением безопасности.

ПРИМЕЧАНИЕ 2 Этот план может входить в другие планы деятельности.

3.20

безопасность security

противодействие умышленным действиям, целью которых является нанесение вреда или повреждений самой цепи поставок или связанных с нею

3.21

происшествие, связанное с нарушением безопасности security incident

любое действие или событие, создающее последствия (3.6)

3.22

персонал, обеспечивающий безопасность security personnel

люди в организации, работающей в цепи поставок, на которых возложены соответствующие обязанности по обеспечению безопасности

ПРИМЕЧАНИЕ Эти люди могут быть сотрудниками организации, а могут и не быть ими.

3.23

секретная информация; секретные материалы security sensitive information; security sensitive materials

информация или материалы, создаваемые или входящие в процесс обеспечения безопасности цепи поставок, содержащие информацию о процессе обеспечения безопасности, поставкам или правительственным директивам, которая недоступна для общественности и может оказаться полезной для людей, желающих инициировать происшествие, связанное с нарушением безопасности

3.24

цепь поставок supply chain

связанный комплекс ресурсов и процессов, которые при размещении заказа на поставку начинаются с получения сырья, после чего следует изготовление, обработка, погрузочно-разгрузочные работы и доставка товаров и соответствующих услуг покупателю

ПРИМЕЧАНИЕ Цепь поставок может включать поставщиков, производственные помещения, поставщиков материально-технического снабжения, внутренние центры распределения, дистрибьюторов, оптовиков и другие организации, участвующие в изготовлении, обработке, погрузке-разгрузке и доставке товаров и соответствующих услуг.

3.25

объект цели target

персонал, транспортные средства, товары, физические активы, процессы изготовления и обработка, системы контроля или документации в организации, участвующей в цепи поставок

3.26
сценарий угроз
threat scenario

происшествия, которые могут произойти вследствие недостаточного обеспечения безопасности

3.27
предшествующие действия
upstream

такие действия, как обработка, процессы и движение товаров, выполняемые до того, как они переходят под контроль организации, участвующей в цепи поставок

3.28
Всемирная таможенная организация
World Customs Organization
WCO

независимый межправительственный орган, задачей которого является повышение результативности и эффективности работы таможенных администраций

ПРИМЕЧАНИЕ Этот орган является межправительственной всемирной организацией, занимающейся только таможенными вопросами.

4 Область применения

4.1 Заявление о применении

Организация, участвующая в цепи поставок, должна изложить в заявлении о применении ее часть международной цепи поставок, которая объявлена ей как соответствующая настоящему стандарту. Заявление о применении должно, как минимум, включать следующую информацию:

- подробное описание организации; [ISO 28001:2007
https://standards.iteh.ai/catalog/standards/sist/a3764b6d-5ec3-49eb-825e-715f88045fb6/iso-28001-2007](https://standards.iteh.ai/catalog/standards/sist/a3764b6d-5ec3-49eb-825e-715f88045fb6/iso-28001-2007)
- сферу услуг;
- названия всех партнеров по бизнесу в установленной сфере услуг и необходимая информация по установлению контактов с ними;
- дату завершения оценки безопасности и время действия документов подтверждения соответствия;
- подпись лица, уполномоченного поставить подпись от имени организации.

Организация, участвующая в цепи поставок, может расширить Заявление о применении, включив в него другие части цепи поставок, например, конечный пункт назначения.

4.2 Партнеры по бизнесу

Если организация, участвующая в цепи поставок, использует партнеров по бизнесу в части международной цепи поставок, то она должна в соответствии с 4.3 и 4.4 потребовать, чтобы такие партнеры предоставили декларацию о безопасности. Организация должна рассмотреть эту декларацию при оценивании её безопасности и может потребовать принятия специальных контрмер.