МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO 28000

Первое издание
2007-09-15

Системы менеджмента безопасности цепи поставок. Технические условия.

Specification for security management systems for the supply chain

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

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

Ссылочный номер
ISO 28000:2007(R)

© ISO 2007

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 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

ДОКУМЕНТ ЗАЩИЩЕН АВТОРСКИМ ПРАВОМ

© ISO 2005

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 членов 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

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 работе. 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 28000 был подготовлен Техническим комитетом ISO/TC 8, *Суда и морские технологии* совместно с другими соответствующими техническими комитетами, ответственными за конкретные элементы цепи поставок.

Настоящее первое издание ISO 28000 отменяет и замещает ISO/PAS 28000:2005, который был технически пересмотрен.

ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

© ISO 2007 – Все права сохраняются

Введение

Настоящий международный стандарт был разработан в ответ на потребность промышленности в стандарте по менеджменту безопасности. Его конечной целью является усовершенствование безопасности цепей поставок. Это стандарт менеджмента высокого уровня, позволяющий организации создать полную систему менеджмента безопасности цепей поставок. В соответствии с требованиями стандарта организация должна оценить свою рабочую среду с точки зрения обеспечения безопасности, а также определить, являются ли меры по обеспечению безопасности, принимаемые на месте, адекватными и существуют ли уже обязательные требования к обеспечению безопасности, которые организация выполняет. Если потребности в обеспечении безопасности определяются этим процессом, организация должна внедрить соответствующие механизмы и процессы. Поскольку цепи поставок по своей природе являются динамичными, некоторые организации, координирующие множество цепей поставок, могут следить за тем, чтобы их поставщики услуг выполняли соответствующие государственные стандарты по безопасности цепи поставок или соответствующие стандарты ISO, как условие включения их в цепь поставок с тем, чтобы упростить менеджмент безопасности, как показано на Рисунке1.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/e4...3b6-8e84-cc2b4d8cf2b6/iso-...

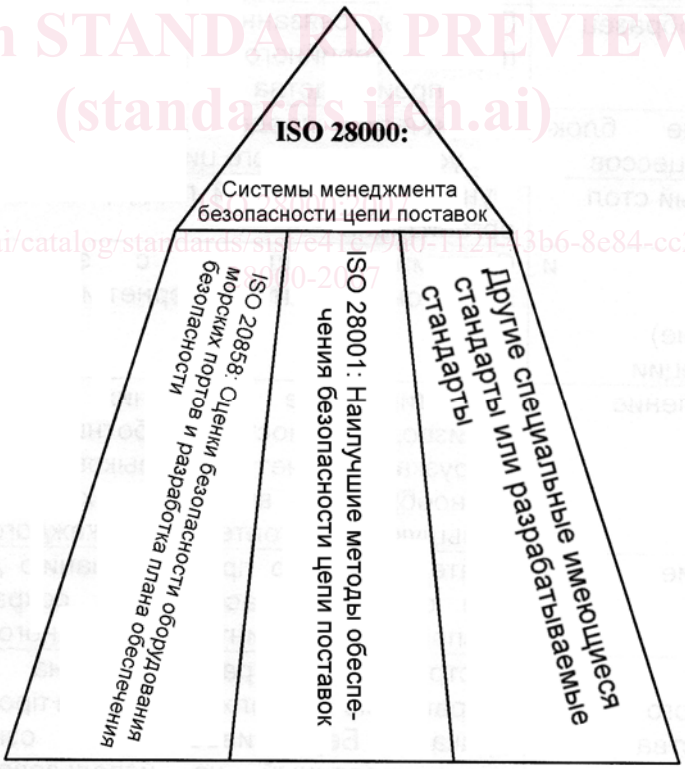

Рисунок 1 – Связь между ISO 28000 и другими соответствующими стандартами

© ISO 2007 – Все права сохраняются

Настоящий международный стандарт предназначен для применения, если цепи поставок организации требуют менеджмента безопасности. Формальный подход к менеджменту безопасности может повлиять на деловые возможности организации и доверие к ней.

Соответствие международному стандарту само по себе не освобождает от правовых обязательств. Для организаций по их желанию соответствие системы менеджмента настоящему международному стандарту может быть проверено путем проведения внешнего или внутреннего аудита.

Настоящий международный стандарт основан на формате ISO, принятом стандартом ISO 14001:2004 из-за его подхода к системам менеджмента, основанного на анализе рисков. Однако организации, которые приняли подход к системам менеджмента, основанный на анализе процесса, (например, ISO 9001:2000), могут использовать свои существующие системы менеджмента как основу для системы менеджмента безопасности, как предписано в настоящем международном стандарте. Целью настоящего документа не является дублирование правительственных требований и стандартов, касающихся менеджмента безопасности цепи поставок, соответствие которым организации уже было сертифицировано или проверено. Проверка может осуществляться первой, второй или третьей организацией.

ПРИМЕЧАНИЕ Настоящий международный стандарт основывается на методологии, известной как "Plan-DO-Check-Act" (PDCA). PDCA можно описать следующим образом:

— Планирование (Plan): *разработка целей и процессов, необходимых для получения результатов в соответствии с политикой организации в области безопасности.*

— *Осуществление (*Do): внедрение процессов.

— Проверка (Check): Мониторинг и измерения процессов по отношению к политике, целям, задачам, правовым и другим требованиям в области обеспечения безопасности и представление результатов.

— Действие (Act): действия по постоянному улучшению характеристик системы менеджмента безопасности.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

 © ISO 2007 – Все права сохраняются

Системы менеджмента безопасности цепи поставок. Технические условия

1 Область применения

Настоящий международный стандарт устанавливает требования к системе менеджмента безопасности, включая аспекты, являющиеся критическими для обеспечения безопасности цепи поставок. Менеджмент безопасности связан со многими другими аспектами управления бизнесом. Аспекты включают все виды деятельности, управляемые или находящиеся под влиянием организаций, которые влияют на безопасность цепи поставок. 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 и кончая многонациональными, занимающимся изготовлением, предоставлением услуг, хранением или транспортировкой на любом этапе производства или цепи поставок, которые хотят:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

b) обеспечить соответствие проводимой политике в области менеджмента безопасности;

c) демонстрировать такое соответствие другим;

ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41e79a0-112f-43b6-8e84-ec2b4d8cf2b6/iso-28000-2007

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 других стандартов для системы менеджмента.

3 Термины и определения

В настоящем документе используются следующие термины и определения.

© ISO 2007 – Все права сохраняются

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

3.5
политика в области обеспечения безопасности
security management policy
общие намерения и направление деятельности организации, относящиеся к обеспечению безопасности, и основа для управления процессами и действиями, связанными с обеспечением безопасности, которые вытекают из политики организации и обязательных требований и согласуются 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.

© ISO 2007 – Все права сохраняются

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

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

© ISO 2007 – Все права сохраняются

4 Элементы системы менеджмента безопасности

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Рисунок 2 – Элементы системы менеджмента безопасности

ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

4.1 Общие требования

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 своей 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.

4.2 Политика в области менеджмента безопасности

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;

© ISO 2007 – Все права сохраняются

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.

iTeh Standards
(standards.iteh.ai)

4.3 Оценка и планирование риска для безопасности

ISO 28000:2007
https://standards.iteh.ai/catalog/standards/sist/e41c79a0-112f-43b6-8e84-cc2b4d8cf2b6/iso-28000-2007

4.3.1 Оценка рисков для безопасности

Организация должна разработать и поддерживать процедуры постоянной идентификации и оценки угроз безопасности и угроз и рисков, относящихся к менеджменту безопасности, а также идентификацию и принятие необходимых мер по корректуре менеджмента. Угрозы безопасности и идентификация рисков, методы оценки и контроля, как минимум, должны соответствовать характеру и масштабу деятельности организации. Оценка должна рассматривать правдоподобие событий и все их последствия, перечисляемые ниже:

a) физические угрозы и риски выхода из строя, например, функциональный отказ, случайный ущерб, злоумышленное причинение вреда или террористические или криминальные действия;

b) угрозы и риски, возникающие в процессе деятельности, включая управление обеспечением безопасности, человеческий фактор и другие действия, влияющие на работу, состояние и безопасность организации;

c) естественные природные явления (шторм, наводнение и т. д.), которые могут привести к тому, что меры по обеспечению безопасности и сохранности оборудования окажутся неэффективными;

d) факторы, не находящиеся под контролем организации, например, дефекты оборудования и недостатки сервиса, предоставляемого внешними организациями;

e) угрозы и риски со стороны заинтересованных сторон, например, невыполнение обязательных требований или нанесение ущерба репутации или бренду;

© ISO 2007 – Все права сохраняются