МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 27000

Третье издание
2014-01-15

Информационные технологии. Методы обеспечения защиты. Системы управления защитой информации. Общий обзор и словарь

Information technology – Security techniques – Information security management systems – Overview and vocabulary

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc380178c97/iso-iec-27000-2014

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

Ссылочный номер
ISO/IEC 27000:2014(R)

© ISO/IEC 2014

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc380178c97/iso-iec-27000-2014

ДОКУМЕНТ ЗАЩИЩЁН АВТОРСКИМ ПРАВОМ

© ISO/IEC 2014

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 получения письменного согласия ISO по указанному ниже адресу или организации-члена ISO в стране запрашивающей стороны.

Бюро ISO по авторским правам:
Case postale 56 • CH-1211 Geneva 20
Тел.: + 41 22 749 01 11
Факс: + 41 22 749 09 47
Эл. почта: copyright@iso.org
Веб-сайт: www.iso.org

Опубликовано в Швейцарии

Содержание

Страница

Предисловие iv

0 Введение v

1 Область применения 1

2 Термины и определения 1

3 Системы управления защитой информации 15
- **3.1 Вводные замечания** 15
- **3.2 Что такое СОИБ?** 16
- **3.3 Технологический подход** 18
- **3.4 Важная роль СОИБ** 18
- **3.5 Внедрение, текущий контроль, техническая поддержка и развитие СОИБ** 20
- **3.6 Критические факторы успеха СОИБ** 23
- **3.7 Выгоды, обеспечиваемые использованием стандартов семейства ISMS** 24

4 Семейство стандартов ISMS 24
- **4.1 Общие сведения** 24
- **4.2 Стандарты, дающие общий обзор и используемую терминологию** 25
- **4.3 Стандарты, определяющие требования** 26
- **4.4 Стандарты, содержащие руководящие указания общего характера** 26
- **4.5 Стандарты, содержащие руководящие указания для подразделений организации** 29

Приложение A (информативное) **Глагольные формы для выражения формулируемых положений** 31

Приложение B (информативное) **Указатель терминов** 32

Библиография 36

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc380178c97/iso-iec-27000-2014

Предисловие

Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) образуют специализированную организацию по международной стандартизации. Национальные органы стандартизации, являющиеся членами ISO или IEC, участвуют в разработке Международных стандартов через технические комитеты, учреждённые соответствующей организацией для компетентного рассмотрения проблем в конкретных предметных областях. Технические комитеты ISO и IEC сотрудничают в сфере общих интересов. Международные правительственные и неправительственные организации, имеющие связь с ISO и IEC, также принимают участие в этой работе. Применительно к сфере информационных технологий ISO и IEC учредили объединённый технический комитет ISO/IEC JTC 1.

Проекты международных стандартов разрабатываются согласно правилам, приведённым в Директивах ISO/IEC, Часть 2.

Разработка международных стандартов является основной задачей технических комитетов. Проекты международных стандартов, принятые техническими комитетами, рассылаются комитетам-членам на голосование. Для публикации в качестве международного стандарта требуется одобрение не менее 75 % комитетов-членов, принявших участие в голосовании.

Принимается во внимание тот факт, что некоторые из элементов настоящего документа могут быть объектом патентных прав. ISO не принимает на себя обязательств по определению отдельных или всех таких патентных прав.

ISO/IEC 27000 был подготовлен Объединённым техническим комитетом ISO/IEC JTC 1, *Информационные технологии,* Подкомитетом SC 27, *Методы обеспечения безопасности в ИТ*.

Настоящее третье издание стандарта отменяет и заменяет собой второе издание ISO/IEC 27000:2012, техническое содержание которого подверглось пересмотру.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc380178c97/iso-iec-27000-2014

 © ISO/IEC 2012 – Все права сохраняются

0 Введение

0.1 Общие замечания

Международные стандарты, касающиеся систем управления, предоставляют эталонную модель для настройки параметров и эксплуатации таких систем. Функциональная структура этой модели обладает характеристиками, по которым достигнуто единогласное мнение специалистов отрасли ИТ, подтверждающих реализацию в модели самых последних мировых достижений научно-технического прогресса. В составе технического комитета ISO/IEC JTC 1/SC 27 имеется экспертная комиссия, специализирующаяся на разработке международных стандартов в сфере систем управления защитой информации, которые широко известны ещё и как семейство стандартов по системе обеспечения информационной безопасности СОИБ [Information Security Management System (ISMS)].

Используя это семейство стандартов, организации получают возможность разработки и реализации инфраструктуры системы управления защитой своих информационных активов, включая финансовую информацию, интеллектуальную собственность и детали кадровой политики, или конфиденциальную информацию, доверенную им клиентами или третьими сторонами. Семейство стандартов ISMS может также использоваться для подготовки к независимой оценке уже внедрённых СОИБ, обеспечивающих защиту информации.

0.2 Семейство стандартов ISMS

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc3801f8c97/iso-iec-27000-2014

Семейство стандартов ISMS (см. раздел 4) предназначено для оказания помощи организациям любых типов и масштабов в эффективной эксплуатации СОИБ и включает в себя перечисленные ниже в порядке возрастания номеров международные стандарты под общим заголовком *Информационные технологии. Методы обеспечения защиты*:

— ISO/IEC 27000, *Системы управления защитой информации. Общий обзор и словарь*

— ISO/IEC 27001, *Системы управления информационной безопасностью. Требования*

— ISO/IEC 27002, *Свод правил по управлению защитой информации*

— ISO/IEC 27003, *Руководство по внедрению системы управления информационной безопасностью*

— ISO/IEC 27004, *Управление информационной безопасностью. Измерения*

— ISO/IEC 27005, *Управление рисками информационной безопасности*

— ISO/IEC 27006, *Требования для органов, обеспечивающих аудит и сертификацию систем управления информационной безопасностью*

— ISO/IEC 27007:2011, *Руководящие указания по аудиту систем управления информационной безопасностью*

— ISO/IEC TR 27008, *Руководящие указания для аудиторов по оценке средств управления систем обеспечения безопасности*

— ISO/IEC 27010:2012, *Руководящие указания по обеспечению защиты информационного обмена между подразделениями и организациями*

— ISO/IEC 27011, *Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002*

© ISO/IEC 2014 – Все права сохраняются

— ISO/IEC 27013, *Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1*

— ISO/IEC FDIS 27014, *Управление защитой информации*

— ISO/IEC TR 27015, *Руководящие указания по управлению защитой информации для финансовых служб*

— ISO/IEC TR 27016, *Управление защитой информации. Экономика организации*

ПРИМЕЧАНИЕ Общий заголовок "*Информационные технологии. Методы обеспечения защиты*" указывает на то, что данные стандарты были подготовлены подкомитетом SC 27 *"Методы обеспечения защиты в ИТ"* Объединённого технического комитета ISO/IEC JTC 1 *Информационные технологии. Методы обеспечения защиты*.

Частью семейства стандартов ISMS является также международный стандарт, не охваченный вышеуказанным общим заголовком:

— ISO 27799:2008, *Информатика в здравоохранении. Управление информационной безопасностью по стандарту ISO/IEC 27002*

0.3 Целевое назначение настоящего международного стандарта

Данный международный стандарт содержит общий обзор систем управления защитой информации и определяет соответствующие отраслевые термины.

ПРИМЕЧАНИЕ В Приложении A поясняется, каким образом в рамках семейства стандартов ISMS используются глагольные словоформы для выражения требований и/или руководящих указаний.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-
2ce4c7c1e1ed/iso-iec-27000-2014

В семейство ISMS входят стандарты, которые:

a) устанавливают требования к самим СОИБ и к органам, проводящим их сертификацию;

b) обеспечивают прямую поддержку, всестороннее консультирование и/или интерпретацию в рамках всего процесса создания, внедрения, сопровождения и развития СОИБ;

c) содержат руководящие указания по использованию СОИБ в рамках определённой сферы их назначения, и

d) касаются оценки соответствия СОИБ предъявляемым требованиям.

Представленные в настоящем стандарте термины и определения

— охватывают понятия и определения, наиболее широко используемые в стандартах семейства ISMS;

— не охватывают всех терминов и определений, применяемых внутри семейства стандартов ISMS,

— не накладывают никаких ограничений на использование в семействе ISMS новых терминов.

 © ISO/IEC 2012 – Все права сохраняются

Информационные технологии. Методы обеспечения защиты. Системы управления защитой информации. Общий обзор и словарь

1 Область применения

В настоящем международном стандарте приводится общий обзор систем управления защитой информации, а также общепринятые термины и определения, используемые в рамках стандартов семейства ISMS. Настоящий международный стандарт применим к организациям любого типа и масштаба (например, к коммерческим организациям, государственным агентствам и некоммерческим организациям).

2 Термины и определения

Термины и определения, используемые в рамках данного стандарта, представлены ниже.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc380178c97/iso-iec-27000-2014

2.1
управление доступом
access control
средство управления, призванное гарантировать, что доступ к *активам* (2.4) санкционирован и ограничен в соответствии с установленными требованиями хозяйственной деятельности компании и соблюдением условий безопасности

2.2
аналитическая модель
analytical model
алгоритм или вычислительный процесс, в котором комбинируются одна или несколько *базовых мер* (2.10) или *производных мер* (2.22) с соответствующими критериями принятия решений

2.3
атака
attack
попытка разрушения, умышленного раскрытия, изменения, блокировки, кражи актива, получения незаконного доступа к нему или его несанкционированного использования

2.4
атрибут
attribute
свойство или характеристика *объекта* (2.55), которые могут различаться по количественному или качественному признаку человеком или автоматическими средствами

[ИСТОЧНИК: ISO/IEC 15939:2007, англоязычное определение модифицировано – термин “entity” заменён термином “object”].

© ISO/IEC 2014 – Все права сохраняются

2.5
аудит, аудиторская проверка
audit
документируемый систематический независимый *процесс* (2.61) получения и объективного оценивания данных, позволяющих определить степень выполнения критериев аудита

Примечание 1 к статье: Аудиторская проверка может быть внутренней (при проведении первой стороной), внешней (при проведении второй либо третьей стороной) и комплексной (по двум и более направлениям)

Примечание 2 к статье: Термины “audit evidence” (результат ревизии) и “audit criteria” (критерии аудита) определены в ISO 19011.

2.6
объём аудита
audit scope
масштабы и границы *аудиторской проверки* (2.5)

[ИСТОЧНИК: ISO 19011:2011]

2.7
аутентификация
authentication
подтверждение достоверности декларированной характеристики объекта

2.8
аутентичность
authenticity
подлинность представляемого объекта

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.9
готовность
availability
свойство, характеризующее доступность и пригодность объекта для использования по запросу уполномоченного лица

ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc3801f8c97/iso-iec-27000-2014

2.10
базовая мера
base measure
мера (2.47), определяемая применительно к *атрибуту* (2.4) и методу его количественного выражения

[ИСТОЧНИК: ISO/IEC 15939:2007]

ПРИМЕЧАНИЕ Базовая мера в функциональном плане не зависит от других мер.

2.11
компетентность
competence
способность применять знания и опыт для достижения желаемых результатов

2.12
конфиденциальность
confidentiality
характеристика, указывающая на то, что данная информация не подлежит передаче либо раскрытию сторонним лицам, организациям или *процессам* (2.61)

© ISO/IEC 2014 – Все права сохраняются

2.13
соответствие
conformity
выполнение установленного *требования* (2.63)

Примечание 1 к статье В английском языке имеется синонимичный термин “conformance”, однако он не рекомендуется к применению.

2.14
последствие
consequence
исход *события* (2.25), влияющий на достижение *целей* (2.56)

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье Событие может вызывать целый ряд последствий.

Примечание 2 к статье Последствие может быть определённым или неопределённым, и в аспекте защиты информации, как правило, негативным.

Примечание 3 к статье Последствия могут оцениваться качественно или количественно.

Примечание 4 к статье Первоначальные последствия могут усугубляться из-за эффектов косвенного влияния.

2.15
непрерывное улучшение
continual improvement
повторяющиеся действия по повышению *эффективности* (2.59)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-abc3a01f8c97/iso-iec-27000-2014

2.16
средство управления
control
способ изменения характеристик *риска* (2.68

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: К числу средств управления относится любой процесс, стратегия, техническое устройство, практический метод или другие действия, которые изменяют риски.

Примечание 2 к статье: Средства управления не всегда могут оказывать предписанное или ожидаемое корректирующее воздействие.

2.17
цель управления
control objective
положение документа, описывающее нужный результат применения *средств управления* (2.16)

2.18
корректировка
correction
действие по устранению обнаруженного *несоответствия* (2.53)

2.19
корректирующее воздействие
corrective action
действие, направленное на устранение причины обнаруженного *несоответствия* (2.53) и на предотвращение её повторного проявления

© ISO/IEC 2014 – Все права сохраняются

2.20
данные
data
коллекция значений, присвоенных *базовым мерам* (2.10), *производным мерам* (2.22) и/или *показателям* (2.30)

[ИСТОЧНИК: ISO/IEC 15939:2007]

Примечание 1 к статье: это определение применимо только в контексте ISO/IEC 27004:2009.

2.21
критерии принятия решений
decision criteria
пороговые значения, целевые значения или модели, используемые для определения необходимости действия либо дальнейшего анализа ситуации, или принятый уровень доверительной вероятности для данного результата

[ИСТОЧНИК: ISO/IEC 15939:2007]

2.22
производная мера
derived measure
мера (2.47), которая определяется как функция двух или более значений *базовых мер* (2.10)

[ИСТОЧНИК: ISO/IEC 15939:2007]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.23
документированная информация
documented information
информация, которая должна контролироваться и поддерживаться *организацией* (2.57), и носитель, на котором она хранится

ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/51012525-1643-4dd2-81e8-abc3801f8c97/iso-iec-27000-2014

Примечание 1 к статье: документированная информация может быть представлена в любом формате, на любом носителе и поступать от любого источника.

Примечание 2 к статье: документированная информация может относиться:

— к *системе управления* (2.46), включая соответствующие *процессы* (2.61);

— к системе документооборота, обеспечивающей функционирование организации (рабочие документы);

— к фактическим данным, характеризующим достигнутые результаты (записи и протоколы)

2.24
эффективность
effectiveness
степень реализации предусмотренных планом действий и достижения запланированных результатов

2.25
событие
event
возникновение или изменение конкретной совокупности обстоятельств

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: событие может происходить один или несколько раз и вызываться несколькими причинами.

Примечание 2 к статье: событие может состоять и в том, что нечто ожидаемое не произошло.

Примечание 3 к статье: событие иногда характеризуется как “инцидент” или “авария”.

© ISO/IEC 2014 – Все права сохраняются

2.26
исполнительное высшее руководство
executive management
должностное лицо или группа должностных лиц, которым делегированы полномочия *органа управления* (2.29) для реализации стратегий и линий поведения, обеспечивающих достижение цели *организации* (2.57)

Примечание 1 к статье: исполнительное высшее руководство иногда называют просто высшим руководством; в его состав могут входить исполнительные директора, финансовые директора, руководители отделов информационных систем и другое аналогичное руководство.

2.27
внешняя обстановка
external context
внешняя среда, в которой организация стремится к достижению своих целей

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: К внешней обстановке могут относиться:

— культурная, социальная, политическая, юридическая, регуляционная, финансовая, технологическая, экономическая, природная и конкурентная среда на международном, национальном, региональном или локальном уровне;

— ключевые движущие силы и тенденции, влияющие на *цели* (2.56) *организации* (2.57), и

— взаимоотношения с внешними *заинтересованными сторонами* (2.82), интерпретация их поведения и системы ценностей.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.28
система управления защитой информации
governance of information security
предписанный порядок действий, разъясняющий, что и как должно быть сделано для достижения целей, намеченных в рамках принятых *стратегий* (2.57)

ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/3f012525-1043-4dd2-8fc8-
ISO/IEC 27000:2014

2.29
руководящий орган
governing body
должностное лицо или группа должностных лиц, областью ответственности которых являются *эффективность функционирования* (2.59) и соответствие *организации* (2.57) требованиям времени

2.30
показатель
indicator
мера (2.47), которая обеспечивает качественную либо количественную оценку конкретных *атрибутов* (2.4), полученных в *аналитической модели* (2.2) с учётом конкретизированных *информационных потребностей* (2.31)

2.31
информационная потребность
information need
осознание необходимости углублённого анализа информации для определения задач, целей, рисков и проблем, подлежащих решению

[ИСТОЧНИК: ISO/IEC 15939:2007]

© ISO/IEC 2014 – Все права сохраняются

2.32
средства обработки информации
information processing facilities
любая система обработки информации, её службы и инфраструктура или места их физического размещения

2.33
защита информации
information security
сохранение *конфиденциальности* (2.12), *целостности* (2.40) и *готовности* (2.9) информации к использованию

Примечание к статье: защита может охватывать и другие характеристики, такие как *аутентичность* (2.8), подотчётность, *невозможность отказа от авторства* (2.54) и *надёжность* (2.62).

2.34
постоянство защиты информации
information security continuity
процессы (2.61) и процедуры обеспечивающие бесперебойную работу *защиты информации* (2.33)

2.35
событие информационной безопасности
information security event
обнаруживаемое состояние системы, системной службы или сети, указывающее на возможную “брешь” в политике обеспечения информационной безопасности либо на сбой средств защиты или на возникновение ранее не известной ситуации, которая может повлиять на работу защиты

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2.36
инцидент информационной безопасности
information security incident
одиночное событие или целый ряд нежелательных либо неожиданных *событий информационной безопасности* (2.35), которые сопряжены со значимой вероятностью компрометации деловых операций и возникновения угроз системе *защиты информации* (2.33)

https://standards.iteh.ai/catalog/standards/iso/ad0f0f65-1043-4dd2-8fc8-abc380178c97/iso-iec-27000-2014

2.37
управление событиями информационной безопасности
information security incident management
процессы (2.61) обнаружения, регистрации, оценивания, реагирования, обработки и анализа **событий** *информационной безопасности* (2.36)

2.38
сообщество пользователей общей информации
information sharing community
группа организаций, совместно использующих информацию по общему согласию

Примечание 1 к статье: организация может быть представлена одним лицом.

2.39
информационная система
information system
прикладная система, служба, актив информационных технологий или любой другой компонент, предназначенный для обработки информации

2.40
целостность
integrity
сохранение характеристик точности и полноты

 © ISO/IEC 2014 – Все права сохраняются

2.41
заинтересованная сторона
interested party
индивидуум или *организация* (2.57), которые могут влиять на принятие того или иного решения либо действия, подвергаться его влиянию или ощущать возможность такого влияния

2.42
внутренний контекст
internal context
внутренняя среда, в которой организация ищет пути к достижению своих целей

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: возможные компоненты внутреннего контекста:

— руководство организации, организационная структура, распределение функций и отношения подотчётности;

— программы действий, целевые установки и реализуемые стратегии их достижения;

— имеющиеся возможности, понимаемые в аспекте требуемых ресурсов и знаний (например, капитала, времени, людей, процессов, систем и технологий);

— информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);

— взаимоотношения с внутренними заинтересованными сторонами, трактовка их действий и систем ценностей;

— организационная культура;

— стандарты, рекомендации и модели, используемые организацией, и

— форма и объём контрактных отношений.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27000:2014
https://standards.iteh.ai/catalog/standards/sist/31012525-1043-4dd2-8fc8-abc380178c97/iso-iec-27000-2014

2.43
проект СОИБ
ISMS project
структурированные действия *организации* (2.57) по внедрению системы обеспечения информационной безопасности (СОИБ)

2.44
уровень риска, степень риска
level of risk
величина *риска* (2.68), определённая с учётом комбинации его возможных *последствий* (2.14) и их *правдоподобия* (2.45)

[ИСТОЧНИК: ISO Guide 73:2009 с изменением – в англоязычном оригинале исключены слова “or combination of risks”]

2.45
правдоподобие
likelihood
вероятность какого-либо события или ситуации

[ИСТОЧНИК: ISO Guide 73:2009]

© ISO/IEC 2014 – Все права сохраняются