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

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)

ДОКУМЕНТ ЗАЩИЩЁН АВТОРСКИМ ПРАВОМ

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

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.

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

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 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.

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.

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.

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”].

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

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

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)

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)

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

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]

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

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”.

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.

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)

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]

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

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)

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

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.

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]

2.46
система управления
management system
совокупность взаимосвязанных или взаимодействующих элементов *организации* (2.57), нацеленная на установление *стратегий* (2.60), *целей* (2.56) и соответствующих *процессов* (2.61) обеспечивающих достижение поставленных целей

Примечание 1 к статье: система управления может охватывать одну или несколько сфер деятельности.

Примечание 2 к статье: к элементам системы относятся организационная структура, должности и сферы ответственности, функции планирования, эксплуатации и др.

Примечание 3 к статье: масштабы системы управления могут определяться организацией в целом, конкретными функциями организации, конкретными подразделениями организация либо одной или несколькими функциями группы организаций.

2.47
мера
measure
переменная величина, которой значение присваивается в результате выполнения процесса *измерения* (2.48)

[ИСТОЧНИК: ISO/IEC 15939:2007]

Примечание 1 к статье: термин “меры” используется как обобщённое название базовых единиц измерения, производных единиц измерения и измеренных показателей.

2.48
измерение
measurement
процесс (2.61) определения конкретного значения

Примечание 1 к статье: в контексте *защиты информации* (2.33) процесс определения конкретного значения требует получения сведений об эффективности (2.24), о *системе управления* (2.46) защитой информации и её *средствах управления* (2.16) с помощью *метода измерения* (2.50), *измерительной функции* (2.49), *аналитической модели* (2.2) и *критериев принятия решений* (2.21)

2.49
измерительная функция
measurement function
алгоритм или вычислительный процесс, выполняемый с целью комбинирования двух и более *базовых мер* (2.10)

[ИСТОЧНИК: ISO/IEC 15939:2007]

2.50
метод измерения
measurement method
описываемая в общем виде логическая последовательность операций количественной оценки *атрибута* (2.4) с помощью некоторой специализированной *шкалы* (2.80)

[ИСТОЧНИК: ISO/IEC 15939:2007]

Примечание к статье: тип метода измерения зависит от характера операций, выполняемых при квантификации атрибута. Выделяются два типа таких операций:

- субъективный - при котором количественное выражение атрибутов осуществляется на основе человеческих суждений,
- объективный, при котором квантификация основывается на численных правилах.

2.51
результаты измерения
measurement results
один или несколько *показателей* (2.30) и связанные с ними интерпретации, которые служат целям удовлетворения *информационных потребностей* (2.31)

2.52
(текущий) контроль, мониторинг
monitoring
определение текущего состояния системы, *процесса* (2.61) или какой-либо работы

2.53
несоответствие
nonconformity
невыполнение *требования* (2.63)

2.54
неотказуемость, невозможность отказа от авторства
non-repudiation
наличие возможности доказать факт совершения конкретного события или выполнения конкретного действия конкретным исполнителем

2.55
объект
object
предмет, характеризуемый посредством *измерения* (2.48) его *атрибутов* (2.4)

2.56
цель, целевая установка
objective
результат, который должен быть достигнут

Примечание 1 к статье: цель может быть стратегической, тактической или оперативной.

Примечание 2 к статье: цели могут относиться к разным сферам знаний (например, к финансовой деятельности, охране здоровья и технике безопасности или к охране окружающей среды) и могут устанавливаться на разных уровнях (например, на стратегическом; на уровне всей организации, на уровне проекта, продукта или *процесса* (2.61).

Примечание 3 к статье: цель может быть выражена разными способами – например, как планируемый выход продукции, как целевой показатель, как рабочий критерий, как задача информационной безопасности или иными словами с тем же смыслом (намерение, глобальная цель, целевая установка).

Примечание 4 к статье: в контексте системы обеспечения информационной безопасности цели защиты информации устанавливаются организацией в соответствии с выбранной стратегией безопасности, ориентированной на получение конкретных результатов.

2.57
организация
organization
отдельное лицо или группа людей, которые выполняют определённые функции, отвечают за свою сферу деятельности, облечены разными полномочиями и объединяются для достижения общих *целей* (2.56)

Примечание 1 к статье: понятие “организация” охватывает, в частности, такие образования как индивидуальный предприниматель, компания, корпорация, фирма, предприятие, орган власти, товарищество, благотворительный фонд, ведомство, либо отдельные части или комбинации этих образований – независимо от того, обладают они юридическими правами или нет и являются ли государственными или частными.

2.58
привлекать соисполнителей, использовать аутсорсинг
outsource
распределять работу организации таким образом, что часть её функций или *процессов* (2.61) выполняется внешней *организацией* (2.57)

Примечание 1 к статье: привлекаемая внешняя организация находится вне границ системы управления (2.46), тогда как отдаваемые на сторону функция или процесс лежат в границах системы.

2.59
эксплуатационные показатели
performance
измеримый результат работы

Примечание 1 к статье: эксплуатационные показатели могут выражаться в количественной или качественной форме.

Примечание 2 к статье: эксплуатационные показатели могут относиться к управлению работами, к *процессам* (2.61), продуктам (включая сферу услуг), системам или *организациям* (2.57).

2.60
стратегия, политика
policy
формальное выражение общей цели движения в определённом направлении, обеспечиваемого *высшим руководством* (2.84) *организации* (2.57)

2.61
(технологический) процесс
process
совокупность взаимосвязанных или взаимодействующих видов деятельности, в ходе которой “входы” преобразуются в “выходы”

2.62
надёжность
reliability
способность к устойчивому сохранению целенаправленного поведения и достоверных результатов

2.63
требование
requirement
определённая или ожидаемая потребность, которая декларируется, общепризнанна или является обязательным условием.

Примечание 1 к статье: общепризнанность означает, что для организации и заинтересованных сторон данная установленная или планируемая потребность организации предусматривается сложившейся практикой

Примечание 2 к статье: определённая потребность – это потребность, которая установлена официально, например, в документированной информации.

2.64
остаточный риск
residual risk
риск (2.68), остающийся после *обработки рисков* (2.79)

Примечание 1 к статье остаточный риск может содержать в себе не выявленный риск.

Примечание 2 к статье остаточный риск называется также “сохранённым риском”.

2.65
анализ
review
деятельность, предпринимаемая для определения пригодности, адекватности и *результативности* (2.24) рассматриваемого объекта для достижения поставленных целей

[ИСТОЧНИК: ISO Guide 73:2009]

2.66
объект анализа
review object
конкретный объект, подлежащий анализу

2.67
цель анализа
review objective
словесное описание конечного результата, который должен быть получен после проведения анализа

2.68
риск
risk
степень влияния неопределённости на достижение целей

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: степень влияния оценивается по отклонению от ожидаемого значения целевого показателя — положительному и отрицательному.

Примечание 2 к статье: неопределённость (даже неполная) – это состояние, при котором испытывается недостаток информации для понимания или познания конкретного *события* (2.25), его *последствия* (2.14) или *правдоподобия* (2.45).

Примечание 3 к статье: риск часто характеризуется путём рассмотрения возможных *событий* (2.25) и *последствий* (2.14) или их различных сочетаний.

Примечание 4 к статье: риск часто выражается комбинацией ожидаемых *последствий* (2.14) события (в том числе изменения обстановки) с соответствующей ему оценкой *правдоподобия* (2.45).

Примечание 5 к статье: в контексте систем обеспечения информационной безопасности риски информационной безопасности могут выражаться как результат влияния неопределённости на цели защиты информации.

Примечание 6 к статье: риск информационной безопасности ассоциируется с вероятностью того, что имеющиеся *угрозы* (2.83) будут материализоваться с использованием *уязвимостей* (2.89) некоторого информационного актива или группы таких активов, принося вред организации.

2.69
принятие риска
risk acceptance
обоснованное решение о приемлемости *риска* (2.68)

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: принятие риска возможно как без *обработки рисков* (2.79), так и в процессе их обработки.

Примечание 2 к статье: принятые риски подлежат *текущему контролю* (2.52) и *анализу* (2.65).

2.70
анализ рисков
risk analysis
процесс всестороннего изучения характера **риска** (2.68) и определения *уровня риска* (2.44)

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: анализ рисков обеспечивает основу для *оценки рисков* (2.74) и для принятия решений относительно *обработки рисков* (2.79).

Примечание 2 к статье: в рамках анализа рисков производится их оценка.

2.71
оценка рисков
risk assessment
единый *процесс* (2.61) *идентификации риска* (2.75), *анализа риска* (2.70) и *оценки риска* (2.74)

[ИСТОЧНИК: ISO Guide 73:2009]

2.72
взаимодействие и консультации по вопросам рисков
risk communication and consultation
непрерывные итеративные процессы, которые выполняются организацией в целях предоставления, совместного использования или получения информации и участия в диалоге с *заинтересованными сторонами* (2.82) по вопросам управления *рисками* (2.68)

Примечание 1 к статье: информация может касаться факта существования риска, его характера, формы проявления, вероятности, значимости, оценки, определения степени приемлемости и его обработки.

Примечание 2 к статье: консультирование – это двусторонний процесс информированного взаимодействия между организацией и её заинтересованными сторонами по вопросу рисков до принятия конкретного решения или определения конкретных направленных действий. Консультация представляет собой:

— процесс, который влияет на принятие решения косвенно, а не в силу каких-то властных полномочий, и

— всего лишь входной фактор для принятия решений, а не процедура выработки совместного решения.

2.73
критерии риска
risk criteria
совокупность факторов, по сопоставлению с которыми оценивается значимость *риска* (2.68)

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: Критерии риска основываются на целях организации и на внешнем и внутреннем контексте.

Примечание 2 к статье: Критерии риска могут выводиться из требований стандартов, действующих законов, принятых стратегий и других требований.

2.74
сравнительная оценка риска
risk evaluation
процесс (2.61) сопоставления результатов *анализа риска* (2.70) с *критериями риска* (2.73) с целью определения, являются ли сам *риск* (2.68) и/или его величина приемлемыми или допустимыми.

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: Наличие такой оценки помогает в принятии решения по *обработке риска* (2.79).

2.75
идентификация рисков
risk identification
процесс поиска, распознавания и описания *рисков* (2.68)

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: Идентификация рисков включает в себя определение их источников, событий, причин и возможных последствий.

Примечание 2 к статье: Идентификация рисков может предусматривать привлечение данных предыстории, теоретический анализ, обоснованные мнения экспертов, учёт потребностей заинтересованных сторон.

2.76
управление рисками
risk management
координируемые действия по выбору направления и текущему контролю работы *организации* (2.57) в условиях **риска** (2.68)

[ИСТОЧНИК: ISO Guide 73:2009]

2.77
процесс управления рисками
risk management process
систематизированное применение управленческих *стратегий* (2.51), *процедур* (2.53) и действующих правил к операциям обмена информацией, консультирования, установления контекста, а также к идентификации, анализу, оценке, обработке, текущему контролю и пересмотру *рисков* (2.68)

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: В ISO/IEC 27005 термин “процесс” используется для описания технологии управления рисками в целом, а отдельные элементы этого процесса называются действиями (“activities”).

2.78
владелец риска
risk owner
подотчётное физическое или юридическое лицо, имеющее полномочия по управлению *риском* (2.68)

[ИСТОЧНИК: ISO Guide 73:2009]

2.79
обработка риска
risk treatment
процесс (2.61) изменения степени *риска* (2.68)

[ИСТОЧНИК: ISO Guide 73:2009]

Примечание 1 к статье: Обработка рисков может включать в себя следующие действия:

— исключение риска путём отказа от начала или завершения операции, которая увеличивает риск;

— принятие или повышение риска в целях использования удобной возможности анализа;

— устранение источника риска;

— изменение правдоподобия;

— изменение последствий;

— разделение риска с другой стороной или несколькими сторонами (путём включения их в контракты) и финансирование действий по обработке риска, и

— обоснование решения о необходимости сохранения риска.

Примечание 2 к статье: действия по обработке риска, которые сопряжены с возможными негативными последствиями, иногда называются "смягчением риска", "устранением риска", "исключением риска" и "снижением риска".

Примечание 3 к статье: обработка риска может порождать новые риски или видоизменять уже существующие.

2.80
оценочная шкала
scale
упорядоченное множество непрерывных или дискретных значений или набор категорий, на которые отображается *атрибут* (2.4)

[ИСТОЧНИК: ISO/IEC 15939:2007]

Примечание 1 к статье: тип шкалы зависит от характера отношения между шкальными значениями. Обычно выделяются четыре типа шкал:

— номинальная – когда измеряемые значения носят категориальный характер;

— порядковая - когда измеряемые значения ранжируются;

— интервальная - когда измеряемые значения располагаются на одинаковом расстоянии друг от друга соответственно разбиению количественных значений контролируемого атрибута;

— шкала отношений - когда измеряемые значения располагаются на равных расстояниях соответственно равным приращениям значений атрибута, и нулевое значение соответствует отсутствию атрибута.

Но это всего лишь отдельные примеры возможных типов шкал.

2.81
стандарт обеспечения безопасности
security implementation standard
документ, определяющий способы реализации защиты

2.82
заинтересованная сторона
stakeholder
физическое лицо или организация, которые могут влиять на принятие того или иного решения либо действия, подвергаться его влиянию или ощущать возможность такого влияния

[ИСТОЧНИК: ISO Guide 73:2009]

2.83
угроза
threat
потенциальная причина нежелательного инцидента, который может причинить вред системе или организации

2.84
высшее руководство
top management
должностное лицо или группа людей, которые управляют *организацией* (2.57) и контролируют её деятельность на высшем уровне иерархии

Примечание 1 к статье: высшее руководство имеет право делегировать свои полномочия и передавать ресурсы в рамках организации.

Примечание 2 к статье: если масштаб *системы управления* (2.46) таков, что она охватывает лишь часть организации (2.57), то высшее руководство взаимодействует с тем персоналом, который осуществляет управление и контроль применительно к этой части организации (2.57).

2.85
доверенная сторона передачи информации
trusted information communication entity
автономная организация, поддерживающая процесс информационного обмена в рамках сообщества, совместно использующего информацию

2.86
единица измерения
unit of measurement
определённая и принятая в рамках соглашения конкретная количественная величина, с которой сопоставляются другие количественные величины того же типа с целью определения их численного значения относительно эталона

[ИСТОЧНИК: ISO/IEC 15939:2007]

2.87
валидация
validation
подтверждение выполнения требований к конкретному целевому использованию изделия или прикладной системы посредством предоставления объективного доказательства

[ИСТОЧНИК: ISO 9000:2005]

2.88
верификация
verification
подтверждение выполнения всех установленных требований путём предоставления объективного доказательства

[ИСТОЧНИК: ISO 9000:2005]

Примечание 1 к статье: эта процедура может также называться проверкой соответствия.

2.89
уязвимость
vulnerability
слабое звено актива или *средства управления* (2.16), которое может быть источником *угроз* (2.83)

3 Системы управления защитой информации

3.1 Вводные замечания

Организации любого типа и любого масштаба:

a) осуществляют сбор, обработку, хранение и передачу информации;

b) понимают, что информация, связанные с ней процессы, системы, сети и люди, являются важными активами, обеспечивающими достижение поставленных целей организации;

c) работают в условиях существующих опасностей, которые могут оказывать неблагоприятное влияние на функционирование активов, и

d) противостоят существующим опасностям путём внедрения различных средств и систем защиты информации.

Вся информация, хранимая и обрабатываемая организацией, подвергается угрозам атак, ошибок, стихийных бедствий (например, наводнения или пожара) и других факторов риска, а также опасности влияния существующих внутренних уязвимостей процесса её использования. Термин “информационная безопасность” обычно ассоциируется с той информацией, которая считается ценным активом организации и потому нуждается в адекватной защите, например, для обеспечения её доступности, конфиденциальности и целостности. Наличие точной и полной информации в нужное время у тех должностных лиц, которым она необходима, является залогом успешной хозяйственной деятельности предприятия.

Защита информационных активов посредством определения, реализации, сопровождения и усовершенствования систем информационной безопасности жизненно важно для достижения организацией своих целей, поддержания и укрепления её нормативно-правового соответствия и деловой репутации. Эти скоординированные действия, направленные на реализацию адекватных средств контроля и обработки неприемлемых рисков информационной безопасности, обычно считаются элементами систему управления защитой информации.

По мере того как риски информационной безопасности изменяются под воздействием меняющихся условий, организациям необходимо:

a) контролировать и оценивать эффективность внедрённых средств управления и процедур защиты;

b) идентифицировать возникающие риски, подлежащие обработке, и

c) выбирать, реализовывать и, если нужно, совершенствовать соответствующие средства управления.

Для увязки и координации таких действий по защите информации каждая организация нуждается в выработке определённой стратегии и целевых установок информационной безопасности и достижении этих целей с использованием высокоэффективной автоматизированной системы управления.

3.2 Что такое СОИБ?

3.2.1 Общее описание и принципы построения

Система обеспечения информационной безопасности (СОИБ) включает в себя стратегии, процедуры, руководящие указания, как и ассоциируемые с ними ресурсы и операции, координируемые организацией в процессе обеспечения защиты своих информационных активов. СОИБ олицетворяет собой систематизированный подход к определению, реализации, использованию, контролю, анализу, технической поддержке и усовершенствованию информационной безопасности организации, обеспечивающий достижение установленных целей хозяйственной деятельности. Этот подход основан на оценке существующих рисков и определении приемлемых для организации уровней опасности, рассчитанных на эффективную обработку рисков и управление ими. Успешной реализации СОИБ способствует надлежащий анализ требований к защите информационных активов и использование адекватных средств управления для

гарантирования требуемого уровня её надёжности. Успешной реализации СОИБ способствуют также следующие основополагающие принципы:

a) выявление потребностей в защите информации;

b) распределение сфер ответственности за обеспечение информационной безопасности;

c) реализация управленческой стратегии с учётом интересов партнёров;

d) расширение системы социальных ценностей;

e) оценка рисков для определения надлежащих средств управления, позволяющих сохранять риски на приемлемом уровне;

f) внедрение защиты информации как необходимого элемента информационных сетей и систем;

g) активное предотвращение и обнаружение инцидентов информационной безопасности;

h) обеспечение комплексного подхода к проблемам управления защитой информации и

i) организация непрерывного контроля информационной безопасности и внесение необходимых корректировок.

3.2.2 Информация

Информация является тем активом, который жизненно важен для эффективной хозяйственной деятельности организации и потому подлежит защите должным образом. Информация может храниться в различных формах, в том числе в цифровой (например, в виде файлов на электронных или оптических носителях), материальной (как на бумаге), а также в нематериальной форме в виде знаний специалистов. Информация может передаваться самыми разными способами, включая доставку курьером, электронную связь и устное общение. Однако независимо от формы и способа передачи информация всегда нуждается в соответствующей защите.

Во многих организациях информация зависит от уровня развития информационных технологий и существующих систем передачи данных, которые часто являются жизненно важным компонентом организации, помогающим эффективно формировать, обрабатывать, хранить, передавать, защищать и аннулировать информацию.

3.2.3 Защита информации

Информационная безопасность имеет три основных измерения: конфиденциальность, доступность и целостность. Защита информации – это применение и координирование соответствующих мер безопасности, которые требуют учёта широкого спектра потенциальных угроз с целью обеспечения успешной бесперебойной хозяйственной деятельности и минимизации неблагоприятного влияния инцидентов информационной безопасности.

Информационная безопасность достигается посредством внедрения целого комплекса методов управления, выбираемых в процессе анализа рисков и реализуемых с помощью СОИБ, включая разнообразные стратегии, технологии, процедуры, организационные структуры и программно-аппаратные средства защиты определённых информационных активов. Эти методы управления нуждаются в чётком определении, эффективной реализации, текущем контроле, регулярном пересмотре и при необходимости – в надлежащем усовершенствовании – для создания надёжной защиты важной информации и успешного достижения организацией поставленных целей. При этом предполагается, что соответствующие средства обеспечения информационной безопасности тесно связаны и согласованы с технологическими процессами организации.

3.2.4 Функции управления

Процесс управления – это совокупность действий по координации, контролю и постоянному улучшению хозяйственной деятельности организации в рамках соответствующих структур. Управленческие операции включают в себя управляющие воздействия, реализацию определённого стиля руководства, мероприятия организационного характера, обработку информации, регулирование, диспетчерское управление и контроль над ресурсами. Управленческие структуры могут насчитывать в своём составе от одного человека (в мелких организациях) до многочисленного штата управленцев, связанных иерархической схемой подчинения, характерной для крупных организаций.

В среде СОИБ управление представляет собой диспетчерский контроль и выработку эффективных решений, необходимых для уверенного достижения поставленных целей хозяйственной деятельности, благодаря надёжной защите информационных активов организации. Управление защитой информации реализуется через формулирование и использование стратегий обеспечения информационной безопасности, адекватных рабочих процедур и руководящих принципов, которые затем становятся обязательными в масштабах всей организации для всех субъектов, ассоциируемых с данной организацией.

3.2.5 Система управления

В системе управления для достижения целей организации используется некоторая совокупность ресурсов. Компонентами такой системы являются организационная структура, принятые стратегии, операции планирования, сферы ответственности, инструкции по эксплуатации, рабочие процедуры, технологические процессы и используемые ресурсы.

В аспекте информационной безопасности система управления позволяет организации:

a) удовлетворять требования к защите информации, выдвигаемые клиентами, заказчиками и другими заинтересованными сторонами;

b) совершенствовать процедуры планирования и выработки управляющих воздействий;

c) успешно достигать устанавливаемых целей обеспечения информационной безопасности;

d) обеспечивать соответствие нормативным документам, действующему законодательству и отраслевым требованиям;

e) организованно управлять информационными активами, что облегчает непрерывное усовершенствование методов управления и их адаптацию к текущим целевым установкам организации.

3.3 Технологический подход

Организации нуждаются в идентификации и упорядочении множества операций, обеспечивающих эффективное и результативное функционирование. Любые операции, при выполнении которых используются те или иные ресурсы, требуют адекватного регулирования с целью преобразования входов в выходы путём совершения цепочки взаимосвязанных действий, которая называется технологическим процессом. Выход одного процесса может становиться входом для другого, и обычно такое преобразование выполняется в соответствии с некоторым планом в контролируемых условиях. Применение системы чётко определённых взаимосвязанных процессов в рамках организации в сочетании с методами их идентификации и регулирования можно определить как “технологический подход”.

3.4 Важная роль СОИБ

Риски, связанные с информационными активами организации, требуют постоянного внимания. Для обеспечения надлежащего уровня информационной безопасности необходимо адекватное

управление рисками, которые порождаются угрозами физического, социального и технологического характера и ассоциируются с любыми формами представления информации создаваемой или используемой в рамках организации.

Считается, что решение о создании СОИБ является стратегическим решением организации, а потому необходимо, чтобы такое решение реализовывалось постепенно, взвешенно и сообразно с конкретными нуждами организации.

Проектирование и внедрение СОИБ диктуется нуждами и целями организации и осуществляется с учётом требований к защите информации, особенностей процесса хозяйственной деятельности организации, её масштаба и структуры. Проект и функциональные возможности СОИБ должны отражать интересы и требования к защите информации, выражаемые всеми сотрудничающими сторонами: заказчиками, поставщиками, деловыми партнёрами, акционерами и ожидаемыми третьими сторонами.

В современном мире с его тесными взаимосвязями разных стран информация и относящиеся к ней процессы, системы и сети составляют важнейшие активы бизнеса. Организации, как и их информационные системы и сети, подвергаются опасностям нарушения защиты под воздействием множества источников угроз, таких как компьютерное мошенничество, шпионаж, саботаж, вандализм и стихийные бедствия (например, пожар и наводнение). Ущерб, наносимый информационным системам и сетям вредоносными программами, злоумышленными действиями хакеров и атаками типа отказа в обслуживании становятся всё более привычными, претенциозными и изощрёнными.

Роль СОИБ одинаково важна как в государственном, так и в частном секторе экономики. В любой отрасли промышленности СОИБ служит стимулирующим фактором развития электронного бизнеса и жизненно важна для решения задачи управления рисками. Взаимосвязь между общедоступными и частными сетями и совместное использование информационных активов затрудняют организацию защищенного доступа к информации и её обработку. Кроме того, эффективность традиционных методов контроля и управления может снижаться из-за широкого распространения мобильных запоминающих устройств, хранящих информационные активы. Когда организации принимают на вооружение семейство стандартов СОИБ, они получают возможность реализации общепризнанных принципов обеспечения информационной безопасности и могут наглядно демонстрировать их своим деловым партнёрам и другим заинтересованным сторонам.

При разработке информационных систем аспекты защиты информации принимаются во внимание далеко не всегда, и зачастую информационная безопасность понимается как чисто техническое решение. Однако в действительности возможности обеспечения информационной безопасности одними лишь техническими средствами сильно ограничены и могут оказаться неэффективными без поддержки соответствующими технологическими процедурами и управленческими решениями в рамках СОИБ. Встраивание функций обеспечения безопасности в уже действующую информационную систему может оказаться делом обременительным и дорогостоящим; в отличие от этого, в процессе создания СОИБ проводится идентификация уже имеющихся средств управления и прорабатываются вопросы детализированного планирования их использования. Например, средства управления доступом, которые могут быть техническими (логическими), физическими, административными (управленческими) или смешанными, позволяют гарантировать, что доступ к информационным активам авторизован и ограничен с учётом требований к защите бизнес-процессов и информации.

Успешное внедрение СОИБ играет важную роль в обеспечении информационной безопасности информационных активов, поскольку организация получает возможность:

a) обрести большую уверенность в том, что её информационные активы в любое время надёжно защищены от потенциальных угроз;

b) создать полнофункциональную структурированную основу для идентификации и оценки рисков информационной безопасности, выбора и использования применимых средств управления, а также измерения и улучшения показателей их эффективности;

c) постоянно улучшать используемые средства управления и

d) успешно достигать соответствия правовым и нормативным требованиям.

3.5 Внедрение, текущий контроль, техническая поддержка и развитие СОИБ

3.5.1 Общий обзор

Для реализации собственной СОИБ организации необходимо предпринять перечисленные ниже шаги по внедрению, контролю, поддержке и дальнейшему совершенствованию системы:

a) выявить имеющиеся информационные активы и связанные с ними требования к защите информации (см. 3.5.2);

b) оценить риски информационной безопасности (см. 3.5.3) и произвести их обработку (см. 3.5.4);

c) выбрать и внедрить адекватные средства преодоления неприемлемых рисков (см. 3.5.5);

d) проконтролировать, обеспечить технической поддержкой и повысить эффективность средств и методов управления, ассоциируемых с информационными активами организации (см. 3.5.6).

Для получения уверенности в том, что СОИБ постоянно обеспечивает эффективную защиту информационных активов организации, требуется, чтобы шаги (a) – (d) регулярно повторялись с целью выявления изменений в оценках рисков, принятых организацией стратегиях или в целевых установках её хозяйственной деятельности.

3.5.2 Выявление требований к защите информации

В рамках общей стратегии и целей организации и в зависимости от её масштабов и территориальной протяжённости требования к защите информации могут быть определены путём осмысления следующих факторов:

a) идентифицированных информационных активов и их ценности;

b) потребностей бизнеса в обработке информации, её хранении и передаче и

c) юридических, регулятивных и контрактных требований.

Проведение методической оценки рисков, ассоциируемых с информационными активами, должно предусматривать анализ потенциальных угроз, которым они подвержены; слабых мест (уязвимостей) информационных активов в случае материализации конкретной угрозы и возможного негативного влияния любого инцидента в системе защиты информации на информационные активы. Считается, что расходы организации на создание надлежащих средств управления рисками должны быть пропорциональны возможным потерям бизнеса в случае материализации конкретного риска.

3.5.3 Оценка рисков информационной безопасности

Для управления рисками информационной безопасности необходимо иметь адекватный метод их оценивания и обработки, в котором определялись бы затраты и выгоды, юридические требования, точки зрения заинтересованных сторон и другие имеющие отношение к делу входные воздействия и контролируемые переменные.

При оценивании рисков должно осуществляться их выявление, представление в количественной форме и упорядочение по критериям приемлемости с учётом релевантных целей организации. По результатам этих операций должны быть выработаны рекомендации относительно надлежащих управляющих воздействий, а также приоритетов управления рисками информационной

безопасности и реализации средств и методов управления, призванных защитить организацию от негативного воздействия этих рисков.

Оценивание рисков должно выполняться с использованием систематического метода определения их величины (на этапе анализа рисков) и процедуры сравнения оцениваемых рисков по критерию их значимости (на этапе оценки рисков).

Процедуры оценивания рисков должны выполняться регулярно с целью обнаружения изменений в требованиях к защите информации и в картине опасных ситуаций, то есть в активах, угрозах, уязвимостях, факторах влияния, оценках рисков, а также в тех случаях, когда происходят существенные общие изменения. Получаемые оценки рисков должны вырабатываться в рамках методического подхода, который способен давать сопоставимые и воспроизводимые результаты.

Для обеспечения надлежащей эффективности задача оценки рисков информационной безопасности должна иметь чётко определённые границы и, если это уместно, обеспечивать возможность сопоставления с масштабами рисков в других областях деятельности организации.

ISO/IEC 27005 содержит в себе руководство по управлению рисками информационной безопасности, включая рекомендации по оценке рисков, их обработке, определению приемлемости, регистрации, текущему контролю, анализу и пересмотру. В этот стандарт включены также примеры методологий оценки рисков.

3.5.4 Обработка рисков информационной безопасности

До начала обработки того или иного риска организация должна установить соответствующие критерии для определения приемлемости или неприемлемости существующего риска. Риски могут быть приемлемыми, например, в том случае, если они оцениваются как низкие или прогнозируемые затраты на их обработку превышают получаемые организацией выгоды от их преодоления; решения о приемлемости рисков подлежат регистрации.

По каждому риску, выявленному на этапе оценки, должно быть принято решение относительно метода его обработки. Здесь возможны следующие варианты:

a) применение адекватных средств контроля и управления, обеспечивающих снижение рисков;

b) осознанное и беспристрастное принятие рисков при условии, что они полностью удовлетворяют принятой организацией стратегии управления рисками и критериям их приемлемости;

c) исключение рисков путём запрета действий, приводящих к их возникновению;

d) разделение тех или иных рисков с другими заинтересованными сторонами: например, со страховщиками или поставщиками.

Применительно к тем рискам, по которым принято решение, предписывающее их обработку, должны быть выбраны и реализованы соответствующие методы и средства управления.

3.5.5 Отбор и реализация средств управления рисками

Как только установлены требования к информационной безопасности (см. 3.5.2), определены и оценены её риски, относящиеся к идентифицированным информационным активам (см. 3.5.3) и приняты решения относительно обработки рисков информационной безопасности (см. 3.5.4), осуществляется отбор и внедрение соответствующих средств снижения рисков.

Применение таких средств должно обеспечивать снижение рисков до приемлемого уровня с учётом следующих факторов:

a) требований и ограничений национального и международного законодательства и действующих нормативов;

b) целей организации;

c) эксплуатационных требований и ограничений;

d) стоимости реализации и эксплуатации средств управления, обеспечивающих снижение рисков соразмерно с требованиями и ограничениями организации;

e) необходимости текущего контроля и повышения эффективности и результативности средств защиты информации для обеспечения успешного достижения целей организации; при этом для удовлетворения требований соответствия процесс выбора и реализации средств управления подлежит документированию в форме заявления о применении;

f) необходимости балансирования затрат на внедрение и использование средств управления рисками и вероятных потерь, которые могут возникнуть при инцидентах информационной безопасности.

Средства управления, представленные в ISO/IEC 27002, признаны большинством организаций лучшими достижениями сложившейся практики и хорошо приспособлены для реализации в рамках организаций разных масштабов и разной степени сложности. Другие стандарты семейства ISMS содержат рекомендации по выбору и применению средств ISO/IEC 27002 в системе управления информационной безопасностью.

Средства управления для защиты информации должны рассматриваться в системных проектах уже на этапе разработки технического задания. Невыполнение этого условия может привести к неоправданным дополнительным затратам и менее эффективным техническим решениям, а в худшем случае – вообще к невозможности достижения адекватного уровня безопасности. Необходимые средства управления могут выбираться из ISO/IEC 27002 или из других наборов элементов управления; возможно также проектирование новых наборов управления специально для нужд конкретной организации. При этом следует понимать, что универсальных наборов, применимых в любой информационной системе или среде, не существует, и что средства, пригодные для использования в одной организации, могут совсем не подходить для другой.

Следует также иметь в виду, что никакие наборы средств управления не способны обеспечить стопроцентную защиту информации. Для достижения конкретных целей организации в этой части необходимо осуществление дополнительных управленческих действий по текущему контролю, оценке и повышению эффективности используемых средств обеспечения информационной безопасности.

Выбор и реализация средств управления подлежат документированию в форме официального “Заявления о применении”, в котором отмечается соответствие различным техническим требованиям.

3.5.6 Контроль, поддержание и повышение эффективности СОИБ

Организация нуждается в поддержании и усовершенствовании своей СОИБ посредством текущего контроля и оценки эффективности системы в рамках принятых стратегий и целей, а также в формировании отчётов по достигнутым результатам для анализа их управленческим персоналом. Такой анализ СОИБ проводится с целью проверки, имеются ли в этой системе конкретные элементы управления, которые способны обеспечить обработку рисков в рамках сферы её применения. Кроме того, на основе накопленных регистрационных записей по контролируемым сферам в системе должна содержаться информация, свидетельствующая о процедурах верификации и о действиях по отслеживанию, корректировке и снижению рисков.

3.5.7 Постоянное улучшение

Цель постоянного развития СОИБ состоит в том, чтобы увеличить вероятность достижения целей организации в части сохранения конфиденциальности, готовности и целостности информации; при этом в центре внимания должен находиться поиск дополнительных возможностей совершенствования системы – без упования на то, что существующие операции управления уже достаточно хороши или что они являются пределом возможностей.

Работа по усовершенствованию СОИБ включает в себя следующие действия:

a) анализ и оценку существующего положения дел определения возможных направлений развития;

b) установление целей и задач развития;

c) поиск возможных технических решений, способствующих достижению поставленных целей;

d) сравнительную оценку решений и обоснованный выбор;

e) реализацию выбранного решения;

f) измерение, верификацию, анализ и оценку результатов внедрения для подтверждения факта достижения поставленных целей;

g) формализацию изменений.

Результаты при необходимости анализируются для определения дальнейших возможных улучшений, то есть усовершенствование становится непрерывным процессом, поскольку соответствующие действия периодически повторяются. Поиск новых возможностей развития может также осуществляться на основе обратной связи с клиентами и другими заинтересованными сторонами, результатов аудиторских проверок и результатов анализа функционирования системы обеспечения информационной безопасности.

3.6 Критические факторы успеха СОИБ

Успех внедрения СОИБ для достижения организацией поставленных целей хозяйственной деятельности определяется множеством критических факторов, к которым относятся:

a) политика в сфере информационной безопасности, целевых установок и методов достижения поставленных целей;

b) методы и инфраструктура для проектирования, внедрения, технической поддержки и усовершенствования средств обеспечения информационной безопасности, совместимых с организационной культурой;

c) реальная поддержка и конкретные обязательства всех уровней управления и особенно – высшего руководства;

d) изучение потребностей в защите информационных активов на основе использования системы управления рисками информационной безопасности (см. ISO/IEC 27005);

e) программа обучения и повышения квалификации в области эффективной защиты информации, нацеленная на информирование всех сотрудников и партнёров об их обязанностях в этой сфере в рамках принятых стратегий обеспечения информационной безопасности, нормативных требований и других аналогичных документов, а также на мотивацию их адекватного поведения;

f) эффективная технология управления инцидентами информационной безопасности;

g) эффективные методы обеспечения непрерывности хозяйственной деятельности и

h) измерительная система для оценки эффективности системы информационной безопасности и получения информации обратной связи с целью выработки решений по развитию СОИБ.

Наличие действующей СОИБ увеличивает вероятность того, что организация будет последовательно добиваться успеха в защите своих информационных активов.

3.7 Выгоды, обеспечиваемые использованием стандартов семейства ISMS

Выгоды от использования семейства стандартов ISMS заключаются, прежде всего, в снижении рисков информационной безопасности (то есть в уменьшении вероятности инцидентов и/или их негативных последствий). В других аспектах преимущества, получаемые организацией в результате успешной реализации концепций, представленных в стандартах этого семейства, обеспечивают:

a) структурированную методологию выполнения процессов определения, реализации, использования и поддержки высокоэффективной многофункциональной, создающей добавленную стоимость, интегрированной и хорошо сбалансированной системы информационной безопасности, которая полностью отвечает нуждам организации во всех сферах её деятельности и во всех подразделениях;

b) помощь управленческому персоналу в достижении понимания и ответственном исполнении своей собственной роли в обеспечении информационной безопасности в контексте управления корпоративными рисками и эффективных методов руководства, включая профессиональное обучение и повышение квалификации как владельцев бизнеса, так и владельцев системы в части всестороннего обеспечения информационной безопасности;

c) внедрение лучших мировых достижений сложившейся практики защиты информации не в приказном порядке, дающее организациям возможность самостоятельно адаптировать и совершенствовать нужные им средства управления, которые лучше всего подходят для их специфических условий, и эффективно развивать достигнутый успех в предвидении внутренних и внешних изменений;

d) предоставление общего языка и концептуальной основы для защиты информации, что способствует установлению доверительных отношений между деловыми партнёрами с помощью СОИБ, особенно в тех случаях, когда требуется аттестация по ISO/IEC 27001 уполномоченным органом сертификации;

e) укрепление доверия к организации со стороны участников совместной деятельности;

f) удовлетворение текущих и ожидаемых социальных нужд и

g) более эффективное управление капиталовложениями в сферу обеспечения информационной безопасности.

4 Семейство стандартов ISMS

4.1 Общие сведения

Семейство стандартов ISMS – это система взаимосвязанных стандартов, уже опубликованных или находящихся в процессе разработки, содержащая в своём составе целый ряд важных структурных компонентов. В этих структурных компонентах основное внимание сосредоточено на нормативных положениях, описывающих требования к СОИБ (ISO/IEC 27001), и на требованиях к органам сертификации (ISO/IEC 27006), подтверждающим соответствие этой системы стандарту ISO/IEC 27001. Другие стандарты этого семейства предоставляют руководство по различным аспектам реализации СОИБ, описывают этот процесс в целом, содержат руководящие указания по системам управления и по специфическим функциям различных подразделений.

Взаимосвязи между стандартами семейства ISMS[1)] отображены на Рисунке 1.

---

1) Информацию о любом стандарте, находящемся в стадии разработки или пересмотра, можно получить по адресу http://www.iso.org/iso/home.html, посредством поиска интересующего стандарта.

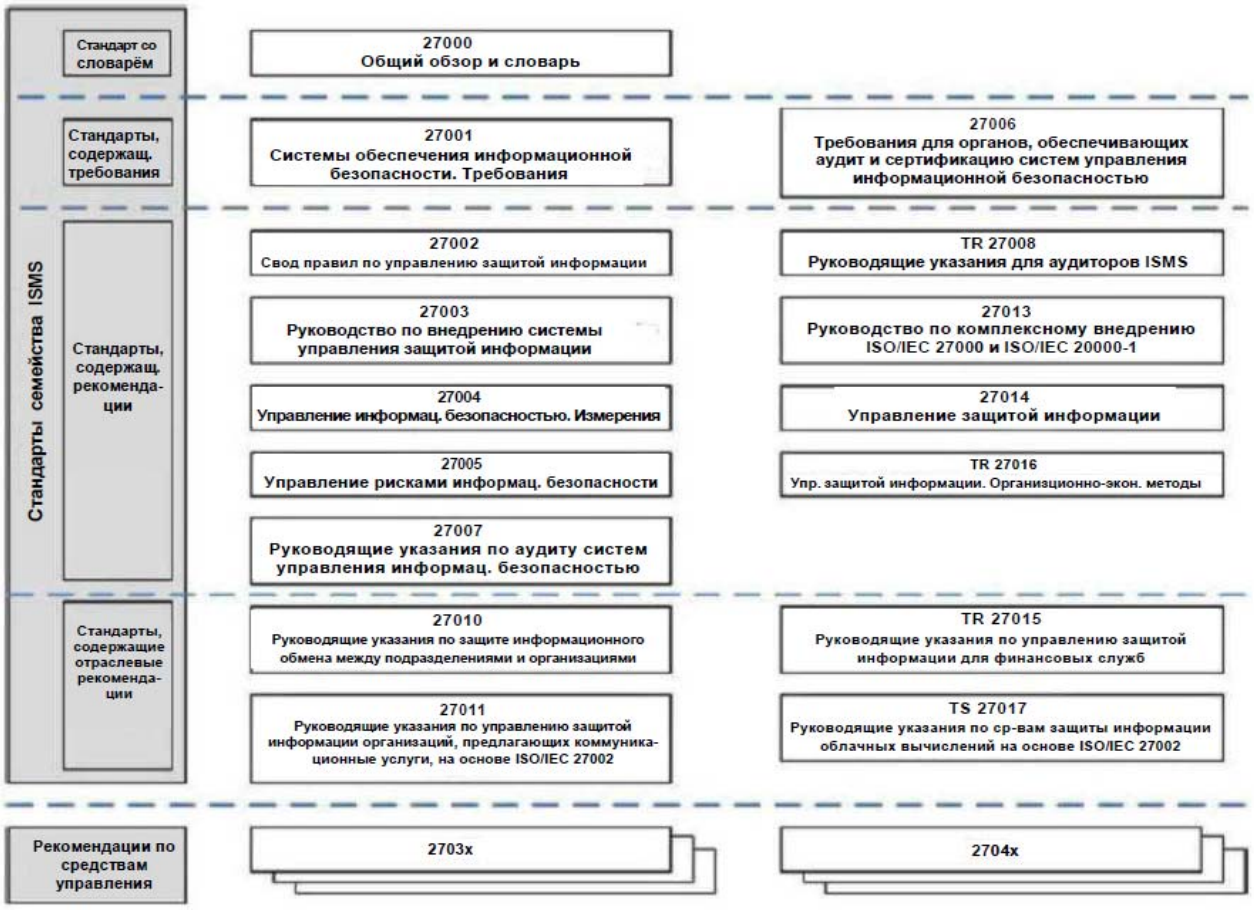

Рисунок 1 — Взаимосвязи стандартов семейства ISMS

Каждый из перечисленных стандартов семейства ISMS описывается ниже с указанием его типа (или роли) и ссылочного номера. Описания распределены по разделам следующим образом:

a) стандарты, дающие общий обзор и используемую терминологию (см. 4.2);

b) стандарты, определяющие требования (см. 4.3);

c) стандарты, содержащие руководящие указания общего характера (см. 4.4);

d) стандарты, содержащие руководящие указания для подразделений организации (см. 4.5).

4.2 Стандарты, дающие общий обзор и используемую терминологию

4.2.1 ISO/IEC 27000 (настоящий документ)

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

Область применения: этот международный стандарт предоставляет организациям и отдельным лицам:

a) общий обзор семейства стандартов ISMS;

b) общие сведения о системах обеспечения информационной безопасности (СОИБ) и

c) термины и определения, используемые в стандартах семейства ISMS.

Целевое назначение: в ISO/IEC 27000 излагаются основы систем обеспечения информационной безопасности, которые являются предметом рассмотрения в стандартах семейства ISMS, и определяются термины, относящиеся к этой предметной области.

4.3 Стандарты, определяющие требования

4.3.1 ISO/IEC 27001

Информационные технологии. Методы обеспечения защиты. Системы управления информационной безопасностью. Требования

Область применения: этот международный стандарт устанавливает требования к реализации, использованию, контролю, анализу, технической поддержке и усовершенствованию формализованной системы обеспечения информационной безопасности организации в контексте её хозяйственной деятельности в условиях существующих рисков предпринимательства. Стандарт определяет требования к внедрению средств и методов управления для защиты информации, адаптируемых к нуждам конкретных организаций или их подразделений, и может использоваться любыми организациями независимо от их типа, масштаба и характера.

Целевое назначение: ISO/IEC 27001 устанавливает нормативные требования к разработке и эксплуатации СОИБ, включая набор элементов управления для контроля и смягчения рисков, сопряжённых с информационными активами, которые организация стремится защитить с помощью своей СОИБ. Организации, использующие СОИБ, имеют возможность провести её аудит и аттестацию на предмет соответствия установленным требованиям. Для обеспечения такого соответствия в качестве элементов СОИБ должны быть выбраны надлежащие цели и средства управления согласно Приложению A ISO/IEC 27001. Необходимые цели и средства управления, перечисленные в Таблице A.1 того же стандарта, непосредственно определяются и согласуются на основе положений разделов с 5-го по 18-й ISO/IEC 27002.

4.3.2 ISO/IEC 27006

Информационные технологии. Методы обеспечения защиты. Требования для органов, обеспечивающих аудит и сертификацию систем управления информационной безопасностью

Область применения: этот стандарт определяет требования и руководящие указания (рекомендации) для органов, проводящих аудит и сертификацию СОИБ согласно ISO/IEC 27001, в дополнение к требованиям ISO/IEC 17021, и предназначен, в первую очередь, для поддержки аккредитации сертификационных органов, которые предоставляют услуги по сертификации СОИБ согласно ISO/IEC 27001.

Целевое назначение: ISO/IEC 27006 дополняет ISO/IEC 17021 в части требований, по которым производится аккредитация органов сертификации, что позволяет таким организациям выдавать сертификаты соответствия на постоянной основе, в соответствии с требованиями, установленными ISO/IEC 27001.

4.4 Стандарты, содержащие руководящие указания общего характера

4.4.1 ISO/IEC 27002

Информационные технологии. Методы обеспечения защиты. Свод правил по управлению защитой информации

Область применения: этот стандарт содержит список общепринятых целей управления и перечень лучших в сложившейся практике средств управления, которые служат эталонами при

выборе компонентов для реализации систем, позволяющих достичь необходимого уровня информационной безопасности.

Целевое назначение: ISO/IEC 27002 – это фактически руководство по внедрению средств обеспечения информационной безопасности. В нём в разделах от 5-го до 15-го даются конкретные рекомендации по внедрению и руководство по реализации лучших достижений сложившейся практики с использованием средств и методов управления, представленных в Разделах A.5 - A.18 ISO/IEC 27001.

4.4.2 ISO/IEC 27003

Информационные технологии. Методы обеспечения защиты. Руководство по внедрению системы управления информационной безопасностью

Область применения: этот международный стандарт содержит практическое руководство по внедрению и предоставляет дополнительную информацию для создания, внедрения, эксплуатации, контроля, анализа, поддержки и развития СОИБ в соответствии с ISO/IEC 27001.

Целевое назначение: в ISO/IEC 27003 представлен технологический подход, обеспечивающий успешное внедрение СОИБ в соответствии с ISO/IEC 27001.

4.4.3 ISO/IEC 27004

Информационные технологии. Методы обеспечения защиты. Управление информационной безопасностью. Измерения

Область применения: этот стандарт содержит руководство и рекомендации по разработке и использованию измерений для оценки эффективности СОИБ, целей управления и средств управления, используемых при внедрении систем защиты информации и обеспечении информационной безопасности согласно ISO/IEC 27001.

Целевое назначение: ISO/IEC 27004 определяет инфраструктуру системы измерений, позволяющую оценивать эффективность СОИБ в соответствии с ISO/IEC 27001.

4.4.4 ISO/IEC 27005

Информационные технологии. Методы обеспечения защиты. Управление рисками информационной безопасности

Область применения: этот международный стандарт содержит руководящие указания по управлению рисками информационной безопасности. Представленный в стандарте подход способствует реализации концепций, изложенных в ISO/IEC 27001.

Целевое назначение: ISO/IEC 27005 предоставляет руководство по реализации технологического подхода к управлению рисками - для обеспечения возможности полного выполнения требований к управлению рисками информационной безопасности, определённых в ISO/IEC 27001.

4.4.5 ISO/IEC 27007

Информационные технологии. Методы обеспечения защиты. Руководящие указания по аудиту систем управления информационной безопасностью

Область применения: этот международный стандарт содержит руководство по проведению аудита СОИБ, а также руководство по оценке компетентности аудиторов системы обеспечения информационной безопасности - в дополнение к тому руководству, которое представлено в ISO 19011, касающемся систем управления в целом.

Целевое назначение: руководство, представленное в ISO/IEC 27007, предназначается для организаций, которые нуждаются в проведении внутреннего или внешнего аудита СОИБ или в выполнении работы по программе проверки СОИБ на соответствие требованиям, установленным в ISO/IEC 27001.

4.4.6 ISO/IEC TR 27008

Информационные технологии. Методы обеспечения защиты. Руководящие указания для аудиторов по оценке средств управления систем обеспечения безопасности

Область применения: Этот технический отчёт содержит руководство по анализу результатов внедрения и использования средств управления, включая проверку соответствия средств информационной системы техническим требованиям согласно действующим стандартам организации, касающимся защиты информации.

Целевое назначение: в данном техническом отчёте основное внимание сосредоточено на анализе работы средств защиты информации и на проверке их соответствия техническим требованиям внутреннего стандарта организации, касающегося реализации системы обеспечения информационной безопасности. Отчёт не содержит никаких рекомендаций по проверке средств измерения, методов оценки рисков или процедур аудита СОИБ согласно ISO/IEC 27004, ISO/IEC 27005 или ISO/IEC 27007, соответственно. Данный технический отчёт не касается также аудиторских проверок автоматизированных систем управления в целом.

4.4.7 ISO/IEC 27013

Информационные технологии. Методы обеспечения защиты. Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1

Область применения: этот международный стандарт будет включать в себя руководство по комплексной реализации положений ISO/IEC 27001 и ISO/IEC 20000-1 организациями, которые намерены:

a) выполнить требования ISO/IEC 27001, когда соответствие ISO/IEC 20000-1 уже достигнуто, или при достигнутом соответствии требованиям ISO/IEC 27001 выполнить требования ISO/IEC 20000-1;

b) выполнить одновременно требования ISO/IEC 27001 и ISO/IEC 20000-1;

c) проверить существующие системы управления на соответствие ISO/IEC 27001 и ISO/IEC 20000-1.

Целевое назначение: оказать помощь организациям в более глубоком понимании характеристик, сходных черт и различий ISO/IEC 27001 и ISO/IEC 20000-1 применительно к задачам планирования и внедрения интегрированной системы управления, полностью соответствующей обоим указанным выше международным стандартам.

4.4.8 ISO/IEC 27014

Информационные технологии. Методы обеспечения защиты. Управление защитой информации

Область применения: в этом международном стандарте будут представлены руководящие материалы по принципам и процедурам управления защитой информации, с помощью которых организации смогут оценивать, направлять и контролировать деятельность по обеспечению информационной безопасности.

Целевое назначение: помощь организациям в надлежащей защите информации, что стало для них важнейшей задачей. В этом разрезе на деловую репутацию организации могут влиять не только постоянно ужесточаемые регулятивные требования, но и её способность или неспособность

к принятию эффективных мер информационной безопасности. Поэтому организации, чтобы гарантировать достижение своих целей, всё чаще обращаются к услугам контролирующих органов, в обязанности которых входит контроль систем защиты информации.

4.4.9 ISO/IEC TR 27016

Информационные технологии. Методы обеспечения защиты. Системы управления информационной безопасностью. Организационно-экономические вопросы

Область применения: этот технический отчёт содержит методологию, которая позволяет организациям лучше понять экономические аспекты точной оценки идентифицируемых информационных активов; определить цену связанных с ними потенциальных рисков; оценить добавленную стоимость, придаваемую этим активам средствами защиты информации, и определить оптимальный объём ресурсов, необходимый для защиты информационных активов.

Целевое назначение: данный отчёт является дополнением к стандартам семейства ISMS в части охвата экономических перспектив защиты информационных активов организации в контексте расширения социальной среды, в которой работает организация, и выдачи рекомендаций по применению организационно-экономических методов для решения задач информационной безопасности путём использования надлежащих моделей и лучших достижений сложившейся практики.

4.5 Стандарты, содержащие руководящие указания для подразделений организации

4.5.1 ISO/IEC 27010

Информационные технологии. Методы обеспечения защиты. Руководящие указания по обеспечению защиты информационного обмена между подразделениями и организациями

Область применения: этот международный стандарт содержит руководящие указания в дополнение к руководству, представленному в семействе стандартов ISO/IEC 27000 для реализации системы обеспечения информационной безопасности в рамках информационного обмена между сотрудничающими сообществами; дополнительно предоставляются средства управления и специальное руководство по вводу в действие, инструментальному оснащению, поддержке и усилению информационной безопасности операций передачи данных между организациями и между их подразделениями.

Целевое назначение: этот международный стандарт применим ко всем формам информационного обмена и совместного использования конфиденциальной информации, как общедоступной, так и личной; как национальной, так и международной; как в рамках одной и той же отрасли или сектора рынка, так и между отраслями или секторами. В частности, он может применяться к информационным обменам и совместному использованию информации, относящейся к формированию, поддержке и защите необходимой инфраструктуры на организационном или национальном уровне.

4.5.2 ISO/IEC 27011

Информационные технологии. Методы обеспечения защиты. Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002

Область применения: этот международный стандарт содержит руководящие указания по реализации управления защитой информации в организациях, предоставляющих телекоммуникационные услуги.

Целевое назначение: ISO/IEC 27011 предоставляет телекоммуникационным организациям уникальный для этой отрасли пакет рекомендаций на основе ISO/IEC 27002, дополняющий руководство по выполнению требований, изложенных в Приложении A ISO/IEC 27001.

4.5.3 ISO/IEC TR 27015

Информационные технологии. Методы обеспечения защиты. Руководящие указания по управлению защитой информации для финансовых служб

Область применения: этот технический отчёт содержит рекомендации, которые дополняют руководство, предложенное в стандартах семейства ISO/IEC 27000, и касаются ввода в действие, инструментального оснащения, поддержки и усиления информационной безопасности организаций, предоставляющих финансовые услуги.

Целевое назначение: этот технический отчёт является специальным дополнением к ISO/IEC 27001 и ISO/IEC 27002, которое предназначено для использования организациями, предоставляющими финансовые услуги, в следующих видах деятельности:

a) при вводе в действие, инструментальном оснащении, поддержке и развитии системы управления защитой информации на основе ISO/IEC 27001:2005;

b) при проектировании и реализации средств управления, определённых в ISO/IEC 27002:2005 или в рамках настоящего международного стандарта.

4.5.4 ISO 27799

Информатика в здравоохранении. Управление информационной безопасностью по ISO/IEC 27002

Область применения: Этот международный стандарт содержит руководящие указания по реализации управления защитой информации в организациях здравоохранения.

Целевое назначение: ISO/IEC 27799 предоставляет организациям здравоохранения уникальный для этой отрасли пакет рекомендаций на основе ISO/IEC 27002, дополняющий руководство по выполнению требований, изложенных в Приложении A ISO/IEC 27001

Приложение A
(информативное)

Глагольные формы для выражения формулируемых положений

Каждый из документов семейства стандартов ISMS сам по себе не накладывает на пользователя никаких обязательств по его исполнению. Однако такие обязательства могут налагаться, например, законодательством или условиями контракта. Чтобы иметь возможность декларирования соответствия нормативным документам, пользователю стандарта нужно выделять требования, которые подлежат обязательному выполнению, и отличать эти требования от рекомендаций, которые дают определённую свободу выбора.

Приведённая ниже таблица поясняет, каким образом словесные выражения положений стандартов семейства ISMS должны дифференцироваться как требования или как рекомендации.

Таблица построена на основе положений Приложения H второй части Директив ISO/IEC *Правила структурирования и подготовки проектов международных стандартов*

ПОКАЗАТЕЛЬ	ПОЯСНЕНИЕ
Требование	английские глаголы “shall” (должен) и “shall not” (не должен) указывают на требование, которое необходимо строго выполнять для обеспечения соответствия конкретному документу и которое не допускает никаких отклонений
Рекомендация	английские глаголы “should” (следует) и “should not” (не следует) указывают на то, что среди нескольких возможностей рекомендуется одна как наиболее подходящая, но не исключающая использование других; или что определённый способ действий предпочтителен, но не обязателен; или что (при отрицательной форме глагола) конкретная возможность либо определённый способ действий не рекомендуется, однако не запрещается
Разрешение	английские глаголы “may” (может, допускается, разрешается) и “need not” (не должен) указывают на способ действий, который разрешён в пределах, оговорённых в документе
Возможность	английские глаголы “can” и “cannot” указывают на возможность или невозможность чего-либо

Приложение B
(информативное)

Указатель терминов

B.1 Принадлежность терминов

В рамках семейства стандартов ISO/IEC 27000 **владельцем термина** считается тот стандарт, в котором этот термин определён изначально; **владелец термина** “отвечает” за сопровождение его определения, то есть

— за представление,

— за пересмотр,

— за обновление и

— за изъятие.

ПРИМЕЧАНИЕ 1 ISO/IEC 27000 сам никогда не определяется как владелец терминов.

ПРИМЕЧАНИЕ 2 ISO/IEC 27001 и ISO/IEC 27006, как нормирующие стандарты (то есть содержащие требования), всегда являются превалирующими владельцами терминов.

B.2 Распределение терминов по стандартам

B.2.1 ISO/IEC 27001

аудит (audit)	2.5	измерение (measurement)	2.48
готовность (availability)	2.9	текущий контроль (monitoring)	2.52
компетентность (competence)	2.11	несоответствие (non-conformity)	2.53
конфиденциальность (confidentiality)	2.12	цель, целевая установка (objective)	2.56
соответствие (conformity)	2.13	организация (organization)	2.57
непрерывное улучшение (continual improvement)	2.15	использовать аутсорсинг [outsource]	2.58
средство управления (control)	2.16	эксплуатационные показатели (performance)	2.59
корректировка (correction)	2.18	стратегия, политика (policy)	2.60
корректирующее воздействие (corrective action)	2.19	процесс (process)	2.61
документированная информация (documented information)	2.23	требование (requirement)	2.63
эффективность (effectiveness)	2.24	анализ (review)	2.65
защита информации (information security)	2.33	риск (risk)	2.68
целостность (integrity)	2.40	владелец риска (risk owner)	2.78
заинтересованная сторона (interested party)	2.41	высшее руководство (top management)	2.84
система управления (management system)	2.46		

B.2.2 ISO/IEC 27002

управление доступом (access control)	2.1	событие информационной безопасности (information security event)	2.35
атака (attack)	2.3	инцидент информационной безопасности (information security incident)	2.36
аутентификация (authentication)	2.7	управление событиями информационной безопасности (information security incident management)	2.37
аутентичность (authenticity)	2.8	информационная система (information system)	2.39
цель управления (control objective)	2.17	неотказуемость (non-repudiation)	2.54
средства обработки информации (information processing facilities)	2.32	надёжность (reliability)	2.62
постоянство защиты информации (information security continuity)	2.34		

B.2.3 ISO/IEC 27003

проект СОИБ (ISMS project)	2.43

B.2.4 ISO/IEC 27004

аналитическая модель (analytical model)	2.2	измерительная функция (measurement function)	2.49
атрибут (attribute)	2.4	метод измерения (measurement method)	2.50
базовая мера (base measure)	2.10	результаты измерений (measurement results)	2.51
данные (data)	2.20	объект (object)	2.55
критерии принятия решений (decision criteria)	2.21	оценочная шкала (scale)	2.80
производная мера (derived measure)	2.22	единица измерения (unit of measurement)	2.86
показатель (indicator)	2.30	валидация (validation)	2.87
информационная потребность (information need)	2.31	верификация (verification)	2.88
мера (measure)	2.47		

B.2.5 ISO/IEC 27005

последствие (consequence)	2.14	взаимодействие и консультации по вопросам рисков (risk communication and consultation)	2.72
событие (event)	2.25	критерии рисков (risk criteria)	2.73
внешняя обстановка (external context)	2.27	сравнительная оценка риска (risk evaluation)	2.74

внутренний контекст (internal context)	2.42	идентификация рисков (risk identification)	2.75
уровень риска (level of risk)	2.44	управление рисками (risk management)	2.76
правдоподобие (likelihood)	2.45	процесс управления рисками (risk management process)	2.77
остаточный риск (residual risk)	2.64	обработка рисков (risk treatment)	2.79
принятие риска (risk acceptance)	2.69	угроза (threat)	2.83
анализ рисков (risk analysis)	2.70	уязвимость (vulnerability)	2.89
оценка рисков (risk assessment)	2.71		

B.2.6 ISO/IEC 27006

сертификат (certificate)	маркировка (mark)
орган сертификации (certification body)	организация (organization)
документ сертификации (certification document)	

B.2.7 ISO/IEC 27007

объём аудита (audit scope)	2.6

B.2.8 ISO/IEC TR 27008

объект анализа (review object)	2.66	стандарт обеспечения безопасности (security implementation standard)	2.81
цель анализа (review objective)	2.67		

B.2.9 ISO/IEC 27010

сообщество пользователей общей информации (information sharing community)	2.38	доверенная сторона передачи информации (trusted information communication entity)	2.85

B.2.10 ISO/IEC 27011

совместное размещение (collocation)	телекоммуникационные средства (telecommunications facilities)
узел связи (communication centre)	телекоммуникационные организации (telecommunications organizations)
важнейшие коммуникации (essential communications)	телекоммуникационные записи (telecommunication records)
неразглашение информации о соединениях (non-disclosure of communications)	телекоммуникационные услуги (telecommunications services)
персональная информация (personal information)	клиент телекоммуникационных служб (telecommunications service customer)
приоритетный вызов (priority call)	пользователь телекоммуникационных услуг (telecommunications service user)
телекоммуникационные приложения (telecommunications applications)	терминальное оборудование (terminal facilities)

телекоммуникационный бизнес (telecommunications business)	пользователь (user)
телекоммуникационная аппаратная (telecommunications equipment room)	

B.2.11 ISO/IEC 27014

высшее исполнительное руководство (executive management)	2.26	руководящий орган (governing body)	2.29
система управления защитой информации (governance of information security)	2.28	заинтересованная сторона (stakeholder)	2.82

B.2.12 ISO/IEC TR 27015

финансовые услуги (financial services)

B.2.13 ISO/IEC TR 27016

ожидаемые потери в годовом выражении (annualized loss expectancy ALE)	потеря, утрата (loss)
прямое значение (direct value)	рыночная стоимость (market value)
технико-экономическое сравнение (economic comparison)	чистая приведённая стоимость (net present value)
экономический фактор (economic factor)	выгода не экономического характера (non economic benefit)
экономическое обоснование (economic justification)	текущая стоимость (present value)
экономическая добавленная стоимость (economic value added)	цена возможности (opportunity cost)
экономика (economics)	стоимость возможности (opportunity value)
ожидаемое значение (expected value)	обязательные требования (regulatory requirements)
расширенное значение (extended value)	окупаемость затрат (return on investment)
опосредованная ценность (indirect value)	социальная ценность (societal value)
экономика защиты информации (information security economics)	значение (value)
управление защитой информации (information security management, ISM	рисковая стоимость (value-at-risk)

Библиография

[1] ISO/IEC 17021:2011, *Оценка соответствия. Требования к органам, обеспечивающим сертификацию и аудит систем управления*

[2] ISO 9000:2005, *Системы управления качеством. Основные положения и словарь*

[3] ISO 19011:2011, *Руководящие указания по аудиту систем управления*

[4] ISO/IEC 27001, *Информационные технологии. Методы обеспечения защиты. Системы управления информационной безопасностью. Требования*

[5] ISO/IEC 27002, *Информационные технологии. Методы обеспечения защиты. Свод правил по управлению защитой информации*

[6] ISO/IEC 27003:2010, *Информационные технологии. Методы обеспечения защиты. Руководство по внедрению системы управления информационной безопасностью*

[7] ISO/IEC 27004:2009, *Информационные технологии. Методы обеспечения защиты. Управление информационной безопасностью. Измерения*

[8] ISO/IEC 27005:2011, *Информационные технологии. Методы обеспечения защиты. Управление рисками информационной безопасности*

[9] ISO/IEC 27006:2011, *Информационные технологии. Методы обеспечения защиты. Требования для органов, обеспечивающих аудит и сертификацию систем управления информационной безопасностью*

[10] ISO/IEC 27007:2011, *Информационные технологии. Методы обеспечения защиты. Руководящие указания по аудиту систем управления информационной безопасностью*

[11] ISO/IEC TR 27008:2011, *Информационные технологии. Методы обеспечения защиты. Руководящие указания для аудиторов по оценке средств управления систем обеспечения безопасности*

[12] ISO/IEC 27010:2012, *Информационные технологии. Методы обеспечения защиты. Руководящие указания по обеспечению защиты информационного обмена между подразделениями и организациями*

[13] ISO/IEC 27011:2008, *Информационные технологии. Методы обеспечения защиты. Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002*

[14] ISO/IEC 27013:2012, *Информационные технологии. Методы обеспечения защиты. Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1*

[15] ISO/IEC 27014:2013, *Информационные технологии. Методы обеспечения защиты. Управление защитой информации*

[16] ISO/IEC TR 27015:2012, *Информационные технологии. Методы обеспечения защиты. Руководящие указания по управлению защитой информации для финансовых служб*

[17] ISO/IEC TR 27016:— [2)], *Информационные технологии. Методы обеспечения защиты. Управление защитой информации. Организационно-экономические методы*

[18] ISO 27799:2008, *Информатика в здравоохранении. Управление информационной безопасностью по ISO/IEC 27002*

---

2 Готовится к публикации.

[19] ISO/IEC Guide 73:2009, *Управление рисками. Словарь*

[20] ISO/IEC 15939:2007, *Технология программного обеспечения. Процесс измерения*

[21] ISO/IEC 20000-1, *Информационные технологии. Управление обслуживанием. Требования к системе управления обслуживанием.*

МКС 01.040.35; 35.040

Цена определяется из расчёта 31 страницы