ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53114— 2008

Защита информации

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Основные термины и определения

Издание официальное

БЗ 12—2008/544

Москва
Стандартинформ
2009

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации —ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»), Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл»)

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст

4 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2009

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
3.1 Общие понятия 2
3.2 Термины, относящиеся к объекту защиты информации 4
3.3 Термины, относящиеся к угрозам безопасности информации 7
3.4 Термины, относящиеся к менеджменту информационной безопасности организации 8
3.5 Термины, относящиеся к контролю и оценке информационной безопасности организации 8
3.6 Термины, относящиеся к средствам обеспечения информационной безопасности организации 9
Алфавитный указатель терминов 11
Приложение А (справочное) Термины и определения общетехнических понятий 13
Приложение Б (справочное) Взаимосвязь основных понятий в области обеспечения информационной безопасности в организации 15
Библиография 16

Введение

Установленные настоящим стандартом термины расположены в систематизированном порядке, отражающем систему понятий в данной области знания.

Для каждого понятия установлен один стандартизованный термин.

Наличие квадратных скобок в терминологической статье означает, что в нее входят два термина, имеющих общие терминоэлементы. В алфавитном указателе данные термины приведены отдельно.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации, при этом не входящая в круглые скобки часть термина образует его краткую форму. За стандартизованными терминами приведены отделенные точкой с запятой их краткие формы, представленные аббревиатурой.

Приведенные определения можно при необходимости изменять, вводя в них производные признаки, раскрывая значения используемых в них терминов, указывая объекты, входящие в объем определяемого понятия.

Изменения не должны нарушать объем и содержание понятий, определенных в настоящем стандарте.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы в тексте и в алфавитном указателе, в том числе аббревиатуры, — светлым, а синонимы — курсивом.

Термины и определения общетехнических понятий, необходимые для понимания текста основной части настоящего стандарта, приведены в приложении А.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Основные термины и определения

Protection of information. Information security provision in organization.
Basic terms and definitions

Дата введения — 2009—10—01

1 Область применения

Настоящий стандарт устанавливает основные термины, применяемые при проведении работ по стандартизации в области обеспечения информационной безопасности в организации.

Термины, установленные настоящим стандартом, рекомендуется использовать в нормативных документах, правовой, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

Настоящий стандарт применяется совместно с ГОСТ 34.003, ГОСТ 19781, ГОСТ Р 22.0.02, ГОСТ Р 51897, ГОСТ Р 50922, ГОСТ Р 51898, ГОСТ Р 52069.0, ГОСТ Р 51275, ГОСТ Р ИСО 9000, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 14001, ГОСТ Р ИСО/ МЭК 27001, ГОСТ Р ИСО/МЭК 13335-1, [1], [2].

Термины, приведенные в настоящем стандарте, соответствуют положениям Федерального Закона Российской Федерации от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» [3], Федерального Закона Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации» [4], Федерального Закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [5], Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 9 сентября 2000 г. Пр -1895 [6].

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ Р 22.0.02—94 Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий

ГОСТ Р ИСО 9000—2001 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 9001—2008 Системы менеджмента качества. Требования

ГОСТ Р ИСО 14001—2007 Системы экологического менеджмента. Требования и руководство по применению

ГОСТ Р ИСО/МЭК 13335-1—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения

ГОСТ Р 51275—2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51897—2002 Менеджмент риска. Термины и определения

Издание официальное

ГОСТ Р 51898—2003 Аспекты безопасности. Правила включения в стандарты

ГОСТ Р 52069.0—2003 Защита информации. Система стандартов. Основные положения

ГОСТ 34.003—90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ 19781—90 Обеспечение систем обработки информации программное. Термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

3.1 Общие понятия

3.1.1

безопасность информации [данных]: Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

[ГОСТ Р 50922—2006, пункт 2.4.5]

3.1.2

безопасность информационной технологии: Состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована.

[Р 50.1.056—2006, пункт 2.4.5]

3.1.3

информационная сфера: Совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

[Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. Пр-1895]

3.1.4 **информационная инфраструктура:** Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

3.1.5

объект информатизации: Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

[ГОСТ Р 51275—2006, пункт 3.1]

3.1.6 **активы организации:** Все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.

Примечание — К активам организации могут относиться:

- информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);
- ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие);
- процессы (технологические, информационные и пр.);
- выпускаемая продукция и/или оказываемые услуги.

3.1.7

ресурс системы обработки информации: Средство системы обработки информации, которое может быть выделено процессу обработки данных на определенный интервал времени.

Примечание — Основными ресурсами являются процессоры, области основной памяти, наборы данных, периферийные устройства, программы.

[ГОСТ 19781—90, пункт 93]

3.1.8 **информационный процесс:** Процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

3.1.9

информационная технология; ИТ: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

[Федеральный Закон Российской Федерации от 27 декабря 2002 г. №184-ФЗ, статья 2, пункт 2)]

3.1.10

техническое обеспечение автоматизированной системы; техническое обеспечение АС: Совокупность всех технических средств, используемых при функционировании АС.

[ГОСТ Р 34.003—90, пункт 2.5]

3.1.11

программное обеспечение автоматизированной системы; программное обеспечение АС: Совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС.

[ГОСТ Р 34.003—90, пункт 2.7]

3.1.12

информационное обеспечение автоматизированной системы; информационное обеспечение АС: Совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании.

[ГОСТ Р 34.003—90, пункт 2.8]

3.1.13 **услуга;** *сервис*: Результат деятельности исполнителя по удовлетворению потребности потребителя.

Примечание — В качестве исполнителя (потребителя) услуги может выступать организация, физическое лицо или процесс.

3.1.14 **услуги информационных технологий**; услуги ИТ: Совокупность функциональных возможностей информационных и, возможно, неинформационных технологий, предоставляемая конечным пользователям в качестве услуги.

Примечание — Примерами услуг ИТ могут служить передача сообщений, бизнес-приложения, сервисы файлов и печати, сетевые сервисы и т.д.

3.1.15 **критически важная система информационной инфраструктуры;** *ключевая система информационной инфраструктуры*; КСИИ: Информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом, или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой (в результате деструктивных информационных воздействий, а также сбоев или отказов) может привести к чрезвычайной ситуации со значительными негативными последствиями.

3.1.16 **критический объект:** Объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб.

Примечание — Ущерб может быть нанесен имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, а также выражаться в причинении вреда жизни или здоровью граждан.

3.1.17

информационная система персональных данных: Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

[Федеральный Закон Российской Федерации от 27 июля 2006 г. №152-ФЗ, статья 3, пункт 9)]

3.1.18

персональные данные: Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

[Федеральный Закон Российской Федерации от 27 июля 2006 г. №152-ФЗ, статья 3, пункт 1)]

3.1.19 **автоматизированная система в защищенном исполнении**; АС в защищенном исполнении: Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

3.2 Термины, относящиеся к объекту защиты информации

3.2.1 **информационная безопасность организации;** ИБ организации: Состояние защищенности интересов организации в условиях угроз в информационной сфере.

Примечание — Защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации.

3.2.2

объект защиты информации: Информация или носитель информации, или информационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации.

[ГОСТ Р 50922—2006, пункт 2.5.1]

3.2.3 **защищаемый процесс (информационной технологии):** Процесс, используемый в информационной технологии для обработки защищаемой информации с требуемым уровнем ее защищенности.

3.2.4 **нарушение информационной безопасности организации;** нарушение ИБ организации: Случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.

3.2.5

чрезвычайная ситуация; *непредвиденная ситуация*; ЧС: Обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Примечание — Различают чрезвычайные ситуации по характеру источника (природные, техногенные, биолого-социальные и военные) и по масштабам (локальные, местные, территориальные, региональные, федеральные и трансграничные).

[ГОСТ Р 22.0.02—94, статья 2.1.1]

3.2.6

опасная ситуация: Обстоятельства, в которых люди, имущество или окружающая среда подвергаются опасности.

[ГОСТ Р 51898—2003, пункт 3.6]

3.2.7

инцидент информационной безопасности: Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание — Инцидентами информационной безопасности являются:
- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

[ГОСТ Р ИСО/МЭК 27001—2006, статья 3.6]

3.2.8 **событие:** Возникновение или наличие определенной совокупности обстоятельств.

Примечания

1 Характер, вероятность и последствия события могут быть не полностью известны.

2 Событие может возникать один или несколько раз.

3 Вероятность, связанная с событием, может быть оценена.

4 Событие может состоять из невозникновения одного или нескольких обстоятельств.

5 Непредсказуемое событие иногда называют «инцидентом».

6 Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

3.2.9 **риск:** Влияние неопределенностей на процесс достижения поставленных целей.

Примечания

1 Цели могут иметь различные аспекты: финансовые, аспекты, связанные со здоровьем, безопасностью и внешней средой, и могут устанавливаться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта и процесса.

2 Риск часто характеризуется ссылкой на потенциальные события, последствия или их комбинацию, а также на то, как они могут влиять на достижение целей.

3 Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и их вероятности.

3.2.10

оценка риска: Процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку.

[ГОСТ Р ИСО/МЭК 13335-1—2006, пункт 2.21]

3.2.11 **оценка риска информационной безопасности (организации);** оценка риска ИБ (организации): Общий процесс идентификации, анализа и определения приемлемости уровня риска информационной безопасности организации.

3.2.12 **идентификация риска:** Процесс обнаружения, распознавания и описания рисков.

Примечания

1 Идентификация риска включает в себя идентификацию источников риска, событий и их причин, а также их возможных последствий.

2 Идентификация риска может включать в себя статистические данные, теоретический анализ, обоснованные точки зрения и экспертные заключения и потребности заинтересованных сторон.

3.2.13

анализ риска: Систематическое использование информации для определения источников риска и количественной оценки риска.

[ГОСТ Р ИСО/МЭК 27001—2006, статья 3.11]

3.2.14 **определение приемлемости уровня риска:** Процесс сравнения результатов анализа риска с критериями риска с целью определения приемлемости или допустимости уровня риска.

Примечание — Определение приемлемости уровня риска помогает принять решения об обработке риска.

3.2.15 **обработка риска информационной безопасности организации;** обработка риска ИБ организации: Процесс разработки и/или отбора и внедрения мер управления рисками информационной безопасности организации.

Примечания

1 Обработка риска может включать в себя:

- избежание риска путем принятия решения не начинать или не продолжать действия, создающие условия риска;
- поиск благоприятной возможности путем принятия решения начать или продолжать действия, могущие создать или увеличить риск;
- устранение источника риска;
- изменение характера и величины риска;
- изменение последствий;
- разделение риска с другой стороной или сторонами;
- сохранение риска как в результате сознательного решения, так и «по умолчанию».

2 Обработки риска с негативными последствиями иногда называют смягчением, устранением, предотвращением, снижением, подавлением и коррекцией риска.

3.2.16 **управление рисками**: Координированные действия по направлению и контролю над деятельностью организации в связи с рисками.

3.2.17 **источник риска информационной безопасности организации;** источник риска ИБ организации: Объект или действие, способное вызвать [создать] риск.

Примечания

1 Риск отсутствует при отсутствии взаимодействия объекта, лица или организации с источником риска.

2 Источник риска может быть материальным или нематериальным.

3.2.18 **политика информационной безопасности (организации);** политика ИБ (организации): Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Примечание — Политики должны содержать:

- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;
- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;
- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

3.2.19 **цель информационной безопасности (организации);** цель ИБ (организации): Заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации).

Примечание — Результатом обеспечения ИБ может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

3.2.20 **система документов по информационной безопасности в организации;** система документов по ИБ в организации: Объединенная целевой направленностью упорядоченная совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности.

3.3 Термины, относящиеся к угрозам безопасности информации

3.3.1 **угроза информационной безопасности организации;** угроза ИБ организации: Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Примечания

1 Формой реализации (проявления) угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств информационной безопасности объекта (ов) защиты организации.

2 Угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы.

3.3.2

угроза (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

[ГОСТ Р 50922—2006, пункт 2.6.1]

3.3.3 **модель угроз (безопасности информации):** Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Примечание — Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

3.3.4

уязвимость (информационной системы); *брешь*: Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Примечания

1 Условием реализации угрозы безопасности, обрабатываемой в системе информации, может быть недостаток или слабое место в информационной системе.

2 Если уязвимость соответствует угрозе, то существует риск.

[ГОСТ Р 50922—2006, пункт 2.6.4]

3.3.5 **нарушитель информационной безопасности организации;** нарушитель ИБ организации: Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

3.3.6 **несанкционированный доступ**: Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

Примечания

1 Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.

2 Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

3.3.7 **сетевая атака:** Действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы.

Примечание — Сетевой протокол — совокупность семантических и синтаксических правил, определяющих взаимодействие программ управления сетью, находящейся в одной ЭВМ, с одноименными программами, находящимися в другой ЭВМ.

3.3.8 **блокирование доступа (к информации):** Прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей).

3.3.9 **атака «отказ в обслуживании»:** Сетевая атака, приводящая к блокированию информационных процессов в автоматизированной системе.

3.3.10 **утечка информации:** Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.

3.3.11 **разглашение информации:** Несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.

3.3.12

перехват (информации): Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

[Р 50.1.053—2005, пункт 3.2.5]

3.3.13

информативный сигнал: Сигнал, по параметрам которого может быть определена защищаемая информация.

[Р 50.1.053—2005, пункт 3.2.6]

3.3.14 **недекларированные возможности:** Функциональные возможности средств вычислительной техники и программного обеспечения, не описанные или не соответствующие описанным в документации, которые могут привести к снижению или нарушению свойств безопасности информации.

3.3.15 **побочные электромагнитные излучения и наводки:** Электромагнитные излучения технических средств обработки информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

3.4 Термины, относящиеся к менеджменту информационной безопасности организации

3.4.1 **менеджмент информационной безопасности организации;** менеджмент ИБ организации: Скоординированные действия по руководству и управлению организацией в части обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации.

3.4.2 **менеджмент риска информационной безопасности организации;** менеджмент риска ИБ организации: Скоординированные действия по руководству и управлению организацией в отношении риска ИБ с целью его минимизации.

Примечание — Основными процессами менеджмента риска являются установление контекста, оценка риска, обработка и принятие риска, мониторинг и пересмотр риска.

3.4.3

система менеджмента информационной безопасности; СМИБ: Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Примечание — Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

[ГОСТ Р ИСО/МЭК 27001—2006, пункт 3.7]

3.4.4 **роль информационной безопасности в организации;** роль ИБ в организации: Совокупность определенных функций и задач обеспечения информационной безопасности организации, устанавливающих допустимое взаимодействие между субъектом и объектом в организации.

Примечания

1 К субъектам относятся лица из числа руководителей организации, ее персонал или инициируемые от их имени процессы по выполнению действий над объектами.

2 Объектами могут быть техническое, программное, программно-техническое средство, информационный ресурс, над которыми выполняются действия.

3.4.5 **служба информационной безопасности организации**: Организационно-техническая структура системы менеджмента информационной безопасности организации, реализующая решение определенной задачи, направленной на противодействие угрозам информационной безопасности организации.

3.5 Термины, относящиеся к контролю и оценке информационной безопасности организации

3.5.1 **контроль обеспечения информационной безопасности организации;** контроль обеспечения ИБ организации: Проверка соответствия обеспечения информационной безопасности в организации,

наличия и содержания документов требованиям нормативных документов, технической, правовой организационно-распорядительной документации в области информационной безопасности.

3.5.2 **мониторинг информационной безопасности организации;** мониторинг ИБ организации: Постоянное наблюдение за процессом обеспечения информационной безопасности в организации с целью установить его соответствие требованиям по информационной безопасности.

3.5.3 **аудит информационной безопасности организации;** аудит ИБ организации: Систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации.

3.5.4 **свидетельства (доказательства) аудита информационной безопасности организации;** свидетельства аудита ИБ организации: Записи, изложение фактов или другая информация, которые имеют отношение к критериям аудита информационной безопасности организации и могут быть проверены.

Примечание — Свидетельства аудита информационной безопасности могут быть качественными или количественными.

3.5.5 **оценка соответствия информационной безопасности организации установленным требованиям;** оценка соответствия ИБ организации установленным требованиям: Деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований информационной безопасности.

3.5.6 **критерий аудита информационной безопасности организации;** критерий аудита ИБ организации: Совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности.

Примечание — Критерии аудита информационной безопасности используют для сопоставления с ними свидетельств аудита информационной безопасности.

3.5.7 **аттестация автоматизированной системы в защищенном исполнении:** Процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии выполнению функции по обработке защищаемой информации на конкретном объекте информатизации.

3.5.8 **критерий обеспечения информационной безопасности организации;** критерий обеспечения ИБ организации: Показатель, на основании которого оценивается степень достижения цели (целей) информационной безопасности организации.

3.5.9 **эффективность обеспечения информационной безопасности;** эффективность обеспечения ИБ: Связь между достигнутым результатом и использованными ресурсами для обеспечения заданного уровня информационной безопасности.

3.6 Термины, относящиеся к средствам обеспечения информационной безопасности организации

3.6.1 **обеспечение информационной безопасности организации;** обеспечение ИБ организации: Деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

3.6.2 **мера безопасности;** *мера обеспечения безопасности*: Сложившаяся практика, процедура или механизм обработки риска.

3.6.3 **меры обеспечения информационной безопасности;** меры обеспечения ИБ: Совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

3.6.4 **организационные меры обеспечения информационной безопасности;** организационные меры обеспечения ИБ: Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

3.6.5 **техническое средство обеспечения информационной безопасности;** техническое средство обеспечения ИБ: Оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами.

Примечание — Такое оборудование может быть представлено техническими и программно-техническими средствами, встроенными в объект защиты и/или функционирующими автономно (независимо от объекта защиты).

3.6.6 **средство обнаружения вторжений,** *средство обнаружения атак*: Программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности.

3.6.7 **средство защиты от несанкционированного доступа:** Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Алфавитный указатель терминов

активы организации 3.1.6
анализ риска 3.2.13
АС в защищенном исполнении 3.1.19
атака «отказ в обслуживании» 3.3.9
атака сетевая 3.3.7
аттестация автоматизированной системы в защищенном исполнении 3.5.7
аудит ИБ организации 3.5.3
аудит информационной безопасности организации 3.5.3
безопасность [данных] 3.1.1
безопасность информации 3.1.1
безопасность информационной технологии 3.1.2
безопасность организации информационная 3.2.1
блокирование доступа (к информации) 3.3.8
брешь 3.3.4
возможности недекларированные 3.3.14
данные персональные 3.1.18
доступ несанкционированный 3.3.6
ИБ организации 3.2.1
идентификация риска 3.2.12
инфраструктура информационная 3.1.4
инцидент информационной безопасности 3.2.7
источник риска ИБ организации 3.2.17
источник риска информационной безопасности организации 3.2.17
ИТ 3.1.9
контроль обеспечения ИБ организации 3.5.1
контроль обеспечения информационной безопасности организации 3.5.1
критерии обеспечения ИБ организации 3.5.8
критерий аудита ИБ организации 3.5.6
критерий аудита информационной безопасности организации 3.5.6
критерий обеспечения информационной безопасности организации 3.5.8
КСИИ 3.1.15
менеджмент ИБ организации 3.4.1
менеджмент информационной безопасности организации 3.4.1
менеджмент риска ИБ организации 3.4.2
менеджмент риска информационной безопасности организации 3.4.2
мера безопасности 3.6.2
мера обеспечения безопасности 3.6.2
меры обеспечения ИБ 3.6.3
меры обеспечения ИБ организационные 3.6.4
меры обеспечения информационной безопасности 3.6.3
меры обеспечения информационной безопасности организационные 3.4.6
модель угроз (безопасности информации) 3.3.3
мониторинг ИБ организации 3.5.2
мониторинг информационной безопасности организации 3.5.2
нарушение ИБ организации 3.2.4
нарушение информационной безопасности организации 3.2.4
нарушитель ИБ организации 3.3.5
нарушитель информационной безопасности организации 3.3.5
обеспечение автоматизированной системы информационное 3.1.12
обеспечение автоматизированной системы программное 3.1.11
обеспечение автоматизированной системы техническое 3.1.10
обеспечение АС информационное 3.1.12
обеспечение АС программное 3.1.11
обеспечение АС техническое 3.1.10
обеспечение ИБ организации 3.6.1
обеспечение информационной безопасности организации 3.6.1
обработка риска ИБ организации 3.2.15

обработка риска информационной безопасности организации 3.2.15
объект защиты информации 3.2.2
объект информатизации 3.1.5
объект критический 3.1.16
определение приемлемости уровня риска 3.2.14
оценка риска 3.2.10
оценка риска ИБ (организации) 3.2.11
оценка риска информационной безопасности (организации) 3.2.11
оценка соответствия ИБ организации установленным требованиям 3.5.5
оценка соответствия информационной безопасности организации установленным требованиям 3.5.5
перехват (информации) 3.3.12
политика ИБ (организации) 3.2.18
политика информационной безопасности (организации) 3.2.18
процесс (информационной технологии) защищаемый 3.2.3
процесс информационный 3.1.8
разглашение информации 3.3.11
ресурс системы обработки информации 3.1.7
риск 3.2.9
роль ИБ в организации 3.4.4
роль информационной безопасности в организации 3.4.4
свидетельства (доказательства) аудита ИБ организации 3.5.4
свидетельства (доказательства) аудита информационной безопасности организации 3.5.4
сервис 3.1.13
сигнал информативный 3.3.13
система в защищенном исполнении автоматизированная 3.1.19
система документов по ИБ в организации 3.2.20
система документов по информационной безопасности в организации 3.2.20
система информационной инфраструктуры ключевая 3.1.15
система информационной инфраструктуры критически важная 3.1.15
система менеджмента информационной безопасности 3.4.3
система персональных данных информационная 3.1.17
ситуация непредвиденная 3.2.5
ситуация опасная 3.2.6
ситуация чрезвычайная 3.2.5
служба информационной безопасности организации 3.4.6
СМИБ 3.4.3
событие 3.2.8
средство защиты от несанкционированного доступа 3.6.7
средство обеспечения ИБ техническое 3.6.5
средство обеспечения информационной безопасности техническое 3.6.5
средство обнаружения атак 3.6.6
средство обнаружения вторжений 3.6.6
сфера информационная 3.1.3
технология информационная 3.1.9
угроза (безопасности информации) 3.3.2
угроза ИБ организации 3.3.1
угроза информационной безопасности организации 3.3.1
управление рисками 3.2.16
услуга 3.1.13
услуги информационных технологий 3.1.14
услуги ИТ 3.1.14
утечка информации 3.3.10
уязвимость (информационной системы) 3.3.4
цель ИБ (организации) 3.2.19
цель информационной безопасности (организации) 3.2.19
ЧС 3.2.5
электромагнитные излучения и наводки побочные 3.3.15
эффективность обеспечения ИБ 3.5.9
эффективность обеспечения информационной безопасности 3.5.9

Приложение А
(справочное)

Термины и определения общетехнических понятий

А.1

организация: Группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений.

[ГОСТ Р ИСО 9000—2001, пункт 3.3.1]

Примечания

1 К организации относятся: компания, корпорация, фирма, предприятие, учреждение, благотворительная организация, предприятие розничной торговли, ассоциация, а также их подразделения или комбинация из них.

2 Распределение обычно бывает упорядоченным.

3 Организация может быть государственной или частной.

А.2 **бизнес:** Экономическая деятельность, дающая прибыль; любой вид деятельности, приносящий доход, являющийся источником обогащения.

А.3 **бизнес-процесс**: Процессы, используемые в экономической деятельности организации.

А.4

информация: Сведения (сообщения, данные) независимо от формы их представления.

[Федеральный Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ, статья 2, пункт 1)]

А.5

активы: Все, что имеет ценность для организации.

[ГОСТ Р ИСО/МЭК 13335-1—2006, пункт 2.2]

А.6 **ресурсы:** Активы (организации), которые используются или потребляются в ходе выполнения процесса.

Примечания

1 Ресурсы могут включать в себя такие разнообразные объекты, как персонал, оборудование, основные средства, инструменты, а также коммунальные услуги: энергию, воду, топливо и инфраструктуру сетей связи.

2 Ресурсы могут быть многократно используемыми, возобновляемыми или расходуемыми.

А.7 **опасность:** Свойство объекта, характеризующее его способность наносить ущерб или вред другим объектам.

А.8 **чрезвычайное событие:** Событие, приводящее к чрезвычайной ситуации.

А.9 **ущерб:** Физическое повреждение или нанесение вреда здоровью людей либо нанесение вреда имуществу или окружающей среде.

А.10 **угроза:** Совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.

А.11 **уязвимость:** Внутренние свойства объекта, создающие восприимчивость к воздействию источника риска, которое может привести к какому-либо последствию.

А.12 **атака**: Попытка преодоления системы защиты информационной системы.

Примечания — Степень «успеха» атаки зависит от уязвимости и эффективности системы защиты.

А.13 **менеджмент:** Скоординированная деятельность по руководству и управлению организацией.

А.14 **менеджмент (непрерывности) бизнеса:** Скоординированная деятельность по руководству и управлению бизнес-процессами организации.

А.15 **роль:** Заранее определенная совокупность правил и процедур деятельности организации, устанавливающих допустимое взаимодействие между субъектом и объектом деятельности.

А.16

обладатель информации: Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

[Федеральный Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ, статья 2, пункт 5)]

А.17

инфраструктура: Совокупность зданий, оборудования и служб обеспечения, необходимых для функционирования организации.

[ГОСТ Р ИСО 9000—2001, пункт 3.3.3]

А.18 **аудит:** Систематический независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита.

Примечания

1 Внутренние аудиты, называемые аудитами первой стороны, проводит для внутренних целей сама организация или от ее имени другая организация. Результаты внутреннего аудита могут служить основанием для декларации о соответствии. Во многих случаях, особенно на малых предприятиях, аудит должен проводиться специалистами (людьми, не несущими ответственности за проверяемую деятельность).

2 Внешние аудиты включают аудиты, называемые аудитами второй стороны и аудитами третьей стороны.

Аудиты второй стороны проводят стороны, заинтересованные в деятельности предприятия, например, потребители или другие лица от их имени. Аудиты третьей стороны проводят внешние независимые организации. Эти организации проводят сертификацию или регистрацию на соответствие требованиям, например, требованиям ГОСТ Р ИСО 9001 и ГОСТ Р ИСО 14001.

3 Аудит систем менеджмента качества и экологического менеджмента, проводимый одновременно, называют «комплексным аудитом».

4 Если аудит проверяемой организации проводят одновременно несколько организаций, то такой аудит называют «совместным аудитом».

А.19 **мониторинг:** Систематическое или непрерывное наблюдение за объектом с обеспечением контроля и/или измерения его параметров, а также проведение анализа с целью предсказания изменчивости параметров и принятия решения о необходимости и составе корректирующих и предупреждающих действий.

А.20

декларирование соответствия: Форма подтверждения соответствия продукции требованиям технических регламентов.

[Федеральный Закон Российской Федерации от 27 декабря 2002 г. № 184-ФЗ, статья 2]

А.21 **технология:** Система взаимосвязанных методов, способов, приемов предметной деятельности.

А.22

документ: Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

[ГОСТ Р 52069.0—2003, пункт 3.18]

А.23 **обработка информации:** Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

Приложение Б
(справочное)

Взаимосвязь основных понятий в области обеспечения информационной безопасности в организации

Взаимосвязь основных понятий приведена на рисунке Б.1.

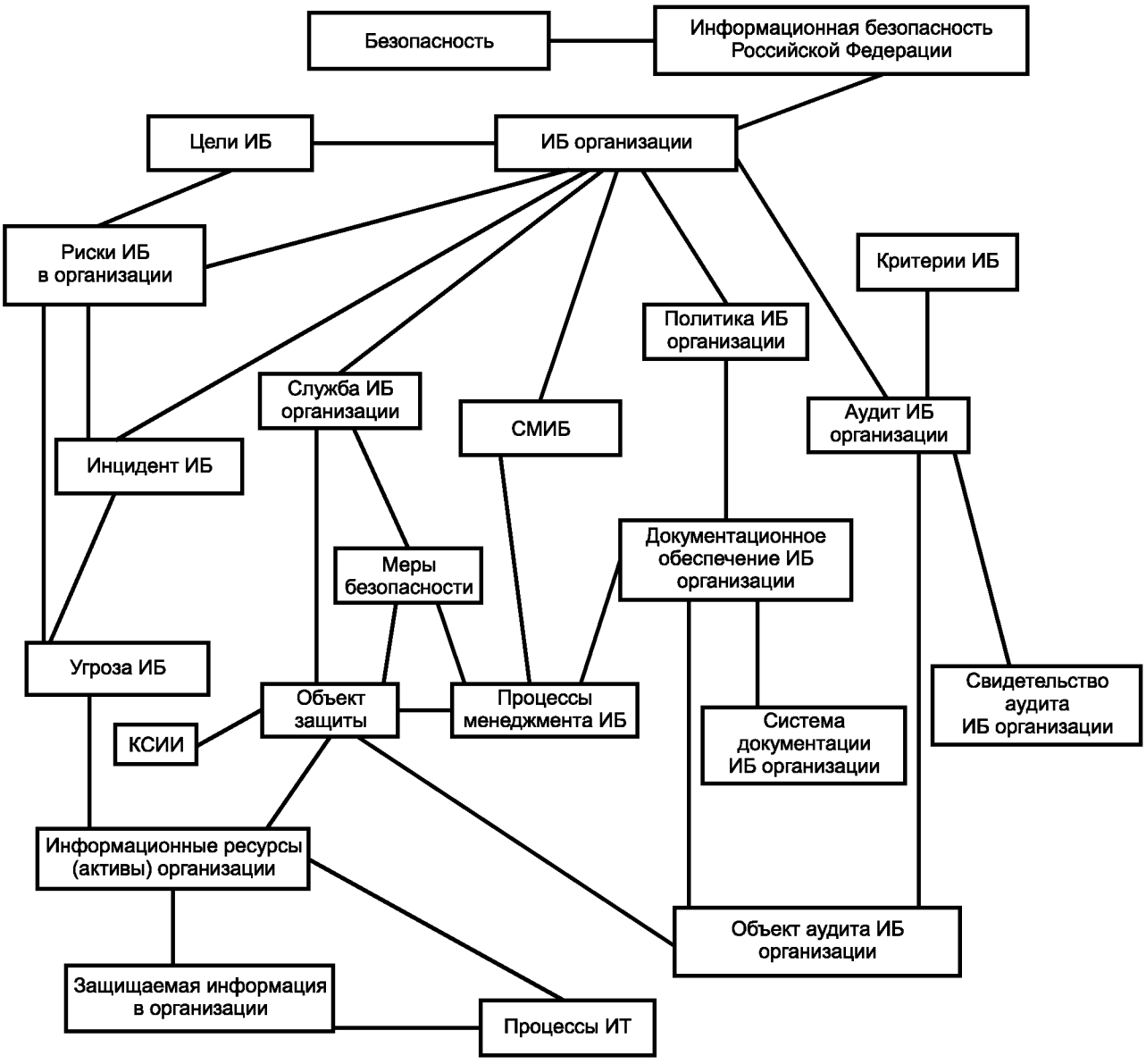

Рисунок Б.1 — Взаимосвязь основных понятий

Библиография

[1]	Р 50.1.053—2005	Информационные технологии. Основные термины и определения в области технической защиты информации
[2]	Р 50.1.056—2005	Техническая защита информации. Основные термины и определения
[3]	Федеральный закон РФ №184-ФЗ от 27 декабря 2002 г.	О техническом регулировании
[4]	Федеральный закон РФ №149-ФЗ от 27 июля 2006 г.	Об информации, информационных технологиях и защите информации
[5]	Федеральный закон РФ №152-ФЗ от 27 июля 2006 г.	О персональных данных
[6]	Утверждена Президентом Российской Федерации № Пр-1895 от 9 сентября 2000 г.	Доктрина информационной безопасности Российской Федерации

УДК 351.864.1:004:006.354 ОКС 35.020 Т00

Ключевые слова: информация, защита информации, информационная безопасность в организации, угрозы безопасности информации, критерии безопасности информации

Редактор *В.Н. Копысов*
Технический редактор *В.Н. Прусакова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 06.11.2009. Подписано в печать 01.12.2009. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 2,32. Уч.-изд. л. 1,90. Тираж 373 экз. Зак. 826.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru