ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 50.1.056— 2005

Техническая защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное

Москва
Стандартинформ
2006

Предисловие

Сведения о рекомендациях

1 РАЗРАБОТАНЫ Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ГНИИИ ПТЗИ ФСТЭК России), Техническим комитетом по стандартизации ТК 362 «Защита информации»

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

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящих рекомендаций, изменениях и поправках, а также тексты изменений и поправок к ним публикуются в информационном указателе «Национальные стандарты»

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
3.1 Общие понятия 1
3.2 Угрозы безопасности информации 2
3.3 Объекты технической защиты информации 4
3.4 Средства технической защиты информации 5
3.5 Мероприятия по технической защите информации 5
Алфавитный указатель терминов на русском языке 8
Алфавитный указатель терминов на английском языке 10
Приложение А (справочное) Общетехнические термины и определения, связанные с областью информационных технологий 11
Приложение Б (рекомендуемое) Схема взаимосвязи стандартизованных терминов 14
Библиография 15

Введение

Установленные настоящими рекомендациями термины расположены в систематизированном порядке, отражающем систему понятий в области технической защиты информации.

Для каждого понятия установлен один стандартизованный термин.

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.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два термина, имеющие общие терминоэлементы.

В алфавитном указателе данные термины приведены отдельно с указанием номера статьи.

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 настоящих рекомендациях.

В настоящих рекомендациях приведены термины на английском языке.

Термины и определения общетехнических понятий, необходимые для понимания текста настоящих рекомендаций, приведены в приложении А.

Схема взаимосвязи стандартизованных терминов приведена в приложении Б.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, — светлым, а синонимы — курсивом.

В настоящих рекомендациях приведен алфавитный указатель терминов на русском языке, а также алфавитный указатель терминов на английском языке.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Техническая защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Technical information protection.
Terms and definitions

Дата введения — 2006—06—01

1 Область применения

Настоящие рекомендации устанавливают термины и определения понятий в области технической защиты информации в различных сферах деятельности.

Термины, установленные настоящими рекомендациями, рекомендуются для использования во всех видах документации и литературы по вопросам технической защиты информации, используемой в сфере работ по стандартизации.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующий стандарты:

ГОСТ Р 50922—96 Защита информации. Основные термины и определения

ГОСТ Р 51275—99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51897—2002 Менеджмент риска. Термины и определения

ГОСТ Р 51898—2002 Аспекты безопасности. Правила включения в стандарты

ГОСТ 1.1—2002 Межгосударственная система стандартизации. Термины и определения

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

ГОСТ 15971—90 Системы обработки информации. Термины и определения

ГОСТ 16504—81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочного стандарта 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 документ заменен (изменен), то при пользовании настоящими рекомендациями следует руководствоваться замененным (измененным) документом. Если ссылочный документ 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 **информационная безопасность объекта информатизации:** Состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки

Издание официальное

3.1.2 **техническая защита информации;** ТЗИ: Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

en Technical Information protection

3.1.3 **безопасность информации [данных]:** Состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность [1].

en Information [data] security

Примечание — Безопасность информации [данных] определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, с несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии [1]

3.1.4 **безопасность информационной технологии:** Состояние защищенности информационной технологии, при котором обеспечивается выполнение изделием, реализующим информационную технологию, предписанных функций без нарушений безопасности обрабатываемой информации

en IT security

3.1.5 **конфиденциальность информации:** Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право [1]

en Confidentiality

3.1.6 **целостность информации:** Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

en Integrity

3.1.7 **целостность ресурсов информационной системы:** Состояние ресурсов информационной системы, при котором их изменение осуществляется только преднамеренно субъектами, имеющими на него право, при этом сохраняются их состав, содержание и организация взаимодействия

3.1.8 **доступность информации [ресурсов информационной системы]:** Состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно [1].

en Availability

Примечание — К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов [1]

3.1.9 **отчетность (ресурсов информационной системы):** Состояние ресурсов информационной системы, при котором обеспечиваются идентификация и регистрация действий с ними

en Accountability

3.1.10 **подлинность (ресурсов информационной системы):** Состояние ресурсов информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается [1]

en Authenticity

3.1.11 **показатель защищенности информации:** Количественная или качественная характеристика безопасности информации, определяющая уровень требований, предъявляемых к конфиденциальности, целостности и доступности этой информации и реализуемых при ее обработке [2]

3.2 Угрозы безопасности информации

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

en Threat

3.2.2 **источник угрозы безопасности информации:** Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации

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

en Vulnerability, breach

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 [3]

3.2.4 **утечка (информации) по техническому каналу:** Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации [1]

en Leakage

3.2.5 **перехват (информации):** Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов [1]

en Interception

3.2.6 **несанкционированный доступ к информации [ресурсам информационной системы];** НСД: Доступ к информации [ресурсам информационной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам информационной системы] с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Примечания

1 Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно [1].

2 Права и правила доступа к информации и ресурсам информационной системы устанавливают для процессов обработки информации, ее обслуживания, изменения программных, технических и информационных ресурсов, а также получения информации о них [1]

3.2.7 **несанкционированное воздействие на информацию [ресурсы информационной системы];** НСВ: Изменение, уничтожение или копирование информации [ресурсов информационной системы], осуществляемое с нарушением установленных прав и (или) правил.

Примечания

1 Несанкционированное воздействие может быть осуществлено преднамеренно или непреднамеренно. Преднамеренные несанкционированные воздействия являются специальными воздействиями [1].

2 Изменение может быть осуществлено в форме замены информации [ресурсов информационной системы]; введения новой информации [новых ресурсов информационной системы], а также уничтожения или повреждения информации [ресурсов информационной системы] [1]

3.2.8 **компьютерная атака:** целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств

en Attack

3.2.9 **сетевая атака:** компьютерная атака с использованием протоколов межсетевого взаимодействия

3.2.10 **несанкционированное блокирование доступа к информации [ресурсам информационной системы];** *отказ в обслуживании*: Создание условий, препятствующих доступу к информации [ресурсам информационной системы] субъекту, имеющему право на него.

en Denial of service

Примечания
1 Несанкционированное блокирование доступа осуществляется нарушителем безопасности информации, а санкционированное — администратором.
2 Создание условий, препятствующих доступу к информации (ресурсам информационной системы). может быть осуществлено по времени доступа, функциям по обработке информации (видам доступа) и (или) доступным информационным ресурсам [1]

3.2.11 **закладочное устройство;** *закладка*: Элемент средства съема информации или воздействия на нее, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации.

Примечание — Местами возможного съема информации могут быть ограждение, конструкция здания, оборудование, предметы интерьера, транспортные средства, а также технические средства и системы обработки информации

3.2.12 **вредоносная программа:** Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы [1]

3.2.13 **(компьютерный) вирус:** Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. **en** Computer virus

Примечание – Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению

3.2.14 **недекларированные возможности (программного обеспечения):** Функциональные возможности программного обеспечения, не описанные в документации [1]

3.2.15 **программная закладка:** Скрытновнесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие **en** Malicious logic

Примечание — программная закладка может быть реализована в виде вредоносной программы или программного кода [1]

3.3 Объекты технической защиты информации

3.3.1 **защищаемый объект информатизации:** Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности

3.3.2 **защищаемая информационная система:** Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности

3.3.3 **защищаемые ресурсы (информационной системы):** Ресурсы, использующиеся в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности

3.3.4 **защищаемая информационная технология:** Информационная технология, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности [1]

3.3.5 **защищаемые программные средства:** Программные средства, используемые в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности

3.3.6 **защищаемая сеть связи:** Сеть связи, используемая при обмене защищаемой информацией с требуемым уровнем ее защищенности

3.4 Средства технической защиты информации

3.4.1

техника защиты информации: Средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

[ГОСТ Р 50922—96, статья 20]

3.4.2 **средство защиты информации от утечки по техническим каналам:** Техническое средство, вещество или материал, предназначенные и (или) используемые для защиты информации от утечки по техническим каналам

3.4.3 **средство защиты информации от несанкционированного доступа:** Техническое, программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации или ресурсам информационной системы

3.4.4 **средство защиты информации от несанкционированного воздействия:** Техническое, программное или программно-техническое средство, предназначенное для предотвращения несанкционированного воздействия на информацию или ресурсы информационной системы

3.4.5 **межсетевой экран:** локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы [4]

3.4.6 **средство поиска закладочных устройств:** Техническое средство, предназначенное для поиска закладочных устройств, установленных на объекте информатизации

3.4.7 **средство контроля эффективности технической защиты информации:** Средство измерений, программное средство, вещество и (или) материал, предназначенные и (или) используемые для контроля эффективности технической защиты информации

3.4.8 **средство обеспечения технической защиты информации:** Техническое, программное, программно-техническое средство, используемое и (или) создаваемое для обеспечения технической защиты информации на всех стадиях жизненного цикла защищаемого объекта

3.5 Мероприятия по технической защите информации

3.5.1 **организационно-технические мероприятия по обеспечению защиты информации:** Совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации.

en Technical safeguards

Примечания

1 Организационно-технические мероприятия по обеспечению защиты информации должны осуществляться на всех этапах жизненного цикла объекта информатизации.

2 Организационные меры предусматривают установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации

3.5.2 **политика безопасности (информации в организации):** Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности

en Organisational security policy

3.5.3 **правила разграничения доступа (в информационной системе):** Правила, регламентирующие условия доступа субъектов доступа к объектам доступа в информационной системе [1]

3.5.4 **аудиторская проверка информационной безопасности в организации;** *аудит информационной безопасности в организации:* Периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организации установленных требований по обеспечению информационной безопасности.

en Security audit

Примечание — Аудит информационной безопасности в организации может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией, а также подразделением или должностным лицом организации (внутренний аудит)

3.5.5 **аудиторская проверка безопасности информации в информационной системе;** *аудит безопасности информации в информационной системе*: Проверка реализованных в информационной системе процедур обеспечения безопасности информации с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию [1]

en Computer system audit

3.5.6 **мониторинг безопасности информации:** Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью выявления его соответствия требованиям по безопасности информации

en Security monitoring

3.5.7

технический контроль эффективности защиты информации: Контроль эффективности защиты информации, проводимый с использованием средств контроля.

[ГОСТ Р 50922—96, статья 31]

3.5.8

организационный контроль эффективности защиты информации: Проверка соответствия полноты и обоснованности мероприятий по защите информации требованиям нормативных документов в области защиты информации.

[ГОСТ Р 50992—96, статья 30]

3.5.9 **контроль доступа (в информационной системе):** Проверка выполнения субъектами доступа установленных правил разграничения доступа в информационной системе

en Access control

3.5.10 **санкционирование доступа;** *авторизация*: Предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ

en Authorization

3.5.11 **аутентификация (подлинности субъекта доступа):** Действия по проверке подлинности субъекта доступа в информационной системе [1]

en Authentication

3.5.12 **идентификация:** Действия по присвоению субъектам и объектам доступа идентификаторов и (или) действия по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов [1]

en Identification

3.5.13 **удостоверение подлинности;** *нотаризация*: Регистрация данных защищенной третьей стороной, что в дальнейшем позволяет обеспечить точность характеристик данных.

en Notarization

Примечание — К характеристикам данных, например, относятся: содержание, происхождение, время и способ доставки

3.5.14 **восстановление данных:** Действия по воссозданию данных, которые были утеряны или изменены в результате несанкционированных воздействий

en Data restoration

3.5.15 **специальная проверка:** Проверка объекта информатизации с целью выявления и изъятия возможно внедренных закладочных устройств

3.5.16 **специальное исследование (объекта технической защиты информации):** Исследования с целью выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте технической защиты информации) требованиям нормативных правовых документов в области безопасности информации

3.5.17 **сертификация средств технической защиты информации на соответствие требованиям по безопасности информации:** Деятельность органа по сертификации по подтверждению соответствия средств технической защиты информации требованиям технических регламентов, положениям стандартов или условиям договоров

3.5.18 **аттестация объекта информатизации:** Деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта информатизации требованиям по безопасности информации

3.5.19 **оценка риска;** *анализ риска*: Выявление угроз безопасности информации, уязвимостей информационной системы, оценка вероятностей реализации угроз с использованием уязвимостей и оценка последствий реализации угроз для информации и информационной системы, используемой для обработки этой информации

en Risk assessment, risk analysis

Алфавитный указатель терминов на русском языке

авторизация 3.5.10
анализ риска 3.5.19
атака компьютерная 3.2.8
атака сетевая 3.2.9
аттестация объекта информатизации 3.5.18
аудит безопасности информации в информационной системе 3.5.5
аудит информационной безопасности в организации 3.5.4
аутентификация 3.5.11
аутентификация подлинности субъекта доступа 3.5.11
безопасность данных 3.1.3
безопасность информации 3.1.3
безопасность информационной технологии 3.1.4
безопасность объекта информатизации информационная 3.1.1
блокирование доступа к информации несанкционированное 3.2.10
блокирование доступа к ресурсам информационной системы несанкционированное 3.2.10
брешь 3.2.3
вирус 3.2.13
вирус компьютерный 3.2.13
воздействие на информацию несанкционированное 3.2.7
воздействие на ресурсы информационной системы несанкционированное 3.2.7
возможности недекларированные 3.2.14
возможности программного обеспечения недекларированные 3.2.14
восстановление данных 3.5.14
доступ к информации несанкционированный 3.2.6
доступ к ресурсам информационной системы несанкционированный 3.2.6
доступность информации 3.1.8
доступность ресурсов информационной системы 3.1.8
закладка 3.2.11
закладка программная 3.2.15
защита информации техническая 3.1.2
идентификация 3.5.12
исследование объекта технической защиты информации специальное 3.5.16
исследование специальное 3.5.16
источник угрозы безопасности информации 3.2.2
контроль доступа 3.5.9
контроль доступа в информационной системе 3.5.9
контроль эффективности защиты информации организационный 3.5.8
контроль эффективности защиты информации технический 3.5.7
конфиденциальность информации 3.1.5
мероприятия по обеспечению защиты информации организационно-технические 3.5.1
мониторинг безопасности информации 3.5.6
нотаризация 3.5.13
объект информатизации защищаемый 3.3.1
отказ в обслуживании 3.2.10
отчетность 3.1.9
отчетность ресурсов информационной системы 3.1.9
оценка риска 3.5.19
перехват 3.2.5
перехват информации 3.2.5
подлинность 3.1.10
подлинность ресурсов информационной системы 3.1.10
показатель защищенности информации 3.1.11
политика безопасности 3.5.2
политика безопасности информации в организации 3.5.2

правила разграничения доступа 3.5.3
правила разграничения доступа в информационной системе 3.5.3
проверка безопасности информации в информационной системе аудиторская 3.5.5
проверка информационной безопасности в организации аудиторская 3.5.4
проверка специальное 3.5.15
программа вредоносная 3.2.12
ресурсы защищаемые 3.3.3
ресурсы информационной системы защищаемые 3.3.3
санкционирование доступа 3.5.10
сертификация средств технической защиты информации на соответствие требованиям по безопасности информации 3.5.17
сеть связи защищаемая 3.3.6
система информационная защищаемая 3.3.2
средства программные защищаемые 3.3.5
средство защиты информации от несанкционированного воздействия 3.4.4
средство защиты информации от несанкционированного доступа 3.4.3
средство защиты информации от утечки по техническим каналам 3.4.2
средство контроля эффективности технической защиты информации 3.4.7
средство обеспечения технической защиты информации 3.4.8
средство поиска закладочных устройств 3.4.6
техника защиты информации 3.4.1
технология информационная защищаемая 3.3.4
угроза 3.2.1
угроза безопасности информации 3.2.1
удостоверение подлинности 3.5.13
устройство закладочное 3.2.11
утечка информации по техническому каналу 3.2.4
утечка по техническому каналу 3.2.4
уязвимость 3.2.3
уязвимость информационной системы 3.2.3
целостность информации 3.1.6
целостность ресурсов информационной системы 3.1.7
экран межсетевой 3.4.5

Алфавитный указатель терминов на английском языке

access control	3.5.9
accountability	3.1.9
attack	3.2.8
authentication	3.5.11
authenticity	3.1.10
authorization	3.5.10
availability	3.1.8
breach	3.2.3
computer system audit	3.5.5
computer virus	3.2.13
confidentiality	3.1.5
data restoration	3.5.14
data security	3.1.3
denial of service	3.2.10
identification	3.5.12
information security	3.1.3
integrity	3.1.6
interception	3.2.5
IT security	3.1.4
Leakage	3.2.4
malicious logic	3.2.15
notarization	3.5.13
organizational security policy	3.5.2
risk analysis	3.5.19
risk assessment	3.5.19
security audit	3.5.4
security minitoring	3.5.6
technical information protection	3.1.2
technical safeguards	3.5.1
threat	3.2.1
vulnerability	3.2.3

Приложение А
(справочное)

Общетехнические термины и определения, связанные с областью информационных технологий

А.1

автоматизированная система, АС: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
[ГОСТ 34.003—90, статья 1.1]

А.2 **информационная система:**

1 Организационно-упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи [5].

2 Автоматизированная система, результатом функционирования которой является представление выходной информации для последующего использования.

А.3

защищаемая информация: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание — Собственником информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.
[ГОСТ Р 50992—96, статья 1]

А.4

данные: Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.
[ГОСТ 15971—90, статья 1]

А.5

безопасность: Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.
[ГОСТ 1.1—2002, статья А.7]

А.6

информационная технология: Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных.
[ГОСТ 34.003—90, приложение 1, статья 4]

А.7

защиты информации; ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
[ГОСТ Р 50922—96, статья 2]

А.8

защита информации от утечки: Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.
[ГОСТ Р 50922—96, статья 3]

А.9 **криптографическая защита (данных):** Защита данных при помощи криптографического преобразования данных [1].

А.10

требование: Положение нормативного документа, содержащее критерии, которые должны быть соблюдены.

[ГОСТ 1.1—2002, статья 6.1.1]

А.11

объект информатизации: Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

[ГОСТ Р 51275—99, пункт 2.1]

А.12

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

А.13 **информативный сигнал:** Сигнал, по параметрам которого может быть определена защищаемая информация.

А.14 **доступ:** Извлечение информации из памяти средства вычислительной техники (электронно-вычислительной машины) или помещение информации в память средства вычислительной техники (электронно-вычислительной машины).

А.15 **доступ к информации (ресурсам информационной системы):** Получение возможности ознакомления с информацией, обработки информации и (или) воздействия на информацию и (или) ресурсы информационной системы с использованием программных и (или) технических средств [1].

Примечание — Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты [1].

А.16 **субъект доступа (в информационной системе):** Лицо или единица ресурса информационной системы, действия которого по доступу к ресурсам информационной системы регламентируются правилами разграничения доступа.

А.17 **объект доступа (в информационной системе):** Единица ресурса информационной системы, доступ к которой регламентируется правилами разграничения доступа [1].

А.18 **средство измерений:** Техническое средство, предназначенное для измерений, имеющее нормированные метрологические характеристики, воспроизводящее и/или хранящее единицу физической величины, размер которой принимают неизменным (в пределах установленной погрешности) в течение известного интервала времени

А.19 **сеть связи:** Технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи [6].

А.20 **ресурсы (информационной системы):** Средства, использующиеся в информационной системе, привлекаемые для обработки информации (например, информационные, программные, технические, лингвистические)

А.21 **нормативный правовой документ:** Письменный официальный документ, принятый в установленном порядке, управомоченного на то органа государственной власти, органа местного самоуправления или должностного лица, устанавливающий правовые нормы (правила поведения), обязательные для неопределенного круга лиц, рассчитанные на неоднократное применение и действующие независимо от того, возникли или прекратились конкретные правоотношения, предусмотренные актом [7].

А.22 **выделенное помещение:** специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед и других мероприятий секретного характера.

А.23

измерительный контроль: контроль, осуществляемый с применением средств измерений.

[ГОСТ 16504—81, статья 111]

А.24

информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

[ГОСТ Р 50922—96, статья Б.1]

А.25 **нарушитель безопасности информации:** Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

А.26 **документированный процесс:** Процесс, реализация которого осуществляется в соответствии с разработанным комплектом документов (документацией) и подтверждается соответствующими записями.

А.27 **свидетельства (доказательства) аудита информационной безопасности:** Записи, изложения фактов или другая информация, которые имеют отношение к критериям аудита информационной безопасности и могут быть проверены.

Примечание — Свидетельства аудита информационной безопасности могут быть качественными или количественными

А.28 **критерии аудита информационной безопасности в 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.

А.29

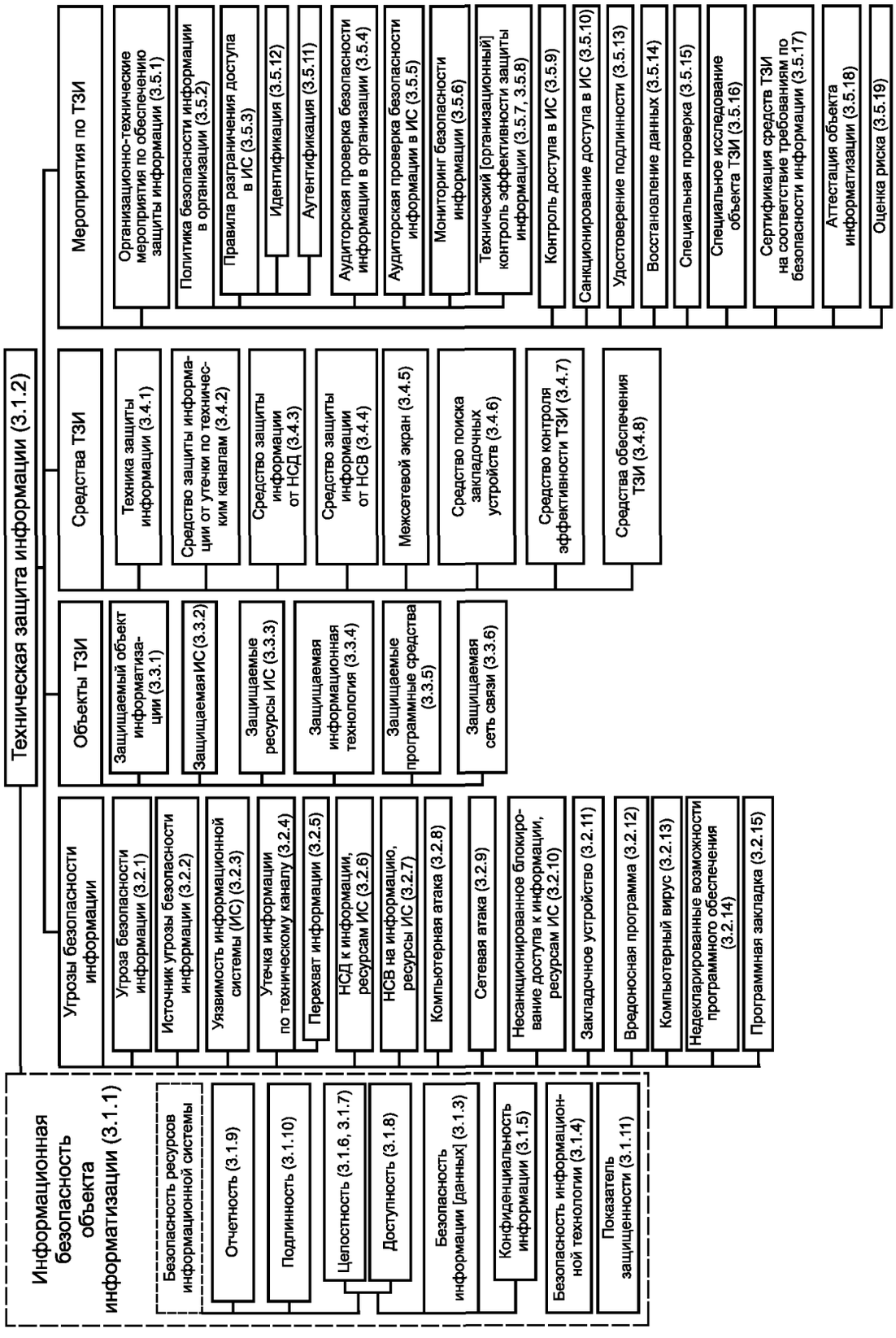
управление риском: Действия, осуществляемые для выполнения решений в рамках менеджмента риска.

Примечание — Управление риском может включать в себя мониторинг, переоценивание и действия, направленные на обеспечение соответствия принятым решениям.

[ГОСТ Р 51897—2002, статья 3.4.2]

Приложение Б
(рекомендуемое)

Схема взаимосвязи стандартизованных терминов



Библиография

[1]	Рекомендации по стандартизации Р 50.1.053—2005	Информационная технология. Основные термины и определения в области технической защиты информации
[2]	Руководящий документ. Гостехкомиссия России, 1998 г.	Защита от несанкционированного доступа к информации. Термины и определения
[3]	ИСО 2382-8:1998	Информационная технология. Словарь. Часть 8. Безопасность
[4]	Руководящий документ. Гостехкомиссия России, 1998 г.	Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации
[5]	Федеральный закон Российской Федерации от 20.02.1995 № 24-ФЗ (в ред. Федерального закона от 10.01.2003 № 15-ФЗ	Об информации, информатизации и защите информации
[6]	Федеральный закон Российской Федерации от 7.07.2003 № 126-ФЗ	О связи
[7]	Пленум Верховного суда Российской Федерации. Постановление от 20.01.2003 г. № 2	О некоторых вопросах, возникших в связи с принятием и введением в действие Гражданского процессуального кодекса Российской Федерации

УДК 001.4:025.4:006.354 ОКС 01.040.01 Т00

Ключевые слова: техническая защита информации, термины, определения, защита информации, безопасность информации, конфиденциальность, доступность, целостность

Рекомендации по стандартизации

Техническая защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Р 50.1.056—2005

БЗ 12—2005/336

Редактор *О.В. Гелемеева*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 24.05.2006. Подписано в печать 16.06.2006. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 2,32. Уч.-изд. л. 1,65. Тираж 428 экз. Изд. № 3467/4. Зак. 405. С 2953.

ФГУП «Стандартинформ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «Стандартинформ» на ПЭВМ.
Отпечатано в филиале ФГУП «Стандартинформ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.