Утверждены

Приказом Федерального

агентства по техническому

регулированию и метрологии

от 29 декабря 2005 г. N 479-ст

Дата введения -

1 июня 2006 года

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

TECHNICAL INFORMATION PROTECTION. TERMS AND DEFINITIONS

Р 50.1.056-2005

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. N 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".

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](#P654).

Схема взаимосвязи стандартизованных терминов приведена в [Приложении Б](#P789).

КонсультантПлюс: примечание.

Текст, выделенный полужирным шрифтом в официальном тексте документа, в электронной версии документа отмечен знаком "&", курсивом, - "#".

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.

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 следующие 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

 3.1.2. &Техническая защита информации&; en Technical

ТЗИ: деятельность, направленная Information

на обеспечение некриптографическими методами protection

безопасности информации (данных), подлежащей

защите в соответствии с действующим

законодательством, с применением технических,

программных и программно-технических средств

 3.1.3. &Безопасность информации [данных]&: en Information

состояние защищенности информации [данных], [data]

при котором обеспечиваются ее [их] security

конфиденциальность, доступность

и целостность [[1]](#P902)

 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]](#P902).

 3.1.4. &Безопасность информационной en IT security

технологии&: состояние защищенности

информационной технологии, при котором

обеспечивается выполнение изделием,

реализующим информационную технологию,

предписанных функций без нарушений

безопасности обрабатываемой информации

 3.1.5. &Конфиденциальность информации&: en Confidentiality

состояние информации, при котором доступ

к ней осуществляют только субъекты, имеющие

на него право [[1]](#P902)

 3.1.6. &Целостность информации&: состояние en Integrity

информации, при котором отсутствует любое ее

изменение либо изменение осуществляется

только преднамеренно субъектами, имеющими на

него право

 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 en Availability

информационной системы]&: состояние информации

[ресурсов информационной системы], при котором

субъекты, имеющие права доступа, могут

реализовать их беспрепятственно [[1]](#P902)

 Примечание - К правам доступа относятся,

право на чтение, изменение, копирование,

уничтожение информации, а также право на

изменение, использование, уничтожение ресурсов

[[1]](#P902).

 3.1.9. &Отчетность (ресурсов en Accountability

информационной системы)&: состояние ресурсов

информационной системы, при котором

обеспечиваются идентификация и регистрация

действий с ними

 3.1.10. &Подлинность (ресурсов en Authenticity

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]](#P902)

 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]](#P906)

 3.2. Угрозы безопасности информации

 3.2.1. &Угроза (безопасности информации)&: en Threat

совокупность условий и факторов, создающих

потенциальную или реально существующую

опасность нарушения безопасности информации

 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 en Vulnerability,

системы)&; #брешь#: свойство информационной breach

системы, предоставляющее 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 [[3]](#P910).

 3.2.4. &Утечка (информации) en Leakage

по техническому каналу&: неконтролируемое

распространение информации от носителя

защищаемой информации через физическую

среду до технического средства,

осуществляющего перехват информации [[1]](#P902)

 3.2.5. &Перехват (информации)&: en Interception

неправомерное получение информации

с использованием технического средства,

осуществляющего обнаружение, прием и обработку

информативных сигналов [[1]](#P902)

 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]](#P902).

 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]](#P902).

 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]](#P902).

 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]](#P902).

 3.2.8. &Компьютерная атака&: en Attack

целенаправленно несанкционированное воздействие

на информацию, на ресурс информационной системы

или получение несанкционированного доступа

к ним с применением программных или

программно-аппаратных средств

 3.2.9. &Сетевая атака&: компьютерная атака

с использованием протоколов межсетевого

взаимодействия

 3.2.10. &Несанкционированное блокирование en Denial of

доступа к информации [ресурсам информационной service

системы]&; #отказ в обслуживании#: создание

условий, препятствующих доступу к информации

[ресурсам информационной системы] субъекту,

имеющему право на него

 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]](#P902).

 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]](#P902)

 3.2.13. &(Компьютерный) вирус&: исполняемый en Computer virus

программный код или интерпретируемый набор

инструкций, обладающий свойствами

несанкционированного распространения

и самовоспроизведения

 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]](#P902)

 3.2.15. &Программная закладка&: en Malicious

скрытновнесенный в программное обеспечение logic

функциональный объект, который при определенных

условиях способен обеспечить

несанкционированное программное воздействие.

 Примечание - программная закладка может

быть реализована в виде вредоносной программы

или программного кода [[1]](#P902).

 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]](#P902)

 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]](#P913)

 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 en Technical

мероприятия по обеспечению защиты информации&: safeguards

совокупность действий, направленных на

применение организационных мер и программно-

технических способов защиты информации на

объекте информатизации

 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 en Organizational

в организации)&: совокупность документированных security

правил, процедур, практических приемов или policy

руководящих принципов в области безопасности

информации, которыми руководствуется

организация в своей деятельности

 3.5.3. &Правила разграничения доступа

(в информационной системе)&: правила,

регламентирующие условия доступа субъектов

доступа к объектам доступа в информационной

системе [[1]](#P902)

 3.5.4. &Аудиторская проверка информационной en Security audit

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

 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 en Computer

информации в информационной системе&; system audit

#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]](#P902)

 3.5.6. &Мониторинг безопасности en Security

информации&: постоянное наблюдение за процессом monitoring

обеспечения безопасности информации

в информационной системе с целью выявления его

соответствия требованиям по безопасности

информации

 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 en Access control

системе)&: проверка выполнения субъектами

доступа установленных правил разграничения

доступа в информационной системе

 3.5.10. &Санкционирование доступа&; en Authorization

#авторизация#: предоставление субъекту прав на

доступ, а также предоставление доступа в

соответствии с установленными правами

на доступ

 3.5.11. &Аутентификация (подлинности en Authentication

субъекта доступа)&: действия по проверке

подлинности субъекта доступа в информационной

системе [[1]](#P902)

 3.5.12. &Идентификация&: действия en Identification

по присвоению субъектам и объектам доступа

идентификаторов и (или) действия по сравнению

предъявляемого идентификатора с перечнем

присвоенных идентификаторов [[1]](#P902)

 3.5.13. &Удостоверение подлинности&; en Notarization

#нотаризация#: регистрация данных защищенной

третьей стороной, что в дальнейшем позволяет

обеспечить точность характеристик данных

 Примечание - К характеристикам данных,

например, относятся: содержание, происхождение,

время и способ доставки.

 3.5.14. &Восстановление данных&: действия en Data

по воссозданию данных, которые были утеряны restoration

или изменены в результате несанкционированных

воздействий

 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#: en Risk

выявление угроз безопасности информации, assessment,

уязвимостей информационной системы, оценка risk analysis

вероятностей реализации угроз с использованием

уязвимостей и оценка последствий реализации

угроз для информации и информационной системы;

используемой для обработки этой информации

 Алфавитный указатель терминов на русском языке

#авторизация# [3.5.10](#P452)

#анализ риска# [3.5.19](#P504)

&атака компьютерная& [3.2.8](#P225)

&атака сетевая& [3.2.9](#P231)

&аттестация объекта информатизации& [3.5.18](#P498)

#аудит безопасности информации в информационной системе# [3.5.5](#P415)

#аудит информационной безопасности в организации# [3.5.4](#P399)

&аутентификация& [3.5.11](#P457)

&аутентификация подлинности субъекта доступа& [3.5.11](#P457)

&безопасность данных& [3.1.3](#P82)

&безопасность информации& [3.1.3](#P82)

&безопасность информационной технологии& [3.1.4](#P97)

&безопасность объекта информатизации информационная& [3.1.1](#P69)

&блокирование доступа к информации несанкционированное& [3.2.10](#P234)

&блокирование доступа к ресурсам информационной системы

несанкционированное& [3.2.10](#P234)

#брешь# [3.2.3](#P160)

&вирус& [3.2.13](#P268)

&вирус компьютерный& [3.2.13](#P268)

&воздействие на информацию несанкционированное& [3.2.7](#P205)

&воздействие на ресурсы информационной системы

несанкционированное& [3.2.7](#P205)

&возможности недекларированные& [3.2.14](#P279)

&возможности программного обеспечения недекларированные& [3.2.14](#P279)

&восстановление данных& [3.5.14](#P474)

&доступ к информации несанкционированный& [3.2.6](#P184)

&доступ к ресурсам информационной системы

несанкционированный& [3.2.6](#P184)

&доступность информации& [3.1.8](#P120)

&доступность ресурсов информационной системы& [3.1.8](#P120)

#закладка# [3.2.11](#P252)

&закладка программная& [3.2.15](#P283)

&защита информации техническая& [3.1.2](#P75)

&идентификация& [3.5.12](#P461)

&исследование объекта технической защиты информации

специальное& [3.5.16](#P482)

&исследование специальное& [3.5.16](#P482)

&источник угрозы безопасности информации& [3.2.2](#P155)

&контроль доступа& [3.5.9](#P448)

&контроль доступа в информационной системе& [3.5.9](#P448)

&контроль эффективности защиты информации организационный& [3.5.8](#P438)

&контроль эффективности защиты информации технический& [3.5.7](#P430)

&конфиденциальность информации& [3.1.5](#P104)

&мероприятия по обеспечению защиты информации

организационно-технические& [3.5.1](#P371)

&мониторинг безопасности информации& [3.5.6](#P424)

#нотаризация# [3.5.13](#P466)

&объект информатизации защищаемый& [3.3.1](#P293)

#отказ в обслуживании# [3.2.10](#P234)

&отчетность& [3.1.9](#P131)

&отчетность ресурсов информационной системы& [3.1.9](#P131)

&оценка риска& [3.5.19](#P504)

&перехват& [3.2.5](#P179)

&перехват информации& [3.2.5](#P179)

&подлинность& [3.1.10](#P136)

&подлинность ресурсов информационной системы& [3.1.10](#P136)

&показатель защищенности информации& [3.1.11](#P143)

&политика безопасности& [3.5.2](#P388)

&политика безопасности информации в организации& [3.5.2](#P388)

&правила разграничения доступа& [3.5.3](#P394)

&правила разграничения доступа в информационной системе& [3.5.3](#P394)

&проверка безопасности информации в информационной

системе аудиторская& [3.5.5](#P415)

&проверка информационной безопасности в организации

аудиторская& [3.5.4](#P399)

&проверка специальная& [3.5.15](#P478)

&программа вредоносная& [3.2.12](#P263)

&ресурсы защищаемые& [3.3.3](#P301)

&ресурсы информационной системы защищаемые& [3.3.3](#P301)

&санкционирование доступа& [3.5.10](#P452)

&сертификация средств технической защиты информации

на соответствие требованиям по безопасности информации& [3.5.17](#P490)

&сеть связи защищаемая& [3.3.6](#P314)

&система информационная защищаемая& [3.3.2](#P297)

&средства программные защищаемые& [3.3.5](#P310)

&средство защиты информации от несанкционированного

воздействия& [3.4.4](#P339)

&средство защиты информации от несанкционированного

доступа& [3.4.3](#P332)

&средство защиты информации от утечки по техническим

каналам& [3.4.2](#P327)

&средство контроля эффективности технической защиты

информации& [3.4.7](#P357)

&средство обеспечения технической защиты информации& [3.4.8](#P363)

&средство поиска закладочных устройств& [3.4.6](#P352)

&техника защиты информации& [3.4.1](#P318)

&технология информационная защищаемая& [3.3.4](#P305)

&угроза& [3.2.1](#P151)

&угроза безопасности информации& [3.2.1](#P151)

&удостоверение подлинности& [3.5.13](#P466)

&устройство закладочное& [3.2.11](#P252)

&утечка информации по техническому каналу& [3.2.4](#P173)

&утечка по техническому каналу& [3.2.4](#P173)

&уязвимость& [3.2.3](#P160)

&уязвимость информационной системы& [3.2.3](#P160)

&целостность информации& [3.1.6](#P108)

&целостность ресурсов информационной системы& [3.1.7](#P113)

&экран межсетевой& [3.4.5](#P345)

 Алфавитный указатель терминов на английском языке

access control [3.5.9](#P448)

accountability [3.1.9](#P131)

attack [3.2.8](#P225)

authentication [3.5.11](#P457)

authenticity [3.1.10](#P136)

authorization [3.5.10](#P452)

availability [3.1.8](#P120)

breach [3.2.3](#P160)

computer system audit [3.5.5](#P415)

computer virus [3.2.13](#P268)

confidentiality [3.1.5](#P104)

data restoration [3.5.14](#P474)

data security [3.1.3](#P82)

denial of service [3.2.10](#P234)

identification [3.5.12](#P461)

information security [3.1.3](#P82)

integrity [3.1.6](#P108)

interception [3.2.5](#P179)

IT security [3.1.4](#P97)

leakage [3.2.4](#P173)

malicious logic [3.2.15](#P283)

notarization [3.5.13](#P466)

organizational security policy [3.5.2](#P388)

risk analysis [3.5.19](#P504)

risk assessment [3.5.19](#P504)

security audit [3.5.4](#P399)

security monitoring [3.5.6](#P424)

technical information protection [3.1.2](#P75)

technical safeguards [3.5.1](#P371)

threat [3.2.1](#P151)

vulnerability [3.2.3](#P160)

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]](#P920).

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]](#P902).

 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]](#P902).

Примечание - Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты [[1]](#P902).

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]](#P902).

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]](#P926).

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]](#P929).

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

┌── ─── ─── ─── ─┐ ┌─────────────────────────────────────┐

 Информационная ├──────────────┤Техническая защита информации [(3.1.2)](#P75)│

│ безопасность │ └────────────────┬────────────────────┘

 объекта ┌───────────────┬───────┴──────┬─────────────────┐

│ информатизации │ ┌─────┴──────┐ ┌──────┴──────┐ ┌─────┴──────┐ ┌────────┴─────────┐

 [(3.1.1)](#P69) │ Угрозы │ │ Объекты ТЗИ │ │Средства ТЗИ│ │Мероприятия по ТЗИ│

│ │ │безопасности│ ├─────────────┘ ├────────────┘ ├──────────────────┘

 ┌────────────┐ │ информации │ │┌────────────┐ │┌───────────┐ │┌─────────────────┐

│ │Безопасность│ │ ├────────────┘ ││Защищаемый │ ││ Техника │ ││Орагиназационно- │

 │ресурсов ин-│ │┌───────────┐ ││объект ин- │ ││ защиты │ ││технические меро-│

│ │формационной│ │ ││Угроза без-│ ├┤форматизации│ ├┤информации │ ├┤приятия по обес- │

 │системы │ ││опасности │ ││[(3.3.1)](#P293) │ ││ [(3.4.1)](#P318) │ ││печению защиты │

│ ├────────────┘ │ ├┤информации │ │└────────────┘ │└───────────┘ ││информации │

 │┌───────────┐ ││[(3.2.1)](#P151) │ │┌────────────┐ │┌───────────┐ ││[(3.5.1)](#P371) │

│ ││Отчетность │ │ │└───────────┘ ││ Защищаемая │ ││Средство │ │└─────────────────┘

 ├┤ [(3.1.9)](#P131) │ │┌───────────┐ ├┤ ИС [(3.3.2)](#P297) │ ││защиты ин- │ │┌─────────────────┐

│ │└───────────┘ │ ││Источник │ │└────────────┘ ││формации от│ ││Политика безопас-│

 │┌───────────┐ ││угрозы без-│ │┌────────────┐ ├┤утечки по │ ││ности информации │

│ ││Подлинность│ │ ├┤опасности │ ││ Защищаемые │ ││техническим│ ││в организации │

 ││ [(3.1.10)](#P136) │ ││информации │ ├┤ ресурсы ИС │ ││каналам │ ││[(3.5.2)](#P388) │

│ │└───────────┘ │ ││[(3.2.2)](#P155) │ ││ [(3.3.3)](#P301) │ ││[(3.4.2)](#P327) │ │├─────────────────┘

 │ ┌───────┐ │└───────────┘ │└────────────┘ │└───────────┘ ││┌────────────────┐

│ │ │Целост-│ │ │┌───────────┐ │┌────────────┐ │┌───────────┐ │││Правила разгра- │

 │ ┌─┤ность │ ││Уязвимость │ ││Защищаемая │ ││Средство │ │├┤ничения доступа │

│ │ │ │([3.1.6](#P108),│ │ ││информаци- │ ││информацион-│ ││защиты ин- │ │││в ИС [(3.5.3)](#P394) │

 └──┤ │ [3.1.7](#P113))│ ├┤онной сис- │ ├┤ная техноло-│ ├┤формации от│ ││├────────────────┘

│ │ └───────┘ │ ││темы (ИС) │ ││гия [(3.3.4)](#P305) │ ││НСД [(3.4.3)](#P332)│ │││┌───────────────┐

 ┌──┤ ┌───────┐ ││[(3.2.3)](#P160) │ │└────────────┘ │└───────────┘ ││├┤ Идентификация │

│ │ │ │Доступ-│ │ │└───────────┘ │┌────────────┐ │┌───────────┐ ││││ [(3.5.12)](#P461) │

 │ └─┤ность │ │┌───────────┐ ││ Защищаемые │ ││Средство │ │││└───────────────┘

│ │ │[(3.1.8)](#P120)│ │ ││Утечка ин- │ ││программные │ ││защиты ин- │ │││┌───────────────┐

 │ └───────┘ ││формации по│ ├┤ средства │ ├┤формации от│ ││││Аутентификация │

│ ├────────────┐ │ ├┤техническо-│ ││ [(3.3.5)](#P310) │ ││НСВ [(3.4.4)](#P339)│ ││└┤ [(3.5.11)](#P457) │

 │Безопасность│ ││му каналу │ │└────────────┘ │└───────────┘ ││ └───────────────┘

│ │ информации │ │ ││[(3.2.4)](#P173) │ │┌────────────┐ │┌───────────┐ ││┌────────────────┐

 │ [данных] │ │├───────────┘ ││ Защищаемая │ ││Межсетевой │ │││Аудиторская про-│

│ │ [(3.1.3)](#P82) │ │ ││┌───────────┐└┤ сеть связи │ ├┤ экран │ │││верка безопасно-│

 ├────────────┘ │││ Перехват │ │ [(3.3.6)](#P314) │ ││ [(3.4.5)](#P345) │ │├┤сти информации │

│ │┌───────────┐ │ │└┤информации │ └────────────┘ │└───────────┘ │││в организации │

 ││Конфедици- │ │ │ [(3.2.5)](#P179) │ │┌───────────┐ │││[(3.5.4)](#P399) │

│ ││альность │ │ │ └───────────┘ ││ Средство │ ││└────────────────┘

 └┤информации │ │┌───────────┐ ││ поиска │ ││┌────────────────┐

│ │[(3.1.5)](#P104) │ │ ││ НСД к │ ├┤закладочных│ │││Аудиторская про-│

 └───────────┘ ├┤информации,│ ││ устройств │ │││верка безопасно-│

│ ┌────────────┐ │ ││ресурсам ИС│ ││ [(3.4.6)](#P352) │ │├┤сти информации в│

 │Безопасность│ ││ [(3.2.6)](#P184) │ │└───────────┘ │││ИС [(3.5.5)](#P415) │

│ │информацион-│ │ │└───────────┘ │┌───────────┐ ││└────────────────┘

 │ной │ │┌───────────┐ ││Средство │ ││┌────────────────┐

│ │технологии │ │ ││ НСВ на │ ││контроля │ │││Мониторинг без- │

 │[(3.1.4)](#P97) │ ││информацию,│ ├┤эффектив- │ │├┤опасности инфор-│

│ └────────────┘ │ ├┤ресурсы ИС │ ││ности ТЗИ │ │││мации [(3.5.6)](#P424) │

 ┌────────────┐ ││ [(3.2.7)](#P205) │ ││[(3.4.7)](#P357) │ ││└────────────────┘

│ │ Показатель │ │ │└───────────┘ │└───────────┘ ││┌────────────────┐

 │защищенности│ │┌───────────┐ │┌───────────┐ │││Технический [ор-│

│ │ [(3.1.11)](#P143) │ │ ││Компьютер- │ ││ Средство │ │││ганизационный] │

 └────────────┘ ├┤ная атака │ ││обеспечения│ │└┤контроль эффек- │

└── ─── ─── ─── ─┘ ││[(3.2.8)](#P225) │ └┤ ТЗИ │ │ │тивности инфор- │

 │└───────────┘ │ [(3.4.8)](#P363) │ │ │мации ([3.5.7](#P430), │

 │┌───────────┐ └───────────┘ │ │[3.5.8](#P438)) │

 ││ Сетевая │ │ └────────────────┘

 ├┤ атака │ │┌─────────────────┐

 ││ [(3.2.9)](#P231) │ ├┤Контроль доступа │

 │└───────────┘ ││ в ИС [(3.5.9)](#P448) │

 │┌───────────┐ │└─────────────────┘

 ││Несанкцио- │ │┌─────────────────┐

 ││нированное │ ││Санкционирование │

 ││блокирова- │ ├┤ доступа в ИС │

 ├┤ние доступа│ ││ [(3.5.10)](#P452) │

 ││к информа- │ │└─────────────────┘

 ││ции, ресур-│ │┌─────────────────┐

 ││сам ИС │ ││ Удостоверение │

 ││[(3.2.10)](#P234) │ ├┤ подлинности │

 │└───────────┘ ││ [(3.5.13)](#P466) │

 │┌───────────┐ │└─────────────────┘

 ││Закладочное│ │┌─────────────────┐

 ├┤устройство │ ││ Восстановление │

 ││ [(3.2.11)](#P252) │ ├┤ данных [(3.5.14)](#P474) │

 │└───────────┘ │└─────────────────┘

 │┌───────────┐ │┌─────────────────┐

 ││Вредоносная│ ││ Специальная │

 ├┤ программа │ ├┤проверка [(3.5.15)](#P478)│

 ││ [(3.2.12)](#P263) │ │└─────────────────┘

 │└───────────┘ │┌─────────────────┐

 │┌───────────┐ ││Специальное ис- │

 ││Компьютер- │ ├┤следование объек-│

 ├┤ный вирус │ ││та ТЗИ [(3.5.16)](#P482) │

 ││[(3.2.13)](#P268) │ │└─────────────────┘

 │└───────────┘ │┌─────────────────┐

 │┌───────────┐ ││Сертификация │

 ││Недеклари- │ ││средств ТЗИ на │

 ││рованные │ ││соответствие тре-│

 ││возможности│ ├┤бованиям по без- │

 ├┤программно-│ ││опасности инфор- │

 ││го │ ││мации [(3.5.17)](#P490) │

 ││обеспечения│ │└─────────────────┘

 ││[(3.2.14)](#P279) │ │┌─────────────────┐

 │└───────────┘ ││Аттестация объек-│

 │┌───────────┐ ├┤та информатизации│

 ││Программная│ ││[(3.5.18)](#P498) │

 └┤ закладка │ │└─────────────────┘

 │ [(3.2.15)](#P283) │ │┌─────────────────┐

 └───────────┘ ││ Оценка риска │

 └┤ [(3.5.19)](#P504) │

 └─────────────────┘

БИБЛИОГРАФИЯ

[1] Рекомендации Информационная технология. Основные

 по стандартизации термины и определения в области

 Р 50.1.053-2005 технической защиты информации

[2] Руководящий документ. Защита от несанкционированного доступа

 Гостехкомиссия к информации. Термины и определении

 России, 1998 г.

[3] ИСО 2382-8.1998 Информационная технология. Словарь.

 Часть 8. Безопасность

[4] Руководящий документ. Средства вычислительной техники.

 Гостехкомиссия Межсетевые экраны. Защита от

 России, 1998 г. несанкционированного доступа к

 информации. Показатели защищенности от

 несанкционированного доступа к

 информации

[5] Федеральный закон Об информации, информатизации и защите

 от 20.02.1995 N 24-ФЗ информации

 (в ред. Федерального

 закона от 10.01.2003

 N 15-ФЗ)

[6] Федеральный закон О связи

 от 07.07.2003 N 126-ФЗ

[7] Пленум Верховного суда О некоторых вопросах, возникших в связи

 Российской Федерации. с принятием и введением в действие

 Постановление Гражданского процессуального кодекса

 от 20.01.2003 N 2 Российской Федерации