



КонсультантПлюс

"Р 50.1.053-2005. Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации" (утв. и введены в действие Приказом Ростехрегулирования от 06.04.2005 N 77-ст)

Документ предоставлен **КонсультантПлюс**

www.consultant.ru

Дата сохранения: 03.07.2025

Утверждены и введены в действие
Приказом Федерального
агентства по техническому
регулированию и метрологии
от 6 апреля 2005 г. N 77-ст

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ ТЕХНИЧЕСКОЙ
ЗАЩИТЫ ИНФОРМАЦИИ

**Information technologies. Basic terms and definitions
in scope of technical protection of information**

Р 50.1.053-2005

Группа Э00

ОКС **01.040.01**

ОКСТУ **0090**

Дата введения
1 января 2006 года

Предисловие

Задачи, основные принципы и правила проведения работ по государственной стандартизации в Российской Федерации установлены **ГОСТ Р 1.0-92** "Государственная система стандартизации Российской Федерации. Основные положения" и **ГОСТ Р 1.2-92** "Государственная система стандартизации Российской Федерации. Порядок разработки государственных стандартов".

Сведения о рекомендациях

1. Разработаны Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Гостехкомиссии России.
2. Внесены Техническим комитетом по стандартизации ТК 362 "Защита информации".
3. Утверждены и введены в действие **Приказом** Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. N 77-ст.
4. Введены впервые.

Информация о введении в действие (прекращении действия) настоящих рекомендаций, изменениях и поправках к ним, а также тексты изменений и поправок публикуются в

информационных указателях "Национальные стандарты". В случае пересмотра или отмены настоящих рекомендаций соответствующая информация будет опубликована в информационном указателе "Национальные стандарты".

Введение

Установленные в настоящих рекомендациях термины расположены в систематизированном порядке, отражающем систему понятий в области технической защиты информации при применении информационных технологий.

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 терминологические элементы.

В алфавитном [указателе](#) данные термины приведены отдельно с указанием номера статьи.

Помета, указывающая на область применения многозначного термина, приведена в круглых скобках светлым шрифтом после термина. Помета не является частью термина.

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 случае, когда в термине содержатся все необходимые и достаточные признаки понятия, определение не приводится и вместо него ставится прочерк.

В настоящих рекомендациях приведены эквиваленты стандартизованных терминов 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.

КонсультантПлюс: примечание.

Стандартизованные термины, набранные полужирным шрифтом в официальном тексте документа, в электронной версии документа выделены прописными буквами.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, - светлым.

1. Область применения

Настоящие рекомендации по стандартизации устанавливают термины и определения

понятий в области технической защиты информации при применении информационных технологий.

Термины, установленные настоящими рекомендациями по стандартизации, рекомендуются для использования во всех видах документации и литературы по вопросам технической защиты информации при применении информационных технологий, входящих в сферу работ по стандартизации и (или) использующих результаты этих работ.

Настоящие рекомендации по стандартизации должны применяться совместно с [ГОСТ Р 50922](#).

2. Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

[ГОСТ 1.1-2002](#) Межгосударственная система стандартизации. Термины и определения

[ГОСТ 34.003-90](#) Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

[ГОСТ 15971-90](#) Системы обработки информации. Термины и определения

[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 51898-2002](#) Аспекты безопасности. Правила включения в стандарты.

Примечание - При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов по указателю "Национальные стандарты", составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящими рекомендациями 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. Стандартизованные термины и определения

3.1. Объекты технической защиты информации

3.1.1. ЗАЩИЩАЕМАЯ АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА: автоматизированная информационная система, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности.

trusted computer
system

3.1.2. ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ (АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ): информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищенности.
Примечание - Информационные ресурсы включают в себя документы и массивы документов, используемые

в автоматизированных информационных системах.

3.1.3. ЗАЩИЩАЕМАЯ ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ:
информационная технология, предназначенная для
сбора, хранения, обработки, передачи
и использования защищаемой информации с требуемым
уровнем ее защищенности.

3.1.4. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ [ДАННЫХ]: состояние
защищенности информации [данных], при котором
обеспечиваются ее [их] конфиденциальность,
доступность и целостность.

information [data]
security

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

3.1.5. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ (ПРИ ПРИМЕНЕНИИ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ): состояние защищенности
информационной технологии, обеспечивающее
безопасность информации, для обработки которой она
применяется, и информационную безопасность
автоматизированной информационной системы,
в которой она реализована.

IT security

3.1.6. БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННОЙ
ИНФОРМАЦИОННОЙ СИСТЕМЫ: состояние защищенности
автоматизированной информационной системы,
при котором обеспечиваются конфиденциальность,
доступность, целостность, подотчетность
и подлинность ее ресурсов.

3.1.7. КОНФИДЕНЦИАЛЬНОСТЬ (ИНФОРМАЦИИ [РЕСУРСОВ
АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ]):
состояние информации [ресурсов автоматизированной
информационной системы], при котором доступ к ней
[к ним] осуществляют только субъекты, имеющие
на него право.

confidentiality

3.1.8. ЦЕЛОСТНОСТЬ (ИНФОРМАЦИИ [РЕСУРСОВ
АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ]):
состояние информации [ресурсов автоматизированной
информационной системы], при котором ее [их]
изменение осуществляется только преднамеренно
субъектами, имеющими на него право.

integrity

3.1.9. ДОСТУПНОСТЬ (ИНФОРМАЦИИ [РЕСУРСОВ
АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ]):
состояние информации [ресурсов автоматизированной
информационной системы], при котором субъекты,
имеющие право доступа, могут реализовать
их беспрепятственно.

availability

Примечание – К правам доступа относятся: право
на чтение, изменение, копирование, уничтожение
информации, а также права на изменение,
использование, уничтожение ресурсов.

3.1.10. ПОДОТЧЕТНОСТЬ (РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ
ИНФОРМАЦИОННОЙ СИСТЕМЫ): состояние ресурсов
автоматизированной информационной системы,
при котором обеспечиваются их идентификация
и регистрация.

accountability

3.1.11. ПОДЛИННОСТЬ (РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ
ИНФОРМАЦИОННОЙ СИСТЕМЫ): состояние ресурсов
автоматизированной информационной системы,
при котором обеспечивается реализация информационной
технологии с использованием именно тех ресурсов,

authenticity

к которым субъект, имеющий на это право, обращается.

3.2. Угрозы безопасности информации

- 3.2.1. УГРОЗА (БЕЗОПАСНОСТИ ИНФОРМАЦИИ): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации. threat
- 3.2.2. ИСТОЧНИК УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ: субъект, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.
- 3.2.3. УЯЗВИМОСТЬ (АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ): недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности обрабатываемой в ней информации. vulnerability
- 3.2.4. УТЕЧКА (ИНФОРМАЦИИ) ПО ТЕХНИЧЕСКОМУ КАНАЛУ: неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. leakage
- 3.2.5. ПЕРЕХВАТ (ИНФОРМАЦИИ): неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов. interception
- 3.2.6. ИНФОРМАТИВНЫЙ СИГНАЛ: сигнал, по параметрам которого может быть определена защищаемая информация. informative signal
- 3.2.7. ДОСТУП (В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ): получение возможности ознакомления с информацией, ее обработки и (или) воздействия на информацию и (или) ресурсы автоматизированной информационной системы с использованием программных и (или) технических средств. access
- Примечание - Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты.
- 3.2.8. СУБЪЕКТ ДОСТУПА (В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ): лицо или единица ресурса автоматизированной информационной системы, действия которой по доступу к ресурсам автоматизированной информационной системы регламентируются правилами разграничения доступа. subject
- 3.2.9. ОБЪЕКТ ДОСТУПА (В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ): единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения доступа. object
- 3.2.10. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (К ИНФОРМАЦИИ [РЕСУРСАМ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ]); НСД: доступ к информации [ресурсам автоматизированной информационной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам автоматизированной информационной системы]. unauthorized access
- 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.

3.2.11. **НЕСАНКЦИОНИРОВАННОЕ ВОЗДЕЙСТВИЕ**
(НА ИНФОРМАЦИЮ [РЕСУРСЫ АВТОМАТИЗИРОВАННОЙ
ИНФОРМАЦИОННОЙ СИСТЕМЫ]) (при применении
информационных технологий); НСВ: изменение
информации [ресурсов автоматизированной
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.
2. Изменение может быть осуществлено в форме замены
информации [ресурсов автоматизированной
информационной системы], введения новой
информации [новых ресурсов автоматизированной
информационной системы], а также уничтожения или
повреждения информации [ресурсов автоматизированной
информационной системы].

3.2.12. **АТАКА** (при применении информационных
технологий): действия, направленные на реализацию
угроз несанкционированного доступа к информации,
воздействия на нее или на ресурсы автоматизированной
информационной системы с применением программных
и (или) технических средств.

attack

3.2.13. **ВТОРЖЕНИЕ (В АВТОМАТИЗИРОВАННУЮ
ИНФОРМАЦИОННУЮ СИСТЕМУ)**: выявленный факт попытки
несанкционированного доступа к ресурсам
автоматизированной информационной системы.

intrusion

3.2.14. **БЛОКИРОВАНИЕ ДОСТУПА (К ИНФОРМАЦИИ)**
(при применении информационных технологий):
создание условий, препятствующих доступу
к информации субъекту, имеющему право на него.
Примечание - Создание условий, препятствующих
доступу к информации, может быть осуществлено
по времени доступа, функциям по обработке
информации (видам доступа) и (или) доступным
информационным ресурсам.

3.2.15. **ЗАКЛАДОЧНОЕ УСТРОЙСТВО**: техническое
средство, скрытно устанавливаемое на объекте
информатизации или в контролируемой зоне с целью
перехвата информации или несанкционированного
воздействия на информацию и (или) ресурсы
автоматизированной информационной системы.
Примечание - Местами установки закладочных устройств
на охраняемой территории могут быть любые элементы
контролируемой зоны, например ограждение,
конструкции, оборудование, предметы интерьера,
транспортные средства.

3.2.16. **ПРОГРАММНОЕ ВОЗДЕЙСТВИЕ**:
несанкционированное воздействие на ресурсы
автоматизированной информационной системы,
осуществляемое с использованием вредоносных программ.

3.2.17. **ВРЕДОНОСНАЯ ПРОГРАММА**: Программа,
предназначенная для осуществления
несанкционированного доступа и (или) воздействия
на информацию или ресурсы автоматизированной
информационной системы.

3.2.18. **(КОМПЬЮТЕРНЫЙ) ВИРУС**: Вредоносная

computer virus

программа, способная создавать вредоносные программы и (или) свои копии.

3.2.19. НЕДЕКЛАРИРОВАННЫЕ ВОЗМОЖНОСТИ (ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ): Функциональные возможности программного обеспечения, не описанные в документации.

3.2.20. ПРОГРАММНАЯ ЗАКЛАДКА: Преднамеренно внесенные в программное обеспечение функциональные объекты, которые при определенных условиях инициируют реализацию недеklarированных возможностей программного обеспечения. malicious logic

Примечание - Программная закладка может быть реализована в виде вредоносной программы или программного кода.

3.3. Меры технической защиты информации

3.3.1. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ; ТЗИ: technical information protection
обеспечение защиты некриптографическими методами информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию и носители информации в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации [1].

Примечание - Техническая защита информации при применении информационных технологий осуществляется в процессах сбора, обработки, передачи, хранения, распространения информации с целью обеспечения ее безопасности на объектах информатизации.

3.3.2. ПОЛИТИКА БЕЗОПАСНОСТИ (ИНФОРМАЦИИ В ОРГАНИЗАЦИИ): organizational security policy
Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

3.3.3. ПРОФИЛЬ ЗАЩИТЫ: совокупность типовых требований по обеспечению безопасности информации, которые должны быть реализованы в защищаемой автоматизированной информационной системе. protection profile
Примечание - Профиль защиты может разрабатываться для автоматизированной информационной системы, средства вычислительной техники, а также их технических и программных средств.

3.3.4. АУДИТ БЕЗОПАСНОСТИ (ИНФОРМАЦИИ): security audit
совокупность действий по независимой проверке и изучению документации автоматизированной информационной системы, а также по испытаниям средств защиты информации, направленная на обеспечение выполнения установленной политики безопасности информации и правил эксплуатации автоматизированной информационной системы, на выявление уязвимостей автоматизированной информационной системы и на выработку рекомендаций по устранению выявленных недостатков в средствах защиты информации, политике безопасности информации и правилах эксплуатации автоматизированной информационной системы.

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

(внутренний аудит) .

3.3.5. АУДИТ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ: проверка реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию.	computer-system audit
3.3.6. МОНИТОРИНГ БЕЗОПАСНОСТИ ИНФОРМАЦИИ (при применении информационных технологий): процедуры регулярного наблюдения за процессом обеспечения безопасности информации при применении информационных технологий.	IT security monitoring
3.3.7. ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА (В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ): правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе.	
3.3.8. АУТЕНТИФИКАЦИЯ (СУБЪЕКТА ДОСТУПА): действия по проверке подлинности субъекта доступа в автоматизированной информационной системе.	authentication
3.3.9. ИДЕНТИФИКАЦИЯ: Действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.	identification

Алфавитный указатель терминов

АТАКА	3.2.12
АУДИТ БЕЗОПАСНОСТИ	3.3.4
АУДИТ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.3.5
АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	3.3.4
АУТЕНТИФИКАЦИЯ	3.3.8
АУТЕНТИФИКАЦИЯ СУБЪЕКТА ДОСТУПА	3.3.8
БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.1.6
БЕЗОПАСНОСТЬ ДАННЫХ	3.1.4
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ	3.1.4, 3.1.5
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	3.1.5
БЛОКИРОВАНИЕ ДОСТУПА	3.2.14
БЛОКИРОВАНИЕ ДОСТУПА К ИНФОРМАЦИИ	3.2.14
ВИРУС	3.2.18
ВИРУС КОМПЬЮТЕРНЫЙ	3.2.18
ВОЗДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОЕ	3.2.11
ВОЗДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОЕ НА ИНФОРМАЦИЮ	3.2.11
ВОЗДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОЕ НА РЕСУРСЫ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.2.11
ВОЗДЕЙСТВИЕ ПРОГРАММНОЕ	3.2.16
ВОЗМОЖНОСТИ НЕДЕКЛАРИРОВАННЫЕ	3.2.19
ВОЗМОЖНОСТИ НЕДЕКЛАРИРОВАННЫЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	3.2.19
ВТОРЖЕНИЕ	3.2.13
ВТОРЖЕНИЕ В АВТОМАТИЗИРОВАННУЮ ИНФОРМАЦИОННУЮ СИСТЕМУ	3.2.13
ДОСТУП	3.2.7
ДОСТУП В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ	3.2.7
ДОСТУП НЕСАНКЦИОНИРОВАННЫЙ	3.2.10
ДОСТУП НЕСАНКЦИОНИРОВАННЫЙ К ИНФОРМАЦИИ	3.2.10
ДОСТУП НЕСАНКЦИОНИРОВАННЫЙ К РЕСУРСАМ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.2.10
ДОСТУПНОСТЬ	3.1.9
ДОСТУПНОСТЬ ИНФОРМАЦИИ	3.1.9
ДОСТУПНОСТЬ РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.1.9
ЗАКЛАДКА ПРОГРАММНАЯ	3.2.20
ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКАЯ	3.3.1

ИДЕНТИФИКАЦИЯ	3.3.9
ИСТОЧНИК УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	3.2.2
КОНФИДЕНЦИАЛЬНОСТЬ	3.1.7
КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ	3.1.7
КОНФИДЕНЦИАЛЬНОСТЬ РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.1.7
МОНИТОРИНГ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	3.3.6
НСВ	3.2.11
НСД	3.2.10
ОБЪЕКТ ДОСТУПА	3.2.9
ОБЪЕКТ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ	3.2.9
ПЕРЕХВАТ	3.2.5
ПЕРЕХВАТ ИНФОРМАЦИИ	3.2.5
ПОДЛИННОСТЬ	3.1.11
ПОДЛИННОСТЬ РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.1.11
ПОДОТЧЕТНОСТЬ	3.1.10
ПОДОТЧЕТНОСТЬ РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.1.10
ПОЛИТИКА БЕЗОПАСНОСТИ	3.3.2
ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ	3.3.2
ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА	3.3.7
ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ	3.3.7
ПРОГРАММА ВРЕДНОСНАЯ	3.2.17
ПРОФИЛЬ ЗАЩИТЫ	3.3.3
РЕСУРСЫ ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ	3.1.2
РЕСУРСЫ ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.1.2
СИГНАЛ ИНФОРМАТИВНЫЙ	3.2.6
СИСТЕМА ЗАЩИЩАЕМАЯ АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ	3.1.1
СУБЪЕКТ ДОСТУПА	3.2.8
СУБЪЕКТ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ	3.2.8
ТЕХНОЛОГИЯ ЗАЩИЩАЕМАЯ ИНФОРМАЦИОННАЯ	3.1.3
ТЗИ	3.3.1
УГРОЗА	3.2.1
УГРОЗА БЕЗОПАСНОСТИ ИНФОРМАЦИИ	3.2.1
УСТРОЙСТВО ЗАКЛАДЧНОЕ	3.2.15
УТЕЧКА ИНФОРМАЦИИ ПО ТЕХНИЧЕСКОМУ КАНАЛУ	3.2.4
УТЕЧКА ПО ТЕХНИЧЕСКОМУ КАНАЛУ	3.2.4
УЯЗВИМОСТЬ	3.2.3
УЯЗВИМОСТЬ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.2.3
ЦЕЛОСТНОСТЬ	3.1.8
ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ	3.1.8
ЦЕЛОСТНОСТЬ РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ	3.1.8

Алфавитный указатель иноязычных
эквивалентов стандартизованных терминов

access	3.2.7
accountability	3.1.10
attack	3.2.12
authentication	3.3.8
authenticity	3.1.11
availability	3.1.9
computer-system audit	3.3.5
computer virus	3.2.18
confidentiality	3.1.7
data security	3.1.4
identification	3.3.9
information security	3.1.4
informative signal	3.2.6

integrity	3.1.8
interception	3.2.5
intrusion	3.2.13
IT security	3.1.5
IT security monitoring	3.3.6
leakage	3.2.4
malicious logic	3.2.20
object	3.2.9
organizational security policy	3.3.2
protection profile	3.3.3
security audit	3.3.4
subject	3.2.8
technical information protection	3.3.1
threat	3.2.1
trusted computer system	3.1.1
unauthorized access	3.2.10
vulnerability	3.2.3

Приложение А
(справочное)

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ОБЩЕТЕХНИЧЕСКИХ ПОНЯТИЙ

А.1. ЗАЩИТА ИНФОРМАЦИИ; ЗИ: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
[ГОСТ Р 50922, [статья 2](#)]

А.2. АВТОМАТИЗИРОВАННАЯ СИСТЕМА: система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
[ГОСТ 34.003, [статья 1](#)]

А.3. ИНФОРМАЦИОННАЯ СИСТЕМА: организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи [\[2\]](#).

А.4. ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ: информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Примечание – Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.
[ГОСТ Р 50922, [статья 1](#)]

А.5. ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ: приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных.
[ГОСТ Р 34.003, [приложение 1, статья 4](#)]

А.6. 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, пункт 2.1]

А.7. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ: состояние информационной технологии, определяющее защищенность информации и ресурсов информационной технологии от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность информационной технологии выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений [3]

А.8. БЕЗОПАСНОСТЬ: отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.
[ГОСТ 1.1, статья А.7]

А.9. ДАННЫЕ: информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.
[ГОСТ 15971, статья 1]

А.10. РИСК: сочетание вероятности нанесения ущерба и тяжести этого ущерба.
[ГОСТ Р 51898, пункт 3.2]

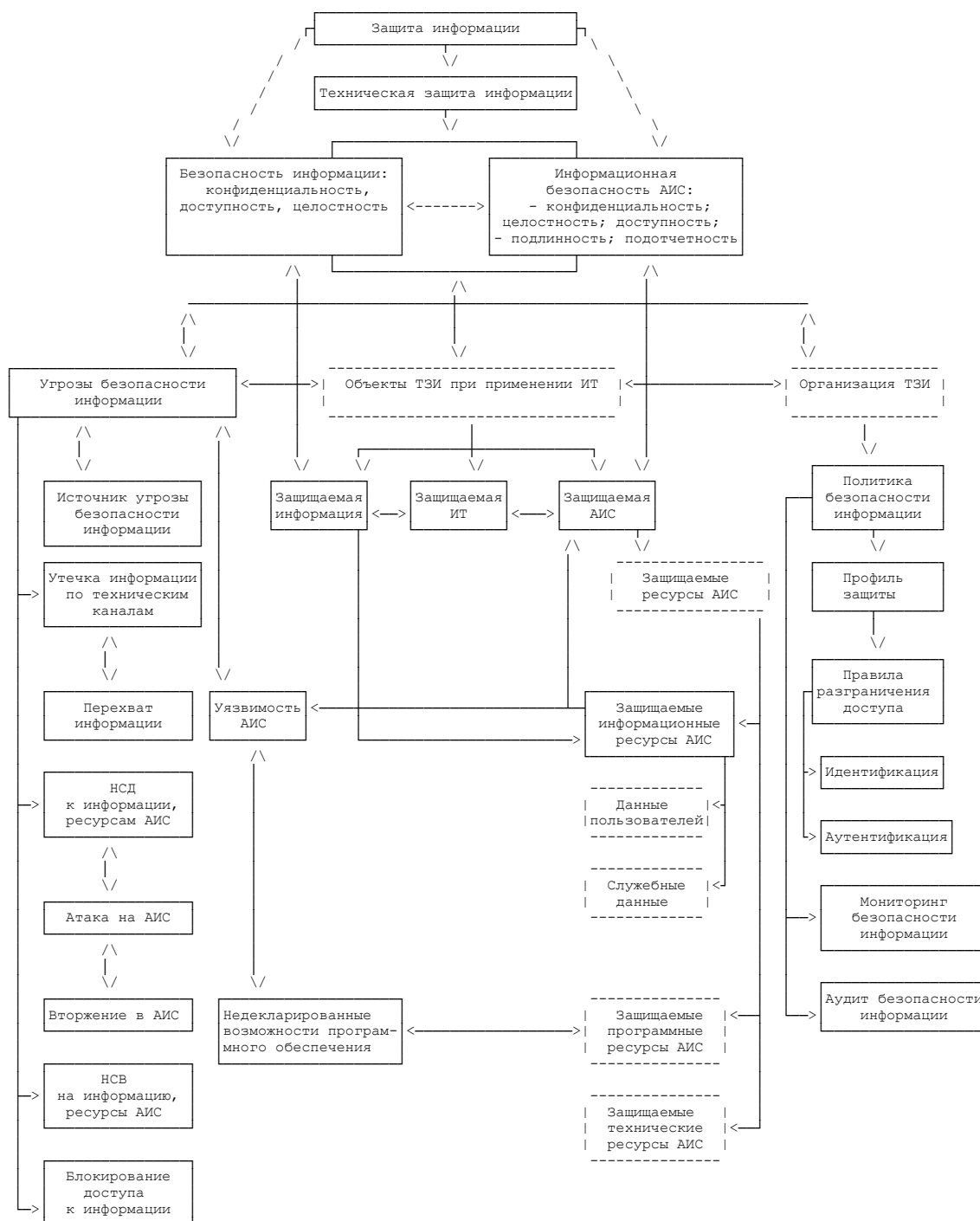
А.11. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ: деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.
[ГОСТ Р 50922, статья 3]

А.12. ТРЕБОВАНИЕ: положение нормативного документа, содержащее критерии, которые должны быть соблюдены.
[ГОСТ 1.1, статья 6.1.1]


А.13. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА: защита данных при помощи криптографического преобразования данных.

Приложение Б
(рекомендуемое)

СХЕМА
ВЗАИМОСВЯЗИ СТАНДАРТИЗОВАННЫХ ТЕРМИНОВ



Условные обозначения:

-
- > - взаимосвязь типа "род-вид";
<———— - ассоциативная взаимосвязь;
 - стандартизованные термины;

|-----| - нестандартизованные термины.

БИБЛИОГРАФИЯ

- [1] [Положение](#) о Федеральной службе по техническому и экспортному контролю. Утверждено Указом Президента Российской Федерации от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"
- [2] Федеральный [закон](#) Российской Федерации от 20.02.1995 N 24-ФЗ (в ред. Федерального закона от 10.01.2003 N 15-ФЗ) "Об информации, информатизации и защите информации"
- [3] Руководящий [документ](#) Гостехкомиссии России "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий". Введен в действие Приказом Гостехкомиссии России от 19.06.02 N 187.
-