

---

---

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

---



РЕКОМЕНДАЦИИ  
ПО СТАНДАРТИЗАЦИИ

**P 50.1.053—  
2005**

---

**Информационные технологии  
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ  
В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ  
ИНФОРМАЦИИ**

Издание официальное

Москва  
Стандартинформ  
2005

## **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. № 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»*

© Стандартинформ, 2005

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

## **Содержание**

<b>1 Область применения . . . . .</b>	<b>1</b>
<b>2 Нормативные ссылки . . . . .</b>	<b>1</b>
<b>3 Стандартизованные термины и определения . . . . .</b>	<b>1</b>
3.1 Объекты технической защиты информации . . . . .	1
3.2 Угрозы безопасности информации . . . . .	2
3.3 Меры технической защиты информации . . . . .	4
<b>Алфавитный указатель терминов . . . . .</b>	<b>5</b>
<b>Алфавитный указатель иноязычных эквивалентов стандартизованных терминов . . . . .</b>	<b>7</b>
<b>Приложение А (справочное) Термины и определения общетехнических понятий . . . . .</b>	<b>8</b>
<b>Приложение Б (рекомендуемое) Схема взаимосвязи стандартизованных терминов . . . . .</b>	<b>10</b>
<b>Библиография . . . . .</b>	<b>11</b>

## 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 терминоэлементы.

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.

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

**Информационные технологии**

**ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ  
ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

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

---

**Дата введения — 2006—01—01**

**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

**П р и м е ч а н и я —** 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 заменным (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.

## **P 50.1.053—2005**

**П р и м е ч а н и е —** 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.

**П р и м е ч а н и е —** 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.

**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.

**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.

**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.

**П р и м е ч а н и е —** 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.

**3.1.11 подлинность (ресурсов автоматизированной информационной системы):** Состояние ресурсов автоматизированной информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, 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.

**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.

information [data]  
security

IT security

confidentiality

integrity

availability

accountability

authenticity

threat

vulnerability

<b>3.2.4 утечка (информации) по техническому каналу:</b> Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.	leakage
<b>3.2.5 перехват (информации):</b> Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.	interception
<b>3.2.6 информативный сигнал:</b> Сигнал, по параметрам которого может быть определена защищаемая информация.	informative signal
<b>3.2.7 доступ (в автоматизированной информационной системе):</b> 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
<b>Примечание —</b> Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты.	
<b>3.2.8 субъект доступа (в автоматизированной информационной системе):</b> Лицо или единица ресурса автоматизированной информационной системы, действия которой по доступу к ресурсам автоматизированной информационной системы регламентируются правилами разграничения доступа.	subject
<b>3.2.9 объект доступа (в автоматизированной информационной системе):</b> Единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения доступа.	object
<b>3.2.10 несанкционированный доступ (к информации [ресурсам автоматизированной информационной системы]); НСД:</b> Доступ к информации [ресурсам автоматизированной информационной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам автоматизированной информационной системы].	unauthorized access
<b>Примечания</b>	
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.	
<b>3.2.11 несанкционированное воздействие (на информацию [ресурсы автоматизированной информационной системы]) (при применении информационных технологий); НСВ:</b> Изменение информации [ресурсов автоматизированной информационной системы], осуществляемое с нарушением установленных прав и (или) правил.	
<b>Примечания</b>	
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].	
<b>3.2.12 атака (при применении информационных технологий):</b> 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
<b>3.2.13 вторжение (в автоматизированную информационную систему):</b> Выявленный факт попытки несанкционированного доступа к ресурсам автоматизированной информационной системы.	intrusion
<b>3.2.14 блокирование доступа (к информации) (при применении информационных технологий):</b> Создание условий, препятствующих доступу к информации субъекту, имеющему право на него.	

**П р и м е ч а н и е —** 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.

**П р и м е ч а н и е —** 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, осуществляющееся 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 программа, способная создавать вредоносные программы и (или) свои копии.

computer virus

**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 недекларированных возможностей программного обеспечения.

malicious logic

**П р и м е ч а н и е —** 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:** 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].

technical information protection

**П р и м е ч а н и е —** 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):** Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

organizational security policy

**3.3.3 профиль защиты:** Совокупность типовых требований по обеспечению безопасности информации, которые должны быть реализованы в защищаемой автоматизированной информационной системе.

protection profile

**П р и м е ч а н и е —** Профиль защиты может разрабатываться для автоматизированной информационной системы, средства вычислительной техники, а также их технических и программных средств.

**3.3.4 аудит безопасности (информации):** 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 инфор-

security audit

мации, политике безопасности информации и правилах эксплуатации автоматизированной информационной системы.

**П р и м е ч а н и е** — Аудит безопасности может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией (внешний аудит), а также подразделением или должностным лицом организации (внутренний аудит).

<b>3.3.5 аудит безопасности автоматизированной информационной системы:</b> 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
<b>3.3.6 мониторинг безопасности информации</b> (при применении информационных технологий): Процедуры регулярного наблюдения за процессом обеспечения безопасности информации при применении информационных технологий.	IT security monitoring
<b>3.3.7 правила разграничения доступа (в автоматизированной информационной системе):</b> Правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе.	
<b>3.3.8 аутентификация (субъекта доступа):</b> Действия по проверке подлинности субъекта доступа в автоматизированной информационной системе.	authentication
<b>3.3.9 идентификация:</b> Действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.	identification

#### Алфавитный указатель терминов

<b>атака</b> . . . . .	3.2.12
<b>аудит безопасности</b> . . . . .	3.3.4
<b>аудит безопасности автоматизированной информационной системы</b> . . . . .	3.3.5
<b>аудит безопасности информации</b> . . . . .	3.3.4
<b>аутентификация</b> . . . . .	3.3.8
<b>аутентификация субъекта доступа</b> . . . . .	3.3.8
<b>безопасность автоматизированной информационной системы</b> . . . . .	3.1.6
<b>безопасность данных</b> . . . . .	3.1.4
<b>безопасность информации</b> . . . . .	3.1.4, 3.1.5
<b>безопасность информации при применении информационных технологий</b> . . . . .	3.1.5
<b>блокирование доступа</b> . . . . .	3.2.14
<b>блокирование доступа к информации</b> . . . . .	3.2.14
<b>вирус</b> . . . . .	3.2.18
<b>вирус компьютерный</b> . . . . .	3.2.18
<b>воздействие несанкционированное</b> . . . . .	3.2.11
<b>воздействие несанкционированное на информацию</b> . . . . .	3.2.11
<b>воздействие несанкционированное на ресурсы автоматизированной информационной системы</b> . . . . .	3.2.11
<b>воздействие программное</b> . . . . .	3.2.16
<b>возможности недекларированные</b> . . . . .	3.2.19
<b>возможности недекларированные программного обеспечения</b> . . . . .	3.2.19
<b>вторжение</b> . . . . .	3.2.13
<b>вторжение в автоматизированную информационную систему</b> . . . . .	3.2.13
<b>доступ</b> . . . . .	3.2.7
<b>доступ в автоматизированной информационной системе</b> . . . . .	3.2.7
<b>доступ несанкционированный</b> . . . . .	3.2.10
<b>доступ несанкционированный к информации</b> . . . . .	3.2.10
<b>доступ несанкционированный к ресурсам автоматизированной информационной системы</b> . . . . .	3.2.10
<b>доступность</b> . . . . .	3.1.9
<b>доступность информации</b> . . . . .	3.1.9
<b>доступность ресурсов автоматизированной информационной системы</b> . . . . .	3.1.9
<b>закладка программная</b> . . . . .	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 вредоносная . . . . .	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 закладочное . . . . .	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

**A.1 защита информации;** ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.  
[ГОСТ Р 50922, статья 2]

**A.2 автоматизированная система:** Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.  
[ГОСТ 34.003, статья 1]

**A.3 информационная система:** Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи [2].

**A.4 защищаемая информация:** Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**П р и м е ч а н и е** — Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

[ГОСТ Р 50922, статья 1]

**A.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]

**A.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]

**A.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]

**A.8 безопасность:** Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.  
[ГОСТ 1.1, статья А.7]

**A.9 данные:** Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.  
[ГОСТ 15971, статья 4]

**A.10 риск:** Сочетание вероятности нанесения ущерба и тяжести этого ущерба.  
[ГОСТ Р 51898, пункт 3.2]

**A.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]

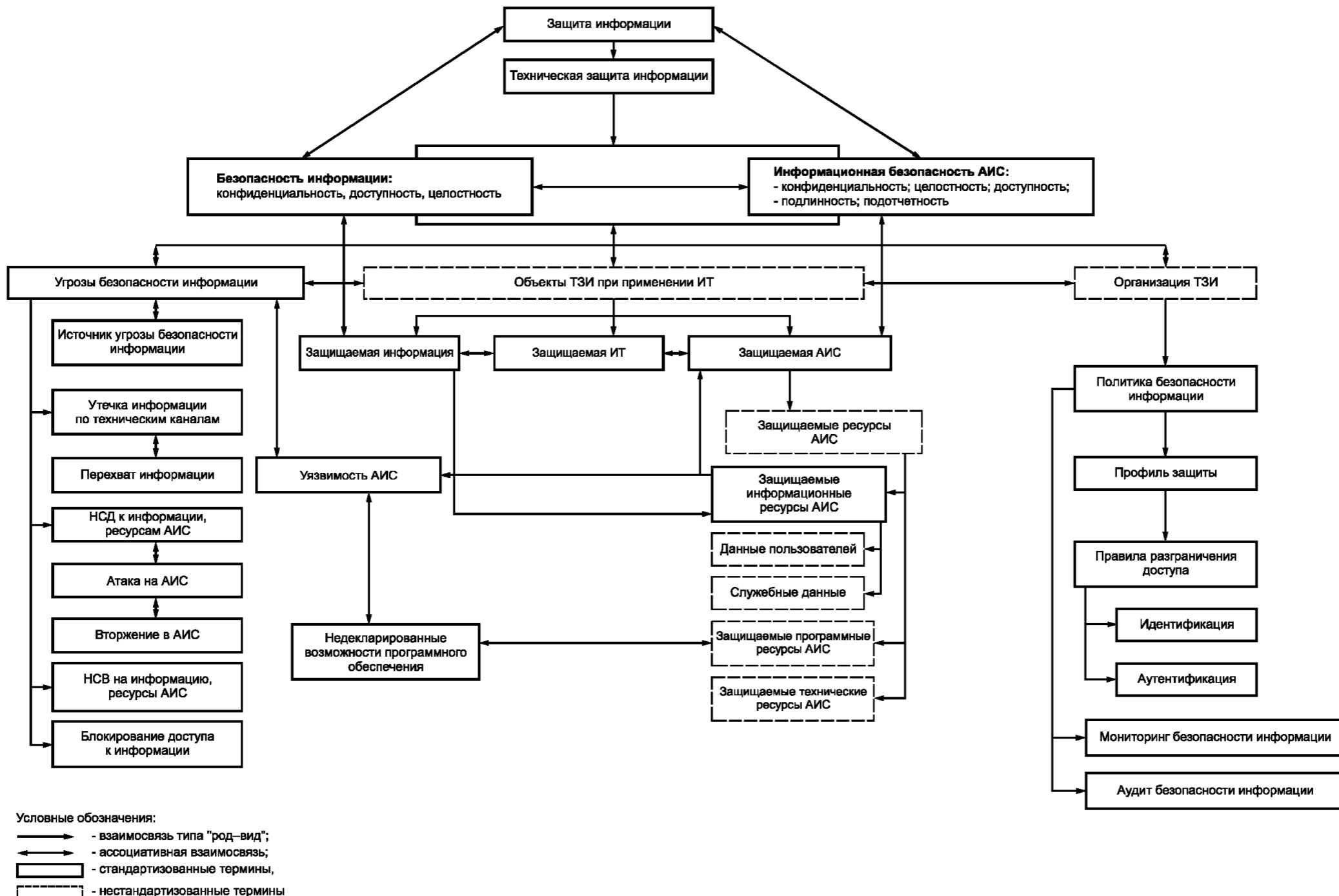
**A.12 требование:** Положение нормативного документа, содержащее критерии, которые должны быть соблюдены.

[ГОСТ 1.1, статья 6.1.1]

**A.13 криптографическая защита:** Защита данных при помощи криптографического преобразования данных.

**Приложение Б  
(рекомендуемое)**

**Схема взаимосвязи стандартизованных терминов**



### **Библиография**

- [1] Положение о Федеральной службе по техническому и экспортному контролю. Утверждено Указом Президента Российской Федерации от 16.08.2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
- [2] Федеральный закон Российской Федерации от 20.02.1995 № 24—ФЗ (в ред. Федерального закона от 10.01.2003 г. № 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 г. № 187

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

**Рекомендации по стандартизации**

**Информационные технологии**

**ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ  
В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

**P 50.1.053—2005**

**Б3 9—2004/9**

Редактор *Л.И. Нахимова*  
Технический редактор *О.Н. Власова*  
Корректор *В.Е. Нестерова*  
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 13.04.2005. Подписано в печать 04.05.2005. Формат 60×84<sup>1/8</sup>. Бумага офсетная. Гарнитура Arial.  
Печать офсетная. Усл. печ. л. 1,86. Уч.-изд. л. 1,30. Тираж 480 экз. Зак. 267. Изд. № 3323/4. С 1017.

ФГУП «Стандартинформ», 123995 Москва, Гранатный пер., 4.  
[www.gostinfo.ru](http://www.gostinfo.ru) [info@gostinfo.ru](mailto:info@gostinfo.ru)

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