

---

ФЕДЕРАЛЬНОЕ АГЕНТСТВО  
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

---



НАЦИОНАЛЬНЫЙ  
СТАНДАРТ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ

ГОСТ Р  
50922—  
2006

---

**Защита информации**

# **ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

БЗ 1—2007/378

Москва

2008

## Предисловие

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

### Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст

4 В настоящем стандарте реализованы нормы Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

5 ВЗАМЕН ГОСТ Р 50922—96

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

## Содержание

1	Область применения . . . . .	1
2	Термины и определения . . . . .	1
2.1	Общие понятия . . . . .	1
2.2	Термины, относящиеся к видам защиты информации . . . . .	1
2.3	Термины, относящиеся к способам защиты информации . . . . .	1
2.4	Термины, относящиеся к замыслу защиты информации. . . . .	2
2.5	Термины, относящиеся к объекту защиты информации . . . . .	2
2.6	Термины, относящиеся к угрозам безопасности информации. . . . .	3
2.7	Термины, относящиеся к технике защиты информации . . . . .	3
2.8	Термины, относящиеся к способам оценки соответствия требованиям по защите информации	4
2.9	Термины, относящиеся к эффективности защиты информации. . . . .	4
	Алфавитный указатель терминов . . . . .	4
	Приложение А (справочное) Термины и определения общетехнических понятий . . . . .	7
	Библиография . . . . .	8

## Введение

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

Для каждого понятия установлен один стандартизованный термин.

Наличие квадратных скобок в терминологической статье означает, что в нее входят два термина, имеющих общие терминологические элементы. В алфавитном указателе данные термины приведены отдельно. Цифра, заключенная в квадратные скобки, означает ссылку на документ, приведенный в структурном элементе «Библиография».

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

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

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

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

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

## Защита информации

## ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Protection of information. Basic terms and definitions

Дата введения — 2008—02—01

## 1 Область применения

Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации.

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

## 2 Термины и определения

### 2.1 Общие понятия

2.1.1 **защита информации; ЗИ:** Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

### 2.2 Термины, относящиеся к видам защиты информации

2.2.1 **правовая защита информации:** Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

2.2.2 **техническая защита информации; ТЗИ:** Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

2.2.3 **криптографическая защита информации:** Защита информации с помощью ее криптографического преобразования.

2.2.4 **физическая защита информации:** Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

### Примечания

1 Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

2 К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

### 2.3 Термины, относящиеся к способам защиты информации

2.3.1 **способ защиты информации:** Порядок и правила применения определенных принципов и средств защиты информации.

**2.3.2 защита информации от утечки:** Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранцами] разведками и другими заинтересованными субъектами.

П р и м е ч а н и е — Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

**2.3.3 защита информации от несанкционированного воздействия;** ЗИ от НСВ: Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**2.3.4 защита информации от непреднамеренного воздействия:** Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**2.3.5 защита информации от разглашения:** Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

**2.3.6 защита информации от несанкционированного доступа;** ЗИ от НСД: Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

П р и м е ч а н и е — Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

**2.3.7 защита информации от преднамеренного воздействия;** ЗИ от ПДВ: Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

**2.3.8 защита информации от [иностранной] разведки:** Защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

## **2.4 Термины, относящиеся к замыслу защиты информации**

**2.4.1 замысел защиты информации:** Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

**2.4.2 цель защиты информации:** Заранее намеченный результат защиты информации.

П р и м е ч а н и е — Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

**2.4.3 система защиты информации:** Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

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

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

## **2.5 Термины, относящиеся к объекту защиты информации**

**2.5.1 объект защиты информации:** Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

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

**Примечание** — Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

**2.5.3 носитель защищаемой информации:** Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

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

## 2.6 Термины, относящиеся к угрозам безопасности информации

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

**2.6.2 фактор, воздействующий на защищаемую информацию:** Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

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

**2.6.4 уязвимость (информационной системы); брешь:** Свойство информационной системы, обуславливающее 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.

**2.6.5 вредоносная программа:** Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы.

**2.6.6 несанкционированное воздействие на информацию:** Воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

**2.6.7 преднамеренное силовое электромагнитное воздействие на информацию:** Несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем.

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

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

## 2.7 Термины, относящиеся к технике защиты информации

**2.7.1 техника защиты информации:** Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

**2.7.2 средство защиты информации:** Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**2.7.3 средство контроля эффективности защиты информации:** Средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

**2.7.4 средство физической защиты информации:** Средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.

**2.7.5 криптографическое средство защиты информации:** Средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

## **2.8 Термины, относящиеся к способам оценки соответствия требованиям по защите информации**

**2.8.1 оценка соответствия требованиям по защите информации:** Прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

**2.8.2 лицензирование в области защиты информации:** Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

**2.8.3 сертификация на соответствие требованиям по безопасности информации:** Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

*Примечание* — К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации.

**2.8.4 специальное исследование (объекта защиты информации):** Исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации.

**2.8.5 специальная проверка:** Проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

**2.8.6 аудиторская проверка информационной безопасности в организации; аудит информационной безопасности в организации:** Периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень 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).

**2.8.7 мониторинг безопасности информации:** Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

**2.8.8 экспертиза документа по защите информации:** Рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение.

*Примечание* — Экспертиза документа по защите информации может включать в себя научно-техническую, правовую, метрологическую, патентную и терминологическую экспертизу.

**2.8.9 анализ информационного риска:** Систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

**2.8.10 оценка информационного риска:** Общий процесс анализа информационного риска и его оценивания.

## **2.9 Термины, относящиеся к эффективности защиты информации**

**2.9.1 эффективность защиты информации:** Степень соответствия результатов защиты информации цели защиты информации.

**2.9.2 требование по защите информации:** Установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

**2.9.3 показатель эффективности защиты информации:** Мера или характеристика для оценки эффективности защиты информации.

**2.9.4 норма эффективности защиты информации:** Значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.



## Алфавитный указатель терминов\*

<b>анализ информационного риска</b>	2.8.9
<i>аудит информационной безопасности в организации</i>	2.8.6
<b>безопасность данных</b>	2.4.5
<b>безопасность информации</b>	2.4.5
<i>брешь</i>	2.6.4
<b>воздействие на информацию несанкционированное</b>	2.6.6
<b>воздействие на информацию электромагнитное силовое преднамеренное</b>	2.6.7
<b>замысел защиты информации</b>	2.4.1
<b>защита информации</b>	2.1.1
<b>защита информации от иностранной разведки</b>	2.3.8
<b>защита информации криптографическая</b>	2.2.3
<b>защита информации от несанкционированного воздействия</b>	2.3.3
<b>защита информации от непреднамеренного воздействия</b>	2.3.4
<b>защита информации от несанкционированного доступа</b>	2.3.6
<b>защита информации правовая</b>	2.2.1
<b>защита информации от преднамеренного воздействия</b>	2.3.7
<b>защита информации от разведки</b>	2.3.8
<b>защита информации от разглашения</b>	2.3.5
<b>защита информации техническая</b>	2.2.2
<b>защита информации от утечки</b>	2.3.2
<b>защита информации физическая</b>	2.2.4
<b>ЗИ</b>	2.1.1
<b>ЗИ от НСВ</b>	2.3.3
<b>ЗИ от НСД</b>	2.3.6
<b>ЗИ от ПДВ</b>	2.3.7
<b>информация защищаемая</b>	2.5.2
<b>исследование объекта защиты информации специальное</b>	2.8.4
<b>исследование специальное</b>	2.8.4
<b>источник угрозы безопасности информации</b>	2.6.3
<b>лицензирование в области защиты информации</b>	2.8.2
<b>модель угроз</b>	2.6.8
<b>модель угроз безопасности информации</b>	2.6.8
<b>мониторинг безопасности информации</b>	2.8.7
<b>норма эффективности защиты информации</b>	2.9.4
<b>носитель защищаемой информации</b>	2.5.3
<b>объект защиты информации</b>	2.5.1
<b>объект информатизации защищаемый</b>	2.5.4
<b>оценка информационного риска</b>	2.8.10
<b>оценка соответствия требованиям по защите информации</b>	2.8.1
<b>показатель эффективности защиты информации</b>	2.9.3
<b>политика безопасности</b>	2.4.4
<b>политика безопасности информации в организации</b>	2.4.4
<b>проверка информационной безопасности в организации аудиторская</b>	2.8.6
<b>проверка специальная</b>	2.8.5
<b>программа вредоносная</b>	2.6.5

\* Здесь и далее краткие формы терминов выделены светлым шрифтом.

## ГОСТ Р 50922—2006

<b>сертификация на соответствие требованиям по безопасности информации</b>	2.8.3
<b>система защиты информации</b>	2.4.3
<b>система информационная защищаемая</b>	2.5.5
<b>способ защиты информации</b>	2.3.1
<b>средство защиты информации</b>	2.7.2
<b>средство защиты информации криптографическое</b>	2.7.5
<b>средство контроля эффективности защиты информации</b>	2.7.3
<b>средство физической защиты информации</b>	2.7.4
<b>техника защиты информации</b>	2.7.1
<b>ТЗИ</b>	2.2.2
<b>требование по защите информации</b>	2.9.2
<b>угроза</b>	2.6.1
<b>угроза безопасности информации</b>	2.6.1
<b>уязвимость</b>	2.6.4
<b>уязвимость информационной системы</b>	2.6.4
<b>фактор, воздействующий на защищаемую информацию</b>	2.6.2
<b>цель защиты информации</b>	2.4.2
<b>экспертиза документа по защите информации</b>	2.8.8
<b>эффективность защиты информации</b>	2.9.1

**Приложение А**  
**(справочное)**

**Термины и определения общетехнических понятий**

- A.1 информация: Сведения (сообщения, данные) независимо от формы их представления [1].
- A.2 документированная информация: Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель [1].
- A.3 информация, составляющая коммерческую тайну: Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны [2].
- A.4 данные: Факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации.
- A.5 носитель информации: Материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
- A.6 информационная система: Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [1].
- A.7 обладатель информации: Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [1].
- A.8 пользователь информации: Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.
- A.9 доступ к информации: Возможность получения информации и ее использования [1].
- A.10 право доступа к защищаемой информации; право доступа: Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.
- A.11 правило доступа к защищаемой информации; правило доступа: Совокупность правил, устанавливающих порядок и условия доступа субъекта к защищаемой информации и ее носителям.
- A.12 конфиденциальность информации: Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [1].
- A.13 предоставление информации: Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц [1].
- A.14 распространение информации: Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц [1].
- A.15 оператор информационной системы: Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных [1].
- A.16 доступность информации [ресурсов информационной системы]: Состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно [3].
- П р и м е ч а н и е — К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов [3].
- A.17 целостность: Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Библиография

- |     |  |   |
|-----|--|---|
| [1] | Российская Федерация.<br>Федеральный закон от 27.07.2006 г. № 149-ФЗ | Об информации, информационных технологиях и о защите информации |
| [2] | Российская Федерация.<br>Федеральный закон от 29.07.2004 г. № 98-ФЗ  | О коммерческой тайне  |
| [3] | Рекомендации по стандартизации Р 50.1.056—2005                       | Техническая защита информации. Основные термины и определения   |

---

УДК 001.4:025.4:006.354

ОКС 01.040.01

Э00

ОКСТУ 0090

Ключевые слова: информация, защита информации, носитель информации, обладатель информации, эффективность защиты информации

---