Утвержден и введен в действие

Приказом Федерального

агентства по техническому

регулированию и метрологии

от 27 декабря 2006 г. N 373-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАЩИТА ИНФОРМАЦИИ

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Protection of information. Basic terms and definitions

ГОСТ Р 50922-2006

Группа Э00

ОКС 01.040.01;

ОКСТУ 0090

Дата введения

1 февраля 2008 года

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 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. N 373-ст.

4. В настоящем стандарте реализованы нормы Федеральных законов от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и от 29 июля 2004 г. N 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.

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 терминоэлементы. В [алфавитном указателе](#P159) данные термины приведены отдельно. Цифра, заключенная в квадратные скобки, означает ссылку на документ, приведенный в структурном элементе ["Библиография"](#P264).

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.

#: примечание.

Стандартизованные термины, набранные полужирным шрифтом в официальном тексте документа, в электронной версии документа отмечены знаком "#"; синонимы, набранные курсивом в официальном тексте документа, в электронной версии документа отмечены знаком "&".

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](#P238).

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, , 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 [иностранными] разведками и другими заинтересованными субъектами.

Примечание. 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.

Примечание. 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.

Примечание. 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, обусловливающее 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 экспертизы.

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 <\*>

--------------------------------

<\*> Здесь и далее краткие формы терминов выделены светлым шрифтом

#анализ информационного риска# [2.8.9](#P149)

&аудит информационной безопасности в организации& [2.8.6](#P142)

#безопасность данных# [2.4.5](#P97)

#безопасность информации# [2.4.5](#P97)

&брешь& [2.6.4](#P114)

#воздействие на информацию несанкционированное# [2.6.6](#P119)

#воздействие на информацию электромагнитное силовое [2.6.7](#P120)

преднамеренное#

#замысел защиты информации# [2.4.1](#P91)

#защита информации# [2.1.1](#P63)

#защита информации от иностранной разведки# [2.3.8](#P87)

#защита информации криптографическая# [2.2.3](#P69)

#защита информации от несанкционированного воздействия# [2.3.3](#P80)

#защита информации от непреднамеренного воздействия# [2.3.4](#P81)

#защита информации от несанкционированного доступа# [2.3.6](#P83)

#защита информации правовая# [2.2.1](#P67)

#защита информации от преднамеренного воздействия# [2.3.7](#P86)

#защита информации от разведки# [2.3.8](#P87)

#защита информации от разглашения# [2.3.5](#P82)

#защита информации техническая# [2.2.2](#P68)

#защита информации от утечки# [2.3.2](#P77)

#защита информации физическая# [2.2.4](#P70)

ЗИ [2.1.1](#P63)

ЗИ от НСВ [2.3.3](#P80)

ЗИ от НСД [2.3.6](#P83)

ЗИ от ПДВ [2.3.7](#P86)

#информация защищаемая# [2.5.2](#P102)

#исследование объекта защиты информации специальное# [2.8.4](#P140)

исследование специальное [2.8.4](#P140)

#источник угрозы безопасности информации# [2.6.3](#P113)

#лицензирование в области защиты информации# [2.8.2](#P136)

модель угроз [2.6.8](#P121)

#модель угроз безопасности информации# [2.6.8](#P121)

#мониторинг безопасности информации# [2.8.7](#P145)

#норма эффективности защиты информации# [2.9.4](#P157)

#носитель защищаемой информации# [2.5.3](#P105)

#объект защиты информации# [2.5.1](#P101)

#объект информатизации защищаемый# [2.5.4](#P106)

#оценка информационного риска# [2.8.10](#P150)

#оценка соответствия требованиям по защите информации# [2.8.1](#P135)

#показатель эффективности защиты информации# [2.9.3](#P156)

политика безопасности [2.4.4](#P96)

#политика безопасности информации в организации# [2.4.4](#P96)

#проверка информационной безопасности в организации аудиторская# [2.8.6](#P142)

#проверка специальная# [2.8.5](#P141)

#программа вредоносная# [2.6.5](#P118)

#сертификация на соответствие требованиям по безопасности [2.8.3](#P137)

информации#

#система защиты информации# [2.4.3](#P95)

#система информационная защищаемая# [2.5.5](#P107)

#способ защиты информации# [2.3.1](#P76)

#средство защиты информации# [2.7.2](#P127)

#средство защиты информации криптографическое# [2.7.5](#P130)

#средство контроля эффективности защиты информации# [2.7.3](#P128)

#средство физической защиты информации# [2.7.4](#P129)

#техника защиты информации# [2.7.1](#P126)

ТЗИ [2.2.2](#P68)

#требование по защите информации# [2.9.2](#P155)

угроза [2.6.1](#P111)

#угроза безопасности информации# [2.6.1](#P111)

уязвимость [2.6.4](#P114)

#уязвимость информационной системы# [2.6.4](#P114)

#фактор, воздействующий на защищаемую информацию# [2.6.2](#P112)

#цель защиты информации# [2.4.2](#P92)

#экспертиза документа по защите информации# [2.8.8](#P146)

#эффективность защиты информации# [2.9.1](#P154)

Приложение А

(справочное)

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ОБЩЕТЕХНИЧЕСКИХ ПОНЯТИЙ

А.1. Информация: сведения (сообщения, данные) независимо от формы их представления [[1]](#P266).

А.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]](#P266).

А.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]](#P269).

А.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.

А.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.

А.6. Информационная система: совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [[1]](#P266).

А.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]](#P266).

А.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.

А.9. Доступ к информации: возможность получения информации и ее использования [[1]](#P266).

А.10. Право доступа к защищаемой информации; право доступа: совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

А.11. Правило доступа к защищаемой информации; правило доступа: совокупность правил, устанавливающих порядок и условия доступа субъекта к защищаемой информации и ее носителям.

А.12. Конфиденциальность информации: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [[1]](#P266).

А.13. Предоставление информации: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц [[1]](#P266).

А.14. Распространение информации: действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц [[1]](#P266).

А.15. Оператор информационной системы: гражданин или юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных [[1]](#P266).

А.16. Доступность информации [ресурсов информационной системы]: состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно [[3]](#P272).

Примечание. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов [[3]](#P272).

А.17. Целостность: состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

БИБЛИОГРАФИЯ

[1] Российская Федерация. Об информации, информационных

 Федеральный закон от 27.07.2006 технологиях и о защите информации

 N 149-ФЗ

[2] Российская Федерация. О коммерческой тайне

 Федеральный закон от 29.07.2004

 N 98-ФЗ

[3] Рекомендации по стандартизации Техническая защита информации.

 Р 50.1.056-2005 Основные термины и определения.