**Обозначение ГОСТа** ГОСТ Р 50922—2006

**Текстовое наименование ГОСТа** Защита информации ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Дата введения** — 2008—02—01

**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.

**Перечень применяемых терминов и определений.**

1 информация: Сведения (сообщения, данные) независимо от формы их представления (1).

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 (1J.

З 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].

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.

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.

6 информационная система: Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (1).

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].

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.

9 доступ к информации: Возможность получения информации и ее использования (1).

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

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

12 конфиденциальность информации: Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (1).

13 предоставление информации: Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц (1).

14 распространение информации: Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц (1].

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].

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].

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

**Краткое описание содержимого ГОСТа**

#### **1.1** **Общие понятия**

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

#### **1.2** **Термины, относящиеся к видам защиты информации**

1.2.1 **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.

1.2.2 **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.

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

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

П р и м е ч а н и я

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.

#### **1.3** **Термины, относящиеся к способам защиты информации**

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

1.3.2 **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.

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

1.3.3 **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.

1.3.4 **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.

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

1.3.6 **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.

1.3.7 **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.

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

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

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

1.4.2 **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.

1.4.3 **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.

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

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

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

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

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

1.5.3 **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.

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

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

#### **1.6** **Термины, относящиеся к угрозам безопасности информации**

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

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

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

1.6.4 **уязвимость (информационной системы);** *брошь*: Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

П р и м е ч а н и я

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.

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

1.6.6 **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.

1.6.7 **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.

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

П р и м е ч а н и е — Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

#### **1.7** **Термины, относящиеся к технике защиты информации**

1.7.1 **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.

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

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

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

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

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

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

1.8.2 **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.

1.8.3 **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.

П р и м е ч а н и е — К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации.

1.8.4 **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.

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

1.8.6 **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.

П р и м е ч а н и е — 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).

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

1.8.8 **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.

П р и м е ч а н и е — Экспертиза документа по защите информации может включать в себя научно-техническую, правовую, метрологическую, патентную и терминологическую экспертизу.

1.8.9 **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.

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

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

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

1.9.2 **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.

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

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