Техническая защитаин формации Основные термины и определения

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 50.1.056-2005

Сведения о рекомендациях

- 1. РАЗРАБОТАНЫ Государственным научно-исследовательским испытательным институтом проблемтехнической защиты информации Федеральной службы по техническому и экспортному контролю (ГНИИИ ПТЗИФСТЭК России), Техническим комитетом по стандартизации ТК 362 «Защита информации»
- 2. ВНЕСЕНЫ Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии
- 3. УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст
- 4. ВВЕДЕНЫ ВПЕРВЫЕ

Область применения

- Настоящие рекомендации устанавливают термины и определения понятий в области технической защиты информации в различных сферах деятельности.
- Термины, установленные настоящими рекомендациями, рекомендуются для использования во всех видах документации и литературы по вопросам технической защиты информации, используемой в сфере работ по стандартизации.

Нормативные ссылки

- 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 51897-2002 Менеджмент риска. Термины и определения
- ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты
- ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения
- ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения.
- ГОСТ 15971-90 Системы обработки информации. Термины и определения
- ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения

Общие понятия

- **информационная безопасность объекта информатизации**: Состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки

- **техническая защита информации** *(Technical Information protection)*; ТЗИ: Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

- **безопасность информации [данных]** *(Information [data] security)*: Состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность
  - Примечание - Безопасность информации [данных] определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, с несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии

Общие понятия

- **безопасность информационной технологии** *(IT security)*: Состояние защищенности информационной технологии, при котором обеспечивается выполнение изделием, реализующим информационную технологию, предписанных функций без нарушений безопасности обрабатываемой информации
- **конфиденциальность информации** *(Confidentiality)*: Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право
- **целостность информации** *(Integrity):* Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право
- **целостность ресурсов информационной системы**: Состояние ресурсов информационной системы, при котором их изменение осуществляется только преднамеренно субъектами, имеющими на него право, при этом сохраняются их состав, содержание и организация взаимодействия

Общие понятия

- **доступность информации [ресурсов информационной системы**] *(Availability)*: Состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно
  - Примечание - К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов
- **отчетность (ресурсов информационной системы)** *(Accountability)*: Состояние ресурсов информационной системы, при котором обеспечиваются идентификация и регистрация действий с ними
- **подлинность (ресурсов информационной системы)** *(Authenticity)***:** Состояние ресурсов информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается
- **показатель защищенности информации**: Количественная или качественная характеристика безопасности информации, определяющая уровень требований, предъявляемых к конфиденциальности, целостности и доступности этой информации и реализуемых при ее обработке

Угрозы безопасности информации

- **угроза (безопасности информации)** *(Threat)***:** Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации
- **источник угрозы безопасности информации**: Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации
- **уязвимость (информационной системы);** *брешь (Vulnerability, breach)*: Свойство информационной системы, предоставляющее 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

Угрозы безопасности информации

- **утечка (информации) по техническому каналу** *(Leakage)*: Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации
- **перехват (информации)** *(Interception)***:** Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов

Угрозы безопасности информации

- **несанкционированный доступ к информации [ресурсам информационной системы];** НСД: Доступ к информации [ресурсам информационной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам информационной системы] с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.
  - Примечания
    - 1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно
    - 2. Права и правила доступа к информации и ресурсам информационной системы устанавливают для процессов обработки информации, ее обслуживания, изменения программных, технических и информационных ресурсов, а также получения информации о них

Угрозы безопасности информации

- **несанкционированное воздействие на информацию[ресурсы информационной системы];** НСВ: Изменение, уничтожение или копирование информации [ресурсов информационной системы], осуществляемое с нарушением установленных прав и (или) правил
  - Примечания
    - 1. Несанкционированное воздействие может быть осуществлено преднамеренно или непреднамеренно. Преднамеренные несанкционированные воздействия являются специальными воздействиями
    - 2. Изменение может быть осуществлено в форме замены информации [ресурсов информационной системы]; введения новой информации [новых ресурсов информационной системы], а также уничтожения или повреждения информации [ресурсов информационной системы
- **компьютерная атака** *(Attack)*: целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств

Угрозы безопасности информации

- **сетевая атака**: компьютерная атака с использованием протоколов межсетевого взаимодействия

- **несанкционированное блокирование доступа к информации [ресурсам информационной системы];** отказ в обслуживании *(Denial of service)*: Создание условий, препятствующих доступу к информации [ресурсам информационной системы] субъекту, имеющему право на него.
  - Примечания
    - 1. Несанкционированное блокирование доступа осуществляется нарушителем безопасности информации, а санкционированное - администратором
    - 2. Создание условий, препятствующих доступу к информации (ресурсам информационной системы), может быть осуществлено по времени доступа, функциям по обработке информации (видам доступа) и (или) доступным информационным ресурсам

Угрозы безопасности информации

- **закладочное устройство; закладка**: Элемент средства съема информации или воздействия на нее, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации
  - Примечание - Местами возможного съема информации могут быть ограждение, конструкция здания, оборудование, предметы интерьера, транспортные средства, а также технические средства и системы обработки информации

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

- **(компьютерный) вирус** *(Computer virus)*: Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.
  - Примечание - Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению

Угрозы безопасности информации

- **недекларированные возможности (программного обеспечения):** Функциональные возможности программного обеспечения, не описанные в документации
- **программная закладка** *(Malicious logic)*: Скрытно внесённый в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие
  - Примечание - программная закладка может быть реализована в виде вредоносной программы или программного кода

Объекты технической защиты информации

- **Защищаемый объект информатизации**: Объект информатизации предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности
- **защищаемая информационная система:** Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности
- **защищаемые ресурсы (информационной системы)**: Ресурсы, использующиеся в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности
- **защищаемая информационная технология**: Информационная технология, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности

Объекты технической защиты информации

- **защищаемые программные средства**: Программные средства, используемые в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности
- **защищаемая сеть связи**: Сеть связи, используемая при обмене защищаемой информацией с требуемым уровнем ее защищенность

Средства технической защиты информации

- **техника защиты информации**: Средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.
- **средство защиты информации от утечки по техническим каналам:** Техническое средство, вещество или материал, предназначенные и (или) используемые для защиты информации от утечки по техническим каналам
- **средство защиты информации от несанкционированного доступа**: Техническое, программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации или ресурсам информационной системы

Средства технической защиты информации

- **средство защиты информации от несанкционированного воздействия**: Техническое, программное или программно-техническое средство, предназначенное для предотвращения несанкционированного воздействия на информацию или ресурсы информационной системы

- **межсетевой экран**: локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство(комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы

- **средство поиска закладочных устройств**: Техническое средство, предназначенное для поиска закладочных устройств, установленных на объекте информатизации

Средства технической защиты информации

- **средство контроля эффективности технической защиты информации**: Средство измерений, программное средство, вещество и (или) материал, предназначенные и (или) используемые для контроля эффективности технической защиты информации
- **средство обеспечения технической защиты информации:** Техническое, программное, программно-техническое средство, используемое и (или) создаваемое для обеспечения технической защиты информации на всех стадиях жизненного цикла защищаемого объекта

Мероприятия по технической защите информации

- **организационно-технические мероприятия по обеспечению защиты информации** *(Technical safeguards)***:** Совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации
  - Примечания
    - 1. Организационно-технические мероприятия по обеспечению защиты информации должны осуществляться на всех этапах жизненного цикла объекта информатизации.
    - 2. Организационные меры предусматривают установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации
- **политика безопасности (информации в организации)** *(Organisational security policy)*: Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности
- **правила разграничения доступа (в информационной системе)**: Правила, регламентирующие условия доступа субъектов доступа к объектам доступа в информационной системе

Мероприятия по технической защите информации

- **аудиторская проверка информационной безопасности в организации**; *аудит информационной безопасности в организации (Security audit)*: Периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени 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)
- **аудиторская проверка безопасности информации в информационной системе**; *аудит безопасности информации в информационной системе (Computer system audit)*: Проверка реализованных в информационной системе процедур обеспечения безопасности информации с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию

Мероприятия по технической защите информации

- **мониторинг безопасности информации** *(Security monitoring)*: Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью выявления его соответствия требованиям по безопасности информации
- **технический контроль эффективности защиты информации**: Контроль эффективности защиты информации, проводимый с использованием средств контроля.
- **организационный контроль эффективности защиты информации:** Проверка соответствия требованиям нормативных документов в области зашиты информации
- **контроль доступа (в информационной системе)** *(Access control)***:** Проверка выполнения субъектами доступа установленных правил разграничения доступа в информационной системе

Мероприятия по технической защите информации

- **санкционирование доступа**; *авторизация (Authorization)*: Предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ
- **аутентификация (подлинности субъекта доступа)** *(Authentication)***:**Действия по проверке подлинности субъекта доступа в информационной системе
- **Идентификация** *(Identification)***:** Действия по присвоению субъектам и объектам доступа идентификаторов и (или) действия по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов
- **удостоверение подлинности**; *нотаризация (Notarization)*: Регистрация данных защищенной третьей стороной, что в дальнейшем позволяет обеспечить точность характеристик данных
  - Примечание - К характеристикам данных, например, относятся: содержание, происхождение, время и способ доставки

Мероприятия по технической защите информации

- **восстановление данных** *(Data restoration)*: Действия по воссозданию данных, которые были утеряны или изменены в результате несанкционированных воздействий
- **специальная проверка**: Проверка объекта информатизации с целью выявления и изъятия возможно внедренных закладочных устройств
- **специальное исследование (объекта технической защиты информации)**: Исследования с целью выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте технической защиты информации) требованиям нормативных правовых документов в области безопасности информации
- **сертификация средств технической защиты информации на соответствие требованиям по безопасности информации**: Деятельность органа по сертификации по подтверждению соответствия средств технической защиты информации требованиям технических регламентов, положениям стандартов или условиям договоров

Мероприятия по технической защите информации

- **аттестация объекта информатизации:** Деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта информатизации требованиям по безопасности информации
- **оценка риска**; *анализ риска*: Выявление угроз безопасности информации, уязвимостей информационной системы, оценка вероятностей реализации угроз с использованием уязвимостей и оценка последствий реализации угроз для информации и информационной системы, используемой для обработки этой информации

Общетехнические термины и определения, связанные с областью информационных технологий

Приложение А
(справочное)

Общетехнические термины и определения

- **автоматизированная система, АС**: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

- **информационная система:**
  - 1. Организационно-упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи
  - 2. Автоматизированная система, результатом функционирования которой является представление выходной информации для последующего использования.

- **защищаемая информация**: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
  - Примечание - Собственником информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Общетехнические термины и определения

- **данные**: Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека
- **безопасность**: Отсутствие недопустимого риска связанного с возможностью нанесения ущерба
- **информационная технология**: Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных
- **защита информации**; ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
- **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.

Общетехнические термины и определения

- **криптографическая защита (данных)**: Защита данных при помощи криптографического преобразования данных
- **требование:** Положение нормативного документа, содержащее критерии, которые должны быть соблюдены
- **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
- **риск:** Сочетание вероятности нанесения ущерба и тяжести этого ущерба
- **информативный сигнал**: Сигнал, по параметрам которого может быть определена защищаемая информация

Общетехнические термины и определения

- **доступ:** Извлечение информации из памяти средства вычислительной техники (электронно-вычислительной машины) или помещение информации в память средства вычислительной техники (электронно-вычислительной машины)

- **доступ к информации** (ресурсам информационной системы): Получение возможности ознакомления с информацией, обработки информации и (или) воздействия на информацию и (или) ресурсы информационной системы с использованием программных и (или) технических средств

  - Примечание - Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты

- **субъект доступа (в информационной системе**): Лицо или единица ресурса информационной системы, действия которого по доступу к ресурсам информационной системы регламентируются правилами разграничения доступа.

Общетехнические термины и определения

- **объект доступа (в информационной системе**): Единица ресурса информационной системы, доступ к которой регламентируется правилами разграничения доступа
- **средство измерений**: Техническое средство, предназначенное для измерений, имеющее нормированные метрологические характеристики, воспроизводящее и/или хранящее единицу физической величины, размер которой принимают неизменным (в пределах установленной погрешности) в течение известного интервала времени
- **сеть связи**: Технологическая система включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи
- **ресурсы (информационной системы):** Средства, использующиеся в информационной системе, привлекаемые для обработки информации (например, информационные, программные, технические, лингвистические)

Общетехнические термины и определения

- **нормативный правовой документ**: Письменный официальный документ, принятый в установленном порядке, управомоченного на то органа государственной власти, органа местного самоуправления или должностного лица, устанавливающий правовые нормы (правила поведения), обязательные для неопределенного круга лиц, рассчитанные на неоднократное применение и действующие независимо от того, возникли или прекратились конкретные правоотношения, предусмотренные актом
- **выделенное помещение**: специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед и других мероприятий секретного характера
- **измерительный контроль**: контроль, осуществляемый с применением средств измерений.
- **информация**: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Общетехнические термины и определения

- **нарушитель безопасности информации**: Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах

- **документированный процесс**: Процесс, реализация которого осуществляется в соответствии с разработанным комплектом документов (документацией) и подтверждается соответствующими записями

- **свидетельства (доказательства) аудита информационной безопасности**: Записи, изложения фактов или другая информация, которые имеют отношение к критериям аудита информационной безопасности и могут быть проверены
  - Примечание - Свидетельства аудита информационной безопасности могут быть качественными или количественными

Общетехнические термины и определения

- **критерии аудита информационной безопасности в организации**: Совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности
  - Примечание - Критерии аудита информационной безопасности используют для сопоставления с ними свидетельств аудита информационной безопасности

- **управление риском**: Действия, осуществляемые для выполнения решений в рамках менеджмента риска
  - Примечание Управление риском может включать в себя мониторинг, переоценивание и действия, направленные на обеспечение соответствия принятым решениям

Схема взаимосвязи стандартизованных терминов