ГОСТ Р 50922-96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное
Госстандарт России
Москва
1996г.

ГОСТ Р 50922-96

Содержание

ГОСТ Р 50922-96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Дата введения _____

1 Область применения

Настоящий стандарт устанавливает основные термины и их определения в области защиты информации.

Термины, установленные настоящим стандартом, обязательны для применения во всех видах документации и литературы по защите информации.

Настоящий стандарт применяется совместно с ГОСТ РВ 50170-92.

2 Общие положения

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

Для каждого понятия установлен один стандартизованный термин.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации. Оставшаяся часть термина является его краткой формой и приводится в алфавитном указателе раздельно с указанием того же номера статьи.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два (три, четыре и т.п.) термина, имеющие общие терминоэлементы. В алфавитном указателе данные термины приведены отдельно с указанием номера статьи.

Разрешается, при необходимости, уточнять приведенные определения, вводя дополнительные признаки, раскрывающие значения терминов, без искажения смысла определения.

Термины и определения общетехнических понятий, необходимые для понимания текста стандарта, приведены в приложении А.

3 Стандартизованные термины и их определения

3.1 Основные понятия

1 **Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание:

Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

2 **Защита информации** - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

3 **Защита информации от утечки** - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.

4 **Защита информации от несанкционированного воздействия** защита информации от НСВ: Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил

на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

5 **Защита информации от непреднамеренного воздействия** - деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

6 **Защита информации от разглашения** - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

7 **Защита информации от несанкционированного доступа** - защита информации от НСД: Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Примечание:

Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

8 **Защита информации от [иностранной] разведки** - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой.

9 **Защита информации от [иностранной] технической разведки** - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой с помощью технических средств.

10 **Защита информации от агентурной разведки** - деятельность по предотвращению получения защищаемой информации агентурной разведкой.

11 **Цель защиты информации** - желаемый результат защиты информации.

Примечание:

Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

12 **Эффективность защиты информации** - степень соответствия результатов защиты информации поставленной цели.

13 **Показатель эффективности защиты информации** - мера или характеристика для оценки эффективности защиты информации.

14 **Нормы эффективности защиты информации** - значения показателей эффективности защиты информации, установленные нормативными документами.

3.2 Организация защиты информации

15 **Организация защиты информации** - содержание и порядок действий по обеспечению защиты информации.

16 **Система защиты информации** - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

17 **Мероприятие по защите информации** - совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

18 **Мероприятие по контролю эффективности защиты информации** - совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.

19 **Техника защиты информации** - средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

20 **Объект защиты** - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

21 **Способ защиты информации** - порядок и правила применения определенных принципов и средств защиты информации.

22 **Категорирование защищаемой информации [объекта защиты]** - установление градаций важности защиты защищаемой информации [объекта защиты].

23 **Метод [способ] контроля эффективности защиты информации** - порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

24 **Контроль состояния защиты информации** - проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

25 **Средство защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

26 **Средство контроля эффективности защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

27 **Контроль организации защиты информации** - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

28 **Контроль эффективности защиты информации** - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

29 **Организационный контроль эффективности защиты информации** - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

30 **Технический контроль эффективности защиты информации** - контроль эффективности защиты информации, проводимой с использованием средств контроля.

4. Алфавитный указатель терминов:

Приложение А (справочное)

Термины и определения, необходимые для понимания текста стандарта

1. **Информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
2. **Доступ к информации** - получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.
3. **Субъект доступа к информации** - субъект доступа: участник правоотношений в информационных процессах.
   Примечание: Информационные процессы - процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.
4. **Носитель информации** - физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.
5. **Собственник информации** - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.
6. **Владелец информации** - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.
7. **Пользователь [потребитель] 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.
8. **Право доступа к информации** - право доступа: совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.
9. **Правило доступа к информации** - правило доступа: совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.
10. **Орган защиты информации** - административный орган, осуществляющий организацию защиты информации.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К проекту Государственного стандарта “Защита информации.

Основные термины и определения”

(окончательная редакция)

1. Основание для разработки стандарта

1. решение Председателя Гостехкомиссии России “О научных исследованиях по защите информации в 1994 году” от 2.06.1993г.
2. Техническое задание на НИР “Фронда-94”, утвержденное Первым заместителем Председателя Гостехкомиссии России 23 января 1994г.
3. Техническое задание на разработку государственного стандарта “Защита информации. Основные термины и определения”, утвержденное Первым заместителем Председателя Гостехкомиссии России 31 октября 1994г.

2. Цель и задачи разработки стандарта

Основной целью разработки стандарта является установление однозначно понимаемой и непротиворечивой терминологии во всех видах документации и литературы, деятельности органов, занимающихся защитой информации (ЗИ).

Основными задачами разработки стандарта являются:

- терминологическое обеспечение для однозначного взаимопонимания между разработчиками, изготовителями, продавцами и потребителями (заказчиками) в области ЗИ;
- фиксация в разрабатываемом стандарте современного уровня научного знания и технического развития в области ЗИ;
- обеспечение взаимосвязанного и согласованного развития лексических средств, используемых в документации и литературе в области ЗИ.

3. Краткая характеристика объекта стандартизации

Стандарт разрабатывается впервые.

В связи с тем, что информация является предметом собственности (государства, коллектива, отдельного лица (субъекта)), то неизбежно возникает проблема угрозы безопасности этой информации, заключающейся в неконтролируемом ее распространении, в хищении, несанкционированном уничтожении, искажении, передаче, копировании, блокировании доступа к информации. Следовательно, возникает проблема защиты информации от утечки и несанкционированных воздействий на информацию и ее носители, а также предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы. В связи с чем понятие “Защита информации” становится основополагающим (ключевым) понятием и рассматривается как процесс или деятельность, направленная на предотвращение утечки защищаемой информации, а также по предотвращению различного рода несанкционированных воздействий (НСВ) на информацию и ее носители.

Значимость защиты информации увеличивается в связи с возрастанием возможностей иностранных разведок за счет совершенствования технических средств разведки, приближения этих средств к объектам разведки (носителям информации) вследствие развертывания инспекционной деятельности, создания совместных предприятий и производств, сокращения закрытых для иностранцев зон и городов.

С развитием конкуренции в среде свободного предпринимательства крупномасштабной задачей в области “Защита информации” становится борьба с промышленным и экономическим шпионажем, распространению которого способствует широкомасштабное применение для обработки информации средств вычислительной техники (особенно персональных ЭВМ), созданием вычислительных сетей, систем, баз данных, многочисленных средств передачи информации. Промышленный шпионаж ведется в основном с целью завоевания рынков сбыта, исключения технологических прорывов конкурентов, срыва переговоров по контрактам, перепродажи фирменных секретов и т.д. По мере ослабления противостояния между Востоком и Западом промышленный шпионаж в работе многих разведок, в том числе и ЦРУ США, становится приоритетным направлением наряду с политической разведкой.

В настоящее время основные вопросы защиты информации регламентированы Законами РФ “О государственной тайне”, “Об информации, информатизации и защите информации”, “О безопасности”, “О связи”, “Положением о государственном лицензировании деятельности в области защиты информации”, документами Гостехкомиссии России и оборонных отраслей промышленности, например, проект ГОСТ по шифровальной технике.

Однако, существующая терминология в области защиты информации не согласована, в некоторых случаях противоречива и не представляет терминологическую систему в проблемной области “Защита информации”.

Поэтому на стадии разработки первой, второй и окончательной редакции проекта стандарта “Защита информации. Основные термины и определения” проведена основная работа по упорядочению стандартизуемой терминологии, включающая:

- уточнение границ предметной области “Защита информации”;
- систематизацию понятий и построение классификации понятий;
- определение структуры разделов стандарта и расположения терминов в разделах.

Методологической основой стандартизации научно-технической терминологии в предметной области “Защита информации” является системный принцип упорядочения, предусматривающий анализ и оценку каждого термина как элемента терминосистемы и каждой терминосистемы как элемента взаимосвязанных (более общих, соподчиненных , более узких) терминосистем.

Классификационная схема понятий в предметной области “Защита информации” приведена на рисунке.

Основополагающим в классификационной схеме принято понятие “Защита информации” с позиции собственника, владельца, пользователя информацией как деятельность (процесс), направленная на предотвращение утечки защищаемой информации, а также по предотвращению различного рода несанкционированных воздействий (НСВ) на информацию и ее носители, т.е. защита информации от угроз безопасности информации. При таком понимании защиты информации предложенная классификация понятий в предметной области “Защита информации” позволяет разрабатывать соподчиненные (более узкие) тнрминосистемы, как элементы взаимосвязанных терминосистем, такие как:

- защита информации от разглашения;
- защита информации от утечки по каналам [иностранной] технической разведки;
- защита информации от физического (частного) лица; защита информации от несанкционированного доступа; защита информации от несанкционированных воздействий.

Еще более узкие терминосистемы, как элементы взаимосвязанных терминосистем, например, могут быть:

- защита информации от утечки по каналам радио-, радиотехнической разведки;
- защита информации от утечки по каналам визуально-оптической разведки;
- защита информации от утечки по акустическому каналу;
- защита информации от утечки за счет ПЭМИН;
- защита информации от утечки по каналам специальных электронных закладных устройств;
- защита информации от НСД при ее обработке с помощью технических средств (средств вычислительной техники, в ТСПИ и средствах связи, в средствах оргтехники);
- защита информации шифрованием; защита информации режимно-секретной деятельностью; защита информации обеспечением безопасности связи.

Соподчиненные терминосистемы могут объединяться или, наоборот, формировать дополнительно более частные соподчиненные терминосистемы.

Соподчиненной терминосистемой является и терминосистема “Информация”, содержащая термины и определения, регламентирующие свойства и состояние информации, такие как: информация; безопасность, секретность (конфиденциальность), доступность, целостность информации; уничтожение, хищение и искажение, подделка, копирование, модификация, преобразование, передача информации и др.

Кроме того, предложенная классификация определяет структуру разделов основополагающего стандарта “Защита информации. Основные термины и определения”.

1. Основные понятия.
2. Организация защиты информации.

Таким образом, предложенная классификация понятий в области защиты информации позволяет представить стройную систему терминов и определений по рассматриваемой проблеме. Причем данная классификационная схема не ограничивает пути ее совершенствования, например, терминосистема “Защита информации от НСД

при ее обработке с помощью технических средств" может быть представлена более частными соподчиненными терминосистемами:

- защита информации, обрабатываемой средствами вычислительной техники, от НСД штатными средствами;
- защита информации от НСД в ТСПИ и средствах связи; защита информации от НСД в средствах оргтехники.

4. Сведения о соответствии проекта стандарта международным (региональным) стандартам (их проектам) и национальным стандартам других стран

Головной разработчик проекта стандарта сведениями о наличии международных (региональных) и национальных стандартов других стран аналогичного содержания не располагает.

5. Сведения о патентной чистоте проекта стандарта При разработке проекта стандарта отечественные и национальные патенты не использовались.
6. Взаимосвязь с другими нормативными документами Разрабатываемый стандарт должен применяться совместно с ГОСТ РВ 50170-92.
7. Сведения о рассылке на отзыв второй редакции проекта стандарта
   Вторая редакция проекта стандарта рассылалась на отзыв в соответствии с утвержденным заказчиком техническим заданием в 29 НИО МО РФ и промышленности, получены отзывы от 24 организаций, из них от 12 организаций - без замечаний.

   Краткая характеристика принципиальных замечаний и предложений на вторую редакцию проекта стандарта:

   - предлагается ряд уточнений для классификационной схемы понятий;
   - предлагается пересмотреть систематизацию понятий в соответствии со схемой классификации;
   - предлагается уточнить понятия "защита информации" и "несанкционированный доступ к информации".
8. Источники информации

   1. Конституция Российской Федерации. М. Юридическая литерату-ра,1993.
   2. Закон Российской Федерации "О государственной тайне". И. N-5486-1 от 21.07.93г.
   3. Закон Российской Федерации "Об информации, информатизации и защите информации" N- 24-ФЗ, 1995.
   4. Закон Российской Федерации "О связи", N- 15-ФЗ,1995.
   5. Закон Российской Федерации "О безопасности", N- 2446-1,1992.
   6. Положение о Государственной системе защиты информации от иностранных технических разведок и от ее утечки по техническим каналам, М.Воениздат,1993.
   7. Положение о государственном лицензировании деятельности в области защиты информации.М.1994.
   8. ГОСТ 14777-76 "Радиопомехи индустриальные. Термины и определения".
   9. ГОСТ 15467-79 "Управление качеством продукции. Основные понятия. Термины и определения".
   10. ГОСТ 16487-83 "Делопроизводство и архивное дело. Термины и определения".
   11. ГОСТ 16504-81 "Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения".
   12. ГОСТ 22515-27 "Связь телеграфная. Термины и определения".
   13. ГОСТ 22670-77 "Сеть связи цифровая интегральная. Термины и определения".
   14. ГОСТ 23611-79 "Совместимость радиоэлектронных средств электромагнитная. Термины и определения".
   15. ГОСТ 24375-80 "Радиосвязь. Термины и определения".
   16. ГОСТ 26883-86 "Внешние воздействующие факторы. Термины и определения".
   17. Проект Государственного стандарта "Защита информации, обрабатываемой с помощью технических средств. Термины и определения", 1993.
   18. Руководящий документ. "Защита от несанкционированного доступа к информации. Термины и определения", Гостехкомиссия России.М.1992.
   19. Г.Н. Устинов. Обеспечение безопасности информации при ее передаче по каналам и сетям связи., "Стандартизация военной техники", N- 3, 1993.
   20. В.А. Герасименко. Концепция современной информатики. "Зарубежная радиоэлектроника", N- 4,1993.
   21. В.П. Харламов. Концептуальный подход и терминология в области защиты информации. Информационный сборник.
   22. Д.Б. Халяпин, В.И. Ярочкин. Основы защиты промышленной и коммерческой информации. Термины и определения. Институт повышения квалификации информационных работников.Москва,1994.
   23. Терминология в области защиты информации. Справочник.

М., ВНИИстандарт,1993.
24. Р50-603-1-89.Рекомендации. Разработка стандартов на термины и определения (Разработчик ВНИИКИ),М.,1990.
25. Р50-603-1-89. Изменение N-1.Рекомендации. Разработка стандартов на термины и определения. (Разработчик ВНИИ-КИ).М.,1993.