ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Каталогизация продукции для федеральных государственных нужд

СЕТИ ТЕЛЕКОММУНИКАЦИОННЫЕ И БАЗЫ ДАННЫХ

Требования информационной безопасности

Издание официальное

БЗ 12—2001/350

ГОССТАНДАРТ РОССИИ
Москва

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Государственным учреждением «Федеральный центр каталогизации» и 46 Центральным научно-исследовательским институтом Министерства обороны Российской Федерации

ВНЕСЕН Научно-техническим управлением Госстандарта России

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 4 апреля 2002 г. № 130-ст

3 ВВЕДЕН ВПЕРВЫЕ

© ИПК Издательство стандартов, 2002

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Госстандарта России

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Определения, обозначения и сокращения 1
4 Общие требования 1
5 Требования к организации защиты информации в Федеральной системе каталогизации продукции для федеральных государственных нужд 2
6 Требования к методам защиты от несанкционированного доступа к информации Федеральной системы каталогизации продукции для федеральных государственных нужд 3
Приложение А Библиография 5

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Каталогизация продукции для федеральных государственных нужд

СЕТИ ТЕЛЕКОММУНИКАЦИОННЫЕ И БАЗЫ ДАННЫХ

Требования информационной безопасности

Catalogization of products for federal state needs. Telecommunication networks and data bases. Requirements of information security

Дата введения 2003—01—01

1 Область применения

Настоящий стандарт распространяется на телекоммуникационные сети и базы данных, используемые в Федеральной системе каталогизации продукции для федеральных государственных нужд, и устанавливает основные требования по обеспечению их информационной безопасности.

Требования настоящего стандарта обязательны для применения при проведении работ по каталогизации продукции для федеральных государственных нужд.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ Р 50739—95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50922—96 Защита информации. Основные термины и определения

ГОСТ Р 51725.2—2001 Каталогизация продукции для федеральных государственных нужд. Термины и определения

3 Определения, обозначения и сокращения

В настоящем стандарте используются следующие термины с соответствующими определениями:

3.1 **информационная безопасность:** Состояние информационных ресурсов и информационных подсистем ФСКП, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т. п.

3.2 **несанкционированный доступ к информационным ресурсам ФСКП:** Доступ к информационным ресурсам ФСКП, нарушающий установленные правила доступа, с использованием штатных средств, предоставляемых ФСКП.

3.3 В настоящем стандарте использовано следующее сокращение:

ФСКП — Федеральная система каталогизации продукции для федеральных государственных нужд.

4 Общие требования

4.1 Защита информации является составной частью работ по созданию, развитию и эксплуатации ФСКП и должна осуществляться непрерывно на всех этапах ее создания и эксплуатации во всех организациях — участниках ФСКП.

Издание официальное

★

4.2 Защита информации в ФСКП должна осуществляться выполнением комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения, а также путем проведения специальных работ.

4.3 Мероприятия по защите информации в ФСКП должны осуществляться во взаимосвязи с другими мерами, обеспечивающими конфиденциальность проводимых работ по каталогизации продукции.

4.4 Проведение любых мероприятий и работ с использованием информационных ресурсов ФСКП, являющихся государственной или служебной тайной, без принятия необходимых мер защиты информации не допускается.

4.5 Защита информации в ФСКП должна осуществляться в соответствии с требованиями, установленными законом [1] и нормативными актами, разработанными Государственной технической комиссией при Президенте Российской Федерации.

5 Требования к организации защиты информации в Федеральной системе каталогизации продукции для федеральных государственных нужд

5.1 Защите должны подлежать информационные ресурсы ФСКП, содержащие сведения, являющиеся государственной или служебной тайной, определенные в установленном порядке федеральными органами исполнительной власти, в том числе:

- информационные ресурсы ФСКП, содержащие сведения, являющиеся государственной или служебной тайной, представленные в виде носителей на магнитной и оптической основе, информационных массивов и баз данных;
- средства вычислительной техники, информационно-вычислительные комплексы, сети и системы, программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), системы связи и передачи данных, технические средства приема, передачи и обработки информации (в том числе средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация, содержащая сведения, являющиеся государственной или служебной тайной, а также эти помещения.

5.2 Цели защиты:

- предотвращение утечки информации путем исключения несанкционированного доступа к ней;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в телекоммуникационных сетях и базах данных ФСКП;
- соблюдение правового режима использования массивов и программ обработки информации;
- обеспечение полноты, целостности, достоверности информации в телекоммуникационных сетях и базах данных ФСКП;
- сохранение возможности управления процессом обработки и пользования информацией.

5.3 Защита информации должна осуществляться путем:

- предотвращения перехвата техническими средствами информации, передаваемой по телекоммуникационным сетям;
- предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами ФСКП, и электроакустических преобразований;
- исключения несанкционированного доступа к обрабатываемой или хранящейся информации в технических средствах ФСКП;
- предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе программно-технического комплекса ФСКП;
- проведения специальных проверок по выявлению внедренных на объекты и в импортные технические средства электронных устройств перехвата информации.

5.4 Предотвращение утечки информации, передаваемой по каналам связи, используемым

ФСКП, должно достигаться использованием методов кодирования информации, а также применением организационно-технических и режимных мероприятий.

5.5 Предотвращение утечки информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований должно достигаться путем применения защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации ФСКП и другими техническими и организационными мерами (в соответствии с требованиями, предъявляемыми к категории данного объекта информации).

5.6 Предотвращение несанкционированного доступа к циркулирующей или хранящейся в технических средствах информации должно достигаться применением специальных программно-технических средств защиты, кодированием информации, а также организационными и режимными мероприятиями.

5.7 Предотвращение специальных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе программных средств информатизации должно достигаться применением специальных программных и аппаратных средств защиты (включая антивирусные программы) и организацией системы контроля безопасности программного обеспечения.

5.8 Информация, содержащая сведения, являющиеся государственной или служебной тайной, должна обрабатываться с использованием технических и программных средств, сертифицированных в установленном порядке.

5.9 При разработке технических заданий на создание технических и программных средств ФСКП должны разрабатываться требования по обеспечению защиты информации в процессе разработки и эксплуатации средств ФСКП. Указанные требования включают в техническое задание отдельным разделом.

5.10 Ответственность за координацию работ по обеспечению защиты информации, содержащейся в базах данных и телекоммуникационных сетях по разделам Федерального каталога продукции для федеральных государственных нужд, возлагается на федеральные органы исполнительной власти, ответственные за разработку и ведение этих разделов.

Ответственность за координацию работ по обеспечению защиты информации, содержащейся в базах данных и телекоммуникационных сетях по разделам сводной части Федерального каталога продукции для федеральных государственных нужд, возлагается на Госстандарт России.

5.11 Порядок доступа к защищаемой информации по разделам Федерального каталога продукции для федеральных государственных нужд устанавливает федеральный орган исполнительной власти, определенный в установленном порядке, ответственный за разработку и ведение этих разделов.

Порядок доступа к защищаемой информации по разделам сводной части Федерального каталога продукции для федеральных государственных нужд устанавливает Госстандарт России.

Порядок доступа к защищаемой общесистемной информации ФСКП устанавливает Госстандарт России.

6 Требования к методам защиты от несанкционированного доступа к информации Федеральной системы каталогизации продукции для федеральных государственных нужд

6.1 Мероприятия, осуществляемые организациями — участниками ФСКП по защите информации от несанкционированного доступа, должны соответствовать требованиям ГОСТ Р 50739.

6.2 В качестве нарушителя правил доступа к информационным ресурсам ФСКП должен рассматриваться субъект (физическое или юридическое лицо), получивший доступ к работе со штатными программно-техническими средствами ФСКП без разрешения, оформленного в установленном порядке.

6.3 Организация, которой в установленном порядке поручено разрабатывать и вести информационный ресурс ФСКП, должна сформулировать, документировать и в установленном порядке утвердить модель нарушителя автоматизированного банка данных и телекоммуникационных сетей ФСКП.

Модель нарушителя должна учитывать следующие уровни возможностей потенциального нарушителя:

первый уровень — возможность запуска программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации;

второй уровень — возможность создания и запуска собственных программ с новыми функциями по обработке информации;

третий уровень — возможность управления функционированием автоматизированной базы данных ФСКП с воздействием на базовое программное обеспечение, состав и конфигурацию программно-технического комплекса;

четвертый уровень — возможности лиц, осуществляющих разработку, реализацию и ремонт технических средств программно-технического комплекса ФСКП, включать собственные технические средства с дополнительными функциями по обработке информации.

6.4 Основными способами несанкционированного доступа к информационным ресурсам ФСКП являются:

- непосредственное обращение к информационным ресурсам;
- создание программных средств, позволяющих получать доступ к информационным ресурсам, минуя средства защиты;
- создание технических средств, позволяющих получать доступ к информационным ресурсам, минуя средства защиты;
- модификация используемых в ФСКП средств защиты, позволяющая получать несанкционированный доступ к информационным ресурсам;
- внедрение в программно-технический комплекс ФСКП программных или технических средств, нарушающих его установленную структуру и функции и позволяющих получать доступ к информационным ресурсам.

6.5 Защита от несанкционированного доступа должна осуществляться по следующим направлениям:

- разграничение доступа субъектов к программно-техническому комплексу и информационным ресурсам ФСКП;
- применение технических и программных средств разграничения доступа.

6.6 Разграничение доступа субъектов к программно-техническому комплексу и информационным ресурсам ФСКП должно осуществляться следующими способами:

- разработкой и реализацией правил разграничения доступа субъектов к информационным ресурсам;
- разработкой и реализацией правил разграничения доступа субъектов к устройствам создания твердых копий документов;
- изоляцией программ, выполняемых в интересах субъекта, от других субъектов.

6.7 Средства разграничения доступа субъектов к программно-техническому комплексу и информационным ресурсам ФСКП должны реализовывать следующие основные функции:

- идентификацию и опознавание субъекта и поддержание соответствия субъекта и процесса, выполняемого для данного субъекта;
- регистрацию действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки несанкционированного доступа, включая сигнализацию, блокирование, восстановление после несанкционированного доступа и др.;
- тестирование программных и технических средств;
- учет выхода печатных и графических форм и твердых копий документов;
- контроль целостности программной и информационной частей средств разграничения доступа.

ПРИЛОЖЕНИЕ А
(справочное)

Библиография

[1] Закон Российской Федерации от 21.07.1993 г. № 5485-I «О государственной тайне»

УДК 025.3:001.4:006.354 ОКС 35.240 Т50 ОКСТУ 0007

Ключевые слова: каталогизация продукции, информационная безопасность, телекоммуникационные сети, база данных

Редактор *Т.А. Леонова*
Технический редактор *В.Н. Прусакова*
Корректор *В.И. Варенцова*
Компьютерная верстка *И.А. Налейкиной*

Изд. лиц. № 02354 от 14.07.2000. Сдано в набор 13.05.2002. Подписано в печать 31.05.2002. Усл. печ. л. 0,93. Уч.-изд.л. 0,60.
Тираж 404 экз. С 6019. Зак. 470.

ИПК Издательство стандартов, 107076 Москва, Колодезный пер., 14.
http://www.standards.ru e-mail: info@standards.ru
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. «Московский печатник», 103062 Москва, Лялин пер., 6.
Плр № 080102

gost.e-ecolog.ru