ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 51725.6–

Каталогизация продукции для федеральных государственных нужд

СЕТИ ТЕЛЕКОММУНИКАЦИОННЫЕ И БАЗЫ ДАННЫХ

Требования информационной безопасности

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Российский институт стандартизации
20__

Предисловие

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием «Научно-исследовательский институт «Центр» (ФГУП «ВНИИ «Центр»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 430 «Каталогизация продукции»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от №

4 ВЗАМЕН ГОСТ Р 51725.6–2002

На основании части 1 статьи 16 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» применение настоящего стандарта является обязательным при разработке национальных стандартов Российской Федерации.

Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (www.gost.ru)

Содержание

НАЦИОНАЛЬНЫЙ 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 — 20__—__—__

1 Область применения

Настоящий стандарт распространяется на телекоммуникационные сети и базы данных, используемые в Федеральной системе каталогизации продукции для федеральных государственных нужд (далее – ФСКП), 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 нормативные 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 51725.2–20ХХ Каталогизация продукции для федеральных государственных нужд. Термины и определения

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования – на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ Р 51725.2, ГОСТ Р 50922, а также применены следующие термины с соответствующими определениями:

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.

несанкционированный доступ к информационным ресурсам ФСКП: Доступ к информационным ресурсам ФСКП, нарушающий

установленные правила доступа, с использованием штатных средств, предоставляемых ФСКП.

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.

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 Защита информации в ФСКП должна осуществляться в соответствии с требованиями, установленными нормативными актами Российской Федерации.

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

5.1 Информационные ресурсы ФСКП должны подлежать защите от доступа пользователя, не зарегистрированного в автоматизированной информационной системе каталогизации продукции (далее - АИС КП).

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;

- 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.

5.4 Предотвращение утечки информации, передаваемой по каналам связи, используемым ФСКП, должно достигаться применением организационных мероприятий и программно-технических средств.

5.5 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.

5.6 Ответственность за координацию работ по обеспечению защиты информации, содержащейся в базах данных и телекоммуникационных сетях ФСКП, возлагается на оператора АИС КП.

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 автоматизированной базы 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.

УДК 025.3:001.4:006.354 ОКС 35.240

Ключевые слова: информационная безопасность, телекоммуникационные сети, база данных, федеральная система каталогизации продукции, информационные ресурсы

Руководитель организации – разработчика стандарта, заместитель генерального директорам по стандартизации оборонной продукции ФГУП «ВНИИ «Центр» В.Д. Киселев

Руководитель подразделения – разработчика стандарта, начальник отделения комплексных исследований по стандартизации оборонной продукции и каталогизации ФГУП «ВНИИ «Центр» В.В. Лавров

Исполнитель – разработчик стандарта, начальник отдела – заместитель начальника отделения комплексных исследований и разработок ДСОП и каталогизации ФГУП «ВНИИ «Центр» И.В. Еманаков