ГОСТ Р 51275—99

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ОБЪЕКТ ИНФОРМАТИЗАЦИИ ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ

Общие положения

Издание официальное

БЗ 5—98/859

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН 5 ЦНИИИ МО РФ

2 ВНЕСЕН Техническим комитетом по стандартизации «Защита информации» (ТК 362Р)

3 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 12 мая 1999 г. № 160

4 ВВЕДЕН ВПЕРВЫЕ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

ОБЪЕКТ ИНФОРМАТИЗАЦИИ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ

Общие положения

Protection of information.
Object of informatization. Factors influencing the information.
General outlines

Дата введения 2000—01—01

1 Область применения

Настоящий стандарт устанавливает классификацию и перечень факторов, воздействующих на защищаемую информацию, в интересах обоснования требований защиты информации на объекте информатизации.

Настоящий стандарт распространяется на требования по организации защиты информации при создании и эксплуатации объектов информатизации, используемых в различных областях деятельности (обороны, экономики, науки и других областях).

Положения настоящего стандарта подлежат применению на территории Российской Федерации органами государственной власти, местного самоуправления, предприятиями и учреждениями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

2 Определения и сокращения

2.1 В настоящем стандарте применяют следующие термины с соответствующими определениями:

информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

защищаемая информация: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

фактор, воздействующий на защищаемую информацию: Явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней;

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;

информационные ресурсы: Отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов);

информационная технология: Приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации;

обработка информации: Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения,регистрации, уничтожения, преобразования, отображения информации;

Издание официальное

★

система обработки информации: Совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации;

средства обеспечения объекта информатизации: Технические средства и системы, их коммуникации, не предназначенные для обработки информации, но устанавливаемые вместе со средствами обработки информации на объекте информатизации;

побочное электромагнитное излучение: Электромагнитное излучение, возникающее при работе технических средств обработки информации;

паразитное электромагнитное излучение: Электромагнитное излучение, вызванное паразитной генерацией в электрических цепях технических средств обработки информации;

наводки: Токи и напряжения в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями;

закладочное устройство: Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации);

программная закладка: Внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, позволяющих осуществлять несанкционированные воздействия на информацию;

программный вирус: Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойством несанкционированного распространения и самовоспроизведения (репликации). В процессе распространения вирусные субъекты могут себя модифицировать. Некоторые программные вирусы могут изменять, копировать или удалять программы или данные.

2.2 В настоящем стандарте приняты следующие сокращения:

ОИ — объект информатизации;

ПЭМИ — побочные электромагнитные излучения;

ТС — техническое средство.

3 Основные положения

3.1 Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и осуществления эффективных мероприятий, направленных на защиту информации на ОИ.

3.2 Полнота и достоверность выявления факторов, воздействующих на защищаемую информацию, должны быть достигнуты путем рассмотрения полного множества факторов, воздействующих на все элементы ОИ (технические и программные средства обработки информации, средства обеспечения ОИ и т. д.) и на всех этапах обработки информации.

3.3 Выявление факторов, воздействующих на защищаемую информацию, должно быть осуществлено с учетом следующих требований:

- достаточности уровней классификации факторов, воздействующих на защищаемую информацию, позволяющей формировать их полное множество;
- гибкости классификации, позволяющей расширять множества классифицируемых факторов, группировок и признаков, а также вносить необходимые изменения без нарушения структуры классификации.

3.4 Основными методами классификации факторов, воздействующих на защищаемую информацию, являются иерархический и фасетный методы.

4 Классификация факторов, воздействующих на защищаемую информацию

4.1 Факторы, воздействующие на защищаемую информацию и подлежащие учету при организации защиты информации, по признаку отношения к природе возникновения делят на классы:

- объективные;
- субъективные.

4.2 По отношению к ОИ факторы, воздействующие на защищаемую информацию, подразделяют на внутренние и внешние.

4.3 Принцип классификации факторов, воздействующих на защищаемую информацию, следующий.

- подкласс;
- группа;
- подгруппа,
- вид;
- подвид.

4.3.1 Перечень объективных факторов, воздействующих на защищаемую информацию, в соответствии с установленным принципом их классификации (4.3)

4.3.1.1 *Внутренние факторы*

4.3.1.1.1 Передача сигналов по проводным линиям связи.

4.3.1.1.2 Передача сигналов по оптико-волоконным линиям связи.

4.3.1.1.3 Излучения сигналов, функционально присущих ОИ.

4.3.1.1.3.1 Излучения акустических сигналов.

4.3.1.1.3.1.1 Излучения неречевых сигналов.

4.3.1.1.3.1.2 Излучения речевых сигналов.

4.3.1.1.3.2 Электромагнитные излучения и поля.

4.3.1.1.3.2.1 Излучения в радиодиапазоне.

4.3.1.1.3.2.2 Излучения в оптическом диапазоне.

4.3.1.1.4 ПЭМИ

4.3.1.1.4.1 ПЭМИ сигналов (видеоимпульсов) от информационных цепей.

4.3.1.1.4.2 ПЭМИ сигналов (радиоимпульсов) от всех электрических цепей ТС ОИ.

4.3.1.1.4.2.1 Модуляция ПЭМИ электромагнитными сигналами от информационных цепей.

4.3.1.1.4.2.2 Модуляция ПЭМИ акустическими сигналами.

4.3.1.1.5 Паразитное электромагнитное излучение.

4.3.1.1.5.1 Модуляция паразитного электромагнитного излучения информационными сигналами.

4.3.1.1.5.2 Модуляция паразитного электромагнитного излучения акустическими сигналами.

4.3.1.1.6 Наводки.

4.3.1.1.6.1 Наводки в электрических цепях ТС, имеющих выход за пределы ОИ.

4.3.1.1.6.1.1 Наводки в линиях связи.

4.3.1.1.6.1.1.1 Наводки, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

4.3.1.1.6.1.1.2 Наводки, вызванные внутренними емкостными и (или) индуктивными связями.

4.3.1.1.6.1.2 Наводки в цепях электропитания.

4.3.1.1.6.1.2.1 Наводки, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

4.3.1.1.6.1.2.2 Наводки, вызванные внутренними емкостными и (или) индуктивными связями.

4.3.1.1.6.1.2.3 Наводки через блоки питания ТС ОИ.

4.3.1.1.6.1.3 Наводки в цепях заземления.

4.3.1.1.6.1.3.1 Наводки, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

4.3.1.1.6.1.3.2 Наводки, вызванные внутренними емкостными и (или) индуктивными связями.

4.3.1.1.6.1.3.3 Наводки, обусловленные гальванической связью схемной (рабочей) «земли» узлов и блоков ТС ОИ.

4.3.1.1.6.2 Наводки на ТС, провода, кабели и иные токопроводящие коммуникации и конструкции, гальванически не связанные с ТС ОИ, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

4.3.1.1.7 Акустоэлектрические преобразования в элементах ТС ОИ.

4.3.1.1.8 Дефекты, сбои, отказы, аварии ТС и систем ОИ.

4.3.1.1.9 Дефекты, сбои и отказы программного обеспечения ОИ.

4.3.1.2 *Внешние факторы*

4.3.1.2.1 Явления техногенного характера.

4.3.1.2.1.1 Непреднамеренные электромагнитные облучения ОИ.

4.3.1.2.1.2 Радиационные облучения ОИ.

4.3.1.2.1.3 Сбои, отказы и аварии систем обеспечения ОИ.

4.3.1.2.2 Природные явления, стихийные бедствия.

4.3.1.2.2.1 Термические факторы (пожары и т. д.).

4.3.1.2.2.2 Климатические факторы (наводнения и т. д.).

4.3.1.2.2.3 Механические факторы (землетрясения и т. д.).

4.3.1.2.2.4 Электромагнитные факторы (грозовые разряды и т. д.).

4.3.1.2.2.5 Биологические факторы (микробы, грызуны и т. д.).

4.3.2 Перечень субъективных факторов, воздействующих на защищаемую информацию, в соответствии с установленным принципом их классификации (4.3)

4.3.2.1 *Внутренние факторы*

4.3.2.1.1 Разглашение защищаемой информации лицами, имеющими к ней право доступа.

4.3.2.1.1.1 Разглашение информации лицам, не имеющим права доступа к защищаемой информации.

4.3.2.1.1.2 Передача информации по открытым линиям связи.

4.3.2.1.1.3 Обработка информации на незащищенных ТС обработки информации.

4.3.2.1.1.4 Опубликование информации в открытой печати и других средствах массовой информации.

4.3.2.1.1.5 Копирование информации на незарегистрированный носитель информации.

4.3.2.1.1.6 Передача носителя информации лицу, не имеющему права доступа к ней.

4.3.2.1.1.7 Утрата носителя с информацией.

4.3.2.1.2 Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации.

4.3.2.1.2.1 Несанкционированное изменение информации.

4.3.2.1.2.2 Несанкционированное копирование информации.

4.3.2.1.3 Несанкционированный доступ к защищаемой информации.

4.3.2.1.3.1 Подключение к техническим средствам и системам ОИ.

4.3.2.1.3.2 Использование закладочных устройств.

4.3.2.1.3.3 Использование программного обеспечения технических средств ОИ.

4.3.2.1.3.3.1 Маскировка под зарегистрированного пользователя.

4.3.2.1.3.3.2 Использование дефектов программного обеспечения ОИ.

4.3.2.1.3.3.3 Использование программных закладок.

4.3.2.1.3.3.4 Применение программных вирусов.

4.3.2.1.3.4 Хищение носителя защищаемой информации.

4.3.2.1.3.5 Нарушение функционирования ТС обработки информации.

4.3.2.1.4 Неправильное организационное обеспечение защиты информации.

4.3.2.1.4.1 Неправильное задание требований по защите информации.

4.3.2.1.4.2 Несоблюдение требований по защите информации.

4.3.2.1.4.3 Неправильная организация контроля эффективности защиты информации.

4.3.2.1.5 Ошибки обслуживающего персонала ОИ.

4.3.2.1.5.1 Ошибки при эксплуатации ТС.

4.3.2.1.5.2 Ошибки при эксплуатации программных средств.

4.3.2.1.5.3 Ошибки при эксплуатации средств и систем защиты информации.

4.3.2.2 *Внешние факторы*

4.3.2.2.1 Доступ к защищаемой информации с применением технических средств.

4.3.2.2.1.1 Доступ к защищаемой информации с применением технических средств разведки.

4.3.2.2.1.1.1 Доступ к защищаемой информации с применением средств радиоэлектронной разведки.

4.3.2.2.1.1.2 Доступ к защищаемой информации с применением средств оптико-электронной разведки.

4.3.2.2.1.1.3 Доступ к защищаемой информации с применением средств фотографической разведки.

4.3.2.2.1.1.4 Доступ к защищаемой информации с применением средств визуально-оптической разведки.

4.3.2.2.1.1.5 Доступ к защищаемой информации с применением средств акустической разведки.

4.3.2.2.1.1.6 Доступ к защищаемой информации с применением средств гидроакустической разведки.

4.3.2.2.1.1.7 Доступ к защищаемой информации с применением средств компьютерной разведки.

4.3.2.2.1.2 Доступ к защищаемой информации с использованием эффекта «высокочастотного навязывания».

4.3.2.2.1.2.1 Доступ к защищаемой информации с применением генератора высокочастотных колебаний.

4.3.2.2.1.2.2 Доступ к защищаемой информации с применением генератора высокочастотного электромагнитного поля.

4.3.2.2.2 Несанкционированный доступ к защищаемой информации.

4.3.2.2.2.1 Подключение к техническим средствам и системам ОИ.

4.3.2.2.2.2 Использование закладочных устройств.

4.3.2.2.2.3 Использование программного обеспечения технических средств ОИ.

4.3.2.2.2.3.1 Маскировка под зарегистрированного пользователя.

4.3.2.2.2.3.2 Использование дефектов программного обеспечения ОИ.

4.3.2.2.2.3 3 Использование программных закладок.

4.3.2.2.2.3.4 Применение программных вирусов.

4.3.2.2.2.4 Несанкционированный физический доступ на ОИ.

4.3.2.2.2.5 Хищение носителя с защищаемой информацией.

4.3.2.2.3 Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

4.3.2.2.4 Действия криминальных групп и отдельных преступных субъектов.

4.3.2.2.4.1 Диверсия в отношении ОИ.

УДК 001.4:025.4:006.354 ОКС 01.040.01 Э00 ОКСТУ 0090

Ключевые слова: информация; защищаемая информация; факторы, воздействующие на информацию; объект информатизации; фактор, воздействующий на защищаемую информацию

Редактор *Л.В. Афанасенко*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *С.В. Рябовой*

Изд. лиц. № 021007 от 10.08.95. Сдано в набор 19.05.99. Подписано в печать 14.07.99. Усл.печ.л. 0,93. Уч.-изд.л. 0,65.
Тираж 298 экз. С 3307. Зак. 577.

ИПК Издательство стандартов, 107076, Москва, Колодезный пер., 14.
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. "Московский печатник", Москва, Лялин пер., 6
Плр № 080102