Утвержден
и введен в действие
Приказом Федерального
агентства по техническому
регулированию и метрологии
от 27 декабря 2006 г. N 374-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАЩИТА ИНФОРМАЦИИ

ОБЪЕКТ ИНФОРМАТИЗАЦИИ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ

ОБЩИЕ ПОЛОЖЕНИЯ

Protection of information. Object of informatisation. Factors influencing the information. General

ГОСТ Р 51275-2006

Дата введения
1 февраля 2008 года

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения".

Сведения о стандарте

1. Разработан Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России").
2. Внесен Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии.
3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 374-ст.
4. Взамен ГОСТ Р 51275-99.

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "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.

1. Область применения

Настоящий стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации.

Настоящий стандарт распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности (обороны, экономики, науки и других областях).

2. Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочного стандарта в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3. Термины и определения

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

3.1. Объект информатизации: совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

3.2. Система обработки информации: совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

3.3. Побочное электромагнитное излучение: электромагнитное излучение, наблюдаемое при работе технических средств обработки информации.

3.4. Паразитное электромагнитное излучение: электромагнитное излучение, являющееся результатом паразитной генерации в электрических цепях технических средств обработки информации.

3.5. Наведенный в токопроводящих линейных элементах технических средств сигнал; наводка: ток и напряжение в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями.

3.6. Закладочное средство (устройство): техническое средство (устройство) приема, передачи и обработки информации, преднамеренно устанавливаемое на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы.

Примечание - Местами установки закладочных средств (устройств) на охраняемой территории могут быть любые элементы контролируемой зоны, например: ограждение, конструкции, оборудование, предметы интерьера, транспортные средства [1].

3.7. Программная закладка: преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

Примечание - Программная закладка может быть реализована в виде вредоносной программы или программного кода [1].

3.8. Недекларированные возможности (программного обеспечения): функциональные возможности программного обеспечения, не описанные в документации [1], [2].

3.9. Вредоносная программа: программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы [1], [2].

3.10. (Компьютерный) вирус: вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы [1].

3.11. Компьютерная атака: целенаправленное несанкционированное воздействие на

информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств [1], [2].

3.12. Сетевая атака: компьютерная атака с использованием протоколов межсетевого взаимодействия [1], [2].

3.13. Программное воздействие: несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ [1].

4. Основные положения

4.1. Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и проведения эффективных мероприятий, направленных на защиту информации на объекте информатизации (далее - ОИ).

4.2. Полнота и достоверность выявленных факторов, воздействующих или могущих воздействовать на защищаемую информацию, достигаются 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.

4.3. Выявление факторов, воздействующих на защищаемую информацию, должно осуществляться с учетом следующих требований:

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

5. Классификация факторов, воздействующих на безопасность защищаемой информации

5.1. Факторы, воздействующие или могущие воздействовать на безопасность защищаемой информации и подлежащие учету при организации защиты информации, по признаку отношения к природе возникновения подразделяют на классы:

- объективные;
- субъективные.

5.2. По отношению к ОИ факторы, воздействующие на безопасность защищаемой информации, подразделяют на внутренние и внешние.

5.3. Факторы, воздействующие на безопасность защищаемой информации, в соответствии с признаками классификации подразделяют на:

- подклассы;
- группы;
- подгруппы;
- виды;
- подвиды.

5.4. Перечень основных подклассов (групп, подгрупп и т.д.) факторов, воздействующих на безопасность защищаемой информации (объективных и субъективных), в соответствии с их классификацией, приведенной в 5.3, представлен в разделе 6.

6. Перечень объективных и субъективных факторов, воздействующих на безопасность защищаемой информации

6.1. Перечень объективных факторов, воздействующих на безопасность защищаемой информации

6.1.1. Внутренние факторы

6.1.1.1. Передача сигналов:

а) по проводным линиям связи;

б) по оптико-волоконным линиям связи;

в) в диапазоне радиоволн и в оптическом диапазоне длин волн.

6.1.1.2. Излучения сигналов, функционально присущие техническим средствам (устройствам) (далее - ТС) ОИ:

а) излучения акустических сигналов:

1) сопутствующие работе технических средств (устройств) обработки и передачи информации (далее - ТС ОПИ);

2) сопутствующие произносимой или воспроизводимой ТС речи;

б) электромагнитные излучения и поля:

1) излучения в радиодиапазоне;

2) излучения в оптическом диапазоне.

6.1.1.3. Побочные электромагнитные излучения:

а) элементов (устройств) ТС ОПИ;

б) на частотах работы высокочастотных генераторов устройств, входящих в состав ТС ОПИ:

1) модуляция побочных электромагнитных излучений информативным сигналом, сопровождающим работу ТС ОПИ;

2) модуляция побочных электромагнитных излучений акустическим сигналом, сопровождающим работу ТС ОПИ;

в) на частотах самовозбуждения усилителей, входящих в состав ТС ОПИ.

6.1.1.4. Паразитное электромагнитное излучение:

а) модуляция паразитного электромагнитного излучения информационными сигналами;

б) модуляция паразитного электромагнитного излучения акустическими сигналами.

6.1.1.5. Наводка:

а) в электрических цепях ТС, имеющих выход за пределы ОИ;

б) в линиях связи:

1) вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

2) вызванная внутренними емкостными и (или) индуктивными связями;

в) в цепях электропитания:

1) вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

2) вызванная внутренними емкостными и (или) индуктивными связями;

3) через блоки питания ТС ОИ;

г) в цепях заземления:

1) вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

2) вызванная внутренними емкостными и (или) индуктивными связями;

3) обусловленная гальванической связью схемной (рабочей) "земли" узлов и блоков ТС ОИ;

д) в технических средствах, проводах, кабелях и иных токопроводящих коммуникациях и конструкциях, гальванически не связанных с ТС ОИ, вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

6.1.1.6. Наличие акустоэлектрических преобразователей в элементах ТС ОИ.

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

6.1.1.8. Дефекты, сбои и отказы программного обеспечения ОИ.

6.1.2. Внешние факторы

6.1.2.1. Явления техногенного характера:

а) непреднамеренные электромагнитные облучения ОИ;

б) радиационные облучения ОИ;

в) сбои, отказы и аварии систем обеспечения ОИ.

6.1.2.2. Природные явления, стихийные бедствия:

а) термические факторы (пожары и т.д.);

б) климатические факторы (наводнения и т.д.);

в) механические факторы (землетрясения и т.д.);

г) электромагнитные факторы (грозовые разряды и т.д.);

д) биологические факторы (микробы, грызуны и т.д.);

е) химические факторы (химически агрессивные среды и т.д.).

6.2. Перечень субъективных факторов, воздействующих на безопасность защищаемой информации

6.2.1. Внутренние факторы

6.2.1.1. Разглашение защищаемой информации лицами, имеющими к ней право доступа, через:

а) лиц, не имеющих права доступа к защищаемой информации;

б) передачу информации по открытым линиям связи;

в) обработку информации на незащищенных ТС обработки информации;

г) опубликование информации в открытой печати и других средствах массовой информации;

д) копирование информации на незарегистрированный носитель информации;

е) передачу носителя информации лицам, не имеющим права доступа к ней;

ж) утрату носителя информации.

6.2.1.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем:

а) несанкционированного изменения информации;

б) несанкционированного копирования защищаемой информации.

6.2.1.3. Несанкционированный доступ к информации путем:

а) подключения к техническим средствам и системам ОИ;

б) использования закладочных средств (устройств);

в) использования программного обеспечения технических средств ОИ через:

1) маскировку под зарегистрированного пользователя;

2) дефекты и уязвимости программного обеспечения ОИ;

3) внесение программных закладок;

4) применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

г) хищения носителя защищаемой информации;

д) нарушения функционирования ТС обработки информации.

6.2.1.4. Недостатки организационного обеспечения защиты информации при:

а) задании требований по защите информации (требования противоречивы, не обеспечивают эффективную защиту информации и т.д.);

б) несоблюдении требований по защите информации;

в) контроле эффективности защиты информации.

6.2.1.5. Ошибки обслуживающего персонала ОИ при:

а) эксплуатации ТС;

б) эксплуатации программных средств;

в) эксплуатации средств и систем защиты информации.

6.2.2. Внешние факторы

6.2.2.1. Доступ к защищаемой информации с применением технических средств:

а) разведки:

1) радиоэлектронной;

2) оптико-электронной;

3) фотографической;

4) визуально-оптической;

5) акустической;

6) гидроакустической;

7) технической компьютерной;

б) съема информации.

6.2.2.2. Несанкционированный доступ к защищаемой информации путем:

а) подключения к техническим средствам и системам ОИ;

б) использования закладочных средств (устройств);

в) использования программного обеспечения технических средств ОИ через:

1) маскировку под зарегистрированного пользователя;

2) дефекты и уязвимости программного обеспечения ОИ;

3) внесение программных закладок;

4) применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

г) несанкционированного физического доступа к ОИ;

д) хищения носителя информации.

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

6.2.2.4. Действия криминальных групп и отдельных преступных субъектов:

а) диверсия в отношении ОИ;

б) диверсия в отношении элементов ОИ.

6.2.2.5. Искажение, уничтожение или блокирование информации с применением технических средств путем:

а) преднамеренного силового электромагнитного воздействия:

1) по сети электропитания на порты электропитания постоянного и переменного тока;

2) по проводным линиям связи на порты ввода-вывода сигналов и порты связи;

3) по металлоконструкциям на порты заземления и порты корпуса;

4) посредством электромагнитного быстроизменяющегося поля на порты корпуса, порты ввода-вывода сигналов и порты связи;

б) преднамеренного силового воздействия различной физической природы;

в) использования программных или программно-аппаратных средств при осуществлении:

1) компьютерной атаки;

2) сетевой атаки;

г) воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

Библиография

[1]	Рекомендации по стандартизации Р 50.1.053-2005	Информационная технология. Основные термины и определения в области технической защиты информации
[2]	Рекомендации по стандартизации Р 50.1.056-2005	Техническая защита информации. Основные термины и определения