

ВИДЫ СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ, ПОДЛЕЖАЩИХ СЕРТИФИКАЦИИ В СИСТЕМЕ
СЕРТИФИКАЦИИ СЗИ - ГТ

1. Технические средства защиты информации, включая средства контроля эффективности принятых мер защиты информации:

1.1. Средства защиты информации от перехвата оптических сигналов (изображений) в видимом, инфракрасном и ультрафиолетовом диапазонах волн.

1.2. Средства защиты информации от перехвата акустических сигналов, распространяющихся в воздушной, водной, твердой средах.

1.3. Средства защиты информации от перехвата электромагнитных сигналов, в том числе от перехвата побочных электромагнитных излучений и наводок (ПЭМИН), возникающих при работе технических средств регистрации, хранения, обработки и документирования информации.

1.4. Средства защиты информации от перехвата электрических сигналов, возникающих в токопроводящих коммуникациях:

- за счет ПЭМИН при работе технических средств регистрации, хранения, обработки и документирования информации;

- вследствие эффекта электроакустического преобразования сигналов вспомогательными техническими средствами и системами.

1.5. Средства защиты информации от деятельности радиационной разведки по получению сведений за счет изменения естественного радиационного фона окружающей среды, возникающего при функционировании объекта защиты.

1.6. Средства защиты информации от деятельности химической разведки по получению сведений за счет изменения химического состава окружающей среды, возникающего при функционировании объекта защиты.

1.7. Средства защиты информации от возможности получения сведений магнитометрической разведкой за счет изменения локальной структуры магнитного поля Земли, возникающего вследствие деятельности объекта защиты.

1.8. Технические средства обнаружения и выявления специальных технических средств, предназначенных для негласного получения информации, устанавливаемых в конструкциях зданий и объектов (помещения, транспортные средства), инженерно - технических коммуникациях, интерьере, в бытовой технике, в технических средствах регистрации, хранения, обработки и документирования информации, системах связи и на открытой территории.

2. Технические средства и системы в защищенном исполнении, в том числе:

2.1. Средства скремблирования, маскирования или шифрования телематической информации, передаваемой по каналам связи.

2.2. Аппаратура передачи видеоинформации по оптическому каналу.

3. Технические средства защиты специальных оперативно - технических мероприятий (специальных технических средств, предназначенных для негласного получения информации).

4. Технические средства защиты информации от несанкционированного доступа (НСД):

4.1. Средства защиты, в том числе:

- замки (механические, электромеханические, электронные);

- пломбы;

- замки разового пользования;

- защитные липкие ленты;

- защитные и голографические этикетки;

- специальные защитные упаковки;

- электрические датчики разных типов;

- телевизионные системы охраны и контроля;

- лазерные системы;
- оптические и инфракрасные системы;
- устройства идентификации;
- пластиковые идентификационные карточки;
- ограждения;
- средства обнаружения нарушителя или нарушающего воздействия;
- специальные средства для транспортировки и хранения физических носителей информации (кассеты стриммеров, магнитные и оптические диски и т.п.).

4.2. Специальные средства защиты от подделки документов на основе оптико - химических технологий, в том числе:

- средства защиты документов от ксерокопирования;
- средства защиты документов от подделки (подмены) с помощью химических идентификационных препаратов;
- средства защиты информации с помощью тайнописи.

4.3. Специальные пиротехнические средства для транспортировки, хранения и экстренного уничтожения физических носителей информации (бумага, фотопленка, аудио- и видеокассеты, лазерные диски).

5. Программные средства защиты информации от НСД и программных закладок:

5.1. Программы, обеспечивающие разграничение доступа к информации.

5.2. Программы идентификации и аутентификации терминалов и пользователей по различным признакам (пароль, дополнительное кодовое слово, биометрические данные и т.п.), в том числе программы повышения достоверности идентификации (аутентификации).

5.3. Программы проверки функционирования системы защиты информации и контроля целостности средства защиты от НСД.

5.4. Программы защиты различного вспомогательного назначения, в том числе антивирусные программы.

5.5. Программы защиты операционных систем ПЭВМ (модульная программная интерпретация и т.п.).

5.6. Программы контроля целостности общесистемного и прикладного программного обеспечения.

5.7. Программы, сигнализирующие о нарушении использования ресурсов.

5.8. Программы уничтожения остаточной информации в запоминающих устройствах (оперативная память, видеопамять и т.п.) после завершения ее использования.

5.9. Программы контроля и восстановления файловой структуры данных.

5.10. Программы имитации работы системы или ее блокировки при обнаружении фактов НСД.

5.11. Программы определения фактов НСД и сигнализации (передачи сообщений) об их обнаружении.

6. Защищенные программные средства обработки информации:

6.1. Пакеты прикладных программ автоматизированных рабочих мест (АРМ).

6.2. Базы данных вычислительных сетей.

6.3. Программные средства автоматизированных систем управления (АСУ).

6.4. Программные средства идентификации изготовителя программного (информационного) продукта, включая средства идентификации авторского права.

7. Программно - технические средства защиты информации:

7.1. Программно - технические средства защиты информации от несанкционированного копирования, в том числе:

- средства защиты носителей данных;

- средства предотвращения копирования программного обеспечения, установленного на ПЭВМ.

7.2. Программно - технические средства криптографической и стенографической защиты информации (включая средства маскирования информации) при ее хранении на носителях данных и при передаче по каналам связи.

7.3. Программно - технические средства прерывания работы программы пользователя при нарушении им правил доступа, в том числе:

- принудительное завершение работы программы;
- блокировка компьютера.

7.4. Программно - технические средства стирания данных, в том числе:

- стирание остаточной информации, возникающей в процессе обработки секретных данных в оперативной памяти и на магнитных носителях;
- надежное стирание устаревшей информации с магнитных носителей.

7.5. Программно - технические средства выдачи сигнала тревоги при попытке несанкционированного доступа к информации, в том числе:

- средства регистрации некорректных обращений пользователей к защищаемой информации;
- средства организации контроля за действиями пользователей ПЭВМ.

7.6. Программно - технические средства обнаружения и локализации действия программных и программно - технических закладок.

8. Специальные средства защиты от идентификации личности:

8.1. Средства защиты от фонографической экспертизы речевых сигналов.

8.2. Средства защиты от дактилоскопической экспертизы.

9. Программно - аппаратные средства защиты от несанкционированного доступа к системам оперативно - розыскных мероприятий (СОРМ) на линиях связи:

9.1. В проводных системах связи.

9.2. В сотовых системах связи.