ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. **Комплексность.** Предполагает:

а) обеспечение безопасности обслуживающего персонала, материальных и финансовых ресурсов от всех возможных угроз всеми доступными законными средствами, методами и мероприятиями;

б) обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, во всех технологических процессах и операциях их создания, обработки, использования и уничтожения;

в) способность системы защиты информации к развитию и совершенствованию в соответствии с изменяющимися внешними и внутренними условиями.

2. **Своевременность** – упреждающий характер мер защиты информации. Предполагает постановку задач по комплексной защите информации на стадии проектирования (создания) системы ее защиты на основе анализа известных и прогнозирования возможных угроз безопасности информации, которые могут появиться в будущем после запуска системы защиты в эксплуатацию (реализацию).

3. **Непрерывность** – постоянное поддержание работоспособности и развитие системы защиты информации.

4. **Активность** – настойчивость в достижении целей и задач защиты информации. Предполагает постоянный маневр силами и средствами защиты информации, а также принятие нестандартных мер защиты.

5. **Законность** – разработка системы защиты информации на основе действующего законодательства, а также иных нормативных актов, регламентирующих безопасность информации. В ходе последующей реализации системы защиты информации – применение всех законных методов и средств обнаружения и пресечения правонарушений в области безопасности информации.

6. **Обоснованность**. Заключается в том, что все методы и средства защиты информации должны быть научно обоснованными и современными, соответствовать последним достижениям науки и техники. В своей совокупности они должны отвечать всем установленным требованиям и нормам по защите информации.

7. **Экономическая целесообразность** – затраты на разработку и реализацию (обеспечение заданных параметров) системы защиты информации не должны превышать размеры потенциального ущерба, который может наступить в результате нарушения безопасности защищаемой информации.

8. **Специализация.** Предполагает привлечение к разработке и внедрению методов и средств защиты информации специализированных субъектов, имеющих государственную лицензию на определенный вид

деятельности в сфере оказания услуг по защите информации. Применяемые ими средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

9. **Взаимодействие и координация деятельности**. Предусматривает организацию четкого взаимодействия между всеми субъектами защиты информации, действующими в рамках единой системы защиты информации, а также координацию их усилий и осуществляемых работ в этой сфере для достижения общих целей. Заключается в интеграции и последовательности деятельности по защите конкретных информационных ресурсов.

10. **Совершенствование**. Предусматривает совершенствование и разработку новых законодательных, организационных и технических мер защиты информации под воздействием объективных и субъективных факторов.

11. **Централизация управления.** Предполагает наличие единого координационного центра (субъекта), занимающегося общими вопросами управления системой защиты информации, а также единых требований по обеспечению безопасности информации.

(см.: *Ярочкин В.И.* Система безопасности фирмы. - 2-е изд. - М., 1998. - С. 8-10)

ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

1. Соблюдение конфиденциальности информации ограниченного доступа.

2. Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к такой информации.

3. Предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию и предоставлению информации, а также иных неправомерных действий в отношении такой информации.

4. Реализация конституционного права граждан на доступ к информации.

5. Недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.

ОСНОВНЫЕ ЗАДАЧИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Проведение единой политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности.

2. Исключение или существенное затруднение добывания информации средствами разведки.

3. Предотвращение утечки информации по техническим каналам и несанкционированного доступа к ней.

4. Предупреждение вредоносных воздействий на информацию, ее носителей, а также технические средства ее создания, обработки, использования, передачи и защиты.

5. Принятие правовых актов, регулирующих общественные отношения в области защиты информации.

6. Анализ состояния и прогнозирование возможностей технических средств разведки, а также способов их применения.

7. Формирование системы информационного обмена сведениями об осведомленности иностранных разведок о силах, методах, средствах и мероприятиях, обеспечивающих защиту информации внутри страны и за ее пределами.

8. Организация сил, разработка научно обоснованных методов, создание средств защиты информации и контроля за ее эффективностью.

9. Контроль состояния защиты информации в органах государственной власти, учреждениях, организациях и на предприятиях всех форм собственности, использующих в своей деятельности охраняемую законом информацию.

СУБЪЕКТЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

1. ПРЕЗИДЕНТ РОССИЙСКОЙ ФЕДЕРАЦИИ:

- определяет основные направления государственной политики в области обеспечения безопасности;
- утверждает Стратегию национальной безопасности Российской Федерации, иные концептуальные и доктринальные документы в области обеспечения безопасности;
- формирует и возглавляет Совет Безопасности;
- устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых он осуществляет
- **решает** в соответствии с законодательством Российской Федерации **вопросы,** связанные с обеспечением **защиты: информации и государственной тайны;**
- утверждает государственные программы в области защиты информации;
- утверждает по представлению Правительства Российской Федерации состав, структуру Межведомственной комиссии по защите государственной тайны и положение о ней;
- утверждает по представлению Правительства Российской Федерации **Перечень должностных лиц** органов государственной власти, наделяемых

полномочиями по отнесению сведений к государственной тайне, а также **Перечень сведений,** отнесенных к государственной тайне;

- заключает международные договоры России о совместном использовании и защите сведений, составляющих государственную тайну;

- определяет полномочия должностных лиц по обеспечению защиты информации в Администрации Президента Российской Федерации;

- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к тому или иному виду тайны, их засекречиванием или рассекречиванием и их защитой.

2. ПАЛАТЫ ФЕДЕРАЛЬНОГО СОБРАНИЯ:

- осуществляют законодательное регулирование отношений в сфере защиты информации;

- рассматривают статьи федерального бюджета в части средств, направляемых на реализацию государственных программ в этой области;

- определяют полномочия должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания.

3. ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ:

- организует исполнение Законов и международных соглашений в области защиты информации;

- представляет на утверждение Президенту состав и структуру межведомственной комиссии по защите государственной тайны, а также положение о ней;

- представляет на утверждение Президенту Перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к тому или иному виду тайны;

- организует разработку и выполнение государственных программ в области защиты информации;

- определяет полномочия должностных лиц по обеспечению защиты информации в аппарате Правительства;

- устанавливает размеры и порядок предоставления льгот гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;

- устанавливает порядок определения размеров ущерба, наступившего в результате несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, наносимого собственнику

информации в результате ее засекречивания;

- заключает межправительственные соглашения, принимает меры по выполнению международных договоров России о совместном использовании и защите сведений, составляющих государственную тайну, принимает решения о возможности передачи их носителей другим государствам;

- в пределах своих полномочий решает иные вопросы, возникающие в связи с отнесением сведений к тому или иному виду тайны, их засекречиванием или рассекречиванием и их защитой.

4. ОРГАНЫ ГОСУДАРСТВЕННОЙ ВЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ОРГАНЫ ГОСУДАРСТВЕННОЙ ВЛАСТИ СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ И ОРГАНЫ МЕСТНОГО САМОУПРАВЛЕНИЯ ВО ВЗАИМОДЕЙСТВИИ С ОРГАНАМИ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ, РАСПОЛОЖЕННЫМИ В ПРЕДЕЛАХ СООТВЕТСТВУЮЩИХ ТЕРРИТОРИЙ:

- обеспечивают защиту переданных им другими органами государственной власти, предприятиями, учреждениями и организациями охраняемой законом информации, а также сведений, засекречиваемых ими;

- обеспечивают защиту государственной тайны на подведомственных им предприятиях, в учреждениях и организациях в соответствии с требованиями законодательства Российской Федерации;

- обеспечивают в пределах своей компетенции проведение проверочных мероприятий в отношении граждан, допускаемых к тайне;

- реализуют предусмотренные законодательством меры по ограничению конституционных прав граждан и предоставлению льгот лицам, имеющим либо имевшим доступ к сведениям, составляющим государственную тайну;

- вносят в полномочные органы государственной власти предложения по совершенствованию системы защиты информации.

5. ОРГАНЫ СУДЕБНОЙ ВЛАСТИ:

- рассматривают уголовные и гражданские дела о нарушениях законодательства в области защиты информации;

- обеспечивают судебную защиту граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите охраняемой законом информации;

- обеспечивают в ходе рассмотрения указанных дел защиту отдельных видов тайны;

- определяют полномочия должностных лиц по обеспечению защиты охраняемой законом информации в органах судебной власти.

6. ОРГАНЫ ЗАЩИТЫ ИНФОРМАЦИИ:

1) **Межведомственная комиссия по защите государственной тайны** - это коллегиальный орган, координирующий работу по защите информации в Российской Федерации.

2) Органы федеральной исполнительной власти. К ним относятся: Федеральная служба безопасности (ФСБ – www.fsb.ru), Министерство обороны (МО – www.mil.ru), Служба внешней разведки (СВР – www.svr.gov.ru), Федеральная служба по техническому и экспортному контролю (ФСТЭК России – **www.fstec.ru –** бывшая Гостехкомиссия при Президенте РФ).

3) Органы государственной власти, предприятия, учреждения, организации и их структурные подразделения по защите охраняемой законом информации.

Федеральная служба безопасности (ФСБ России) - единая централизованная система органов федеральной службы безопасности, осуществляющая решение в пределах своих полномочий задач по обеспечению безопасности Российской Федерации. по следующим основным направлениям:

контрразведывательная деятельность;
борьба с терроризмом;
борьба с преступностью;
разведывательная деятельность;
пограничная деятельность;
обеспечение информационной безопасности.

Обеспечение информационной безопасности - деятельность органов федеральной службы безопасности, осуществляемая ими в пределах своих полномочий:

при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;

при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу шифрованной информации, в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) –

является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура);

2) противодействия иностранным техническим разведкам на территории Российской Федерации (далее - противодействие техническим разведкам);

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания,

уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее - техническая защита информации);

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации

ФСТЭК России и ее территориальные органы входят в состав государственных органов обеспечения безопасности.

Деятельность ФСТЭК России обеспечивают Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, а также другие подведомственные ФСТЭК России организации.

Решения ФСТЭК России являются обязательными для исполнения всеми органами государственной власти и местного самоуправления, государственными и негосударственными предприятиями, учреждениями, организациями, должностными лицами и гражданами.

Основными задачами ФСТЭК России являются:

1. Реализация в пределах своей компетенции государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.

2. Осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

3. Организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой.

4. Осуществление самостоятельного нормативно-правового регулирования вопросов:

- обеспечения безопасности информации в ключевых системах информационной инфраструктуры;

- противодействия техническим разведкам;

- технической защиты информации;

- размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров России, иных программ и проектов на территории России, на континентальном шельфе и в исключительной экономической зоне России;

- координации деятельности органов государственной власти по подготовке развернутых перечней сведений, подлежащих засекречиванию, а также методического руководства этой деятельностью;

- осуществления экспортного контроля.

5. Обеспечение в пределах своей компетенции безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях.

6. Прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации.

7. Противодействие добыванию информации техническими средствами разведки, техническая защита информации.

8. Осуществление координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и организаций по государственному регулированию размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров России, иных программ и проектов на территории России, на континентальном шельфе и в исключительной экономической зоне России.

9. Осуществление в пределах своей компетенции контроля деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях.

10. Реализация государственной политики и организация межведомственного взаимодействия в области экспортного контроля.

11. Осуществление контроля за соблюдением российскими участниками внешнеэкономической деятельности законодательных и иных нормативных правовых актов Российской Федерации в области экспортного контроля.

12. Осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны и Комиссии по экспортному контролю Российской Федерации.

НАПРАВЛЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1. Подготовка и принятие законодательных и иных нормативно-правовых актов в области защиты информации.

2. Обеспечение контроля за их исполнением.

3. Финансовое и кадровое обеспечение мероприятий по защите информации.

4. Обеспечение эффективного управления системой защиты информации.

5. Определение сведений, подлежащих охране, и демаскирующих признаков, раскрывающих эти сведения.

6. Анализ и оценка угроз безопасности охраняемой законом информации.

7. Разработка организационно-технических мероприятий по защите информации и их реализация.

8. Организация и проведение контроля состояния защиты информации.

9. Анализ и оценка эффективности системы защиты информации, ее своевременная корректировка.

ОСНОВНЫЕ ОРГАНИЗАЦИОННО - ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1. Лицензирование деятельности предприятий в области защиты информации.

2. Аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.

3. Сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам.

4. Категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной,

экономической, политической, научно-технической и других сферах деятельности.

5. Обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений.

6. Оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории России.

7. Введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите.

8. Создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

9. Разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи.

10. Разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование.

11. Применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам электросвязи.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Средство защиты информации – техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации.

Средства защиты информации делятся на:

1. ФИЗИЧЕСКИЕ – различные инженерные средства и сооружения, затрудняющие или исключающие физическое проникновение (или доступ) правонарушителей на объекты защиты и к материальным носителям конфиденциальной информации:

2. АППАРАТНЫЕ – механические, электрические, электронные и другие устройства, предназначенные для защиты информации от утечки, разглашения, модификации, уничтожения, а также противодействия средствам технической разведки:

3. ПРОГРАММНЫЕ – специальные программы для ЭВМ, реализующие функции защиты информации от несанкционированного доступа, ознакомления, копирования, модификации, уничтожения и блокирования.

4. КРИПТОГРАФИЧЕСКИЕ – технические и программные средства шифрования данных, основанные на использовании разнообразных математических и алгоритмических методов.

5. КОМБИНИРОВАННЫЕ – совокупная реализация аппаратных и программных средств и криптографических методов защиты информации.

ВИДЫ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ:

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 документиро-вания 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 функциониро-вании 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, предназначен-ных для негласного получения информации, устанавливаемых в конструкциях зданий и объектов (помеще-ния, 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, переда-ваемой по каналам связи.

2.2. Аппаратура передачи видеоинформации по оптическому каналу.

3. Технические средства защиты специальных оперативно-технических мероприятий (специ-альных 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 уничтоже-ния 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 призна-кам (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) продук-та, 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.

ОБЪЕКТЫ ЗАЩИТЫ

Объект защиты – это информация, носитель информации или информационный процесс, в отноше-нии которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Типичные объекты защиты:

1. Лица, допущенные к работе с охраняемой законом информацией либо имеющие доступ в помеще-ния, где эта информация обрабатывается.

2. Объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназна-ченные для проведения служебных совещаний, заседаний и переговоров.

3. Охраняемая законом информация – информация, доступ к которой ограничен в соответствии с законодательством России (сведения (сообщения, данные), составляющие государственную, банковскую, коммерческую, налоговую, служебную, профессиональную, семейную и иную тайну, включая персональные данные физических лиц).

4. Материальные носители охраняемой законом информации.

5. Средства защиты информации.

6. Технологические отходы (мусор), образовавшиеся в результате обработки охраняемой законом информации.

ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

УГРОЗА – это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

ЕСТЕСТВЕННЫЕ:

1. Стихийные бедствия, природные явления (пожары, землетрясения, наводнения, ураганы, смерчи, тайфуны, циклоны и т.п.).
2. Самопроизвольное разрушение элементов, из которых состоит средство электронно-вычислитель-ной техники, электросвязи и защиты информации.

ИСКУССТВЕННЫЕ
(деятельность человека):

1. Умышленные (правонарушения).

1) Пассивный (бесконтактный) несанкционированный доступ к информации:

а) визуальное наблюдение за объектами информатизации (невооруженным глазом; с помощью оптических и оптико-электронных приборов и устройств);

б) перехват речевой информации (с помощью остро направленных микрофонов, электронных стетоскопов, лазерного луча, устройств дистанционного съема речевой информации с проводных линий электросвязи, радиомикрофонных закладок, телефонных закладок, микрофонных закладок, минимагнитофонов и диктофонов);

в) электромагнитный перехват информации (в радиосетях связи, побочных электромагнитных излу-чений, побочных электромагнитных наводок, паразитных модуляций ВЧ сигналов, паразитных информа-тивных токов и напряжений во вспомогательных сетях технических средств передачи информации.

2) Активный (контактный) несанкционированный доступ к информации:

а) с использованием физического доступа путем непосредственного воздействия на материальные носители, иные средства обработки и защиты информации;

б) с использованием штатных и специально разработанных (приспособленных, запрограммирован-ных) средств для негласного получения, уничтожения, модификации и блокирования информации.

2. Неумышленные
(ошибки деятельности человека – непреодолимые факторы).

1) Ошибки при создании (изготовлении) средств электронно-вычислительной техники, электросвязи и защиты информации (ошибки проектирования, кодирования информации, изготовления элементов технических средств и систем);

2) Ошибки, возникающие в процессе работы (эксплуатации) средств электронно-вычислительной техники, электросвязи и защиты информации (неадекватность концепции обеспечения безопасности; ошибки управления системой защиты; ошибки персонала; сбои и отказы оборудования и программного обеспе-чения; ошибки при производстве пуско-наладочных и ремонтных работ.

МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Машинный носитель информации – любое техническое устройство либо физическое поле, предназ-наченное для фиксации, хранения, накопления,

преобразования и передачи компьютерной информации. Наиболее распространены следующие виды материальных носителей информации:

• ***ферромагнитная полимерная лента или полоса*** (в кассетах, бобинах, на плоских носителях – картах, бумажных документах, ценных бумагах и денежных купюрах);

• ***ферромагнитная металлическая нить*** (в кассетах и бобинах для бортовых самописцев транспортных средств («черных ящиков»), на пластиковых картах, бумажных документах, ценных бумагах и денежных купюрах);

• ***гибкий полимерный магнитный диск*** (дискета, ZIP-диск);

• ***диски Бернулли*** (Bernoulli removable media drive) – техническое устройство размером 5’’, содержащее пакет гибких полимерных магнитных дисков 3.5’’ с плавающими электромагнитными головками для записи/чтения информации (далее – «головки»), представляющее собой кассету с жестким корпусом;

• ***жесткий магнитный диск*** (Jas-диск);

• ***внутренние и внешние кассетные устройства с жесткими магнитными дисками и головками*** (винчестер, PDC (Power Disk Cartridge), SparQ, SyJet);

• ***гибкая оптическая или магнитооптическая полимерная пленка*** («цифровая бумага» английской фирмы Imagedata);

• ***гибкие магнитооптические диски*** (floptical drives) – магнитная запись/считывание с оптическим позиционированием;

• ***жесткий оптический или магнитооптический диск*** (MOD – Magneto-Optical Drives): CD-ROM (Compact Disc Read Only Memory) – постоянное запоминающее устройство только для чтения на основе компакт-диска; CD-R (Recordable), CD-WORM (Write Once, Read Many), CD-WO (Write Once) – однократно записываемый и многократно считываемый; CD-RW (ReWritable), PD (Phase change Disk) – многократно перезаписываемый и считываемый CD-ROM; DVD-ROM (Digital Video Disk Read-Only Memory) – постоянное запоминающее устройство на основе цифрового видеодиска; DVD-RAM; DVD-RW;

• ***интегральная микросхема с памятью*** – микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы памяти ЭВМ и других компьютерных устройств, элементы и связи которого неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие (энергозависимая – оперативное запоминающее устройство (ОЗУ); энергонезависимая – постоянное запоминающее устройство (ПЗУ), программируемое ПЗУ (ППЗУ), электрически стираемое ППЗУ (ЭСППЗУ));

• ***электромагнитное поле***;

• ***комбинированные*** (содержащие два и более разнородных машинных носителя).

Классификация машинных носителей информации

1. По времени хранения информации:

• ***оперативные*** – обеспечивающие кратковременное хранение данных и команд, например, оперативное запоминающее устройство (ОЗУ) или электромагнитное поле;

• ***постоянные*** – время хранения информации ограничивается лишь сроком службы (физическим износом) материала МНИ, например, постоянное запоминающее устройство (ПЗУ) или магнитная лента.
2. По условиям корректировки информации:

• ***не перезаписываемые*** – МНИ, на которые информация записывается один раз и хранится постоянно до момента физического уничтожения или полного старения (износа) ее носителя – позволяют использовать информацию без корректировки только в режиме "чтение", например, перфокарта, перфолента, карта со штрих-кодом, не перезаписываемый оптический диск (компакт-диск), не перезаписываемая ИМСП;

• ***однократно перезаписываемые*** – машинные носителя, позволяющие произвести одноразовую корректировку ранее записанной на них информации - информация на них записывается частями (порциями, импульсами) до тех пор, пока объем свободной памяти не будет исчерпан, либо один раз с одновременной перезаписью всех ранее записанных данных, например, интегральная микросхема ПЗУ ЭВМ или иного компьютерного устройства;

• ***многократно перезаписываемые*** – МНИ, допускающие многократную перезапись и чтение компьютерной информации, например, магнитные диски и ленты, магнитооптические диски, интегральная микросхема ОЗУ, электромагнитное поле.

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Абонент Сети – лицо, являющееся сотрудником учреждения (предприятия), имеющее соответствующим образом оформленное разрешение и технические возможности на подключение и взаимодействие с Сетями.

Абонентский пункт (АП) – средства вычислительной техники учреждения (предприятия), подключаемые к Сетям с помощью коммуникационного оборудования. АП могут быть в виде автономных персональных электронно-вычислительных машин (ПЭВМ) с модемом и не иметь физических каналов связи с другими средствами вычислительной техники (СВТ) предприятия, а также в виде одной или нескольких объединенных локальных вычислительных сетей (ЛВС) с рабочими станциями и серверами, соединенными с Сетями через коммуникационное оборудование (модемы, мосты, шлюзы, маршрутизаторы-роутеры, мультиплексоры, коммуникационные серверы и т.п.).

Автоматизированная система (АС) – система, состоящая из персонала и

комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация - процесс удостоверения прав пользователей на осуществление каких-либо действий над компьютерной информацией, содержащейся в системе или сети ЭВМ.

Администратор АС – физическое лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

Администратор защиты (безопасности) - физическое лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

Антивирусная программа - программа для ЭВМ, предназначенная для поиска, регистрации и уничтожения вредоносных программ для ЭВМ.

Аттестованное средство электронно-вычислительной техники - средство электронно-вычислительной техники в отношении которого проведено специальное исследование на предмет отсутствия вредоносных программных и аппаратных средств с выдачей Аттестата соответствия требованиям по безопасности информации.

Аутентификации - процесс определения подлинности объектов - автоматов и (или) субъектов - пользователей, устанавливающих связь.

База данных - это объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Банковская тайна – информация об операциях, счетах и вкладах клиентов и корреспондентов кредитной организации, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

Блокирование компьютерной информации - физическое воздействие на компьютерную информацию, ее машинный носитель и (или) программно-технические средства ее обработки и защиты, результатом которого явилась временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией.

Вредоносная программа для ЭВМ - программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети без предварительного предупреждения пользователя о характере действия программы и не запрашивающая его разрешения на реализацию программой своего назначения.

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, а также их коммуникации, в том числе транзитные линии, не предназначенные для обработки, передачи и хранения охраняемой законом информации, устанавливаемые совместно с основными техническими средствами и системами (ОТСС) или в защищаемых помещениях. К ним относятся: различного рода телефонные средства и системы; средства и системы передачи данных в системе радиосвязи; средства и системы охранной и пожарной сигнализации;

средства и системы оповещения и сигнализации; контрольно-измерительная аппаратура; средства и системы кондиционирования; средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры, радиоприемники, видеокамеры и т.д.); средства электронной оргтехники; средства и системы электрочасофикации; банкоматы и торговые автоматы; иные технические средства и системы.

Выделенные помещения - помещения в которых обрабатывается и распространяется охраняемая законом информация.
Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно - розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
Документированная информация (документ) - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством РФ случаях ее материальный носитель.

Достоверность передачи информации - соответствие принятого сообщения переданному. Определяет степень вероятности отсутствия ошибок в полученном сообщении.

Доступ к информации – возможность получения информации и ее использования.

Доступ к компьютерной информации - всякая форма проникновения к ней с использованием СВТ, позволяющая манипулировать информацией (уничтожать ее, блокировать, модифицировать и копировать).

Доступность (санкционированная доступность) информации – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Закладное устройство – элемент съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации, в т.ч. в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от несанкционированного доступа (НСД)– деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию) с нарушением установленных прав или правил.

Защита информации от утечки - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.

Защита информации от несанкционированного воздействия - защита информации от НСВ: Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою

функционирования носителя информации.

Защита информации от непреднамеренного воздействия - деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защищаемые помещения (ЗП) – помещения (служебные кабинеты, актовые и конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, семинаров, переговоров, деловых бесед и т.п.).

Информативные сигналы - электрические сигналы, а также акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах и циркулирующая в ЗП.

Информация – сведения (сообщения, данные), независимо от формы их представления.

Информация, составляющая коммерческую тайну - научно-техническая, технологическая, производственная, финансово- экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации т обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Категорирование защищаемой информации (объекта защиты) -установление градаций важности защиты защищаемой информации [объекта защиты].

Категорирование объекта информатизации - процесс присвоения объекту 1-й, 2-й или 3-й категории по требованиям безопасности информации.

Код - система условных знаков для передачи, обработки и хранения (запоминания) информации; система условных знаков или сигналов для передачи сведений; программа для ЭВМ, находящаяся в формате машинного языка.

Кодирование - процесс зашифровывания при помощи кода, преобразования в код какой-либо информации в целях ее сбора, хранения, обработки, передачи и использования.

Коммерческая тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Контролируемая зона – пространство (территория, здание или его часть), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска к охраняемой законом информации, и посторонних транспортных средств.

Контроль состояния защиты информации - проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

Контроль организации защиты информации - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль эффективности защиты информации - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Конфиденциальность информации – обязательное для выполнения лицом, получившем доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее правообладателя.
Копирование компьютерной информации - это повторение и устойчивое запечатление компьютерной информации любыми способами на отличном от оригинала материальном носителе при одновременной сохранности признаков, идентифицирующих ее.
Криптография - специальная система изменения открытого письма с целью сделать текст понятным лишь для тех лиц, которые знают эту систему; тайнопись (от греч. "криптос" - скрытый и "графо" - пишу).

Криптографический протокол - совокупностью действий (инструкций, команд, вычислений, алгоритмов), выполняемых в заданной последовательности двумя или более объектами (субъектами) криптографической системы для достижения следующих целей: обмена ключевой информацией с последующей установкой засекреченного режима передачи и приема сообщений; аутентификации; авторизации. Субъекты криптографической системы - это люди (пользователи), а объекты - автоматы (технические устройства).

Локальная вычислительная сеть (ЛВС) – совокупность ЭВМ, сетевого оборудования и структурированной кабельной системы, осуществляющая обмен информацией с другими информационными системами, в т.ч. ЛВС, через определенные точки входа/выхода информации, которые являются границами ЛВС.

Межсетевой экран (МЭ) – это локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс),

реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в/из АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС.

Мероприятие по защите информации - совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации - совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.

Нарушение работы ЭВМ, системы ЭВМ или их сети - это временное или устойчивое создание помех для их функционирования в соответствии с назначением.

Несанкционированный доступ (НСД) к информации - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или АС; преднамеренное обращение субъекта к компьютерной информации, доступ к которой ему не разрешен, независимо от цели обращения.

Носитель информации - физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка информации - любые действия с информацией, связанные с ее изменением, воспроизведением, передачей и (или) хранением.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Общие и частные модели угроз - описание возможных угроз безопасности информации и объекту информатизации, выполненное на основе данных о возможностях потенциального противника.

Объект информатизации - средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров.

Оператор информационной системы (ИС) – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в т.ч. по обработке информации, содержащейся в ее базах данных.

Орган защиты информации - административный орган, осуществляющий организацию защиты информации.

Основные технические средства и системы - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи охраняемой законом информации.

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности этой подписи в электронном документе.

Паспортизация объекта информатизации - оформление на объект информатизации технического паспорта.

Персональная ЭВМ (персональный компьютер) - универсальная ЭВМ, предназначенная для использования в автономном режиме, системе ЭВМ или их сети для решения задач различной профессиональной ориентации, например, используемая в качестве рабочего места специалиста.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Пользователь сертификата ключа электронной цифровой подписи (ЭЦП) - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Право доступа к информации - право доступа: совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

Правило доступа к информации - правило доступа: совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Предоставление информации – это действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Программа для ЭВМ - это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.
Профессиональная тайна – информация, полученная физическими лицами при исполнении ими профессиональных обязанностей или юридическими лицами при осуществлении ими определенных видов деятельности. Подлежит защите в случаях, если на эти лица Федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Разглашение информации, составляющей коммерческую тайну - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Распространение информации – это действия, направленные на получение

информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Режим разграничения доступа - порядок доступа к компьютерной информации в соответствии с установленными правилами.

Режим коммерческой тайны - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Сертификация - деятельность, подтверждающая соответствие свойств и технических параметров технического или программного средства свойствам и параметрам, заданным в данной системе сертификации.
Система защиты информации - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.
Служебная тайна – несекретная информация, касающаяся деятельности организации, ограничения на распространение которой диктуются служебной необходимостью.
Специальная проверка - проверка объекта информатизации на предмет обнаружения встроенных (установленных) специальных технических и программных средств перехвата (съема) информации.
Специальное исследование - исследование объекта информатизации с целью выявления возможных технических каналов утечки информации, проводимое путем измерений, выполняемых по специальным методикам.
Специальное обследование - обследование объекта информатизации с целью определения его соответствия требованиям защиты информации. Состоит из следующих видов деятельности:
1) проверка правильности категорирования и паспортизации объекта информатизации (ОИ);
2) изучение имеющейся технической, технологической, учетной и другой документации на ОИ, в том числе на системы ВТСС;
3) анализ результатов специальных исследований;
4) анализ и оценка возможных угроз защищаемого ОИ с учетом особенностей его размещения и функционирования;
5) классификация АИС или СВТ, имеющихся в составе ОИ по требованиям защиты информации от несанкционированного доступа.
Средства и системы информатизации - средства электронно-вычислительной техники, системы и сети ЭВМ, системы и сети электросвязи, программные средства.
Средство защиты информации - техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации.
Средство электронно-вычислительной техники (СВТ) - электронное техническое устройство, предназначенное для создания, сбора, хранения, обработки, передачи и (или) уничтожения данных и команд в процессе решения вычислительных и информационных задач; совокупность программных и технических элементов систем обработки данных и команд, способных функционировать самостоятельно или в составе других систем.
Техническая защита конфиденциальной информации (ТЗИ) – защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, блокирования и модификации.
Технический канал утечки информации – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства приема, передачи и обработки информации - средства телефонии, звукозаписи, звукоусиления, звуковоспроизведения; переговорные и телевизионные устройства; средства изготовления и тиражирования документов; технические средства обработки речевой, графической, видео-, смысловой и буквенно-цифровой информации.

Транзитные линии вспомогательных технических средств и систем - проводные коммуникации, не относящиеся к вспомогательным техническим средствам и системам объекта информатизации, но расположенные в пределах ограждающих его конструкций, в том числе по внешнему периметру этих конструкций.
Угрозы объекту информатизации - любые возможные процессы и (или) действия, которые могут привести к утечке, хищению (в т.ч. копированию), разрушению, блокированию или потере защищаемой информации, обрабатываемой на объекте информатизации.
Уничтожение компьютерной информации - ликвидация компьютерной информации любыми способами без возможности ее восстановления.
Утечка информации - неправомерный выход охраняемой законом информации за пределы пространства, контролируемого ее правообладателем.
Физическое поле - материальный носитель физических взаимодействий искусственного или естественного происхождения; особая форма существования материи.
Целостность информации – это устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.
Электронная вычислительная машина (ЭВМ) - программируемое электронное техническое устройство, состоящее из одного или нескольких взаимосвязанных центральных процессоров и периферийных устройств, управление которых осуществляется посредством программ, и предназначенное для автоматической обработки информации в процессе решения вычислительных и (или) информационных задач.
электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;
сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;
квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);
владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;
ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;
ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);
удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные

настоящим Федеральным законом;
аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;
средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;
средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;
участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;
корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;
информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

АДРЕСА САЙТОВ ОРГАНИЗАЦИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

www.fstec.ru – Федеральная служба по техническому и экспортному контролю (ФСТЭК России);

www.academy.fsb.ru – Институт криптографии, связи и информатики (ИКСИ) ФСБ России;

www.infotecs.ru – ОАО "Инфотекс" (Информационные Технологии и Коммуникационные Системы);

www.infosec.ru – НИП "Информзащита";

www.novocom.ru – Компания "НОВО" (ЗАО "НОВО-Техника", НОУ "НОВО-УТЦ", ЗАО "НОВО-ГАЛС");

www.confident.ru – ООО "Конфидент"; журнал "Защита информации. Конфидент";

www.inside-zi.ru – Информационно-методический журнал "Защита информации. Инсайд."

www.st.ess.ru – Журнал "Специальная техника";

www.spymarket.com – Компания "СмерШ Техникс";

www.pps.ru – ООО «Лаборатория "ППШ" (противодействие промышленному шпионажу);

www.lancrypto.com – Компания "ЛАН-Крипто" (электронно-цифровые подписи (ЭЦП), конверты и сейфы);

www.aladdin.ru – Компания «Аладдин» (электронно-цифровые ключи HASP , eToken , eSafe , iButton);

www.zaoanna.ru – ЗАО "Анна" (комплексы экстренного уничтожения информации на магнитных носителях);

www.bugtrack.ru – Федеральный портал по информационной безопасности;

www.ssl.stu.neva.ru – Специализированный Центр Защиты Информации при СПбГПУ;

www.security.ru – Московское отделение Пензенского НИИ защиты информации (СКЗИ).