РОССИЙСКАЯ ФЕДЕРАЦИЯ
ПРАВИТЕЛЬСТВО КАЛИНИНГРАДСКОЙ ОБЛАСТИ
АГЕНТСТВО ПО РАЗВИТИЮ СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ КАЛИНИНГРАДСКОЙ ОБЛАСТИ

Семинар

«Организация защиты персональных данных в информационных системах персональных данных»

Руководитель (директор)

Агентства по развитию связи и массовых коммуникаций Калининградской области

ЦЕДИЛИН Сергей Геннадьевич

Программа семинара

1. Правовые основы организации защиты персональных данных в информационных системах персональных данных
   - Директор КГ НИЦ Воронков Сергей Александрович
2. Методы защиты информации в информационных системах персональных данных
   - Руководитель сектора безопасности автоматизированных систем лаборатории защиты информации КГ НИЦ Толков Александр Юрьевич
3. Порядок проведения мероприятий по защите персональных данных в информационных системах персональных данных
   - Директор КГ НИЦ Воронков Сергей Александрович
4. Обсуждение вопросов организации защиты персональных данных
5. Поведение итогов семинара
   - Директор КГ НИЦ Воронков Сергей Александрович

Организация защиты персональных данных в информационных системах персональных данных

Директор
государственного учреждения Калининградский государственный научно-исследовательский центр информационной и технической безопасности»
(КГ НИЦ)
руководитель органа по аттестации объектов информатизации и аттестационного центра ФСТЭК России, руководитель Регионального аттестационного центра специальной экспертизы по Калининградской области ФСБ России,
кандидат физико-математических наук, доцент
Воронков Сергей Александрович
99-22-86, 99-22-64, 99-22-65
+7 921-710-11-08
kgnic@kanet.ru

Основные регламентирующие документы для операторов персональных данных

1. Постановление Правительства РФ от 17 ноября 2007 года № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".
2. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
3. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20 "Об утверждении порядка проведения классификации информационных систем персональных данных".
4. «Положение о методах и способах защиты в информационных системах персональных данных» (введено в действие Приказом директора ФСТЭК России от 5 февраля 2010 г. № 58).
5. «Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 14 февраля 2008 г. ФСТЭК России);
6. «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008 г. ФСТЭК России);
7. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены 21 февраля 2008 г. ФСБ России).
8. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены 21 февраля 2008 г. ФСБ России).
9. Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28 марта 2008 г. № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных».
10. Приказ Федеральной службы по надзору в сфере связи и массовых коммуникаций от 17 июля 2008 г. № 08 «Об утверждении образца формы уведомления об обработке персональных данных».

Документы, утратившие силу

- Утверждено
  первым заместителем
  директора ФСТЭК России
  5 марта 2010 г.

- **Р Е Ш Е Н И Е**
- В связи с изданием приказа ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (зарегистрирован Минюстом России 19 февраля 2010 г., регистрационный № 16456; опубликован: «Российская газета», 5 марта 2010 г., № 46) **не применять с 15 марта 2010 г.** для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных следующие методические документы ФСТЭК России:
- **Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.;**
  Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.

Основные документы, регламентирующие отношения в сфере оказания услуг по технической защите конфиденциальной информации и защите информации криптографическими средствами

- **Указ Президента РФ** «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188 (в ред. Указа Президента РФ от 23.09.2005 N 1111)
- 1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
- **Федеральный закон** "О лицензировании отдельных видов деятельности" от 08.08.2001 N 128-ФЗ
- Статья 17. Перечень видов деятельности, на осуществление которых требуются лицензии
- 5) деятельность по распространению шифровальных (криптографических) средств (ФСБ России);
- 6) деятельность по техническому обслуживанию шифровальных (криптографических) средств (ФСБ России);
- 7) предоставление услуг в области шифрования информации;
- 8) разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем (ФСБ России);
- 11) деятельность по технической защите конфиденциальной информации (ФСТЭК России).

Основные документы, определяющие требования к юридическим лицам и индивидуальным предпринимателям в сфере оказания услуг по технической защите конфиденциальной информации и защите информации криптографическими средствами

- **Положение** о лицензировании деятельности по технической защите конфиденциальной информации
  Утверждено постановлением Правительства Российской Федерации от 15 августа 2006 г. № 504

2. Под технической защитой конфиденциальной информации понимается **комплекс мероприятий и (или) услуг** по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

- **Положения** о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами.
  Утверждено постановлением Правительства Российской Федерации от 29 декабря 2007 N 957

Основные документы, устанавливающие ограничения на ведение предпринимательской деятельности

- **Уголовный кодекс (УК РФ)**
- **Статья 171. Незаконное предпринимательство**
- 1. Осуществление предпринимательской деятельности **без регистрации или с нарушением правил регистрации**, а равно представление в орган, осуществляющий государственную регистрацию юридических лиц и индивидуальных предпринимателей, документов, содержащих заведомо ложные сведения, либо осуществление предпринимательской деятельности **без лицензии в случаях, когда такая лицензия обязательна**, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере, -
- наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от четырех до шести месяцев.
- 2. То же деяние:
- а) **совершенное организованной группой;**
- б) сопряженное с извлечением дохода в особо крупном размере,
- наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового.

Особенности осуществления деятельности вне места регистрации юридического лица

- **Обособленное подразделение:**
- **Пункт 2 статьи 11 НК РФ: обособленным подразделением организации считается любое территориально обособленное от нее подразделение, по месту нахождения которого оборудованы стационарные рабочие места. Рабочее место считается стационарным, если оно создается на срок более одного месяца.**
- **Федеральный закон от 17.07.99 № 181-ФЗ «Об основах охраны труда в Российской Федерации», статья 1, статья 209 Трудового кодекса: рабочее место - это место, в котором работник должен находиться или в которое ему необходимо прибыть в связи с его работой и которое прямо или косвенно находится под контролем работодателя.**

Установление правомерности оказания услуг по технической защите персональных данных

- Федеральная служба по техническому и экспортному контролю
- http://www.fstec.ru/
- http://www.fstec.ru/_razd/_lico.htm
- **РЕЕСТР ЛИЦЕНЗИЙ НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

Основные регламентирующие документы системы сертификации средств защиты информации ФСТЭК России

1. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденный Приказом Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 г. №282;
2. Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное Председателем Государственной технической комиссии при Президенте Российской Федерации от 25.11.1994 г.;
3. Руководящий документ «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам», Гостехкомиссия России, 2002 г.;
4. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», Гостехкомиссия России, 1998 г.;
5. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Гостехкомиссия России, 1998 г.;
6. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации», Гостехкомиссия России, 1998 г.;
7. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей», Гостехкомиссия России, 2000 г.;
8. Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации», Гостехкомиссия России, 1998 г.;
9. Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель», Гостехкомиссия России, 2002 г.

Характеристика информационных систем персональных данных по назначению

- **Примеры информационных систем, эксплуатируемых в целях внутреннего обеспечения органа власти, организации:**
- 1. Информационные системы бухгалтерии;
- 2. Информационные системы отдела кадров;
- 3. Информационные системы, используемые для внутреннего учёта материальных средств.

- **Информационные системы, предназначенные для обеспечения функций органов власти или организаций, содержащие сведения о физических лицах, не являющихся сотрудниками органов власти или организаций**

Задачи защиты информации в информационных системах

- Предотвращение несанкционированного доступа
- Обеспечение целостности
- Обеспечение доступности

Классификация информационных систем персональных данных

- **Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных“**

Основные понятия

- **Информационные системы персональных данных** - совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.
- **Оператор** - государственный орган, муниципальный орган, юридическое и физическое лица, организующие и (или) осуществляющие обработку персональных данных, а также определяющими цели и содержание обработки персональных данных.
- **Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
- **Класс информационной системы персональных данных** – показатель, связанный с масштабом негативных последствий для субъектов персональных данных при нарушении заданной характеристики безопасности персональных данных и характеризующий значимость ИСПДн:
- **класс 1 (К1)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к **значительным негативным последствиям** для субъектов персональных данных;
- **класс 2 (К2)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к **негативным последствиям** для субъектов персональных данных;
- **класс 3 (К3)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к **незначительным негативным последствиям** для субъектов персональных данных;
- **класс 4 (К4)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, **не приводит к негативным последствиям** для субъектов персональных данных.

Главные характеристики информационных систем персональных данных

- категория обрабатываемых в информационной системе персональных данных – Хпд;
- объём обрабатываемых персональных данных – Хнпд;
- вид информационной системы персональных данных: типовая или специальная информационная система.

Классификационная матрица типовых ИСПДн

	3 (Хнпд)	2 (Хнпд)	1 (Хнпд)
Категория 4 (Хпд)	**К4**	**К4**	**К4**
Категория 3 **(Хпд)**	**К3**	**К3**	**К2**
Категория 2 **(Хпд)**	**К3**	**К2**	**К1**
Категория 1 **(Хпд)**	**К1**	**К1**	**К1**

Исходные данные информационной системы

1. Хпд (категория персональных данных):

- категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 – обезличенные и (или) общедоступные персональные данные.

2. Хнпд (объём персональных данных):

- 1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных ***или*** **персональные данные субъектов персональных данных в пределах субъекта Российской Федерации** или Российской Федерации в целом;
- 2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных ***или*** персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации**, в органе государственной власти, проживающих в пределах муниципального образования**;
- 3 – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных ***или*** **персональные данные субъектов персональных данных в пределах конкретной организации**.

Типовые и специальные информационные системы

- **Типовые** информационные системы – информационные системы, в которых требуется обеспечение **только конфиденциальности персональных данных**.
- **Специальные** информационные системы – информационные системы,
  в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных **требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности** (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).
- К специальным информационным системам должны быть отнесены:
- информационные системы, в которых обрабатываются персональные данные, касающиеся **состояния здоровья** субъектов персональных данных;
- информационные системы, в которых предусмотрено **принятие на основании исключительно автоматизированной обработки** персональных данных решений, **порождающих юридические последствия** в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Исходные данные информационной системы

- **По структуре** информационные системы подразделяются:
- на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);
- на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
- на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).
- **По наличию подключений** к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.
- **По режиму обработки** персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.
- **По разграничению прав доступа** пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.
- **В зависимости от местонахождения их технических средств и**нформационные системы подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

Определение класса специальной информационной системы персональных данных

- По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Акт классификации информационной системы персональных данных

- Для служебного пользования
- Экз. № ___
- УТВЕРЖДАЮ
- «___»_____ 201__ года
- АКТ
- классификации информационной системы персональных данных -
- _____

- Комиссия в составе:
- Председателя комиссии:
- Членов комиссии:
- назначенная приказом №__ от «___» _____ 201__ г. «О назначении комиссии по классификации информационных систем персональных данных», рассмотрев исходные данные информационной системы персональных данных _____,

Акт классификации информационной системы персональных данных

- УСТАНОВИЛА:
  - **Категория** обрабатываемых в информационной системе персональных данных (персональные данные, касающиеся состояния здоровья): **ХПД = 1**.
  - **Объем обрабатываемых персональных данных** (в информационной системе одновременно обрабатываются персональные данные менее чем 1000 субъектов персональных данных – субъектов персональных данных в пределах конкретной организации): **ХНПД = 3**.
  - **Тип** ИСПДн (в информационной системе обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных): **специальная информационная система.**
  - **Структура** ИСПДн (информационная система представляет собой комплекс автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа): **локальная информационная система**.
  - **Наличие подключений** к сетям связи общего пользования и (или) сетям международного информационного обмена: информационная система **не имеет подключений** к сетям связи общего пользования и (или) сетям международного информационного обмена.

Акт классификации информационной системы персональных данных

- **Режим разграничения прав доступа** пользователей ИСПДн: **информационная система с равными правами доступа.**
- **Местонахождение технических средств** ИСПДн: технические средства информационной системы **находятся в пределах Российской Федерации**.
- Режим обработки персональных данных: **многопользовательская** информационная система**.**

- **Руководствуясь Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации «Об утверждении Порядка проведения классификации информационных систем персональных данных» от 13 февраля 2008 г. №55/86/20, Частной моделью угроз безопасности персональных данных при их обработке в информационной систем персональных данных – _____* комиссия**
- **РЕШИЛА**
- **установить информационной системе персональных данных - _____, для которой нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных, класс К1.**
- **Председатель комиссии:**
- **члены комиссии:**
- *** Примечание – только для специальных ИСПДн.**

Состав обязательных требований к защите персональных данных в ИСПДн

- **П о с т а н о в л е н и е Правительства Российской Федерации**
- № 781 от 17.11.2007 **Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных:**
- **11. При обработке персональных данных в информационной системе должно быть обеспечено:**
  а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
  б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;
  в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
  г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
  д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Состав обязательных мероприятий по защите персональных данных в ИСПДн

- **12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя**:
  а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
  б) разработку на основе **модели угроз** системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
  в) проверку готовности средств защиты информации к использованию с **составлением заключений** о возможности их эксплуатации;
  г) установку и ввод в эксплуатацию средств защиты информации в соответствии с **эксплуатационной и технической документацией**;
  д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
  е) **учет** применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
  ж) **учет** лиц, допущенных к работе с персональными данными в информационной системе;
  з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
  и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
  к) **описание системы защиты персональных данных**.

Состав мероприятий по защите персональных данных в ИСПДн

1. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20 "Об утверждении порядка проведения классификации информационных систем персональных данных".
2. «Положение о методах и способах защиты в информационных системах персональных данных» (введены в действие Приказом директора ФСТЭК России от 5 февраля 2010 г. № 58).
3. «Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 14 февраля 2008 г. ФСТЭК РФ);
4. «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008 г. ФСТЭК РФ);
5. «Положение о методах и способах защиты в информационных системах персональных данных» (введены в действие Приказом директора ФСТЭК России от 5 февраля 2010 г. № 58).

- **Аудит системы, классификация.**
- **Разработка модели угроз, определение состава средств защиты информации**
- **Закупка, монтаж оборудования**
- **Разработка и реализация организационных мероприятий**
- **Ввод системы в эксплуатацию**
- **Поддержка системы в ходе эксплуатации**

Методы и способы защиты от НСД

- реализация разрешительной системы допуска пользователей к информационным ресурсам;
- ограничение доступа пользователей в помещения, где размещены технические средства, а также, хранятся носители информации;
- разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей, контроль несанкционированного доступа и действий пользователей и посторонних лиц;
- учет и хранение съемных носителей информации и контроль за их обращением;
- резервирование технических средств, носителей информации;
- использование сертифицированных средств защиты информации;
- защита информации при передаче по каналам связи м использованием криптографическмх средств;
- размещение технических средств в пределах контролируемой зоны;
- организация физической защиты помещений и технических средств;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

Методы и способы защиты от НСД при использовании сетей международного обмена (Интернет)

- межсетевое экранирование, фильтрации сетевых пакетов и трансляции сетевых адресов;
- обнаружение вторжений в информационную систему; анализ защищенности информационных систем, применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- использование средств антивирусной защиты;
- централизованное управление системой защиты персональных данных информационной системы

Защита информации от утечки информации за счёт побочных электромагнитных излучений и наводок

«Положение о методах и способах защиты в информационных системах персональных данных» (введено в действие Приказом директора ФСТЭК России от 5 февраля 2010 г. № 58):

- **ИСПДн класса К1**:
- использование технических средств в защищенном исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.
- **ИСПДн класса К2**:
- **для** обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.

Оценка защищённости информации от утечки информации за счёт побочных электромагнитных излучений и наводок

Руководящий документ «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам», Гостехкомиссия России, 2002 г.

Примерный состав документов

- 1. Приказ о назначении комиссии по классификации ИСПДн
- 2. Приказ о допуске к обработке ПД (список лиц), утвержденный список лиц, допущенных к работе со средствами криптографической защиты (СКЗИ).
- 3. Приказ о допуске в помещения
- 4. Приказ (схема) о контролируемой зоне (территории)
- 5. Акт классификации информационной системы персональных данных
- 6. Акт классификации автоматизированной системы
- 7. Модель угроз безопасности персональных данных.
- 8. Техническое задание на разработку системы защиты информации
- 9. Документы по поставке СКЗИ оператору.
- 10. Акты установки и ввода в эксплуатацию СКЗИ в эксплуатацию.
- 11. Акты установки и ввода в эксплуатацию средств защиты информации (НСД, ПЭМИН)
- 12. Лицензии и сертификаты на используемые СКЗИ и средства защиты информации (НСД, ПЭМИН)
- 13. Положение по обработке ПД
- 14. Уведомление об обработке персональных данных.
- 15. Письменное согласие субъекта персональных данных на обработку его персональных данных.
- 16. Инструкция оператору (пользователю)

Примерный состав документов

- 17. Инструкция по антивирусной защите
- 18. Инструкция администратору безопасности
- 10. Технический паспорт объекта ВТ
- 20. Документы, подтверждающие соответствие требованиям по защите информации ИСПДн
- 21. Приказ о вводе в эксплуатацию ИСПДн
- Журналы:
- 22. Журнал учета СКЗИ.
- 23. Журнал учета пользователей криптосредств.
- 24. Журнал учета и выдачи машинных носителей информации.
- 25. Журнал учета проверок.
- 26. Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в ИСПД
- 27. Журнал учета паролей.
- 28. Журнал учёта персональных идентификаторов.
- 29. Акты стирания информации о персональных данных субъектов персональных данных по достижении цели обработки.
- 30. План мероприятий по проведению проверок

Состав документов, разрабатываемых при проведении аттестации ИСПДн по требованиям безопасности информации

1. Программа и методики аттестационных испытаний объекта вычислительной техники по требованиям безопасности информации
2. Протокол контроля защищённости информации, обрабатываемой средствами вычислительной техники, от утечки за счёт побочных электромагнитных излучений и наводок
3. Протокол оценки эффективности средств защиты информации от утечки за счёт побочных электромагнитных излучений и наводок
4. Протокол контроля защищённости информации, обрабатываемой средствами вычислительной техники, от утечки за счёт несанкционированного доступа
5. Заключение по результатам аттестационных испытаний
6. Аттестат соответствия объекта информатизации требованиям по безопасности информации
7. Приложения к аттестату соответствия объекта информатизации требованиям по безопасности информации
8. Предписание на эксплуатацию объекта информатизации