Dr.WEB®
www.drweb.com

Защити созданное

Защита персональных данных

Часть 2
Угрозы в области технической защиты информации
Оценка рисков
Определение класса системы защиты персональных данных

Порядок организации защиты персональных данных в ИСПДн

- Провести обследование ИС с целью оценки текущего состояния ИБ и определения необходимых ИД для создания СЗПДн
- **Определить перечень ПДн** и **провести классификацию ИСПДн**
- **Урегулировать правовые вопросы обработки ПДн**
- **Направить в Роскомнадзор уведомление о намерении осуществлять обработку ПДн**
- **Разработать модель угроз безопасности ПДн**
- **Обосновать требования по обеспечению безопасности ПДн**
- Спроектировать систему защиты ПДн, включая выбор целесообразных способов (мер и средств) защиты ПДн
- Получить лицензию на деятельность по ТЗИ *(не для всех)*
- Организовать и провести работы по созданию системы защиты персональных данных (СЗПДн), включая разработку документов по организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн
- Провести оценку соответствия ИСПДн требованиям
- Организовать контроль соблюдения использования СЗИ и обеспечить управление обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты

Используемые документы

- Федеральный Закон Российской Федерации «О персональных данных» № 152-ФЗ от 27 июля 2006 года
- Приказ от 13 февраля 2008 года ФСТЭК / ФСБ РФ / Мин.Инф.Тех. и Связи РФ № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в ИСПДн с использованием средств автоматизации
- 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 ИСПДн

Dr.WEB®
www.drweb.com

Постановление 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»

Положение устанавливает требования к обеспечению безопасности ПД при их обработке в ИСПДн, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Требования являются обязательными к выполнению для:

- федеральных органов государственной власти;
- органов государственной власти субъектов Российской Федерации;
- иных государственных органов;
- органов местного самоуправления;
- юридических и физических лиц, участвующих в создании и эксплуатации информационных систем персональных данных

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных

Основные требования по обеспечению безопасности персональных данных при их обработке в информационных системах

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных. Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

Информационные системы классифицируются оператором в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Dr.WEB®
www.drweb.com

Базовая модель угроз безопасности персональным данным при их обработке в информационных системах персональных данных
Термины и определения в области безопасности персональных данных

Информационная система ПД

Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии

Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Технические средства информационной системы ПД

Средства ВТ, ИВК и сети, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства ЗИ, применяемые в информационных системах.

Угрозы безопасности персональных данных

Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Защити созданное

Приказ 55/86/20
Основные положения

ИСПДн делятся на «типовые» (необходима защита только конфиденциальности) и «специальные» (защита конфиденциальности + хотя бы 1 характеристика безопасности дополнительно)

> «Порядок проведения классификации ИС ПДн» (Приказ № 55/86/20, п. 14 -16)

Закон устанавливает необходимость обеспечения для всех ИС не только конфиденциальности, но и других характеристик безопасности, а нормативный документ выделяет ИС, в которых защищается только конфиденциальность

Приказ 55/86/20
Основные положения

Специальные информационные системы - ИС, в которых вне зависимости от необходимости обеспечения конфиденциальности 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.

Приказ 55/86/20
Основные положения

«Оператор при обработке персональных данных ***обязан*** принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, ***для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий***».

ч. 1 ст. 19 федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

Закон устанавливает ***необходимость*** обеспечения ***для всех ИС ПДн*** кроме конфиденциальности и других характеристик безопасности – в том числе их защиту от модификации и др. Следовательно согласно этого Порядка классификации все ИС, в которых осуществляется обработка персональных данных, должны быть отнесены к ***специальным*** ИС, а ***типовых*** ИС согласно Закону быть не может.

Приказ 55/86/20
Основные положения

Классификация ИСПДн проводится государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку ПДн, а также определяющими цели и содержание обработки ПДн (операторами)

Типовая СОБИ	Специальная СОБИ
Нормативные документы содержат Типовую модель угроз и перечень мер по обеспечению безопасности ПД	Модель угроз разрабатывается индивидуально на основе аудита, меры по обеспечению безопасности ПДн - индивидуальные, подтверждение соответствия СОБИ ПДн требованиям – затрудняется.

Возможность: ОБОСНОВАННО отнести свою ИСПДн к типовым

Приказ 55/86/20
Основные положения

Класс ИСПДН зависит от:

- категории важности персональных данных;
- объема обрабатываемых данных
- выбранных характеристик безопасности защищаемых персональных данных
- структуры информационной системы - наличия подключений информационной системы к сетям связи общего пользования и/или сетям международного информационного обмена (в том числе сети Интернет), местонахождением технических средств информационной системы, в том числе наличия обмена персональными данными по каналам данных, выходящих за пределы охраняемых территорий и наличия режима трансграничной передачи данных
- режима обработки персональных данных;
- режима разграничения прав доступа пользователей информационной системы

Требования по защите напрямую зависят от выбранного класса защиты АС или ИСПДн.

Приказ 55/86/20
Структура системы

1. автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (**автоматизированные рабочие места**);
2. комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (**локальные информационные системы**);
3. комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (**распределенные информационные системы**).

Приказ 55/86/20
Режим обработки персональных данных в информационной системе

- Однопользовательские
- Многопользовательские

Приказ 55/86/20
По разграничению прав доступа пользователей

- Без разграничения прав доступа
- С разграничением прав доступа

Приказ 55/86/20
Класс ИСПДн

При классификации **типовых** информационных систем персональных данных (ИСПДн) учитываются комбинации следующих признаков:

- Категория обрабатываемых данных
- Объем обрабатываемых данных
- Заданные оператором характеристики безопасности персональных данных с учетом:
  - наличия подключений к сетям связи общего пользования и (или) сетям международного информационного обмена
  - режима обработки персональных данных
  - режима разграничения прав доступа пользователей
  - местонахождения технических средств

Приказ 55/86/20
Объем 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.

Приказ 55/86/20
Классификация системы

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.

Пункт 14 Приказа №55/86/20

Приказ 55/86/20
Категории ПД

Категория 1. ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

Необходимо шифрование данных на всех этапах хранения и обработки

Категория 2. ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1;

Шифрование данных не требуется

Категория 3. ПД, позволяющие идентифицировать субъекта ПД;

Категория 4. Обезличенные и (или) общедоступные ПДн

Пункт 6 Приказа №55/86/20

Приказ 55/86/20
Таблица классификации типовой ИС

Категория обрабатываемых ПДн (Хпд) \ Количество субъектов ПДн в системе (Хнпд)	Хнпд = 1			Хнпд = 2				Хнпд = 3	
	Более 100 000 ПДн	В объеме РФ	В объеме субъекта РФ	От 1000 до 100 000 ПДн	В объеме отрасли	В объеме органа власти	В объеме муниципального образования	До 1000 ПДн	В объеме одной организации
$X_{пд}$ = 1 (Расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь)	К1								
$X_{пд}$ = 2 (Данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию)				К2					
$X_{пд}$ = 3 (Персональные данные, позволяющие идентифицировать субъекта персональных данных)	К2			К3					
$X_{пд}$ = 4 (Обезличенные и (или) общедоступные персональные данные)	К4								

В случае выделения в составе информационной системы подсистем, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем

Dr.WEB®
www.drweb.com

Классификация ИС

- «Типовых» ИС практически нет, классы «специальных» не определены.
- Любая «специальная» ИСПДн обладает признаками «типовой».
- В соответствии с «Положением о методах и способах защиты информации…» выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых угроз безопасности и в зависимости от класса информационной системы.
  - Для любой «специальной» ИС выбираются соответствующие её условиям функционирования «типовые» признаки.
  - Формируется номенклатура требований, в соответствии с выбранными «типовыми» признаками.
  - Для «специальной» ИС проводится анализ уязвимых звеньев, возможных угроз и формирование модели актуальных угроз.
  - Анализ необходимости (обоснование) и дополнение номенклатуры требований, на основании сведений из сформированной модели актуальных угроз.
  - Выбор способов, мер, механизмов защиты в соответствии с дополненной номенклатурой и обоснование их эффективности.

Классификация ИС при наличии подсистем

17. В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

«Порядок проведения классификации информационных систем персональных данных»
(Утвержден приказом ФСТЭК России, ФСБ России, и Миниинформсвязи России от 13 февраля 2008г. № 55/86/20)

5.1.7 Если классифицированная АС интегрируется в состав вычислительной сети, то классификации подлежит образуемая в результате интеграции вычислительная сеть.

«Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К)
(Утверждены приказом Гостехкомиссии от 30 августа 2002 г.)

Пример частной модели угроз

Частная модель угроз безопасности
информационной системы персональных данных

_____

(наименование информационной системы персональных данных)

Исходная степень защищенности информационной системы персональных данных: _____

Показатель защищенности Y_1 = _____(0 – для высокой степени исходной защищенности, 5 – для средней, 10 – для низкой)

Справочно:		
Вероятность реализации Y_2 = 0 для маловероятной угрозы; 2 для низкой вероятности угрозы; 5 для средней вероятности угрозы; 10 для высокой вероятности угрозы.	Коэффициент реализуемости угрозы $Y = (Y1 + Y2)/20$.	Возможность реализации угрозы $0 < Y < 0,3$, - низкая; $0,3 < Y < 0,6$, - средняя; $0,6 < Y < 0,8$, - высокая, $Y > 0,8$, - очень высокая.

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
Угрозы преднамеренного электромагнитного воздействия на ее элементы					Экранирование зданий и помещений, технических средств.	Удаление от границы контролируемой зоны
Угрозы от утечки по техническим каналам						
Угрозы утечки акустической информации	**Мало вероятная**	**Низкая**	**Низкая**	**Неактуальная**	Виброгенераоры, генераторы шумов, звукоизоляция.	Инструкция пользователя Технологический процесс
Угрозы утечки видовой информации						
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных						Инструкция пользователя
Просмотр информации на дисплее посторонними лица, находящимися в помещении в котором ведется обработка персональных данных						Инструкция пользователя Пропускной режим

Пример частной модели угроз

Утверждаю
Руководитель органа
исполнительной власти
(органа местного самоуправления)
И.О.Фамилия

_____
«___» _____2008 г.

Акт
классификации информационной системы персональных данных

_____
_____

Исходные данные для классификации информационной системе персональных данных:

Обрабатываемы персональные данные	ФИО, адрес проживания, дата рождения, номер паспорта, ИНН, должность, заработная плата,
Категория обрабатываемых персональных данных	Категория 2
Объем обрабатываемых персональных данных	число субъекта персональных данных
Структура информационной системы	Автономная
Режим обработки персональных данных	Однопользовательский
Режим разграничения прав доступа пользователей к информационной системе	----
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена.	Не имеет подключения

Дополнительные информация	К персональным данным предъявляется требование целостности
Тип информационной системы персональных данных:	Специальная

На основании анализа исходных данных информационной системы и в соответствии с классификацией утвержденной приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» и с учетом модели угроз информационной системе присвоен **3 класс**.

Dr.WEB®
www.drweb.com

Классифицируем ИСПДн

Для каждой ИСПДн должна быть составлена своя модель угроз.

Результаты классификации оформляются актом классификации ИСПДн (свой акт для каждой ИСПДн).

Персональные и конфиденциальные данные

Персональные данные также относятся, согласно Указу Президента РФ №188 от 16.03.1997, к сведениям конфиденциального характера

Персональные и конфиденциальные данные

Персональные данные могут иметь статус государственной тайны. Это касается например персональных данных государственных служащих, внесенных в личные дела и документы учета

> Федеральный закон от 27.05.2003 N 58-ФЗ "О системе государственной службы в Российской Федерации" (в ред. от 11.11.2003).

Персональные и конфиденциальные данные

К сведениям конфиденциального характера можно отнести:

- персональные данные гражданина;
- тайна следствия и судопроизводства;
- служебная тайна;
- врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.;
- коммерческая тайна;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Указ Президента РФ №188 от 6 марта 1997 года

По разным оценкам к конфиденциальной информации относится от 60% до 80% всей информации, циркулирующей в информационных системах **государственных** и, **коммерческих** предприятий.

Когда можно начинать обработку персональных данных ?

	Класс информационной системы			
	К1	К2	К3	К4
созданные до 1 января 2010 года	• получить согласие субъектов ПДн на обработку их ПДн • направить в Роскомнадзор уведомление об обработке ПДн • привести ИСПДн в соответствие требованиям ФЗ «О персональных данных» до 1 января 2011 года			
созданные после 1 января 2010 года	выполнить требования ФЗ «О персональных данных» до начала обработки ПДн (до ввода ИСПДн в эксплуатацию)			

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Базовая модель угроз предназначена для решения следующих задач:

- разработки частных моделей угроз безопасности персональных данных в конкретных информационных системах с учетом их назначения, условий и особенностей функционирования;
- анализа защищенности информационных систем персональных данных от угроз безопасности в ходе организации и выполнения работ по обеспечению безопасности персональных данных;
- разработки системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем персональных данных;
- проведения мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущения воздействия на технические средства информационных систем персональных данных , в результате которого может быть нарушено их функционирование;
- контроля за обеспечением уровня защищенности персональных данных.

Базовая модель угроз безопасности персональных данных
Содержание документа

Классификация угроз безопасности персональных данных.

Анализ и характеристики угроз возможной утечки информации по техническим каналам.

Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных, включая характеристики источников угроз несанкционированного доступа, характеристики уязвимостей системного и прикладного программного обеспечения, характеристики угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия и программно-математических воздействий, характеристики нетрадиционных информационных каналов и результатов несанкционированного или случайного доступа.

Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Модель угроз безопасности ПД

Модель угроз безопасности должна включать список действующих угроз, содержащий:

- описание угрозы;
- вероятность реализации угрозы;
- путь реализации угрозы.

Модель угроз безопасности ПД
Типы персональных данных

Информация может содержаться в виде:

- буквенно-цифровой информации в виде файлов, структур протоколов, электрических, электромагнитных, оптических сигналов;
- речевой информации – в виде произносимой речи или в виде полей при вводе и выводе акустической информации;
- видовой информация – в виде текста и изображений различных устройств отображения.

Модель угроз безопасности ПД
Классификация угроз безопасности

Угрозы классифицируются:

- по видам возможных источников:
  - угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих или не имеющих доступа к ИСПДн;
- по структуре ИСПДн:
  - на базе автоматизированного рабочего места, локальных или распределенных информационных систем;
- по виду несанкционированных действий - угрозы, приводящие к нарушению конфиденциальности ПДн, изменению, блокированию или уничтожению;
- по способам реализации - угрозы, реализуемые при подключении к сетям общего пользования или сетям международного информационного обмена;
- по виду каналов, используемых для реализации.

Модель угроз безопасности ПД
угрозы внедрения вредоносных программ

Угрозы несанкционированного доступа:

- угрозы непосредственного или удаленного проникновения с использованием средств операционной системы или прикладных программ;
- угрозы создания нештатных режимов работы программных или программно-аппаратных средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, модификации самих данных и т. п.;
- угрозы внедрения вредоносных программ.

Источниками угроз НСД могут быть:

- нарушитель – имеющий или не имеющий доступ к ИСПДн;
- носитель вредоносной программы – аппаратный элемент компьютера (микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, – видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т. п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода-вывода, микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.)) или программный контейнер (в том числе оптический диск, флэш-память, отчуждаемый винчестер);
- аппаратная закладка - угрозы безопасности, связанные с внедрением аппаратных закладок, определяются в соответствии с нормативным документами ФСБ РФ.

Модель угроз безопасности ПД
угрозы уязвимостей

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного/программно-аппаратного обеспечения, в том числе сетевых протоколов;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного/программно-аппаратного обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное использование неучтенных программ;
- внедрение вредоносных программ;
- несанкционированные неумышленные действия пользователей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов, внешними воздействиями электромагнитных полей технических устройств и др.).

Модель угроз безопасности ПД
Результаты несанкционированного или случайного доступа

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование на внешние носители, неправомерное распространение по сети);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

Модель угроз безопасности ПД
Типовые модели угроз

- По структуре ИСПДн - автоматизированные рабочие места, локальные и распределенные информационные системы
- Подключенные или не подключенные к сетям связи общего пользования и/или сетям международного информационного обмена
- По режиму обработки персональных данных - однопользовательские и многопользовательские
- По разграничению прав доступа пользователей - без разграничения и с разграничением прав доступа
- По местоположению – по нахождению технических средств в пределах РФ

Модель угроз безопасности ПД
Типовые модели угроз – локальная АРМ

- Угрозы внедрения вредоносных программ
- Угрозы НСД
- Угрозы утечки информации по техническим каналам:
  - угрозы утечки акустической (речевой) информации;
  - угрозы утечки видовой информации;
  - угрозы утечки информации по каналу ПЭМИН.

Модель угроз безопасности ПД
Типовые модели угроз – ЛВС, имеющая или не имеющая выход в Интернет

- Угрозы внедрения вредоносных программ
- Угрозы анализа и перехвата сетевого трафика
- Угрозы анализа структуры сети и внедрения в нее или подмены доверенного объекта
- Угрозы типа «отказ в обслуживании»
- Угрозы удаленного запуска приложений
- Угрозы НСД
- Угрозы утечки информации по техническим каналам:
  - угрозы утечки акустической (речевой) информации;
  - угрозы утечки видовой информации;
  - угрозы утечки информации по каналу ПЭМИН.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Методика определения актуальных угроз безопасности предназначена для формирования перечня актуальных угроз безопасности персональных данных, обрабатываемых в информационных системах:

- Формирование перечня источников угроз персональным данным осуществляется методом экспертного опроса. На основе экспертного опроса и анализа результатов сетевого сканирования информационной системы формируется перечень ее уязвимых звеньев. По данным обследования информационной системы формируется перечень возможных технических каналов утечки информации.
- Путем анализа указанных перечней определяются условия существования в информационной системе угроз безопасности информации и составляется их полный перечень.
- На основании полного перечня угроз в соответствии с порядком определения актуальных угроз формируется перечень актуальных угроз безопасности персональным данным.

Методика определения актуальных угроз

Методика предназначена для:

- государственных или муниципальных ИСПДн;
- ИСПДн, используемых организациями независимо от форм собственности;
- ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд.

ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Угрозы безопасности могут быть связаны как с непреднамеренными действиями, так и со специально осуществляемыми неправомерными действиями, а также иными источниками угроз (в том числе вирусами и аппаратными закладками).

Методика определения актуальных угроз

Под угрозами безопасности понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Выявление угроз, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц. При этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн.

Dr.WEB®
www.drweb.com

Перечень типов объектов защиты

- Линии связи и сети передачи данных
- Сетевые программные и аппаратные средства, в том числе сетевые серверы
- Файлы данных, базы данных, хранилища данных
- Носители информации, в том числе бумажные носители
- Прикладные и общесистемные программные средства
- Программно-технические компоненты автоматизированных систем
- Помещения, здания, сооружения
- Платежные и информационные технологические процессы
- Бизнес-процессы

Методика определения актуальных угроз
Оценка защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: распределенная ИСПДн, городская, областная и т. п.	–	–	+
распределенная ИСПДн, охватывающая подразделения одной организации или несколько зданий	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования: ИСПДн, имеющая многоточечный выход в сеть общего пользования	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных: чтение, поиск;	+	–	–
запись, удаление, сортировка	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным:	–	+	–
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн	–	–	+

Методика определения актуальных угроз
Оценка защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПД: интегрированная ИСПДн (организация использует несколько баз ПДн, но не владеет ими всеми)	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации	+	–	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные являются обезличенными	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, предоставляющая всю базу данных с ПДн	–	–	+
ИСПДн, предоставляющая часть ПДн	–	+	–
ИСПДн, не предоставляющая никакой информации	+	–	–

Методика определения актуальных угроз
Оценка защищенности ИСПДн

Исходная степень защищенности:

ВЫСОКАЯ (**Y1=10**) - не менее 70% характеристик ИСПДн соответствуют уровню «высокий»

СРЕДНЯЯ (**Y1=5**) - выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний»

НИЗКАЯ (**Y1=0**) **-** не выполняются условия по пунктам 1 и 2

Методика определения актуальных угроз
Оценка вероятности реализуемости угроз

МАЛАЯ ВЕРОЯТНОСТЬ (**Y2=0**) - отсутствуют объективные предпосылки для осуществления угрозы

НИЗКАЯ ВЕРОЯТНОСТЬ (**Y2=2**) - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию

СРЕДНЯЯ ВЕРОЯТНОСТЬ (**Y2=5**) - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны

ВЫСОКАЯ ВЕРОЯТНОСТЬ (**Y2=10**) - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты

Dr.WEB®
www.drweb.com

Методика определения актуальных угроз
Оценка реализуемости угроз

Коэффициент реализуемости угрозы **Y = (Y1+Y2)/20**

По значению коэффициента Y формируется интерпретация следующим образом:

0<Y<0,3 возможность реализации угрозы признается низкой

0,3<Y<0,6 возможность реализации угрозы признается средней

0,6<Y<0,8 возможность реализации угрозы признается высокой

Y>0,8 возможность реализации угрозы признается очень высокой

Методика определения актуальных угроз
Оценка опасности угроз безопасности

низкая опасность - реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

Методика определения актуальных угроз

Правила отнесения угрозы безопасности к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкий	Средний	Высокий
Низкая	**неактуально**	**неактуально**	**актуально**
Средняя	**неактуально**	**актуально**	**актуально**
Высокая	**актуально**	**актуально**	**актуально**
Очень высокая	**актуально**	**актуально**	**актуально**

Методика определения актуальных угроз
Пример опросного листа

Защити созданное

ОПРОСНЫЙ ЛИСТ НА ИСПДн

Полное наименование Информационная системы персональных данных (ИСПДн):_____

_____

Адрес: _____

_____

Контактное лицо: _____

Контактный телефон:

_____

Количество компьютеров обрабатывающих персональные данные (ПДн):_____

Обрабатываемые персональные данные (перечень):

_____

_____

Объем обрабатываемых персональных данных (число субъектов персональных данных):

_____

Режим обработки персональных данных (Однопользовательский/многопользовательский):

_____

Наличие подключения информационной системы к сетям связи общего пользования и (или)

Методика определения актуальных угроз
Пример

Гриф конфиденциальности
Экз. № ___

УТВЕРЖДАЮ
Генеральный директор
_____
« » _____ 200_г.

ПЕРЕЧЕНЬ И КАТЕГОРИИ

персональных данных, обрабатываемых в информационных системах персональных данных

_____
наименование оператора

№ п/п	Наименование сведений	Наименование ИСПДн, где возможна обработка ПДн	Типы документов, где возможно появление ПДн
КАТЕГОРИЯ 4			
обезличенные ПД			
общедоступные ПД			
КАТЕГОРИЯ 3 **ПД, позволяющие идентифицировать субъекта персональных данных**			
анкетные и биографические данные, в т.ч.:			
сведения об имущественном положении, об имуществе и имущественных правах, находящихся в собственности, залоге, доверительном управлении, на основании иных прав, в т.ч:			
ПД, позволяющие идентифицировать субъекта персональных данных и получить о нём дополнительную информацию (категория 2)			
Биометрические персональные данные			

Председатель комиссии _____
должность, ФИО, подпись

Члены комиссии _____
должность, ФИО, подпись
_____
должность, ФИО, подпись
_____
должность, ФИО, подпись
_____

Методика определения актуальных угроз
Пример

Гриф конфиденциальности

Экз. №__

УТВЕРЖДАЮ

Генеральный директор

_____

_____

«___» _____ 200_ г.

Перечень информационных систем персональных данных и помещений, в которых обрабатываются персональные данные

Перечень информационных систем персональных данных и помещений, в которых обрабатываются персональные данные (с использованием средств автоматизации), приведён в таблице № 1:

Таблица № 1

№ п/п	Наименование	Адрес
1	2	3

Перечень информационных систем персональных данных и помещений, в которых обрабатываются персональные данные (без использования средств автоматизации), приведён в таблице № 2:

Таблица № 2

№ п/п	Наименование	Адрес
1	2	3

Председатель комиссии _____

Члены комиссии _____

_____

_____

_____

Методика определения актуальных угроз
Пример

Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности			Для расчёта Y1 Уровень защищенности		
	Высокий	Средний	Низкий	Высокий	Средний	Низкий
1. По территориальному размещению:						
распределённая ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;			+			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);			+			
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;		+				
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;		+				
локальная ИСПДн, развернутая в пределах одного здания.	+					
2. По наличию соединения с сетями общего пользования:						
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			+			
ИСПДн, имеющая одноточечный выход в сеть общего пользования;		+				
ИСПДн, физически отделенная от сети общего пользования.	+					
3. По встроенным (легальным) операциям с записями баз персональных данных:						
чтение, поиск;	+					
запись, удаление, сортировка;		+				
модификация, передача.			+			
4. По разграничению доступа к персональным данным:						
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+				
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			+			
ИСПДн с открытым доступом.			+			

Методика определения актуальных угроз
Пример

По документу ФСТЭК России БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ	Внешний	Категории внутренних нарушителей							
	1	1	2	3	4	5	6	7	8
	физич. лица	без дост. к ПДн	лок.польз ПДн	уд.польз ПДн	адм.ИБ сегмента	сист. админ	АИБ	програм. сопр.ПП	ремонт ТС
иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;			как 1	как 2	как 3	как 4	как 5		
располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;									
располагать именами и вести выявление паролей зарегистрированных пользователей;									
изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.									
знает по меньшей мере одно легальное имя доступа;									
обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;									
располагает конфиденциальными данными, к которым имеет доступ.									
располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн;									
имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.									
обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;									
обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;									
имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;									
имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;									

Положение о методах и способах защиты информации в ИСПДн

Положение устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных государственными и муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных

В Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

Положение о методах и способах защиты информации в ИСПДн
Средства защиты

Методы защиты информации, обрабатываемой техническими средствами информационной системы, - методы и способы защиты информации от несанкционированного доступа.

Методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, - методы и способы защиты информации от утечки по техническим каналам

Необходимость защиты от утечки речевой и видовой информации, а также утечки по каналам побочных электромагнитных излучений и наводок определяется в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781.

Положение о методах и способах защиты информации в ИСПДн
Назначение ответственного лица

Для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Положение о методах и способах защиты информации в ИСПДн
Назначение ответственного лица

В целях обеспечения режима конфиденциальности проводимых работ и в соответствии с требованиями руководящих документов ФСТЭК России по защите информации, содержащей персональные данные, обрабатываемой на объектах информатизации наименование органа исполнительной власти

п р и к а з ы в а ю:

1. Назначить ответственным за защиту информации, содержащей персональные данные на объектах информатизации наименование органа исполнительной власти, должность ФИО.

2. Ответственному за защиту информации, содержащей персональные данные:

- организовать проведение работ по защите информации. В своей работе ответственному руководствоваться методическими документами "Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных", "Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", "Базовая модель угроз безопасности персональных данных", "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных", другими руководящими и нормативными документами ФСТЭК России по защите информации.

3. Ответственному за защиту информации, содержащей персональные данные, в срок до _____ 200 г. организовать проведение работ по защите персональных данных в соответствие требованиями ФСТЭК России объектов вычислительной техники в составе автоматизированных рабочих мест на базе автономной ПЭВМ (инв. № 0000000) наименование органа исполнительной власти (далее - объект ВТ) и представить на утверждение организационно-распорядительные документы на объекты ВТ.

4. Назначить ответственным за обеспечение безопасности информации на объекте ВТ – администратором информационной безопасности должность ФИО.

6. Назначить ответственным за эксплуатацию объекта ВТ должность ФИО.

6. Обработку информации, отнесенной законами Российской Федерации к персональным данным, производить на объектах информатизации, удовлетворяющих соответствующим требованиям защиты персональных данных, в соответствии с Приказом о вводе в эксплуатацию и списком допущенных лиц.

7. Приказ довести до ответственных лиц в части касающейся.

8. Контроль за исполнением приказа оставляю за собой.

Положение о методах и способах защиты информации в ИСПДн
Методы защиты информации от несанкционированного доступа

Реализованные методы защиты информации должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных на основе определяемых оператором (уполномоченным лицом) угроз. Выбор методов осуществляется в зависимости от класса информационной системы.

Методы защиты информации от несанкционированного доступа:

- реализация разрешительной системы допуска пользователей;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории и ограничение доступа пользователей в помещения;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей;
- контроль несанкционированного доступа и действий пользователей;
- учет и хранение съемных носителей информации и их обращение;
- резервирование технических средств;
- использование защищенных каналов связи;
- предотвращение внедрения вредоносных программ.

- *Для информационных систем 1 класса использование сертифицированных средств защиты информации соответствующее 4 уровню контроля отсутствия недекларированных возможностей.*

Положение о методах и способах защиты информации в ИСПДн
Дополнительные способы защиты при обмене через Интернет

Методы защиты информации от несанкционированного доступа:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему;
- анализ защищенности информационных систем и активный аудит безопасности информационной системы;
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации пользователей;
- использование средств антивирусной защиты, в том числе для анализа трафика;
- централизованное управление системой защиты.

Подключение информационных систем к информационно-телекоммуникационным сетям осуществляется в соответствии с Указом Президента Российской Федерации от 17 марта 2008 г. № 351

Dr.WEB®
www.drweb.com

Положение о методах и способах защиты информации в ИСПДн
Дополнительные способы защиты при удаленном доступе

Методы защиты информации от несанкционированного доступа:

- проверка подлинности отправителя;
- проверка целостности передаваемых данных;
- управление доступом к защищаемым персональным данным;
- использование атрибутов безопасности.

Защити созданное

Положение о методах и способах защиты информации в ИСПДн
Дополнительные способы защиты при распределенных сетях

Методы защиты информации от несанкционированного доступа:

- создание защищенного канала связи;
- аутентификация взаимодействующих информационных систем
- проверка подлинности пользователей;
- предотвращение возможности отрицания пользователем факта отправки или получения персональных данных;
- проверка целостности передаваемых данных.

Положение о методах и способах защиты информации в ИСПДн
Способы защиты от НСД в сетях 4-го класса

Методы защиты информации от несанкционированного доступа определяются оператором.

Положение о методах и способах защиты информации в ИСПДн
Способы защиты от НСД в сетях 3-го класса

Методы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учёта, обеспечения целостности и безопасного межсетевого взаимодействия:

- проверка подлинности пользователя при входе в систему;
- регистрация и учет:
  - регистрация входа/выхода пользователя в/из системы;
  - учет всех защищаемых носителей информации;
- обеспечение целостности:
  - программных средств системы защиты и программной среды;
  - физическая охрана технических средств и носителей информации;
  - разграничение и контроль доступа в помещения;
  - периодическое тестирование функций системы защиты при изменении программной среды и пользователей информационной системы;
  - наличие средств восстановления системы защиты персональных данных;
- обеспечение безопасного межсетевого взаимодействия достигается путем применения межсетевых экранов, обеспечивающих фильтрацию на сетевом уровне для каждого сетевого пакета, идентификацию и аутентификацию администратора, контроль целостности, восстановление свойств после сбоев и отказов

При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом.

Положение о методах и способах защиты информации в ИСПДн
Способы защиты от НСД в сетях 2-го класса

Методы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учёта, обеспечения целостности и безопасного межсетевого взаимодействия в многопользовательских сетях (дополнительно к требованиям для 3-го класса):

- обеспечение безопасного межсетевого взаимодействия достигается путем применения межсетевых экранов, обеспечивающих фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов, фильтрацию с учетом любых значимых полей сетевых пакетов, регистрацию и учет фильтруемых пакетов, аудит действий администратора.

Положение о методах и способах защиты информации в ИСПДн
Способы защиты от НСД в сетях 1-го класса

Методы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учёта, обеспечения целостности и безопасного межсетевого взаимодействия в многопользовательских сетях (дополнительно к требованиям для 2-го класса):

- регистрация печати документов на бумажный носитель;
- дублирующий учет защищаемых носителей информации;
- очистка освобождаемых областей оперативной памяти и внешних носителей информации
- обеспечение целостности - физическая охрана технических средств, предусматривающая постоянное наличие охраны территории и здания;
- идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам);
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрация и учет:
  - регистрация запуска (завершения) программ и процессов;
  - регистрация попыток доступа программных средств к защищаемым файлам и защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей.

Обеспечение безопасного межсетевого взаимодействия достигается путем применения межсетевых экранов, обеспечивающих возможность дистанционного управления, фильтрацию на транспортном уровне, фильтрацию с учетом даты и времени, аутентификацию запросов методами, устойчивыми к пассивному и активному прослушиваниям сети, регистрацию и учет фильтруемых пакетов и запросов на установление соединения.

Положение о методах и способах защиты информации в ИСПДн
Метод защиты от утечек

Методы защиты от утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса:

- использование технических средств в защищенном исполнении;
- использование сертифицированных средств защиты;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров;
- 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.

Для защиты от утечки по акустическим каналам в информационных системах 1-го класса должны использоваться как организационные, так и технические мероприятия, в том числе звукоизоляция помещений.

Для сетей 1-го и 2-го классов должны использоваться средства вычислительной техники, удовлетворяющие требованиям соответствующих национальных стандартов.

Защита персональных данных

Статья 11. Биометрические персональные данные
1. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

Защита персональных данных

В соответствии с законом
Обработка возможна оператором при наличии согласия субъекта
Критерием отнесения персональных данных к категории биометрических является возможность идентификации субъекта персональных данных на основе биометрических данных

Защита персональных данных

Меры безопасности

Необходимо принимать организационные и технические меры, исключающие случайное или преднамеренное разрушение данных, хранимых на материальных носителях, их изменение, несанкционированный доступ к ним и т.д. Сам материальный носитель должен обеспечивать:

- защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;
- возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;

Защита персональных данных

Меры безопасности
Оператор обязан:
а) осуществлять учет количества экземпляров материальных носителей;
б) осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

Защита персональных данных

Меры безопасности

9. Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

б) применение средств электронной цифровой подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;

в) проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

Защита персональных данных

Меры безопасности

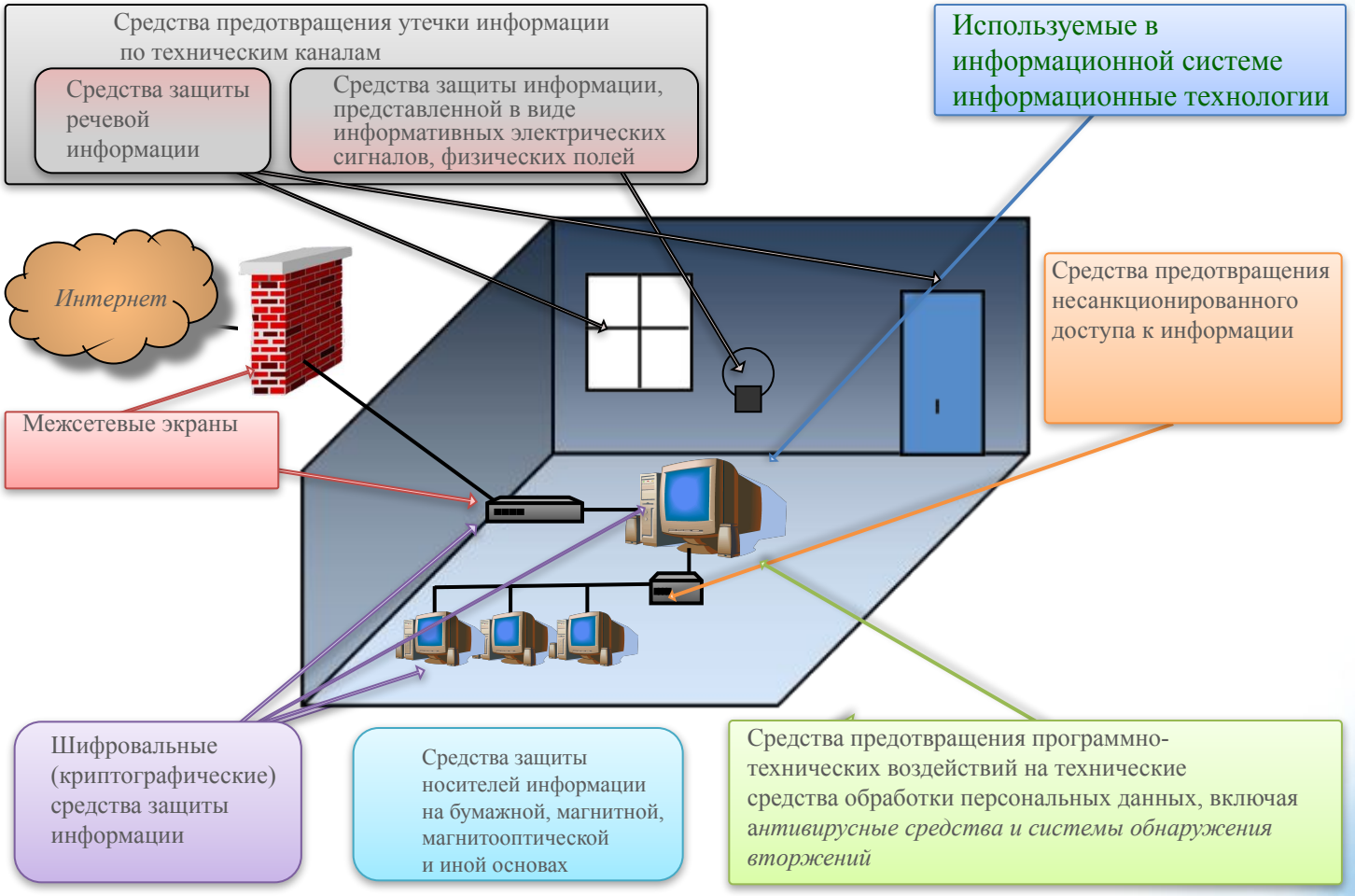
10. В случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим персональным данным, то такая информация должна быть подписана электронной цифровой подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель. Использование шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

Защита персональных данных

Меры безопасности

11. При хранении биометрических персональных данных вне информационных систем персональных данных должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

Система защиты ИСПДн



Dr.WEB®
www.drweb.com

Внимание!

Материалы, изложенные в данной презентации, рассматривают только основные аспекты, связанные с защитой персональных данных.

Более подробную информацию можно получить, обратившись в компанию «Доктор Веб» по адресу:

reseach@drweb.com

Защити созданное

www.drweb.com

Dr.WEB®
www.drweb.com

Защити созданное

Вопросы?

Благодарим за внимание!

Желаем Вам процветания и еще больших успехов!

www.drweb.com