МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Направление подготовки	10.03.01 Информационная безопасность
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск 2020 г.

СОДЕРЖАНИЕ

Введение

Практическая работа должна быть оформлена в электронном виде и на листах формата А4. Печатная работа выполняется в сброшюрованных листах.

На титульном листе указывается фамилия, имя, отчество, наименование работы, вариант, курс, группа. Задание работы содержит 20 вариантов. Выбор варианта осуществляется по номеру в списке преподавателя.

Специальные документы ФСТЭК РФ по защите ПДн:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Утверждена заместителем директора ФСТЭК России 15.02.2008 г. ДСП.);
- Приказ ФСТЭК №21 от 18.02.13г «Состав и содержание организационных и технических мер по защите ПДн при их обработке в информационных системах персональных данных»;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных,утверждена заместителем директора ФСТЭК России 14.02.2008г.
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Термины и определения:

Персональные данные (ПДн)– это любая информация о людях. Это могут быть персональные данные сотрудников, данные пациентов (если речь идет о медучреждении), данные граждан (если речь идет о госучреждении) и т.д.

Контролируемая зона (КЗ) – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Информационная система персональных данных (ИСПДн) – это совокупность программных и технических средств (компьютеры, принтеры, сканеры, коммутационное оборудование и т.д.) на которых обрабатываются персональные данные.

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.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

ИСПДн-С - информационная система, обрабатывающая специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

ИСПДн-О – информационная система, обрабатывающая общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

ИСПДн-Б - информационная система, обрабатывающая биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

ИСПДн-И - информационная система, обрабатывающая иные категории персональных данных, если в ней не обрабатываются персональные данные специальные, общедоступные и биометрические.

«Базовая модель» - Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Утверждена заместителем директора ФСТЭК России 15.02.2008 г. ДСП.).

АРМ - автоматизированное рабочее место.

ПО - программное обеспечение.

МИО – международный информационный обмен.

БПДн – безопасность персональных данных.

Характеристики ИСПДн, обусловливающие возникновение угроз БПДн:

1) структура ИСПДн:

a) автономные ИСПДн АРМ;

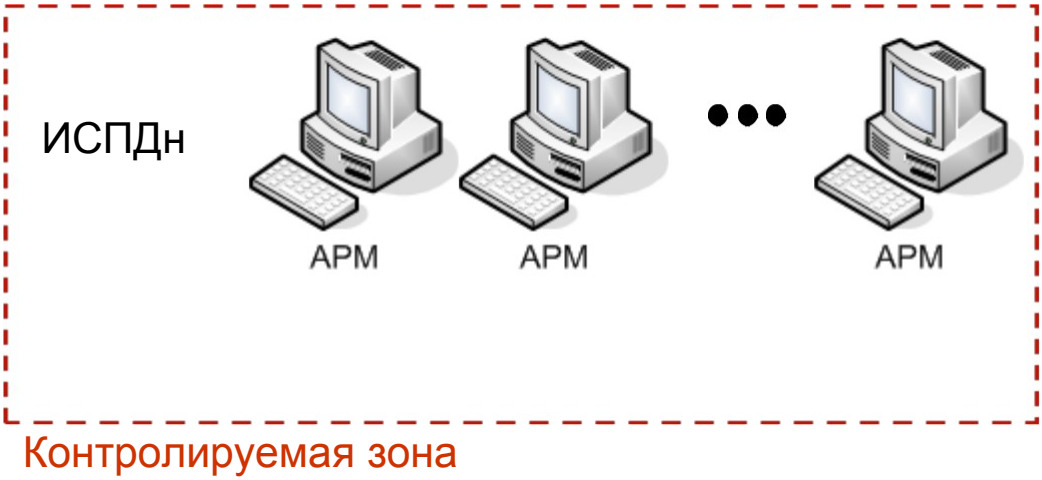

Рисунок 1. Автономные ИСПДн АРМ.

b) локальные ИСПДн:

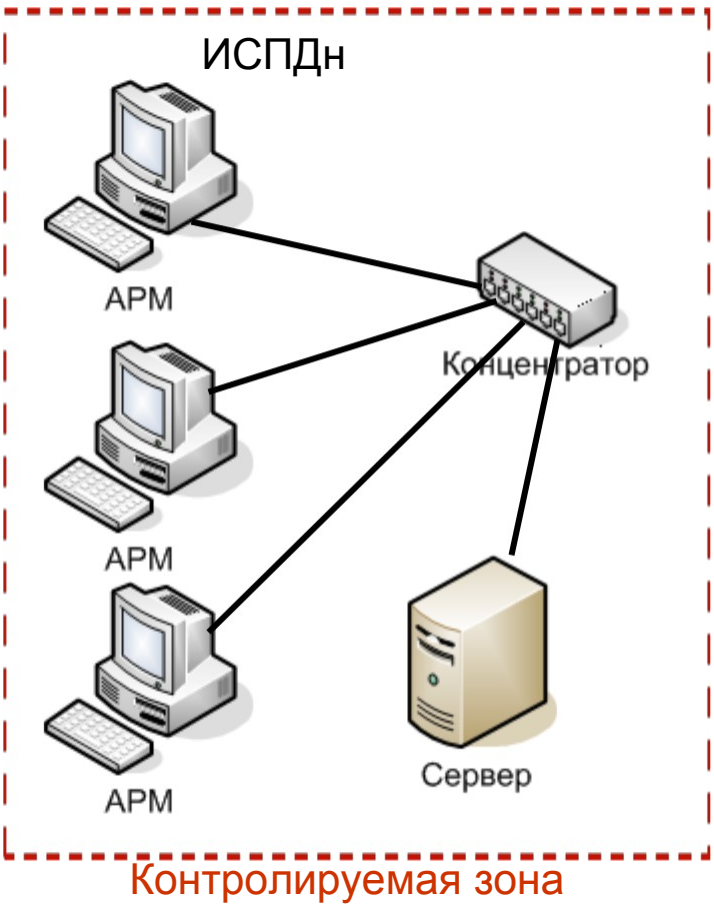

Рисунок 2. Локальные ИСПДн АРМ.

с) распределенные ИСПДн):

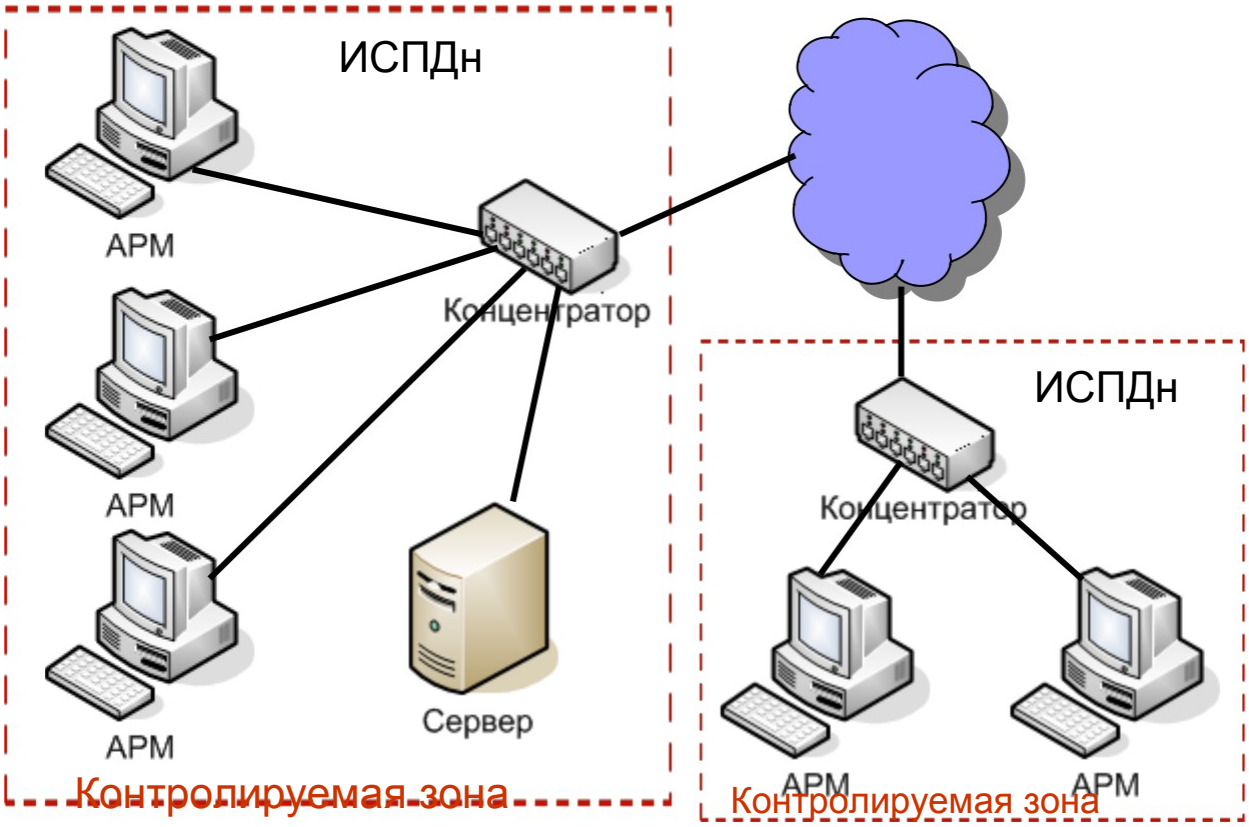

Рисунок 3. Распределенные ИСПДн АРМ с выходом в Internet.

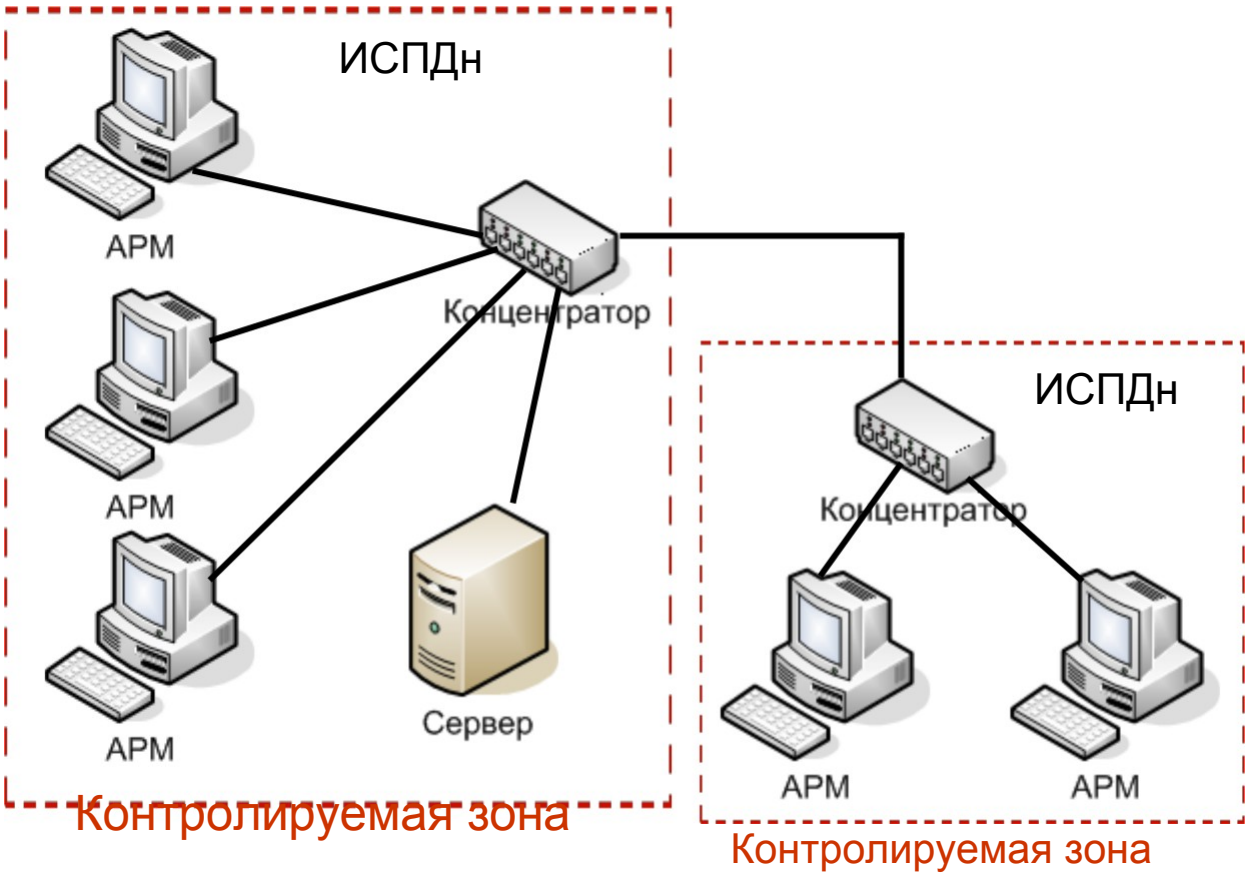

Рисунок 4. Распределенные ИСПДн АРМ без выхода в Internet.

2) категория обрабатываемых в ИСПДн персональных данных:
    a) ИСПДн-С;
    b) ИСПДн–Б;
    c) ИСПДн-И;
    d) ИСПДн-О.
3) Объем обрабатываемых в ИСПДн персональных данных:
    a) менее чем 100 000 субъектов;
    b) более чем 100 000 субъектов.
4) наличие подключений ИСПДн к сетям связи общего пользования/сетям МИО:
    a) не имеющие подключение;
    b) имеющие подключение.
5) характеристики подсистемы безопасности ИСПДн;
6) режимы обработки персональных данных:
    a) однопользовательские ИСПДн;
    b) многопользовательские ИСПДН.
7) режимы разграничения прав доступа пользователей ИСПДн:
    a) с разграничением доступа;
    b) без разграничения доступа;
8) условия размещения технических средств ИСПДн:
    a) в пределах контролируемой зоны;
    b) вне контролируемой зоны.
9) по территориальному размещению:
    a) распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;
    b) городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);
    c) корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;
    d) локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;
    e) локальная ИСПДн, развернутая в пределах одного здания.

Основные этапы расчётов.

1. Определение модели угроз безопасности ПДн.
2. Определение актуальных угроз ПДн.
3. Определение уровня защищенности ПДн.
4. Определение мер по защите ПДн от актуальных угроз.

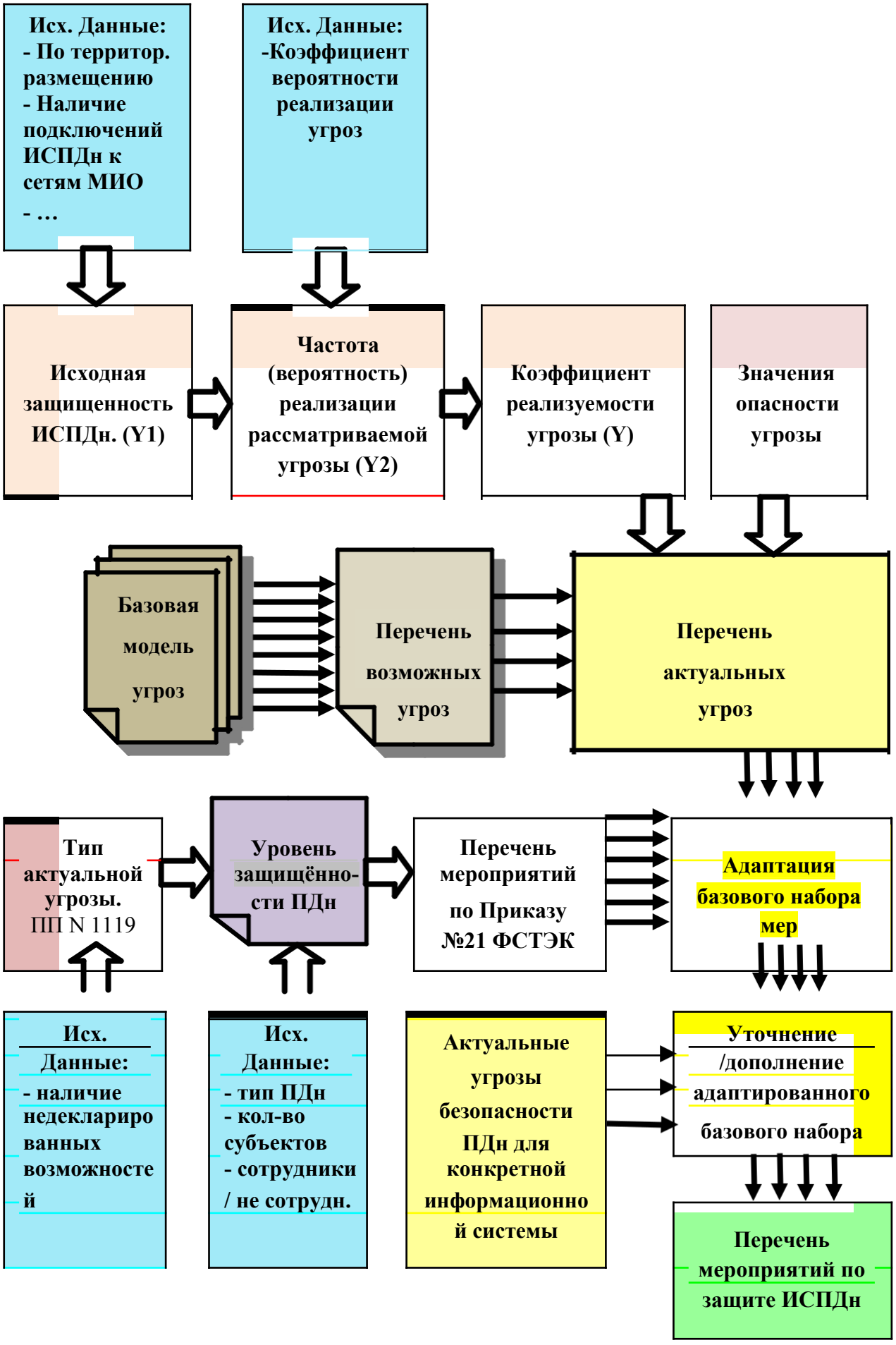

Рисунок 4. Схема определения организационно-технических мер по защите ПДн.

Лабораторное занятие №1.
Тема: Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения задач определения модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России 15.02.2008 г. ДСП.»

2.1. Модель вероятного нарушителя безопасности ИСПДн.

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

2.1.2 Внешние нарушители.

В роли внешних нарушителей информационной безопасности могут выступать лица, описанные в таблице 1.

Таблица 1.

Категория нарушителя	Описание категории нарушителя
Лица, не имеющие санкционированного доступа к ИСПДн	- физические лица - организации (в том числе конкурирующие) - криминальные группировки

2.1.3 Внутренние нарушители.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

Под внутренним нарушителем информационной безопасности рассматривается нарушитель, имеющий непосредственный доступ к каналам связи, техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны, на территории Российской федерации.

К внутренним нарушителям могут относиться лица, описанные в таблице 2. Таблица 2.

Категория нарушителя	Перечень лиц	Описание категории нарушителя
1	Работники предприятия, не имеющие санкционированного доступа к ИСПДн	• имеет доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; • располагает фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; • располагает именами и возможностью выявления паролей зарегистрированных пользователей; • изменяет конфигурацию технических средств ИСПДн, вносит в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.
2	Пользователи ИСПДн	• обладает всеми возможностями лиц первой категории; • 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.
3	Администраторы ППО ИСПДн	• Обладает всеми возможностями лиц первой и второй категорий; • располагает информацией о топологии ИСПДн на

		базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн; • имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.
4	Администраторы локальной сети	• Обладает всеми возможностями лиц предыдущих категорий; • 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; • обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн Администраторы информационной безопасности	• Обладает всеми возможностями лиц предыдущих категорий; • обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; • обладает полной информацией о технических средствах и конфигурации ИСПДн; • имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; • обладает правами конфигурирования и административной настройки технических средств ИСПДн
6	Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн	• обладает всеми возможностями лиц предыдущих категорий; • обладает полной информацией об ИСПДн; • имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; • не имеет прав доступа к конфигурированию технических средств сети за исключением

		контрольных (инспекционных).
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	• обладает информацией об алгоритмах и программах обработки информации на ИСПДн; • обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; • может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	• обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; • может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

2.2. Типовые модели угроз безопасности ИСПДн.

Применительно к основным типам информационных систем разработаны типовые модели угроз безопасности ПДн, характеризующие наступление различных видов последствий в результате несанкционированного или случайного доступа и реализации угрозы в отношении персональных данных. Всего таких моделей шесть и описаны они в документе ФСТЭК России «Базовая модель»:

1) типовая модель угроз безопасности ПДн, обрабатываемых в автоматизированных рабочих местах, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
2) типовая модель угроз безопасности ПДн, обрабатываемых в автоматизированных рабочих местах, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
3) типовая модель угроз безопасности ПДн, обрабатываемых в локальных ИСПДн, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;

4) типовая модель угроз безопасности ПДн, обрабатываемых в локальных ИСПДн, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
5) типовая модель угроз безопасности ПДн, обрабатываемых в распределенных ИСПДн, не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена;
6) типовая модель угроз безопасности ПДн, обрабатываемых в распределенных ИСПДн, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Угрозы безопасности информации (УБИ) определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и 8 внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Модель угроз безопасности информации представляет собой формализованное описание угроз безопасности информации для конкретной информационной системы или группы информационных систем в определенных условиях их функционирования.

3. Методика и порядок выполнения работы.

На данном практическом занятии студенты выполняют следующие задания: 3.1. Изучают категории нарушителей, описанные в документе ФСТЭК России «Базовая модель». Для конкретной информационной системы определяют перечень вероятных нарушителей ИСПДн с учетом всех исключений. Результаты записывают в таблицу (см. таблицу 2).

3.2. Изучают модели безопасности, описанные в документе ФСТЭК России «Базовая модель». Составляют перечень всех возможных угроз по документу ФСТЭК России «Базовая модель». Результаты записывают в таблицу 3, представленную в виде примера.

Таблица 3.

Перечень всех возможных угроз безопасности ПДн.

Возможные угрозы безопасности ПДн
1. Угрозы от утечки по техническим каналам
1.1. Угрозы утечки акустической информации
1.2. Угрозы утечки видовой информации

1.3. Угрозы утечки информации по каналам ПЭМИН
2. Угрозы несанкционированного доступа к информации
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн
2.1.1. Кража ПЭВМ
2.1.2. Кража носителей информации
2.1.3. Кража ключей и атрибутов доступа
2.1.4. Кражи, модификации, уничтожения информации
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ
2.1.7. Несанкционированное отключение средств защиты
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)
2.2.1. Действия вредоносных программ (вирусов)
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера
2.3.1. Утрата ключей и атрибутов доступа
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками
2.3.3. Непреднамеренное отключение средств защиты
2.3.4. Выход из строя аппаратно-программных средств
2.3.5. Сбой системы электроснабжения
2.3.6. Стихийное бедствие
2.4. Угрозы преднамеренных действий внутренних нарушителей
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке
2.5.Угрозы несанкционированного доступа по каналам связи
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:
2.5.1.1. Перехват за переделами с контролируемой зоны
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.

2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
2.5.3.Угрозы выявления паролей по сети
2.5.4.Угрозы навязывание ложного маршрута сети
2.5.5.Угрозы подмены доверенного объекта в сети
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
2.5.7.Угрозы типа «Отказ в обслуживании»
2.5.8.Угрозы удаленного запуска приложений
2.5.9.Угрозы внедрения по сети вредоносных программ

3. Задания

1. Изучить документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России от 15.02.2008 г.

2. На основании документа «Базовая модель угроз» определяют Модель вероятного нарушителя путём сбора всех возможных категорий нарушителей.

3. На основании документа «Базовая модель угроз», пп. 6.1-6.6 определить перечень угроз безопасности для конкретной структуры ИСПДн, указанной в Приложении 1 данной методики в пункте таблицы, соответствующему порядковому номеру студента в списке преподавателя.

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Вопросы для защиты работы

1) Перечислите Источники угроз НСД в ИСПДн
2) По режиму обработки персональных данных в информационной системе информационные системы подразделяются на два вида. Назовите, какие.

3) К каким видам нарушения безопасности информации может привести реализация угроз НСД?

Лабораторное занятие №2.
Тема: Определение уровня исходной защищённости (Y_1).

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения проблем определения уровня исходной защищённости (Y_1) в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 4.

Таблица 4.

Показатели исходной защищенности ИСПДн.

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
Распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
Городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
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 имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются			

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
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	+	-	-
Количество «+» в колонках	5*	4*	1*
РЕЗУЛЬТАТ (*Y_1*)	5*		

Примечание: * - значения, полученные в виде примера

Где Y_1- числовой коэффициент исходной защищенности, определяется так:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Если не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний", то Y_1=5.

3. Методика и порядок выполнения работы.

На данном практическом занятии студенты выполняют следующие задания: 3.1. Изучают документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

3.2. Определяют исходную степень защищенности по следующей методике:

1) ИСПДн имеет ***высокий*** уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).
2) ИСПДн имеет ***средний*** уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.
3) ИСПДн имеет ***низкую*** степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

3. Задания

1. Изучить документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

2. Согласно технических и эксплуатационных характеристик ИСПДн, данных в индивидуальном задании определить показатели ***высокого, среднего*** и ***низкого*** уровня защищённости для соей ИСПДн.

3. Рассчитать исходную степень защищенности.

4. Результаты занести в таблицу.

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Контрольные вопросы и тестовые задания

1) Что понимается под угрозами безопасности ПДн при их обработке в ИСПДн?
2) Как могут быть реализованы угрозы безопасности ПДн?

3) Перечислите источники угроз, реализуемые за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения.
4) Какая угроза считается актуальной?

Лабораторное занятие №3.

Тема: Определение частоты (вероятности) реализации рассматриваемой угрозы (Y_2).

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения проблем определения частоты (вероятности) реализации рассматриваемой угрозы (Y_2) в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработана ФСТЭК России.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Таблица 5. Пример записи показателей Коэффициент вероятности реализации (Y_2) и Оценка опасности угрозы

Возможные угрозы безопасности ПДн	**Коэффициент вероятности реализации нарушителем категории n**								**Оценка опасности угрозы****
	1	**2**	**3**	**4**	**5**	**6**	**Внешние**	**Итог (Y2)***	
1. Угрозы от утечки по техническим каналам									
1.1. Угрозы утечки акустической информации	0	0	0	0	0	0	0	0	маловероятная
1.2. Угрозы утечки видовой информации	0	0	2	2	2	2	0	2	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0	0	0	0	0	0	0	0	маловероятная
2. Угрозы несанкционированного доступа к информации									
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн									
2.1.1. Кража ПЭВМ	0	0	0	0	0	0	2	2	Низкая
2.1.2. Кража носителей информации	0	0	0	0	0	0	2	2	Низкая
2.1.3. Кража ключей и атрибутов доступа	0	0	0	2	0	0	0	2	Низкая
2.1.4. Кражи, модификации, уничтожения информации	0	0	0	0	0	0	2	2	Низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0	0	0	0	0	0	0	0	маловероятная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0	0	0	0	2	0	2	2	низкая
2.1.7. Несанкционированное отключение средств защиты	0	0	0	0	0	0	2	2	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)									
2.2.1. Действия вредоносных программ (вирусов)	2	0	0	2	0	0	2	2	низкая
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	2	2	0	0	0	0	2	2	низкая
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	0	0	0	0	0	0	0	0	маловероятная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера									
2.3.1. Утрата ключей и атрибутов доступа	2	0	2	0	0	0	0	2	низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0	0	0	0	2	0	0	2	низкая
2.3.3. Непреднамеренное отключение средств защиты	0	0	0	0	0	0	0	0	маловероятная

2.3.4. Выход из строя аппаратно-программных средств	0	0	0	0	0	0	0	0	маловероятная
2.3.5. Сбой системы электроснабжения	0	0	0	0	0	0	0	0	маловероятная
2.3.6. Стихийное бедствие	0	0	0	0	0	0	0	0	маловероятная
2.4. Угрозы преднамеренных действий внутренних нарушителей									
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке	2	0	2	2	0	0	0	2	низкая
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0	0	5	0	0	0	5	средняя
2.5.Угрозы несанкционированного доступа по каналам связи									
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	2	2	0	0	0	0	5	5	средняя
2.5.1.1. Перехват за переделами с контролируемой зоны	0	0	0	0	0	0	2	2	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0	0	0	0	0	0	5	5	средняя
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0	0	0	0	0	0	0	0	маловероятная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	2	2	2	0	0	0	0	2	низкая
2.5.3.Угрозы выявления паролей по сети	0	0	0	0	0	0	0	0	маловероятная
2.5.4.Угрозы навязывание ложного маршрута сети	0	0	0	0	0	0	0	0	маловероятная
2.5.5.Угрозы подмены доверенного объекта в сети	0	0	0	0	0	0	0	0	маловероятная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	2	0	0	0	0	0	0	2	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	2	0	0	0	0	0	0	2	низкая
2.5.8.Угрозы удаленного запуска приложений	2	2	0	0	0	0	0	2	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	2	0	0	2	0	0	10	10	высокая

*При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2, а именно:

0 – для маловероятной угрозы (отсутствуют объективные предпосылки для осуществления угрозы);

2 – для низкой вероятности угрозы (объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию);

5 – для средней вероятности угрозы (объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны);

10 – для высокой вероятности угрозы (объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты).

**Оценка опасности угрозы определяется на основе опроса специалистов по вербальным показателям опасности с тремя значениями:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

3. Задания

1. Изучить документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

2. Пользуясь таблицей 5, определить частоту (вероятность) реализации (Y_2) каждой угрозы для всех категорий нарушителей. Определяющим значением в строке угрозы будет максимальное значение вероятности реализации.

3. Произвести оценку опасности угрозы с присвоением одного из 3-х значений: низкая, средняя, высокая.

4. Результаты занести в таблицу.

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Контрольные вопросы

1) Какие показатели применяются для оценки возможности реализации угрозы?
2) Что понимается под уровнем исходной защищенности ИСПДн?
3) Что понимается под частотой (вероятностью) реализации угрозы?

Лабораторное занятие №4.

Тема: Определение коэффициента реализуемости угрозы (*Y*) и возможности реализации

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения проблем определения коэффициента реализуемости угрозы (*Y*) и возможности реализации в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработана ФСТЭК России.

Коэффициент реализуемости угрозы *Y* будет определяться соотношением:

$Y = (Y_1 + Y_2)/20.$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;
- если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы признается средней;
- если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы признается высокой;

- если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Пример: рассмотрим угрозу для ИСПДн и определим её актуальность для системы. Возьмём угрозу утечки видовой информации. Ранее мы уже рассчитали, что данная ИСПДн имеет уровень исходной защищенности **средний**, а числовой коэффициент Y_1=5. Далее определим частоту (вероятность) реализации угрозы (Значение коэффициента Y_2). Она будет иметь значение – **низкая(0)**, поскольку в организации введён пропускной режим и ограничен доступ в помещение, где обрабатываются персональные данные. А также рабочие места организованы так, что нет возможности съёма информации по оптическому каналу. Теперь мы можем рассчитать коэффициент реализуемости угрозы по формуле $Y = (Y_1 + Y_2)/20$. Получаем Y=0.25 и определяем, что Y лежит в промежутке между 0 и 0.3, а, значит, возможность реализации угрозы признается **низкой**.

Результаты заносим в таблицу 6.

Таблица 6. Пример расчёта реализуемости и возможности реализации.

Тип угроз безопасности ПДн	**Коэффициент реализуемости угрозы (*Y*)**	**Возможность реализации**
1. Угрозы от утечки по техническим каналам		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств	0,25	низкая

защиты		
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
2.2.1. Действия вредоносных программ (вирусов)	0,35	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,35	средняя
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	0,25	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера		
2.3.1. Утрата ключей и атрибутов доступа	0,35	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,25	низкая
2.3.3. Непреднамеренное отключение средств защиты	0,25	низкая
2.3.4. Выход из строя аппаратно-программных средств	0,25	низкая
2.3.5. Сбой системы электроснабжения	0,25	низкая
2.3.6. Стихийное бедствие	0,25	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами не допущенными к ее обработке	0,35	средняя
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,5	средняя
2.5.Угрозы несанкционированного доступа по каналам связи		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	0,35	средняя
2.5.1.1. Перехват за переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны	0,25	низкая

внешними нарушителями		
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,35	средняя
2.5.3.Угрозы выявления паролей по сети	0,25	низкая
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,35	средняя
2.5.7.Угрозы типа «Отказ в обслуживании»	0,35	средняя
2.5.8.Угрозы удаленного запуска приложений	0,25	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0,75	высокая

3. Задания (указания по порядку выполнения работы)

1. Изучить документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

2. Определить коэффициенты реализуемости угрозы (*Y*) и возможности реализации для всех пунктов угроз.

3. Результаты оформить в виде таблицы.

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Контрольные вопросы

1) Как определяется коэффициент реализуемости угрозы Y?

2) Перечислите вербальные показатели опасности для рассматриваемой ИСПДн.

3) Какое значение имеет вербальный показатель, если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных?

Лабораторное занятие №5.

Тема: Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения проблем определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработана ФСТЭК России.

Оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

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

- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Рекомендации по определению опасности угрозы:

- чем больше количество субъектов ПДн, тем выше опасность угрозы;
- опасность угрозы выше в зависимости от типа ИСПДн (в порядке возрастания):
  - ИСПДн – О;
  - ИСПДн – И;
  - ИСПДн – Б;
  - ИСПДн – С.
- в зависимости от угрозы ПДн.

Для примера значений опасности каждой угрозы в ИСПДн-О возможно использовать следующую таблицу 7.

Таблица 7.

Пример значений опасности угрозы.

Наименование угрозы	Возможность реализации угрозы
1. Угрозы от утечки по техническим каналам	
1.1. Угрозы утечки видовой информации	низкая
1.2. Угрозы утечки информации по каналам ПЭМИН	низкая
2. Угрозы НСД к информации	
2.1. Угрозы уничтожения, хищения аппаратных средств и носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	низкая
2.1.2. Кража носителей информации	низкая
2.1.3. Кража ключей и атрибутов доступа	низкая

2.1.4. Кража, модификация, уничтожение информации	низкая
2.1.5. Вывод из строя узлов ИСПДн, каналов связи	низкая
2.1.6. НСД к перс. данным при техобслуживании (ремонте, уничтожении) узлов ИСПДн	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	низкая
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	высокая
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности ПДн из-за сбоев в программном обеспечении, а также от угроз не антропогенного и стихийного характера.	
2.3.1. Утрата ключей и атрибутов доступа	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Сбой электропитания, аварии, отказы, стихийные бедствия и т.п.	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. НСД к перс. данным лиц, не допущенных к ее обработке	низкая
2.4.2. НСД к перс. данным лиц, допущенных к ее обработке	низкая
2.5.Угрозы несанкционированного доступа по каналам связи	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая

2.5.2.Угрозы сканирования, направленные на выявление типа операционных систем, сетевых адресов рабочих, топологии сети, открытых портов и служб и т.п.	низкая
2.5.3.Угрозы выявления паролей по сети	средняя
2.5.4.Угрозы навязывания ложного маршрута сети	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	низкая
2.5.3.Угрозы выявления паролей по сети	средняя
2.5.4.Угрозы навязывания ложного маршрута сети	низкая

Осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 8.

Таблица 8.

Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Обобщенный список актуальных угроз в ИСПДн представлен в таблице 9.

Таблица 9.

Перечень актуальных угроз.

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная

1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
2.2.1. Действия вредоносных программ (вирусов)	**актуальная**
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера	
2.3.1. Утрата ключей и атрибутов доступа	**актуальная**
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	неактуальная
2.3.3. Непреднамеренное отключение средств защиты	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, копирование, модификация, уничтожение,	**актуальная**

лицами не допущенными к ее обработке	
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	**актуальная**
2.5.Угрозы несанкционированного доступа по каналам связи	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	неактуальная
2.5.1.1. Перехват за переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	**актуальная**
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	**актуальная**
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

Вывод: актуальными угрозами безопасности ПДн в ИСПДн являются:

- угрозы от действий вредоносных программ (вирусов);
- угрозы утраты ключей и атрибутов доступа;
- доступ к информации, копирование, модификация, уничтожение лицами, не допущенными к ее обработке
- разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке
- угрозы выявления паролей по сети;
- угрозы внедрения по сети вредоносных программ.

3. Задания (указания по порядку выполнения работы)

1. Изучить документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

2. Определить значения опасности угрозы.

3. Используя таблицу 7, определить актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

4. Результаты оформить в виде таблицы.

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Контрольные вопросы

1) Каковы правила выбора из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн?
2) Перечислите показатели опасности угрозы.
3) Для каких дальнейших действий необходимо составление перечня актуальных угроз?

Лабораторное занятие №6.

Тема: Определение типа актуальной угрозы.

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения проблем определения типа актуальной угрозы в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18 Федерального закона "О персональных данных", и в соответствии с

нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

3. Методика и порядок выполнения работы.

На данном практическом занятии студенты выполняют следующие задания: 3.1. Изучают документ Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

3.2. Для определения типа актуальной угрозы использовать правило: актуальные угрозы, не связанны с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, если используемое ПО сертифицировано. Тогда для информационной системы актуален 3-й тип угрозы; соответственно наличие несертифицированного ПО в системном программном обеспечении определит 1-й тип актуальных угроз, а наличие несертифицированного ПО в прикладном программном обеспечении определит 2-й тип актуальных угроз.

3. Задания

1. Изучить документ Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

2. С учётом исходных данных и на основании требований Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", определить тип актуальной угрозы.

3. Результат записать в отчёте.

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Контрольные вопросы

1) Какие меры включает в себя система защиты персональных данных?

2) Кто обеспечивает безопасность персональных данных при их обработке в информационной системе?

3) Продолжите предложение: Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если…

Лабораторное занятие №7.

Тема: Определение уровня защищенности ПДн.

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения проблем определения уровня защищенности ПДн при их обработке в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

1) Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории

персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

2) Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

3) Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных

сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

4) Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Вся описанная информация может быть представлена в виде таблицы 10.

Таблица 10. Определение уровня защищенности ПДн

Тип ИСПДн	**Сотрудники оператора**	**Количество субъектов**	**Тип актуальных угроз**		
			1	**2**	**3**
ИСПДн-С	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-Б			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-1	УЗ-3	УЗ-4
	Да				
ИСПДн-О	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4

3. Методика и порядок выполнения работы.

На данном практическом занятии студенты выполняют следующие задания:

1. Изучают документ Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

2. По Таблице 10 определяют уровень защищенности ПДн в зависимости от типа актуальной угрозы, типа ИСПДн, категории субъектов и количества субъектов.

3. Результаты работы занести в отчёт.

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Контрольные вопросы и тестовые задания

1) При наличии каких условий необходим 3-й уровень защищенности персональных данных?

2) При наличии каких условий необходим 4-й уровень защищенности персональных данных?

3) При наличии каких условий необходим 2-й уровень защищенности персональных данных?

Лабораторное занятие №8.

Тема: Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах ПДн.

1. Цель и содержание

Целью практических занятий является теоретическая и практическая подготовка студентов в области изучения проблем определения состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, научиться работать с нормативными документами по защите персональных данных.

2. Теоретическое обоснование

Данное практическое задание предполагает использование документа Приказ ФСТЭК России от 18.02.2013 № 21"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки

соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к документу «Приказ ФСТЭК России от 18.02.2013 № 21», Приложение 1.

3. Методика и порядок выполнения работы.

На данном практическом занятии студенты выполняют следующие задания:

3.1. Изучают документ Постановление Правительства от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.2. Составляются Требования для обеспечения необходимого уровня защищенности персональных данных при их обработке в информационных системах Описаны в Постановление Правительства от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

«*…13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:*

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 …, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований,

предусмотренных пунктом 14 ..., необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 15 ..., необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.»

3.3 Составляется модель защиты, заключающаяся в выборе мер, закрывающих актуальные угрозы безопасности. Модель защиты, в соответствии с пунктом 9 Приказа ФСТЭК России от 18.02.2013 № 21, составляется по следующему алгоритму:

1) определяется базовый набор мер, а именно составляется перечень тех мер, которые отмечены плюсами для соответствующего УЗ в приложении к Приказу ФСТЭК России от 18.02.2013 № 21;

2) проводится адаптация базового набора мер. На этом этапе из базового набора мер исключаются те, которые не актуальны из-за особенностей конкретной ИСПДн (например, исключаются меры по защите виртуализации, если виртуализация не используется); Для адаптации мер необходимо соотнести возможные угрозы безопасности ПДн к мерам по приложению Приказа №21 ФСТЭК. Для этого необходимо воспользоваться таблицей 11.

3) уточнение адаптированного базового набора мер. На этом этапе добавляются ранее не выбранные меры, если в соответствии с частной моделью угроз какие-либо из актуальных угроз остались незакрытыми.

3.4 Студенты составляют «АКТ определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных», содержащий обязательные поля для заполнения, отмеченные красным шрифтом. Акт оформляется в виде модели защиты с составом и содержанием мер по обеспечению безопасности ПДн, согласно формы для заполнения, см. приложение 3 данной методики. В Акт необходимо

включить следующие требования обязательные для выполнения. Требования перечислены в Постановлении Правительства от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», п.13.

Таблица 11. Соответствие угроз безопасности ПДн мерам по обеспечению безопасности ПДн.

Возможные угрозы безопасности ПДн	**Меры по Приказу №21 ФСТЭК**	
1. Угрозы от утечки по техническим каналам	XII. Защита технических средств (ЗТС)	
1.1. Угрозы утечки акустической информации		
1.2. Угрозы утечки видовой информации		ЗТС.4
1.3. Угрозы утечки информации по каналам ПЭМИН		ЗТС.1
2. Угрозы несанкционированного доступа к информации		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ		ЗТС.3
2.1.2. Кража носителей информации	IV. Защита машинных носителей персональных данных (ЗНИ)	ЗНИ.1 ЗНИ.2
2.1.3. Кража ключей и атрибутов доступа		ЗНИ.5
2.1.4. Кражи, модификации, уничтожения информации		ЗНИ.8
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	V. Регистрация событий безопасности (РСБ) II. Управление доступом субъектов доступа к объектам доступа (УПД)	РСБ.1-3
2.1.7. Несанкционированное отключение средств защиты		ЗТС.3
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3

Возможные угрозы безопасности ПДн	Меры по Приказу №21 ФСТЭК	
программных средств (в том числе программно-математических воздействий)		
2.2.1. Действия вредоносных программ (вирусов)	VI. Антивирусная защита (АВЗ)	АВЗ.1-2
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	III. Ограничение программной среды (ОПС)	ОПС.2
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей		ОПС.3
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера	X. Обеспечение доступности персональных данных (ОДТ)	ОДТ.4
2.3.1. Утрата ключей и атрибутов доступа	I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	ИАФ.4
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	V. Регистрация событий безопасности (РСБ)	РСБ.7
2.3.3. Непреднамеренное отключение средств защиты	VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	АНЗ.3
2.3.4. Выход из строя аппаратно-программных средств	IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)	ОЦЛ.1
2.3.5. Сбой системы электроснабжения		
2.3.6. Стихийное бедствие		
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке	X. Обеспечение доступности персональных данных (ОДТ)	ОЦЛ.2
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке		ОЦЛ.2
2.5.Угрозы несанкционированного доступа по каналам связи		

Возможные угрозы безопасности ПДн	Меры по Приказу №21 ФСТЭК	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
2.5.1.1. Перехват за переделами контролируемой зоны		ОЦЛ.4
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями		ОЦЛ.1
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.		ОЦЛ.1
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	АНЗ.1-2
2.5.3.Угрозы выявления паролей по сети	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	АНЗ.3
2.5.4.Угрозы навязывание ложного маршрута сети		ЗИС.3
2.5.5.Угрозы подмены доверенного объекта в сети		ЗИС.11
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях		
2.5.7.Угрозы типа «Отказ в обслуживании»		
2.5.8.Угрозы удаленного запуска приложений		
2.5.9.Угрозы внедрения по сети вредоносных программ	VI. Антивирусная защита (АВЗ)	

3. Задания

1. Изучить документ Приказу ФСТЭК России от 18.02.2013 № 21, разработанный ФСТЭК России.

2. Определить базовый набор мер для соответствующего УЗ по приложению Приказа ФСТЭК России от 18.02.2013 № 21, разработанного ФСТЭК России.

3. Адаптировать базовый набор мер путём исключения тех мер, которые не актуальны из-за особенностей конкретной ИСПДн.

4. Уточнить адаптированный базовый набор мер путём добавления ранее не использованных мер.

4. Результаты занести в таблицу.

5. Составить Акт в виде модели защиты с составом и содержанием мер по обеспечению безопасности ПДн,

4. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, студента, курс, группа, проверил: преподаватель ФИО.

5. Контрольные вопросы

1) Какое основное требование к средствам защиты информации установлено в Приказе №21?

2) Что должны обеспечивать меры по идентификации и аутентификации субъектов доступа и объектов доступа?

3) Что должны обеспечивать меры по антивирусной защите?

4) Что включает в себя выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных?

5) В каких случаях применяются компенсирующие меры?

6) Какого класса применяются средства вычислительной техники для обеспечения 3 уровня защищенности персональных данных?

Лабораторное занятие **№ 9**

Тема: Разработка системы защиты информации Информационной системы

Теоретическая часть

Разработка системы защиты информации информационной системы организуется обладателем информации (заказчиком).

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее – ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

- проектирование системы защиты информации информационной системы;
- разработку эксплуатационной документации на систему защиты информации информационной системы;
- макетирование и тестирование системы защиты информации информационной системы (при необходимости).

Система защиты информации информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке системы защиты информации информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также применение вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

После выбора мер защиты информации:

- определяются классы, виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
- определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;
- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также уровня защищенности информационной системы;
- определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.

Результаты проектирования системы защиты информации информационной

системы отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на информационную систему (систему защиты информации информационной системы), разрабатываемых с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее – ГОСТ 34.201).

Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

- структуры системы защиты информации информационной системы;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- правил эксплуатации системы защиты информации информационной системы.

Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности.

В этом случае в информационных системах 1 и 2 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 3 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 5 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

- межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

В информационных системах 4 класса защищенности применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;
- межсетевые экраны не ниже 4 класса.

В информационных системах 1 и 2 классов защищенности применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Результат описанных выше требований сведён в таблицу 12.

Таблица 12. Требования к СЗИ по сертификации в зависимости от уровня защищенности ГИС.

<table>
<tr><td rowspan="3">Уровень защищенности ПДн</td><td colspan="7">Класс защиты СрЗИ</td><td rowspan="3">Уровень контроля ПО СрЗИ на отсутствие НДВ</td></tr>
<tr><td rowspan="2">СВТ</td><td colspan="2">Средства антивирусной защиты</td><td colspan="2">Системы обнаружения вторжений</td><td colspan="2">Межсетевые экраны</td></tr>
<tr><td>Угрозы 2 типа или взаимодействие с сетями МИО</td><td>Угрозы 3 типа и отсутствие взаимодействия с сетями МИО</td><td>Угрозы 2 типа или взаимодействие с сетями МИО</td><td>Угрозы 3 типа и отсутствие взаимодействия с сетями МИО</td><td>Угрозы 1 и 2 типа или взаимодействие с сетями МИО</td><td>Угрозы 3 типа и отсутствие взаимодействия с сетями МИО</td></tr>
<tr><td>УЗ1</td><td rowspan="3">Не ниже 5 класса</td><td colspan="2" rowspan="2">Не ниже 4 класса</td><td colspan="2" rowspan="2">Не ниже 4 класса</td><td rowspan="3">Не ниже 3 класса</td><td rowspan="3">Не ниже 4 класса</td><td>4 уровень</td></tr>
<tr><td>УЗ2</td><td rowspan="2">4 уровень (если актуальны угрозы 2 типа)</td></tr>
<tr><td>УЗ3</td><td colspan="2">Не ниже 5 класса</td><td colspan="2">Не ниже 5 класса</td></tr>
<tr><td>УЗ4</td><td>Не ниже 5 класса</td><td colspan="2">Не ниже 5 класса</td><td colspan="2">Не ниже 5 класса</td><td colspan="2">5 класс</td><td>—</td></tr>
</table>

2. Практическая часть.

1. Составить технический паспорт в соответствии с приложением 7:

- Заполнить технический паспорт «Форма технического паспорта на

автоматизированную систему», приложение 4;

- Заполнить табл. 2 «Перечень средств защиты информации, установленных на АС».

Рекомендации:

В соответствии с «Государственным реестром сертифицированных средств защиты информации», ФСТЭК России от 2015г. подобрать оборудование соответствующее следующим подсистемам:

1) **Средства защиты ПДн от утечки по техническим каналам**

С целью предотвращения утечек акустической (речевой), видовой информации, а также утечек информации за счет побочных электромагнитных излучений и наводок применяются специальные технические средства. При этом выделяются пассивные и активные средства защиты.

Пассивные средства защиты, как правило, реализуются на этапе разработки проектных решений при строительстве или реконструкции зданий. Преимущества применения пассивных средств заключаются в том, что они позволяют заранее учесть типы строительных конструкций, способы прокладки коммуникаций, оптимальные места размещения защищаемых помещений.

Защита ПДн при осуществлении пользователями информационных систем голосового ввода данных в ИСПДн или их воспроизведении акустическими средствами ИСПДн обеспечивается путем звукоизоляции помещений, в которых устанавливаются аппаратные средства ИСПДн, систем инженерного обеспечения (вентиляции, отопления и кондиционирования), а также ограждающих конструкций помещений (стены, пол, потолок, окна, двери).

Что использовать: встроенные или наложенные средства защиты?

Опираясь на накопленный опыт в области защиты информации, специалисты компании «Инфосистемы Джет» в проектировании решений по защите информации при их обработке в АС стараются комбинировать как наложенные средства защиты информации, так и встроенные механизмы защиты в общесистемное и прикладное программное обеспечение (ПО), используемое в АС. Каждый вариант имеет свои достоинства и недостатки. Наложенные средства далеко не всегда могут в полной мере реализовать требования регуляторов, а также могут оказаться несовместимыми с уже используемыми в АС программными решениями. Применение встроенных механизмов приводит к

возникновению проблем, связанных с обязательным наличием у такого ПО сертификатов соответствия российских регуляторов.

Многие специалисты компаний отдают предпочтение встроенным механизмам реализации управления доступом к информации.

Данный подход обусловлен тем, что позволяет минимизировать изменения в структуре как самих АС, так и механизмов безопасности.

Звукоизоляция обеспечивается с помощью архитектурных и инженерных решений, применением специальных звукопоглощающих строительных и отделочных материалов, виброизолирующих опор, которыми разделяют друг от друга различные ограждающие конструкции. Для обеспечения требований по защите информации достаточным является повышение звукоизоляции на 10-15 дБ. Для снижения вероятности перехвата информации такого рода необходимо исключить возможность установки посторонних предметов на внешней стороне ограждающих конструкций помещений и выходящих из них инженерных коммуникаций.
В случае технической невозможности использования пассивных средств защиты помещений, применяют **активные меры защиты**, заключающиеся в создании маскирующих акустических и вибрационных помех.

Средства акустической маскировки используется для защиты речевой информации от утечки по прямому акустическому каналу путем создания акустических шумов в местах возможного размещения средств подслушивания или нахождения посторонних лиц.

Средства виброакустической маскировки применяются для защиты информации от перехвата с помощью электронных стетоскопов, радиостетоскопов, а также лазерных акустических систем подслушивания.

С целью предотвращения утечки информации по телефонным каналам связи необходимо оконечные устройства телефонной связи, которые имеют прямой выход на городскую автоматическую телефонную станцию, оборудовать специальными средствами защиты информации, которые используют электроакустическое преобразование.

2) Средства защиты от несанкционированного доступа

Для осуществления мероприятий по защите информации при их обработке в информационных системах от несанкционированного доступа (НСД) и

неправомерных действий пользователей и нарушителей средства защиты (СЗ) могут включать в себя следующие подсистемы:

- управления доступом;
- регистрации и учета;
- обеспечения целостности;
- антивирусной защиты;
- обеспечения безопасности межсетевого взаимодействия АС;
- анализа защищенности;
- обнаружения вторжений.

3) **Подсистема управления доступом, регистрации и учета**, как правило, реализуется с помощью программных средств блокирования НСД, сигнализации и регистрации. Это специальные, не входящие в ядро операционной системы программные и программно-аппаратные средства защиты самих операционных систем, СУБД и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения несанкционированных действий пользователей или нарушителей. К ним относятся специальные утилиты и программные комплексы защиты, в которых реализуются функции диагностики (тестирование файловой системы), регистрации (журналирование действий и операций), сигнализации.
4) **Подсистема обеспечения целостности** также реализуется преимущественно средствами самих операционных систем и СУБД. Работа данных средств основана на расчете контрольных сумм, уведомлении о сбое в передаче пакетов сообщений, повторе передачи непринятых пакетов. Частота применения в российских компаниях в качестве операционной системы продуктов компании Microsoft вызвала необходимость использовать в качестве базовой платформы для построения решения подсистемы разграничения и контроля доступа к ресурсам информационной системы функционал Microsoft Windows Server 2003.

   Эта сетевая операционная система наряду с необходимым для обеспечения безопасности ПДн набором технологических параметров обладает всеми необходимыми сертификатами на соответствие требованиям регулирующих органов. ФСТЭК России в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 сертифицировал:

- русскую версию Windows Server 2003 (Standard Edition и Enterprise Edition);
- русскую версию Windows Server 2003 R2 (Standard Edition и Enterprise Edition).

Компанией Microsoft также производится сертификация ежемесячно выходящих новых патчей к данным продуктам.

ФСБ России сертифицировала русскую версию серверной операционной системы Windows Server 2003 Enterprise Edition. Сертификат ФСБ удостоверяет, что продукт соответствует требованиям ФСБ России к защите информации, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа в автоматизированных информационных системах класса АК2. Таким образом, данная система может быть использована в качестве средства для защиты информации в АС.

.

5) **Для обеспечения безопасности информации программно-аппаратной среды** АС, обеспечивающей обработку этой информации, рекомендуется применять специальные средства антивирусной защиты (подсистема антивирусной защиты). Такие средства способны обеспечивать:

- обнаружение и блокирование деструктивных вирусных воздействий на общесистемное и прикладное ПО, реализующее обработку информации;
- обнаружение и удаление «неизвестных» вирусов (т.е. вирусов, сигнатуры которых еще не внесены в антивирусные базы данных);
- обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

Для реализации подсистемы антивирусной защиты информации возможно использование антивирусных средств компании «Лаборатория Касперского».

Продукты компании «Лаборатория Касперского» сертифицированы Федеральной службой безопасности России. Данные сертификаты удостоверяют, что Антивирус Касперского 6.0 для Windows Servers соответствует требованиям к антивирусным средствам класса А1с, Антивирус Касперского 5.5 для Linux и FreeBSD Workstations и File Server соответствует требованиям к антивирусным средствам класса А2с и Kaspersky Administration Kit 6.0 соответствует требованиям к антивирусным средствам класса А3с. Указанные продукты могут использоваться в органах государственной власти Российской Федерации для

защиты информации, содержащей сведения, составляющие государственную тайну.

Кроме того, продукты Антивирус Касперского 6.0 для Windows Servers, Антивирус Касперского 6.0 для Windows Workstation и Kaspersky Administration Kit 6.0 соответствуют требованиям руководящего документа ФСТЭК – по 3 уровню контроля и требованиям технических условий.

6) Для осуществления разграничения доступа к ресурсам АС при межсетевом взаимодействии **(подсистема обеспечения безопасности межсетевого взаимодействия ИСПДн)** применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран устанавливается между защищаемой внутренней и внешней сетями. МЭ входит в состав защищаемой сети. За счет соответствующих настроек задаются правила, которые позволяют ограничивать доступ пользователей из внутренней сети во внешнюю и наоборот.

7) Подсистема анализа защищенности предназначена для осуществления контроля настроек защиты операционных систем на рабочих станциях и серверах и позволяет оценить возможность проведения нарушителями атак на сетевое оборудование, контролирует безопасность программного обеспечения. С помощью таких средств (средства обнаружения уязвимостей) производится сканирование сети с целью исследования ее топологии, осуществления поиска незащищенных или несанкционированных сетевых подключений, проверки настроек межсетевых экранов и т.п. Данный анализ производится на основании детальных описаний уязвимостей настроек средств защиты (например, коммутаторов, маршрутизаторов, межсетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения. Результатом работы средств анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях.

Средства обнаружения уязвимостей могут функционировать на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения (application-based). Применяя сканирующее ПО, можно составить карту доступных узлов АС, выявить используемые на каждом из них сервисы и протоколы, определить их основные настройки и сделать предположения относительно вероятности реализации НСД. По результатам сканирования системы вырабатываются рекомендации и меры, позволяющие устранить выявленные недостатки.

В качестве средства, применяемого в подсистеме анализа защищенности, специалисты компаний часто используют Xspider компании Positive

Technologies. Сетевой сканер Xspider сертифицирован ФСТЭК России (сертификат соответствия № 1323от 23 января 2007 г., действителен до 23 января 2010 г.) и Министерством Обороны (сертификат соответствия № 354). Xspider – сетевой сканер безопасности, построенный на базе интеллектуального сканирующего ядра, которое обеспечивает максимально полное и надежное определение уязвимостей на системном и прикладном уровне. XSpider работает под управлением Microsoft Windows, он проверяет все возможные уязвимости независимо от программной и аппаратной платформы узлов, работает с уязвимостями на разном уровне – от системного до прикладного. В частности, XSpider включает мощный и глубокий анализатор защищенности WEB-серверов и WEB-приложений. Xspider поддерживает различные способы сканирования, в том числе и удаленное, при гарантии доступности сетевого сегмента.

Применение системы MaxPatrol позволяет:

- Оценивать защищенность информационных систем. MaxPatrol выявляет бреши в защите автоматизированных систем (АС), формирует задание на их устранение, отслеживает эффективность и своевременность устранения найденных уязвимостей.
- Отслеживать текущее состояние информационных ресурсов. MaxPatrol проводит инвентаризацию защищаемых ресурсов и позволяет своевременно обнаруживать изменения в АС, в частности, в настройках сетевого оборудования, правах пользователей на рабочих станциях, таблицах БД, мандантах ERP-систем.
- Контролировать соответствие АС техническим политикам. MaxPatrol формирует технические стандарты с использованием имеющейся в системе Базы Знаний, включающей комплексные стандарты для сетевого оборудование Cisco/Nortel/Huawei, платформ Windows/Linux/Solaris/, СУБД Microsoft SQL/Oracle, сетевых приложений, Web-служб, почтовых систем, ERP-приложений. MaxPatrol автоматически проводит инспекции на предмет соответствия АС сформированным техническим политикам безопасности.
- Измерять эффективность процессов ИБ в организации. На основе постоянно собираемой информации система формирует метрики безопасности (KPI), по которым оценивается эффективность процессов обеспечения ИБ. Существуют десятки различных метрик: от технических (например, процент рабочих станций, не удовлетворяющих антивирусной политике) до высокоуровневых (процент выполнения филиалом требований по безопасности в сравнении с другими филиалами на протяжении определенного времени). Метрики рассчитываются на основе

реальных количественных данных, собранных модулями оценки защищенности, инвентаризации, контроля соответствия.

В данный момент ведется сертификация системы MaxPatrol.

8) Выявление угроз НСД при межсетевом взаимодействии производится с помощью систем обнаружения вторжений **(подсистема обнаружения вторжений)**. Такие системы строятся с учетом особенностей реализации атак и этапов их развития. Они основаны на следующих методах обнаружения атак: сигнатурные методы, методы выявления аномалий, комбинированные методы с использованием обоих названных методов. В качестве средства для реализации подсистемы обнаружения и предотвращения вторжений специалисты часто используют продукты компании Cisco. Данные средства сертифицированы ФСТЭК и соответствуют требованиям технических условий и стандарту ГОСТ Р ИСО/МЭК 15408-2002.

   К таким продуктам, в частности, относится Cisco Intrusion Detection System/Intrusion Preventing System (IPS/IDS), который является основным компонентом решений Cisco Systems по обнаружению и отражению атак. Наряду с традиционными механизмами в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки. Встроенные технологии корреляции событий безопасности Cisco Threat Response, Threat Risk Rating и Meta Event Generator не только помогают существенно уменьшить число ложных срабатываний, но и позволяют администраторам реагировать лишь на действительно критичные атаки, которые могут нанести серьезный ущерб ресурсам корпоративной сети.

9) **Средства защиты каналов при передаче информации**

Для обеспечения безопасности информации при передаче по открытым каналам или в несегментированной сети служит подсистема криптографической защиты каналов связи. Помимо вышеназванной задачи данная подсистема позволяет обеспечивать безопасное взаимодействие с технологическими сетями и доступ для осуществления удаленного администрирования. Данная подсистема может быть реализована на основе программно-аппаратного комплекса Cisco Adaptive Security Appliance. Этот комплекс сертифицирован ФСТЭК (соответствие руководящим документам по межсетевым экранам (3 и 4 Класс) и требованиям технических условий).

Cisco ASA 5500 предназначен для решения сразу нескольких задач – разграничения доступа к сетевым ресурсам, защиты от атак, защиты взаимодействия с удаленными территориями, блокирования вирусов, червей, шпионского ПО и других вредоносных программ, спама и атак типа «фишинг». Это достигается за счет объединения в одном устройстве лучших защитных средств – межсетевого экрана Cisco Pix, системы предотвращения атак Cisco IPS и Cisco VPN 3000 Concentrator.

Помимо описанных выше программно-технических средств защиты широко используют продукты других ведущих производителей на рынке информационной безопасности. К ним, в частности, относятся Oracle, Aladdin, Check Point, «С-Терра СиЭсПи», «КриптоПро». Данные компании проводят активную позицию по соответствию требований регуляторов и сертификации своих продуктов с целью их применения в решениях по защите персональных данных.

10) Требования к средствам защиты информации

К средствам защиты информации прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Все сертифицированные ФСТЭК средства защиты представлены на сайте ФСТЭК (http://www.fstec.ru/) в разделе «Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации» (http:// www.fstec.ru/_ razd/_serto.htm) в подразделе «Государственный реестр сертифицированных средств защиты информации».

Приложение 1

Общие исходные данные для расчётов:

- Наличие подключений ИСПДн к сетям связи общего пользования/сетям МИО - *имеющие подключение*.
- Режим обработки персональных данных: *многопользовательская ИСПДН.*
- *Все элементы ИСПДн находятся в пределах КЗ.*
- *Пользователи имеют разные права доступа к ПДн.*
- *Недекларированные возможности в ПО отсутствуют.*

Приложение 2

Таблица 1. Индивидуальные исходные данные для расчётов:

№ п/п	Категория ПДн	Структура ИСПДн	Категории субъектов	Число субъектов ПДн
1	ПДн-Б	распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Не сотрудников	>100 000
2	ПДн–И	локальная, развернутая в пределах одного здания	Сотрудников	<100 000
3	ПДн–О	локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Не сотрудников	>100 000
4	ПДн–Б	корпоративная распределенная, охватывающая многие подразделения одной организации	Сотрудников	<100 000
5	ПДн–И	городская, охватывающая не более одного населенного пункта (города, поселка);	Не сотрудников	>100 000
6	ПДн–И	распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Сотрудников	<100 000
7	ПДн–Б	локальная, развернутая в пределах одного здания	Не сотрудников	>100 000
8	ПДн–И	локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Сотрудников	<100 000
9	ПДн–О	корпоративная распределенная, охватывающая многие подразделения одной организации	Не сотрудников	>100 000
10	ПДн–Б	распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Сотрудников	<100 000
11	ПДн-Б	локальная, развернутая в пределах одного здания	Не сотрудников	<100 000
12	ПДн–И	локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Сотрудников	>100 000
13	ПДн–О	корпоративная распределенная, охватывающая многие подразделения одной организации	Не сотрудников	>100 000
14	ПДн–Б	распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Сотрудников	>100 000

15	ПДн–И	локальная, развернутая в пределах одного здания	Не сотрудников	<100 000
16	ПДн–И	локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Сотрудников	>100 000
17	ПДн–Б	распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Не сотрудников	<100 000
18	ПДн–И	локальная, развернутая в пределах одного здания	Сотрудников	>100 000
19	ПДн–О	распределенная, которая охватывает несколько	Не сотрудников	<100 000
20	ПДн–Б	распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Сотрудников	>100 000

Форма для заполнения

Приложение 3

к распоряжению «О проведении работ по защите персональных данных администрации сельского поселения «Пажга» от 15.02.2013г. № 6-Р

АКТ
определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных

2015г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Классификация ИСПДн была проведена в соответствии с совместным Приказом ФСТЭК/ФСБ/Минсвязи «Об утверждении порядка проведения классификации информационных систем персональных данных» от 13.02.2008г. № 55/86/20, «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (далее – ПП №1119), Моделью угроз безопасности персональных данных.

Классификацию ИСПДн проводила комиссия, назначенная распоряжением Главы администрации сельского поселения "XXXXX" от __.__.2014г. №___., в составе:

Председатель:	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Должность,	ФИО
Члены комиссии:	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Должность,	ФИО
	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Должность,	ФИО
	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Должность,	ФИО

2. АКТ ОПЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИСПДн «СОТРУДНИКИ»

В ходе работы комиссия установила:

1) категория персональных данных – иные;

2) обрабатываются персональных данных сотрудников оператора;

3) объем обрабатываемых персональных данных – менее 100000 субъектов персональных данных;

4) структура информационной системы: автономная ИС.

5) наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена: да;

6) режим обработки персональных данных: многопользовательский;

7) режим разграничения прав доступа пользователей информационной системы: с разграниченными правами доступа;

8) местонахождение технических средств: в пределах Российской Федерации;

По результатам анализа исходных данных и модели определения угроз исходящих от НДВ в ПО ИСПДн, ИСПДн «Сотрудники» присваивается 4 уровень защищенности.

Требования по защищенности для 4 уровня (согласно ПП №1119):

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения
- обеспечение сохранности носителей персональных данных
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

Председатель:	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Подпись	ФИО
Члены комиссии:	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Подпись	ФИО
	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Подпись	ФИО
	XXXXXXXXXXXXX	XXXXXXXXXXXXX
	Подпись	ФИО

Приложение 7.

Форма технического паспорта на автоматизированную систему

УТВЕРЖДАЮ
Руководитель организации

_____
(подпись, инициалы, фамилия)

_____
(дата)

ТЕХНИЧЕСКИЙ ПАСПОРТ

_____

указывается полное наименование автоматизированной системы

СОСТАВИЛ

_____
(должность, подпись, инициалы, фамилия специалиста подразделения по защите информации)

_____
(дата)

ОЗНАКОМЛЕН

_____
_
(должность, подпись, инициалы, фамилия ответственного за помещение)

_____
(дата)

1. Общие сведения об АС

1.1. Наименование АС: *полное наименование АС*

1.2. Расположение АС: *адрес, здание, строение, этаж, комнаты*

1.3. Класс АС: *номер и дата акта классификации АС, класс АС*

2. Состав оборудования АС

2.1. Состав ТСЗ:

Таблица 1

ПЕРЕЧЕНЬ
средств защиты информации, установленных на АС
«_XXXXXXXXXXXXXXXXX_»

№ п/п	Наименование и тип и технического средства	Заводской номер	Сведения о сертификате	Место и дата установки
1	Windows 8.1	-	3263 до 07.11.2017	Пк, 1-10, 28.02
2	Kaspersky Endpoint Security 8 для Windows	-	2682 до 26.07.2018	ПК 1-10, 03.03
3				
4				
5				
6				
7				
8				

9				
10				
11				

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ, Об информации, информационных технологиях и о защите информации
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ О персональных данных
3. «Порядок проведения классификации информационных систем персональных данных», утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. №. 55/86/20
4. Приказ ФСТЭК от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
5. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 г. № 996 Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России от 15.02.2008 г.
7. Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 20.07.2013) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"
8. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
9. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996, утвержденные 13.12.2013 г. Руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций
10. «Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн». Статья, август 2013. Код безопасности
11. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказ ФСТЭК России от «18» февраля 2013 г. № 21.// Официальный сайт ФСТЭК России. URL: http://fstec.ru/component/attachments/download/562 (дата обращения: 15.09.2014).

12. «Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн». Статья, август 2013. Код безопасности http://www.securitycode.ru/upload/iblock/8e9/algoritm-deystviy-operatora-pdn-po-sozdaniyu-sistemy-zashchity-ispdn.pdf