МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	Бакалавр
Форма обучения	Очная
Учебный план	2020 г.

Пятигорск 2020 г.

Введение

Основной целью современного высшего образования является развитие компетентностного подхода.

Профессиональные компетенции – готовность и способность целесообразно действовать в соответствии с предъявляемыми требованиями, методически организованно и самостоятельно решать задачи и профессионально трактовать проблемы.

При выполнении лабораторного практикума студенты приобретают необходимые навыки, которые пригодятся в научно исследовательской и профессиональной деятельности.

Целями лабораторных работ является теоретическая и практическая подготовка студентов в области защиты персональных данных, формирование набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01

Работа в лаборатории для студентов является одной из важнейших форм учебной работы, при которой формируются личностные качества будущего специалиста:

- самостоятельность в принципиальных решениях;
- проявление инициативы;
- умение логически мыслить.

При построении курса важной задачей являлся отбор содержания материала, подлежащего изучению. При изучении курса «Организации защиты персональных данных», а также закрепления полученных теоретических знаний предлагается последовательно выполнить лабораторные работы данного учебного пособия.

Все лабораторные работы посвящены организации защиты персональных данных в информационных системах персональных данных в соответствии с :

− Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

−Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Утверждена заместителем директора ФСТЭК России 15.02.2008 г. ДСП.);

−Приказом ФСТЭК №21 от 18.02.13г «Состав и содержание организационных и технических мер по защите ПДн при их обработке в информационных системах персональных данных»;

−Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14.02.2008г.

−Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

СОДЕРЖАНИЕ

Введение ……4

ЛАБОРАТОРНАЯ РАБОТА № 1. Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных …….……..... 11

ЛАБОРАТОРНАЯ РАБОТА № 2. Определение уровня исходной защищённости (Y_1)…….……..... 28

ЛАБОРАТОРНАЯ РАБОТА № 3. Определения частоты (вероятности) реализации рассматриваемой угрозы (Y_2)…….……..... …35

ЛАБОРАТОРНАЯ РАБОТА № 4. Определения коэффициента реализуемости угрозы (Y) и возможности реализации……..... 45

ЛАБОРАТОРНАЯ РАБОТА № 5. Определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных…….……..... 54

ЛАБОРАТОРНАЯ РАБОТА № 6. Определение типа актуальной угрозы ……..……..... 62

ЛАБОРАТОРНАЯ РАБОТА № 7. Определение уровня защищенности ПДн……..……..……..... 68

ЛАБОРАТОРНАЯ РАБОТА № 8. Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах ПДн……..……..……..... 76

ЛАБОРАТОРНАЯ РАБОТА № 9. Составление акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных…… 84

СПИСОК ЛИТЕРАТУРЫ ……..……93

Приложения ……95

Лабораторная работа №1.

Тема: «Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

1. Цель работы

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

2. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

3. Теоретическая часть

3.1 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»

3.2 Характеристики ИСПДн, обусловливающие возникновение угроз БПДн:

1) структура ИСПДн:

a) автономные ИСПДн АРМ;

Рисунок 1. Автономные ИСПДн АРМ.

b) локальные ИСПДн:

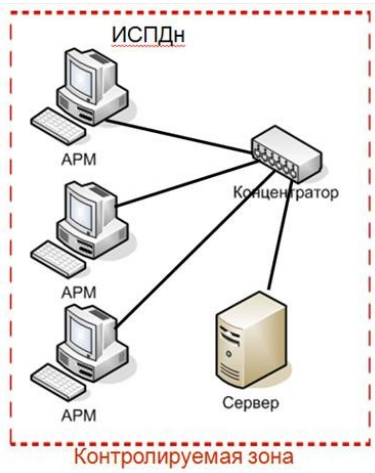

Рисунок 2. Локальные ИСПДн АРМ.

c) распределенные ИСПДн):

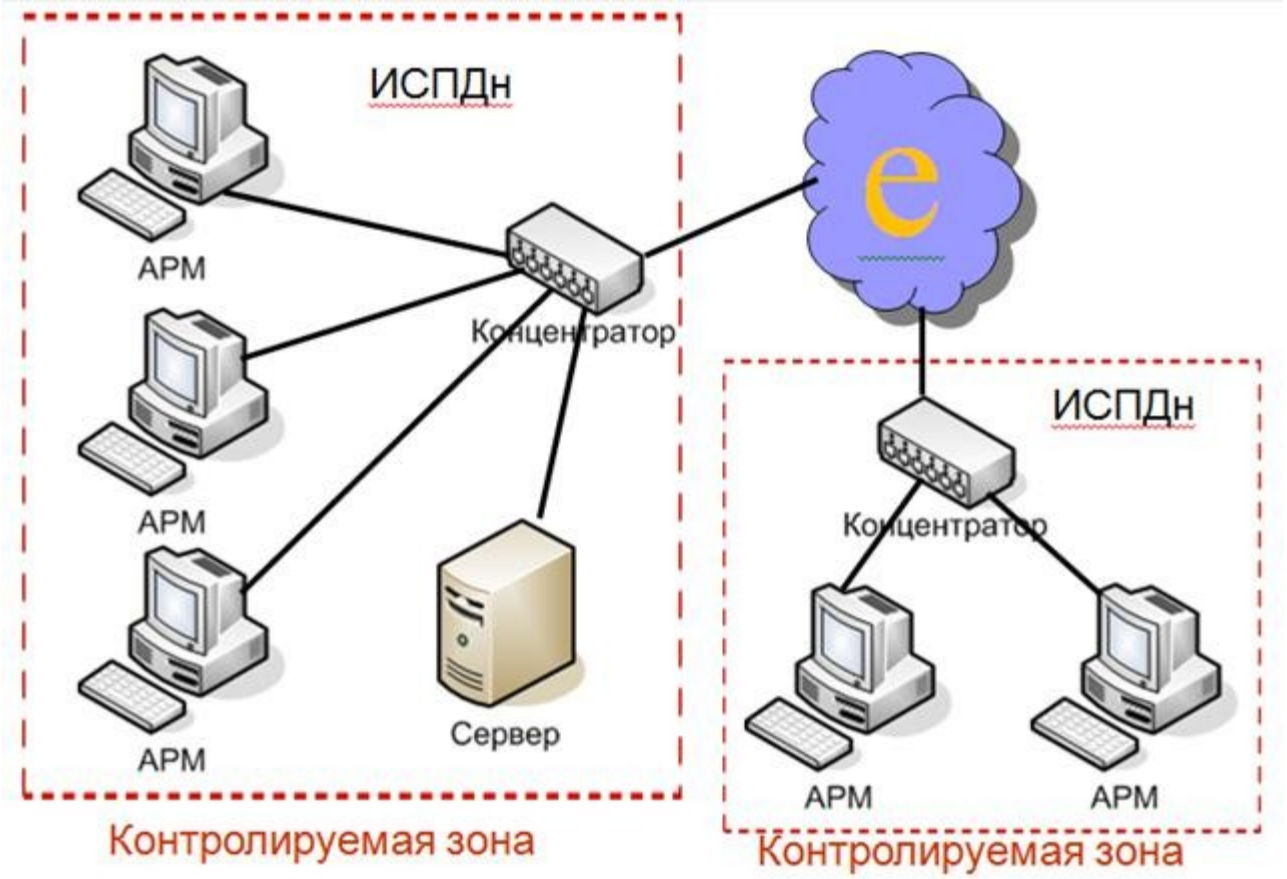

Рисунок 3. Распределенные ИСПДн АРМ.

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.

4.3 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.

4.4 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.

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

Таблица 1. Внешние нарушители

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

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. Характеристика внутренних нарушителей

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.

4.5 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.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом

работы Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время

работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;
- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы).

Данное 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» (далее «Базовая модель»).

6.1. Изучают категории нарушителей, описанные в документе ФСТЭК России «Базовая модель». Для конкретной информационной системы определяют перечень вероятных нарушителей ИСПДн с учетом всех исключений.

6.2. 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, см. пример 1.

Пример 1:

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

6.3. По заданию преподавателя определяют типовую модель угроз для конкретных значений, указанных в Приложении 1 данной методики.

6.4. По заданию преподавателя определяют угрозы безопасности для конкретных значений, указанных в Приложении 2данной методики. Данный набор угроз дополняет составленный перечень по п. 3.2. Из обоих наборов моделей угроз необходимо сформировать один, исключающий повторение угроз.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяем методический документ «Базовая модель», пп. 6.1-6.6. Полученные результаты записываются, см. пример 2.

Пример 2:

Типовая модель угроз безопасности ПДн, обрабатываемых в автоматизированных рабочих местах, имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена по «Базовой модели», п. 6.1будет следующего содержания:

<u>угрозы утечки информации по техническим каналам:</u>

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

угрозы НСД к ПДн, обрабатываемым в автоматизированном рабочем месте:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ.

Угрозы из внешних сетей:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

7. Содержание отчёта

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. Контрольные вопросы и тестовые задания

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?

Выберите правильный ответ.

Что из перечисленного не относится перечню сведений конфиденциального характера:

а) Персональные данные;
б) Сведения, составляющие тайну следствия и судопроизводства;
в) Сведения, связанные с профессиональной деятельностью; г)
Сведения, связанные с государственной деятельностью.

Выберите правильный ответ

Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств – это…

а) информационная система;
б) информационно-телекоммуникационная сеть;
в) конфиденциальность информации;
предоставление информации.

Лабораторная работа №2.

Тема: «Определение уровня исходной защищённости (Y_1)»

1. Цель работы

Целью Лабораторной работы 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. Формируемые компетенции или их части

- ОК-4 - способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач;
- ОК-5 - способностью к кооперации с коллегами, работе в коллективе;
- ОК-6 - способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;
- ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;
- ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

− ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности.

3. Теоретическая часть

Данная работа 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);	–	–	+
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;	–	+	–

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
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 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;	–	–	+
Количество «+» в колонках	4	6	7
РЕЗУЛЬТАТ (*Y_1*)	5		

Где Y_1- числовой коэффициент исходной защищенности, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

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

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5 Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом работы Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;

- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы).

На данном занятии студенты выполняют следующие задания:

6.1. Изучают документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанную ФСТЭК России.

6.2. 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.

6.3. Результат записывается в таблицу.

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

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

Выберите правильный ответ

Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя – это…

а) конфиденциальность;
б) целостность;
в) доступность;
предоставление информации.

Лабораторная работа №3.

Тема: «Определения частоты (вероятности) реализации рассматриваемой угрозы (Y_2)»

1. Цель работы

Целью Лабораторной работы 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. Формируемые компетенции или их части

- ОК-7 - способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;
- ОК-8 - способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
- ОК-9 - способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
- ОК-10 - способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
- ОК-11 - способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

− ОК-12 - способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

− ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;

− ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

− ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности;

− ПК-27 - способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

3. Теоретическая часть

Данное 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 Опас-ности угрозы**
	внеш ние	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Итог (Y2)**	
1. Угрозы от утечки по техническим каналам											
1.1. Угрозы утечки акустической информации	0	0	0	0	0	0	0	0	0	2	низкая
1.2. Угрозы утечки видовой информации	0	0	0	0	2	5	2	0	2	5	средняя
1.3. Угрозы утечки информации по каналам ПЭМИН	0	0	0	0	2	5	2	0	2	5	средняя
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	0	0	0	0	низкая
2.1.2. Кража носителей информации	0	0	5	5	0	5	5	0	5	5	средняя
2.1.3. Кража ключей и атрибутов доступа	0	0	0	2	2	5	0	5	0	5	средняя

2.1.4. Кражи, модификации, уничтожения информации	0	0	2	5	2	5	0	0	0	5	средняя
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0	0	0	0	0	2	0	0	0	2	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0	0	0	0	0	0	2	0	5	5	средняя
2.1.7. Несанкционированное отключение средств защиты	0	0	0	0	0	2	0	0	0	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)	0	0	0	0	2	2	0	2	0	2	низкая
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0	0	0	0	0	0	0	0	0	низкая
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	0	0	0	0	0	0	0	0	0	0	низкая
2.3. Угрозы непреднамеренных 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	0	5	5	0	2	0	0	0	5	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0	0	0	2	0	2	0	0	2	2	низкая
2.3.3. Непреднамеренное отключение средств защиты	0	0	0	0	0	0	0	0	0	0	низкая

2.3.4. Выход из строя аппаратно-программных средств	0	0	0	0	0	0	0	0	0	0	низкая
2.3.5. Сбой системы электроснабжения	0	0	0	0	0	0	0	0	0	0	низкая
2.3.6. Стихийное бедствие	0	0	0	0	0	0	0	0	0	0	средняя
2.4. Угрозы преднамеренных действий внутренних нарушителей											
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке	2	2	0	0	2	2	2	0	2	2	низкая
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	0	0	5	10	0	2	0	0	0	5	высокая
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 контролируемой зоны	2	2	0	0	0	0	0	0	0	2	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0	0	0	0	0	0	0	0	0	0	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0	0	2	2	5	5	0	0	2	5	средняя
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	2	5	5	2	0	2	5	средняя

2.5.3.Угрозы выявления паролей по сети	0	0	0	0	2	2	0	0	0	2	низкая
2.5.4.Угрозы навязывания ложного маршрута сети	0	0	0	0	5	2	0	0	0	5	средняя
2.5.5.Угрозы подмены доверенного объекта в сети	0	0	0	0	2	2	0	0	0	2	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	2	0	0	0	2	5	2	0	2	5	средняя
2.5.7.Угрозы типа «Отказ в обслуживании»	2	0	0	0	0	0	0	0	0	2	низкая
2.5.8.Угрозы удаленного запуска приложений	0	0	2	2	5	5	0	2	0	5	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	10	2	2	2	5	5	0	0	2	5	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.

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом

работы Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время

работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;
- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы)

Пользуясь таблицей 5:

1. Определить частоту (вероятность) реализации рассматриваемой угрозы (Y_2):

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).

2. Провести оценку опасности угрозы 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.

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. Контрольные вопросы и тестовые задания

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?

Выберите правильный ответ

Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) – это…

а) Персональные данные;
б) Коммерческая тайна;
в) Государственная тайна
г) Профессиональная тайна.

Выберите правильный ответ

Действия, направленные на раскрытие персональных данных неопределенному кругу лиц – это…

а) распространение персональных данных;
б) предоставление персональных данных; в)
искажение персональных данных;
уничтожение персональных данных.

Лабораторная работа №4.

Тема: «Определения коэффициента реализуемости угрозы (*Y*) и возможности реализации»

1. Цель работы

Целью Лабораторной работы 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. Формируемые компетенции или их части

- ОК-7 - способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной

безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

- ОК-8 - способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
- ОК-9 - способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
- ОК-10 - способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
- ОК-11 - способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
- ОК-12 - способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;
- ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;
- ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;
- ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности;
- ПК-27 - способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых

программно-аппаратных, криптографических и технических средств защиты информации.

3. Теоретическая часть

Данное 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: $Y = (Y_1 + Y_2) / 20$ (1).

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 – **маловероятно (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 (1). Получаем Y=0.25 и определяем, что Y лежит в промежутке между 0 и 0.3, а, значит, возможность реализации угрозы признается **низкой**. Далее экспертным путём

оцениваем опасность угрозы как **среднюю** - реализация угрозы может привести к негативным последствиям для субъектов персональных данных. Исходя из возможности реализации угрозы (низкая) и показателя опасности угрозы (средняя) делаем вывод, что данная угроза является неактуально для ИСПДн.

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 защиты	0,25	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)	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 внешними нарушителями	0,25	низкая
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

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом работы

Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время

работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;
- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы)

Определить коэффициент реализуемости угрозы (*Y*) и возможности реализации

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. Контрольные вопросы и тестовые задания

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?

Выберите правильный ответ

Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц – это…

а) распространение персональных данных;
б) предоставление персональных данных ;
в) блокирование персональных данных; г)
искажение персональных данных.

Выберите правильный ответ

Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) – это…

а) распространение персональных данных;
б) предоставление персональных данных;
в) блокирование персональных данных; г)
искажение персональных данных.

Лабораторная работа №5.

Тема: «Определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

1. Цель работы

Целью Лабораторной работы 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. Формируемые компетенции или их части

- ОК-7 - способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;
- ОК-8 - способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
- ОК-9 - способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
- ОК-10 - способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
- ОК-11 - способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

- ОК-12 - способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;
- ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;
- ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;
- ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности;
- ПК-27 - способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

3. Теоретическая часть

Данное 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.

Осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 7.

Таблица 7 Правила отнесения угрозы безопасности ПДнк 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

Пример обобщенного списка актуальных угроз в ИСПДн представлен в таблице 8.

Таблица 8. Обобщенный список актуальных угроз в ИСПДн

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, лицами не допущенными к ее обработке	**актуальная**
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.

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом

работы Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время

работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;
- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы)

Определить актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. Контрольные вопросы и тестовые задания

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?

Выберите правильный ответ

Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных – это…

а) уничтожение персональных данных;
б) предоставление персональных данных;
в) блокирование персональных данных; г)
искажение персональных данных.

Выберите правильный ответ

Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных – это…

а) уничтожение персональных данных; б)
обезличивание персональных данных; в)
блокирование персональных данных; г)
искажение персональных данных.

Лабораторная работа №6.

Тема: «Определение типа актуальной угрозы».

1. Цель работы

Целью Лабораторной работы 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. Формируемые компетенции или их части

- ОК-7 - способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;
- ОК-8 - способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
- ОК-9 - способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
- ОК-10 - способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
- ОК-11 - способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
- ОК-12 - способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

− ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;

− ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

− ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности;

− ПК-27 - способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

3. Теоретическая часть

Данное 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".

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;

- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом работы

Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время работы

Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;
- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы).

На данном практическом занятии студенты выполняют следующие задания:

6.1. 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".

6.2. 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.

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. 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…

Лабораторная работа №7.

Тема: «Определение уровня защищенности ПДн».

1. Цель работы

Целью Лабораторной работы 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. Формируемые компетенции или их части

- ОК-7 - способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;
- ОК-8 - способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
- ОК-9 - способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
- ОК-10 - способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
- ОК-11 - способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
- ОК-12 - способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

− ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;

− ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

− ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности;

− ПК-27 - способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

3. Теоретическая часть

Данное задание предполагает использование документа Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 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.

Таблица 9. Определение уровня защищенности ПДн

Тип ИСПДн	**Категории субъектов**	**Количество субъектов**	**Тип актуальной угрозы**		
			1	**2**	**3**
ИСПДн–С	**Не сотрудников**	**> 100 000**	**1**	**1**	**2**
		< 100 000	**1**	**2**	**3**
	Сотрудников	**> 100 000**	**1**	**2**	**3**
		< 100 000	**1**	**2**	**3**
ИСПДн – Б	**Не сотрудников**	**> 100 000**	**1**	**2**	**3**
		< 100 000	**1**	**2**	**3**
	Сотрудников	**> 100 000**	**1**	**2**	**3**
		< 100 000	**1**	**2**	**3**
ИСПДн – И	**Не сотрудников**	**> 100 000**	**1**	**2**	**3**
		< 100 000	**1**	**3**	**4**
	Сотрудников	**> 100 000**	**1**	**3**	**4**
		< 100 000	**1**	**3**	**4**
ИСПДн – О	**Не сотрудников**	**> 100 000**	**2**	**2**	**4**
		< 100 000	**2**	**3**	**4**
	Сотрудников	**> 100 000**	**2**	**3**	**4**
		< 100 000	**2**	**3**	**4**

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими

выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом работы

Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время

работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;
- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы).

На данном занятии студенты выполняют следующие задания:

6.1. 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".

6.2. По Таблице 9 определяют уровень защищенности ПДн в зависимости от типа актуальной угрозы, типа ИСПДн, категории субъектов и количества субъектов.

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. 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?

Выберите правильный ответ

Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных – это…

а) специальные категории персональных данных;
б) биометрические персональные данные; в) общедоступные персональные данные; г) иные категории персональных данных.

Выберите правильный ответ

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 – это…

а) специальные категории персональных данных;
б) биометрические персональные данные; в) общедоступные персональные данные; иные категории персональных данных.

Лабораторная работа №8.

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

1. Цель работы

Целью Лабораторной работы 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. Формируемые компетенции или их части

- ОК-7 - способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;
- ОК-8 - способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
- ОК-9 - способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
- ОК-10 - способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
- ОК-11 - способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
- ОК-12 - способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;
- ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;
- ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации

проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

− ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности;

− ПК-27 - способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

3. Теоретическая часть

Данное 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.

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом работы Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;
- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;

- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы).

На данном занятии студенты выполняют следующие задания:

6.1. Изучают документ 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".

6.2. 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) 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);

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.

Пример:

Таблица 10. Базовый набор мер по актуальным угрозам.

Актуальная угроза	**Меры по противодействию угрозе**	
	Технические	**Организационные**
Воздействие вредоносных программ (вирусов)	Применение средств антивирусной защиты	- Инструкция администратора безопасности - Инструкция пользователя Регламентация процесса обработки ПДн - Инструкция по антивирусной защите - Обновление САВЗ
Утрата ключей и атрибутов доступа	Настройка и выбор режимов средств управления доступом	- Порядок восстановления ключей (раздел Положения) - Инструкция администратора безопасности - Инструкция пользователя (санкции) - Резервное копирование

Угрозы выявления паролей по сети.	Межсетевое экранирование	- Инструкция адмиин-ра безопасности - Инструкция пользователя - Выбор настроек МЭ в соответствии с угрозами
Угрозы внедрения по сети вредоносных программ.	Применение средств антивирусной защиты	- Инструкция администратора безопасности - Инструкция пользователя - Регламентация процесса обработки ПДн - Акт установки СЗИ
Угроза установки ПО, не связанного с исполнением сл. обязанностей	Настройка и выбор режимов средств контроля и управления доступом	- Инструкция пользователю (санкции) - Инструкция администратора безопасности - Периодический контроль.

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. Контрольные вопросы и тестовые задания

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?

Выберите правильный ответ

Персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных" – это…

а) специальные категории персональных данных;
б) биометрические персональные данные; в)
общедоступные персональные данные; г) иные
категории персональных данных.

Выберите правильный ответ

Сколько мер входит в состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий?

а) 14
б) 12
в) 15
г) 13

Лабораторная работа №9.

Тема: «Составление акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных»

1. Цель работы

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

2. Формируемые компетенции или их части

- ОК-7 - способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной

безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

- ОК-8 - способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
- ОК-9 - способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
- ОК-10 - способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
- ОК-11 - способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
- ОК-12 - способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;
- ПК-1 - способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности ;
- ПК-2 - способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;
- ПК-3 - способностью использовать нормативные правовые документы в своей профессиональной деятельности;
- ПК-27 - способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых

программно-аппаратных, криптографических и технических средств защиты информации.

3. Теоретическая часть

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа; ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или)
- обрабатываются персональные данные (далее - машинные носители персональных
- данных);
- регистрация событий безопасности; антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных; защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных; выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению

функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в

информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных

сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

4. Оборудование и материалы

Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 15 шт., объединенными в локальную сеть и имеющими выход в Интернет. Программное обеспечение: Microsoft Office System 2007, 2010.

5. Указания по технике безопасности

5.1. Общие требования безопасности

К работе на персональном компьютере допускаются лица, прошедшие обучение безопасным методам труда, вводный инструктаж, первичный инструктаж на рабочем месте.

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

- повышенный уровень электромагнитных излучений;
- повышенный уровень статического электричества;
- пониженная ионизация воздуха;
- статические физические перегрузки;
- перенапряжение зрительных анализаторов.

Работник обязан:

Выполнять только ту работу, которая определена его должностной инструкцией.

Содержать в чистоте рабочее место.

Женщины со времени установления беременности и в период кормления грудью к выполнению всех видов работ, связанных с использованием компьютеров, не допускаются.

За невыполнение данной Инструкции виновные привлекаются к ответственности согласно правилам внутреннего трудового распорядка или взысканиям, определенным Кодексом законов о труде Российской Федерации.

5.2. Требования безопасности перед началом работы Подготовить рабочее место.

Проверить правильность подключения оборудования к электросети.

Проверить исправность проводов питания и отсутствие оголенных участков проводов.

Убедиться в наличии заземления системного блока, монитора и защитного экрана.

Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Проверить правильность установки стола, стула, угла наклона экрана, положение клавиатуры, положение "мыши", при необходимости произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

5.3. Требования безопасности во время работы Работнику при работе на ПК запрещается:

- прикасаться к задней панели системного блока (процессора) при включенном питании;
- переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;
- допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;

- производить самостоятельное вскрытие и ремонт оборудования;
- работать на компьютере при снятых кожухах;
- отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Продолжительность непрерывной работы с компьютером без регламентированного перерыва не должна превышать 2-х часов.

Во время регламентированных перерывов с целью снижения нервно - эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления выполнять комплексы упражнений.

5.4. Требования безопасности в аварийных ситуациях.

Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

Не приступать к работе до устранения неисправностей.

При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь.

5.5. Требования безопасности по окончании работы.

Отключить питание компьютера.

Привести в порядок рабочее место.

Выполнить упражнения для глаз и пальцев рук на расслабление.

6. Задания (указания по порядку выполнения работы).

На данном занятии студенты составляют итоговый документ в виде модели защиты с составом и содержанием мер по обеспечению безопасности ПДн. Согласно формы для заполнения, см. приложение 4, составить акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных.

7. Содержание отчёта и его форма

Отчёт выполняется каждым студентом индивидуально. Содержание и формы отчёта приведены в Приложении 3.

8. Контрольные вопросы

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

2) В каких случаях применяются компенсирующие меры?

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

Выберите правильный ответ

Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам – это…

а) Обладатель информации;
б) оператор информационной системы;
в) субъект персональных данных; г)
объект персональных данных.

Выберите правильный ответ

Информационные системы включают в себя:

а) государственные информационные системы;
б) муниципальные информационные системы;
в) иные информационные системы;
типовые информационные системы.

СПИСОК ЛИТЕРАТУРЫ

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. «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. №. 55/86/20

4. Приказа 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

Приложение 1

Общие исходные данные для расчётов:

−Персональные данные - *не общедоступные*

−Наличие подключений ИСПДн к сетям связи общего пользования/сетям МИО - *имеющие подключение*.

−*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	Не сотрудников	>100 000
2	ПДн–И	локальная	Сотрудников	>100 000
3	ПДн–О	автономная	Не сотрудников	>100 000
4	ПДн–Б	автономная	Сотрудников	>100 000
5	ПДн–И	локальная	Не сотрудников	< 100 000
6	ПДн–И	распределенная	Сотрудников	< 100 000
7	ПДн–Б	автономная	Не сотрудников	< 100 000
8	ПДн–И	распределенная	Сотрудников	< 100 000
9	ПДн–О	автономная	Не сотрудников	< 100 000
0	ПДн–Б	локальная	Сотрудников	< 100 000

Приложение 3

Лабораторная работа должна быть оформлена в электронном виде и на листах формата А4.

На титульном листе указывается фамилия, имя, отчество, наименование работы, вариант, курс, группа и домашний адрес, согласно образцу Титульного листа.

Титульный лист лабораторной работы

Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
Северо-Кавказский федеральный университет
Институт сервиса туризма и дизайна (филиал) СКФУ в г. Пятигорске Кафедра

Комплексной защиты информации и стандартизации

ЛАБОРАТОРНАЯ РАБОТА
по курсу
«Организация защиты персональных данных»

Вариант № _____

Выполнил:
студент _____ курса_____ группы
_____факультета
_____
(Ф.И. О. студента разборчиво)

Проверил:
_____
(Ф.И. О. преподавателя)
_____
(подпись)

«_____» _____
(дата)

г. Пятигорск 2014

Форма для заполнения

Приложение 4

к распоряжению «О проведении работ по защите персональных данных _____ «Xxxxx» от «___»_____ 20____г. № _____

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

201_г.

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 __._____.201_г. №___., в составе:

Председатель:

_____	_____
Должность	ФИО

Члены комиссии:

_____	_____
Должность	ФИО
_____	_____
Должность	ФИО
_____	_____
Должность	ФИО

2. АКТ ОПЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИСПДн «СОТРУДНИКИ (НЕ СОТРУДНИКИ)»

В ходе работы комиссия установила:

1) категория персональных данных – иные;

2) обрабатываются персональных данных сотрудников (не 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:

_____ _____
подпись ФИО

Члены комиссии:

_____ _____
подпись ФИО

_____ _____
подпись ФИО

_____ _____
подпись ФИО

Учебное пособие (лабораторный практикум)

Авторы: Анатолий Михайлович Макаров,
Игорь Владимирович Калиберда,
Карина Овиковна Бондаренко

Редактор: Карина Овиковна Бондаренко