ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Кафедра «Инфокоммуникационные технологии и системы связи»

Методические указания к выполнению практических занятий

по дисциплине
«Защита персональных данных»

для студентов по направлению подготовки
11.03.02 Инфокоммуникационные технологии и системы связи
профиль «**Защищенные инфокоммуникационные системы**» квалификации бакалавр

Ростов-на-Дону
2019

УДК

Составители: доцент кафедры ИТСС Борисов Б.П.

Данное методическое пособие предназначено для обеспечения проведения практических занятий со студентами направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи, профиля «**Защищенные инфокоммуникационные системы**» квалификации «бакалавр.

Пособие обеспечивает получение практических навыков по основополагающим вопросам изучаемой дисциплины.

Объем методического пособия определен программой по дисциплине «Защита персональных данных».

Рецензент: Зав. кафедрой ИТСС, к.т.н., доцент Юхнов В.И.

Методическое пособие рассмотрено и утверждено на заседании кафедры ИТСС «26» августа 2019 г. Протокол № 1.

СОДЕРЖАНИЕ

1 Организация и проведение практических занятий

Цели практических занятий:

- помочь обучающимся систематизировать, закрепить и углубить знания теоретического характера;
- научить студентов приемам решения практических задач, способствовать овладению навыками и умениями выполнения расчетов, графических и других видов заданий;
- научить их работать с книгой, служебной документацией и схемами, пользоваться справочной и научной литературой;
- формировать умение учиться самостоятельно, т.е. овладевать методами, способами и приемами самообучения, саморазвития и самоконтроля.

Практические занятия — метод репродуктивного обучения, **обеспечивающий связь теории и практики, содействующий выработке у** студентов умений и навыков применения знаний, полученных на лекции и в ходе самостоятельной работы.

Практические занятия играют важную роль в выработке у студентов навыков применения полученных знаний для решения практических задач совместно с преподавателем.

Структура практических занятий:

1. Вступление преподавателя – 5мин.
2. Ответы на вопросы студентов по неясному материалу – до 10 мин. вначале и далее по мере необходимости.
3. Практическая часть – до 160 мин.
4. Заключительное слово преподавателя – до 5мин.

Практические занятия представляют собой занятия по решению различных прикладных задач, теоритический материал для которых был дан на лекциях. В итоге у каждого обучающегося должен быть выработан определенный профессиональный подход к решению каждой задачи и интуиция. На практические занятия выносятся четыре задачи. Преподаватель стремится к тому, чтобы занятие давало целостное представление о предмете и методах изучаемой дисциплине, причем методическая функция выступает здесь в качестве ведущей.

Практическое занятие № 1

Тема: Защита персональных данных в нормативно-правовых актах РФ

Задание:

1. Составить перечень нормативно-правовых актов РФ.
2. Конституция РФ о защите персональных данных.
3. Защита персональных данных в трудовом кодексе РФ.
4. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

Исходные данные:

Персональные данные (ПДн) — любая информация, относящаяся прямо или косвенно к абсолютно любому человеку, которая предоставляется другому человеку или организации людей, сугубо по желанию человека, чьи данные интересуют тех или иных (субъекту персональных данных).

Субъект персональных данных — физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Содержание и оформление отчета

Отчет должен содержать:

1. Краткое содержание вопросов защиты персональных данных в нормативно-правовых актах РФ представленных в виде реферата
2. Выводы.

Контрольные вопросы:

1. Правовое и нормативное обеспечение защиты ПДн.
2. Назначение и средства антивирусной защиты.
3. Категории ПДн.
4. Назначение и средства идентификации и аутентификации субъектов.
5. Контролирующие органы в области ПДн, их функции.
6. Назначение и способы ограничения программной среды.
7. Мероприятия по обеспечению защиты ПДн при их обработке в информационных системах ПДн.

8. Согласие субъекта на обработку ПДн.

9. Назначение и способы физической защиты технических средств компьютерной системы.

Список рекомендованных источников

1. "Конституция Российской Федерации" (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ).

2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015).

3. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 16.12.2019).

4. А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. Защита информации: Учебное пособие / - 2-е изд. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.

Практическое занятие № 2

Тема: Административная ответственность за нарушение требований по обращению с персональными данными

Задание:

1. Безопасность обработки персональных данных.
2. Ответственность в Кодекс об Административных Правонарушениях Российской Федерации за нарушение требований ФЗ «О персональных данных».

Исходные данные:

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Содержание и оформление отчета

Отчет должен содержать:

1. Тему, постановку задачи.
2. Действия оператора по:
- автоматизированной обработке персональных данных;
- распространению персональных данных;
- блокированию персональных данных;
- уничтожению персональных данных;
- обезличиванию персональных данных;
- трансграничной передаче персональных данных.
3. Выводы.

Контрольные вопросы:

1. Документы определяющие административную ответственность за нарушение требований по обращению с персональными данными.
2. Назначение и способы обеспечения доступности персональных данных.

3. Назначение выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них.

4. Условия обработки персональных данных.

5. Назначение средств обнаружения (предотвращения) вторжений.

Список рекомендованных источников

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015).

2. А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. Защита информации: Учебное пособие / - 2-е изд. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.

3. Е.Б. Белов и др. Основы информационной безопасности: Учебное пособие для вузов / Горячая линия-Телеком, 2011. - 558 с.

Практическое занятие № 3

Тема: Разграничение прав доступа в информационных системах персональных данных

Задание:

1. Структура механизмов разграничения доступа в информационной системе персональных данных.

2. Реализация механизмов разграничения доступа в информационной системе персональных данных.

Исходные данные:

1. Группа/должность

2. Уровень доступа к ПДн.

3. Разрешенные действия.

4. Оператор по обработке ПДн.

Содержание и оформление отчета

Отчет должен содержать:

1. Тему, постановку задачи.

2. Положение о разграничении прав доступа в государственной информационной системе персональных данных

3. Выводы

Контрольные вопросы:

1. Информация как объект правовой защиты.

2. Раскройте понятие "информационное общество" и дайте его основные признаки?

3. Какими документами на международном уровне регулируется вопрос о защите персональных данных?

4. Какими основными законодательными актами регулируется вопрос защиты персональных данных на территории Российской Федерации?

5. Перечислите основные положения Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных".

6. Понятие и состав персональных данных. Что относится к специальным категориям персональных данных?

7. Понятие оператора персональных данных. Его основные права и обязанности.

8. Субъект персональных данных: понятие, права и обязанности.

9. При каком условии оператор персональных данных может начать осуществлять обработку персональных данных?

Список рекомендованных источников

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015).

2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016)

3. А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. Защита информации: Учебное пособие / - 2-е изд. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.

4. Е.Б. Белов и др. Основы информационной безопасности: Учебное пособие для вузов / Горячая линия-Телеком, 2011. - 558 с.

Практическое занятие № 4

Тема: Нормативно-правовой подход к защите информационной системы персональных данных

Задание:

1. Аттестации информационной системы обработки персональных данных.

2. Подготовка пакета документов, необходимого для аттестации информационной системы персональных данных.

Исходные данные:

1. Требования к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ Р 51583 (Порядок создания АС в защищенном исполнении. Общие положения) и ГОСТ Р 51624 (АС в защищенном исполнении. Общие требования).

2. ГОСТ 34.601 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы.

Содержание и оформление отчета

Отчет должен содержать:

1. Требования к защите информации, содержащейся в информационной системе.

2. Пакет документов, необходимых для аттестации информационной системы персональных данных.

3. Выводы.

Контрольные вопросы:

1. Какие документы по защите и обработке персональных данных должны быть, опубликованы на официальном сайте государственного или муниципального органа в соответствии с положениями постановления Правительства РФ от 21.03.2012 N 211?

2.Какие виды ответственности предусмотрены действующим законодательством Российской Федерации за нарушения существующих требований по защите персональных данных?

3. Какие виды ответственности предусмотрены действующим законодательством Российской Федерации за нарушения существующих требований по обработке персональных данных?

4. Какая ответственность предусмотрена за нарушение трудового законодательства Российской Федерации в части персональных данных?

5. Какая ответственность предусмотрена за нарушение гражданского кодекса Российской Федерации в части персональных данных?

6. Какие документы являются обязательными при организации системы защиты персональных данных?

Список рекомендованных источников

1. Федотова Е.Л. - Информационные технологии и системы: учеб. пособие. - М.: ИД «ФОРУМ»: ИНФРА-М, 2009. - 352 с.: ил. - (Профессиональное образование).

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоиздат, 1994.

3. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119)

4. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17

Практическое занятие № 5

Тема: Классификация информационных систем персональных данных

Задание:

1.Определение уровня защищённости информационных систем персональных данных.

2. Исследование классов систем.

Исходные данные:

1. Категории и объем накапливаемых, обрабатываемых и распределяемых с их использованием ПДн.

2. Требованиями к защите ПДн при их обработке в информационных системах (Утв. Постановлением Правительства № 1119 от 01.11.2012).

Содержание и оформление отчета

Отчет должен содержать:

1. Тему, постановку задачи.

2. Требованиями к защите ПДн при их обработке в информационных системах и уровни защищенности.

3. Выводы.

Контрольные вопросы:

1. Какие информационные системы называют типовыми?

2. Какие информационные системы называют специальными?

3. Какие категории ИСПД выделяют в зависимости от объема обрабатываемых в ИСПД данных?

4. Что определяется на основе частной модели угроз организации в соответствии с методическими документами ФСТЭК?

5. Когда может быть пересмотрен класс ИСПД ?

6. Как оформляется результат классификации ИСПД?

7. От чего должна быть защищена информационная система при обработке персональных данных в ней?

8. В чем заключается построение частной модели угроз организации?

9. Какие мероприятия применяют для исключения утечки через ПЭМИН в ИСПД 1 класса?

Список рекомендованных источников

1. Федотова Е.Л. - Информационные технологии и системы: учеб. пособие. - М.: ИД «ФОРУМ»: ИНФРА-М, 2009. - 352 с.: ил. - (Профессиональное образование).

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоиздат, 1994.

3. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119)

4. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17

Практическое занятие № 6

Тема: Модель угроз для информационных систем персональных данных

Задание:

1. Разработка модели угроз для информационных систем персональных данных.

2. Разработка частной модели угроз информационной системы персональных данных.

Исходные данные:

1. Угрозы утечки информации по техническим каналам.

2. Угрозы НСД к ПДн, обрабатываемым в автоматизированном рабочем месте.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008).

Содержание и оформление отчета

Отчет должен содержать:

1. Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Модель злоумышленника информационных систем персональных данных.

3. Выводы

Контрольные вопросы:

1. Существуют ли временные ограничения на обработку персональных данных?

2. В каких случаях оператор персональных данных не может осуществлять обработку персональных данных?

3.Дайте определение понятию «Нарушитель информационной безопасности».

4. Какие типы нарушителей информационной безопасности существуют согласно действующим правилам разграничения доступа к информации?

5. На сколько категорий делится внутренний нарушитель информационной безопасности и по каким критериям?

6. Какими возможностями обладают лица, отнесенные к первой категории внутренних нарушителей?

7. Что такое информационная система персональных данных?

8. Что такое модель угроз безопасности персональных данных?

9.Какими возможностями обладает Федеральная Служба Безопасности Российской Федерации в части решения вопросов по защите и обработке персональных данных?

10. Какими возможностями обладает Федеральная Служба Технического и Экспертного Контроля Российской Федерации в части решения вопросов по защите и обработке персональных данных?

Список рекомендованных источников

1. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119).

2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну содержащихся в государственных информационных системах».

4. Приказ ФСБ России от 10.07. 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»

Практическое занятие № 7

Тема: Организация и обеспечение режимов защиты персональных данных

Задание:

1. Организация защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.
2. Обеспечение защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.

Исходные данные:

1. Жизненный цикл персональных данных.
2. Локальная сеть передачи данных

Содержание и оформление отчета

Отчет должен содержать:

1. Мероприятия и их характеристика по организации защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.
2. Обязанности оператора по обеспечению безопасности персональных данных.
3. Выводы.

Контрольные вопросы:

1. Особенности гарантированного уничтожения информации на полупроводниковых носителях с использованием термических воздействий.
2. Перечислить и описать угрозы безопасной передачи данных в телекоммуникационных системах.
3. Перечислить и описать задачи защиты информации в телекоммуникационных системах.
4. Перечислить и описать механизмы защиты информации в телекоммуникационных системах.

5. Физический уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

6. Канальный уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

7. Сетевой уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

8. Транспортный уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

9. Сеансовый уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

10. Уровень представления модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

11. Прикладной уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

12. Структура семиуровневой модели OSI с примерами протоколов на каждом уровне.

Список рекомендованных источников

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015).

2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016)

3. А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. Защита информации: Учебное пособие / - 2-е изд. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.

4. Е.Б. Белов и др. Основы информационной безопасности: Учебное пособие для вузов / Горячая линия-Телеком, 2011. - 558 с.

Практическое занятие № 8

Тема: Оценка эффективности систем защиты информационных систем персональных данных

Задание:

1. Определение эффективности систем защиты информационных систем персональных данных.
2. Оценка эффективности систем защиты информационных систем персональных данных.

Исходные данные:

1. Требования к мерам защиты информации, реализуемые в рамках системы ЗПДн

Содержание и оформление отчета

Отчет должен содержать:

1. Анализ требований по защите персональных данных, обрабатываемых в информационных системах.
2. Критерии оценки эффективности системы защиты персональных данных.
3. Оценку эффективности системы защиты персональных данных в сети передачи данных.
4. Выводы.

Контрольные вопросы:

1. Что разрабатывается в случае выявления несоответствия ИСПД установленным требованиям?
2. Метод с установлением логического соединения. Схема и описание. Пример протокола, использующего метод.
3. Адресация в сетях. IP-адрес, IP-порт и MAC-адрес. Назначение, структура адресов. Специальные и фиктивные IP-адреса.
4. IP-сети класса A. Характеристика класса: диапазон IP-адресов, идентификатор сети, граница «сеть-узел», количество сетей и узлов.

5. IP-сети класса B. Характеристика класса: диапазон IP-адресов, идентификатор сети, граница «сеть-узел», количество сетей и узлов.

6. IP-сети класса C. Характеристика класса: диапазон IP-адресов, идентификатор сети, граница «сеть-узел», количество сетей и узлов.

7. Межсетевое экранирование. Принципы межсетевого экранирования.

8. Виды и варианты подключения межсетевых экранов.

9. Назовите последовательность испытания ИСПД на соответствие требованиям по защищенности ПД от угроз безопасности ПД?

10. Назовите порядок оценки соответствия ИСПД организационно-техническим требованиям по защите ПД?

Список рекомендованных источников

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 6-е изд. Спб.: Питер, 2016.

2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016).

3. Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (с изменениями и дополнениями от 21 октября 2008 г., 14 января 2011 г., 1, 25 июля 2014 г., 22 мая 2015 г.

4. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой Технические, организационные и кадровые аспекты управления информационной безопасно-стью: Учебное пособие для вузов / М.: Гор. линия-Телеком, 2013. - 214 с.

5. В.В. Бухтояров, В.Г. Жуков, В.В. Золотарев Поддержка принятия решений при проектировании систем защиты информации: Монография / М.: НИЦ ИНФРА-М, 2018. - 131 с.