МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Н.В. Калинина
31 августа 2022 г

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНЫХ РАБОТ

по учебной дисциплине
ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)
квалификация
техник по защите информации
среднего профессионального образования

СПбГУТ))) **Документ подписан простой электронной подписью**

Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

Санкт-Петербург
2022

ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Методические указания по выполнению самостоятельных работ.

Составил: Н.В. Кривоносова. – Санкт-Петербург, 2022.

Методические указания содержат описания самостоятельных работ, предусмотренных рабочей программой ОП.04 Основы информационной безопасности. Количество внеурочных самостоятельных работ 10, общий объём составляет 20 часов. Методические указания предназначены для обучающихся очной формы обучения по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Рассмотрено и одобрено предметной (цикловой) комиссией обеспечения информационной безопасности телекоммуникационных систем Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля

Содержание

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Самостоятельные работы разработаны в рамках рабочей программы учебной дисциплины «Информатика» являющейся частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Учебная дисциплина ЕН.04 Обеспечение информационной безопасности обеспечивает формирование общих компетенций по всем видам деятельности ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 09	Использовать информационные технологии в профессиональной деятельности

ПК 1.3	Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей.
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.
ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.

2. ПЕРЕЧЕНЬ САМОСТОЯТЕЛЬНЫХ РАБОТ

№	Наименование	Часы
1	Работа в программе Консультант Плюс. Работа со статьями ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации».	2ч.
2	Работа с требованиями по надзору ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации».	2ч.
3	Работа со статьями ФЗ № 152-ФЗ «О персональных данных». Изучение порядка работы с персональными данными работника.	2ч.
4	Изучение мер по обеспечению безопасности персональных данных при их обработке в ИСПДн. Изучение методов	2ч.

	обезличивания персональных данных.	
5	Подготовка документа для вида осуществления деятельности по технической защите конфиденциальной информации согласно, требований ФСТЭК	2ч.
6	Подготовка документа для вида осуществления деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) согласно требований ФСБ. Подготовка документа для вида осуществления деятельности по распространению шифровальных (криптографических) средств согласно требований ФСТЭК.	2ч.
7	Работа с риск-подходами к моделированию угроз ИБ. Разработка моделей угроз безопасности в информационных системах персональных данных (ИСПДн)	2ч.
8	Реализация модели угроз безопасности персональных данных при их обработке в информационных системах.	2ч.
9	Проведение анализа сетевых ресурсов организации. Проведение анализа сотрудников организации с точки зрения информационный безопасности	2ч.
10	Работа с основными понятиями служебной тайны.	2ч.

Самостоятельная работа № 1
ТЕМА: РАБОТА В ПРОГРАММЕ КОНСУЛЬТАНТ ПЛЮС. РАБОТА СО СТАТЬЯМИ ФЗ № 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»..

1. **Цель (и) работы**: изучение и овладение навыками работы с программой Консультант Плюс, а также ознакомление с основными статьями ФЗ № 149-ФЗ, регулирующими вопросы информации, информационных технологий и защиты информации..

2. **Задачи:**
   - Изучение основных возможностей программы Консультант Плюс.
   - Поиск и анализ статей ФЗ № 149-ФЗ, касающихся информации, информационных технологий и защиты информации.
   - Ознакомление с требованиями нормативных и правовых документов по информационной безопасности РФ.
   - Составление рекомендаций по защите информации объекта информатизации в соответствии с требованиями ФЗ № 149-ФЗ.

3. **Подготовка к работе и порядок выполнения:**
   - Изучить предложенную литературу;
   - Изучить основные возможности программы Консультант Плюс.
   - Найти и ознакомиться с тремя статьями ФЗ № 149-ФЗ, касающимися информационной безопасности.
   - Составить список требований по защите информации объекта информатизации, основываясь на найденных статьях.
   - Составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчета и поиск информации.

5. **Критерии оценки**

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них
- Наличие анализа и выводов на основе представленной информации

Оценка 4 –
- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения

- Грамотное использование терминов и понятий, но с некоторыми неточностями
- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

ФЗ № 149-ФЗ "Об информации, информационных технологиях и о защите информации" устанавливает правовые основы в области информационной безопасности в Российской Федерации. Закон определяет права и обязанности субъектов информационных отношений, регулирует отношения, связанные с использованием информационных технологий, и устанавливает меры по защите информации.

Программа Консультант Плюс представляет собой средство автоматизации работы с нормативными документами и законодательством. В ней можно найти тексты нормативных актов, анализы и комментарии к ним, что упрощает работу со статьями ФЗ № 149-ФЗ.

Самостоятельная работа № 2
ТЕМА: РАБОТА С ТРЕБОВАНИЯМИ ПО НАДЗОРУ ФЗ № 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ».

1. **Цель (и) работы**: ознакомление с требованиями по надзору ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и изучение процедуры работы с ними.

2. **Задачи:**
   - Изучение основных требований ФЗ № 149-ФЗ к объектам информатизации.
   - Ознакомление с процедурой прохождения надзора по требованиям ФЗ № 149-ФЗ.
   - Определение необходимых мер для обеспечения соответствия объекта информатизации требованиям ФЗ № 149-ФЗ.
   - Практическое применение полученных знаний при составлении плана мероприятий по обеспечению защиты информации на объекте информатизации.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - ознакомиться с текстом ФЗ № 149-ФЗ и выделить основные требования к объектам информатизации, а также процедуру прохождения надзора по требованиям ФЗ.
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить составление отчета и поиск информации.

5. **Критерии оценки**

Оценка 5 –
   - Исчерпывающее изложение темы
   - Четкая логика и последовательность изложения материала
   - Грамотное и точное использование терминов и понятий
   - Использование достаточного количества источников и ссылок на них
   - Наличие анализа и выводов на основе представленной информации

Оценка 4 –
   - Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
   - Грамотное использование терминов и понятий, но с некоторыми неточностями
   - Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
   - Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает требования к защите информации, которые должны быть выполнены объектами информатизации в России. Кроме того, ФЗ устанавливает процедуру прохождения надзора по требованиям ФЗ, которая предусматривает проверку соответствия объекта информатизации установленным требованиям, а также выявление и устранение нарушений в области защиты информации. Знание требований и процедуры надзора по ФЗ № 149-ФЗ необходимо для организации и обеспечения защиты информации на объекте информатизации в соответствии с законодательством РФ.

Самостоятельная работа № 3
ТЕМА: РАБОТА СО СТАТЬЯМИ ФЗ № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ». ИЗУЧЕНИЕ ПОРЯДКА РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКА

1. **Цель (и) работы**: ознакомиться с требованиями ФЗ № 152-ФЗ «О персональных данных» и порядком работы с персональными данными работников.
2. **Задачи:**
   - Изучить основные положения ФЗ № 152-ФЗ «О персональных данных».
   - Определить, какие персональные данные работников подпадают под действие закона.
   - Изучить порядок работы с персональными данными работников в организации.
   - Определить меры по защите персональных данных работников.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - изучить статьи ФЗ № 152-ФЗ «О персональных данных», относящиеся к работе с персональными данными работников, и определить основные требования к работе с такими данными.
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчетов и поиск информации.

5. **Критерии оценки**

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них
- Наличие анализа и выводов на основе представленной информации

Оценка 4 –
- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
- Грамотное использование терминов и понятий, но с некоторыми неточностями
- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

ФЗ № 152-ФЗ «О персональных данных» устанавливает требования к обработке персональных данных, включая персональные данные работников. Работодатель обязан обеспечить защиту персональных данных работников и соблюдать порядок работы с такими данными. Для этого необходимо определить, какие персональные данные подпадают под действие закона, какие меры необходимо предпринимать для их защиты и какие правила необходимо соблюдать при обработке таких данных.

Самостоятельная работа № 4

ТЕМА: ИЗУЧЕНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН. ИЗУЧЕНИЕ МЕТОДОВ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ. ПОДГОТОВКА ДОКУМЕНТА ДЛЯ ВИДА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СОГЛАСНО, ТРЕБОВАНИЙ ФСТЭК.

1. **Цель (и) работы**: изучение мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДН) и подготовка документа для видов деятельности по технической защите конфиденциальной информации согласно требованиям ФСТЭК.

2. **Задачи:**
   - изучение методов обезличивания персональных данных;
   - изучение мер по обеспечению безопасности персональных данных при их обработке в ИСПДН;
   - подготовка документа для видов деятельности по технической защите конфиденциальной информации согласно требованиям ФСТЭК.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - Разработать презентацию на тему "Меры по обеспечению безопасности персональных данных при их обработке в ИСПДН", включающую следующие разделы:
     - Определение понятия персональных данных и ИСПДН;
     - Методы обезличивания персональных данных;
     - Меры по обеспечению безопасности персональных данных в ИСПДН;
     - Практические примеры реализации мер по обеспечению безопасности персональных данных в ИСПДН;
     - Требования ФСТЭК по технической защите конфиденциальной информации.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчета и поиск информации.

5. **Критерии оценки**

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них

- Наличие анализа и выводов на основе представленной информации

Оценка 4 –

- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
- Грамотное использование терминов и понятий, но с некоторыми неточностями
- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

Персональные данные - любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных). ИСПДН - это информационная система, в которой осуществляется обработка персональных данных.

Методы обезличивания персональных данных включают анонимизацию, псевдонимизацию и шифрование.

Меры по обеспечению безопасности персональных данных в ИСПДН включают организационные, технические и юридические меры. Организационные меры включают установление правил доступа к персональным данным, контроль за обработкой персональных данных и обучение персонала. Технические меры включают использование средств защиты информации, контроль за доступом к информационной системе, контроль целостности данных и др. Юридические меры включают заключение договоров на обработку персональных данных и определение ответственных

Самостоятельная работа № 5
ТЕМА: ПОДГОТОВКА ДОКУМЕНТА ДЛЯ ВИДА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СОГЛАСНО, ТРЕБОВАНИЙ ФСТЭК

1. **Цель (и) работы**: подготовка документа для вида деятельности по технической защите конфиденциальной информации в соответствии с требованиями ФСТЭК..

2. **Задачи:**
   - Изучение требований ФСТЭК к документу для вида деятельности по технической защите конфиденциальной информации.
   - Сбор и анализ информации об объекте информатизации, который нуждается в защите конфиденциальной информации.
   - Определение угроз безопасности информации и разработка мер по их предотвращению.
   - Определение требований к системе защиты информации и выбор необходимых технических средств защиты.
   - Разработка документа для вида деятельности по технической защите конфиденциальной информации в соответствии с требованиями ФСТЭК.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - Собрать информацию о любом объекте информатизации (например, банковская система, интернет-магазин, государственный сайт) и определить угрозы безопасности информации, а также предложить меры по их предотвращению.
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчетов и поиск информации.

5. **Критерии оценки**

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них
- Наличие анализа и выводов на основе представленной информации

Оценка 4 –
- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения

- Грамотное использование терминов и понятий, но с некоторыми неточностями
- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

Документ для вида деятельности по технической защите конфиденциальной информации является обязательным требованием для организаций и предприятий, которые работают с конфиденциальной информацией. Он должен соответствовать требованиям ФСТЭК и содержать информацию о системе защиты информации, включая описание используемых технических средств защиты и процедур обработки конфиденциальной информации. При подготовке документа необходимо учитывать особенности объекта информатизации и возможные угрозы безопасности информации, а также выбирать технические средства защиты в соответствии с требованиями ФСТЭК.

Самостоятельная работа № 6

ТЕМА: ПОДГОТОВКА ДОКУМЕНТА ДЛЯ ВИДА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ВЫЯВЛЕНИЮ ЭЛЕКТРОННЫХ УСТРОЙСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ, В ПОМЕЩЕНИЯХ И ТЕХНИЧЕСКИХ СРЕДСТВАХ (ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЯ, ЕСЛИ УКАЗАННАЯ ДЕЯТЕЛЬНОСТЬ ОСУЩЕСТВЛЯЕТСЯ ДЛЯ ОБЕСПЕЧЕНИЯ СОБСТВЕННЫХ НУЖД ЮРИДИЧЕСКОГО ЛИЦА ИЛИ ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ) СОГЛАСНО ТРЕБОВАНИЙ ФСБ. ПОДГОТОВКА ДОКУМЕНТА ДЛЯ ВИДА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПО РАСПРОСТРАНЕНИЮ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ СОГЛАСНО ТРЕБОВАНИЙ ФСТЭК.

1. **Цель (и) работы**: подготовить документ для получения вида деятельности по выявлению электронных устройств, предназначенных для негласного получения информации в помещениях и технических средствах в соответствии с требованиями ФСБ, а также подготовить документ для получения вида деятельности по распространению шифровальных (криптографических) средств согласно требованиям ФСТЭК..

2. **Задачи:**
   - Изучение требований ФСБ и ФСТЭК по организации деятельности по выявлению электронных устройств и распространению шифровальных средств соответственно.
   - Определение требований к документации для получения вида деятельности по выявлению электронных устройств и распространению шифровальных средств.
   - Составление документов для получения вида деятельности по выявлению электронных устройств и распространению шифровальных средств.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - Ознакомиться с требованиями ФСБ и ФСТЭК по организации деятельности по выявлению электронных устройств и распространению шифровальных средств.
   - Составить перечень необходимых документов для получения вида деятельности по выявлению электронных устройств и распространению шифровальных средств в соответствии с требованиями ФСБ и ФСТЭК.
   - Составить текст заявления для получения вида деятельности по выявлению электронных устройств и распространению шифровальных средств в соответствии с требованиями ФСБ и ФСТЭК.
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчетов и поиск информации.

5. Критерии оценки

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них
- Наличие анализа и выводов на основе представленной информации

Оценка 4 –
- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
- Грамотное использование терминов и понятий, но с некоторыми неточностями
- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –
- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –
- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

Федеральная служба безопасности России (ФСБ) и Федеральная служба по технической и экспортной контролю (ФСТЭК) устанавливают требования для организации деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, а также по распространению шифровальных (криптографических) средств.

При осуществлении деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, необходимо учитывать требования, установленные Федеральной службой безопасности (ФСБ) Российской Федерации. В соответствии с данными требованиями, владельцы помещений и технических средств должны обеспечивать защиту от несанкционированного доступа к информации, а также проводить регулярные проверки на наличие негласных устройств.

Деятельность по распространению шифровальных (криптографических) средств также регулируется Федеральной службой технической и экспортной контроля (ФСТЭК) Российской Федерации. При этом необходимо соблюдать требования, установленные законодательством, связанные с защитой информации от несанкционированного доступа.

Самостоятельная работа № 7
ТЕМА: РАБОТА С РИСК-ПОДХОДАМИ К МОДЕЛИРОВАНИЮ УГРОЗ ИБ. РАЗРАБОТКА МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН)

1. **Цель (и) работы**: ознакомление с риск-подходами к моделированию угроз информационной безопасности (ИБ) и разработкой моделей угроз безопасности в информационных системах персональных данных (ИСПДН)..

2. **Задачи:**
   - Изучение основных подходов к моделированию угроз ИБ.
   - Изучение методик проведения анализа рисков и угроз ИБ.
   - Разработка моделей угроз безопасности в ИСПДН.
   - Оценка эффективности разработанных моделей угроз безопасности в ИСПДН.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - Изучить принципы риск-подхода к моделированию угроз ИБ.
   - Составить список возможных угроз ИБ в ИСПДН.
   - Оценить уровень риска каждой угрозы в ИСПДН и определить меры по их предотвращению.
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчетов и поиск информации.

5. **Критерии оценки**

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них
- Наличие анализа и выводов на основе представленной информации

Оценка 4 –
- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
- Грамотное использование терминов и понятий, но с некоторыми неточностями
- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

Моделирование угроз информационной безопасности (ИБ) представляет собой процесс создания математической модели, которая описывает потенциальные угрозы для информационных систем и средств. Риск-подход к моделированию угроз ИБ основывается на оценке вероятности возникновения угроз и их последствий для ИБ. Для этого используется методика проведения анализа рисков и угроз ИБ. В информационных системах персональных данных (ИСПДН) угрозы ИБ могут иметь серьезные последствия для конфиденциальности, целостности и доступности персональных данных. Разработка моделей угроз безопасности в ИСПДН позволяет определить наиболее вероятные угрозы ИБ и принять меры по их предотвращению.

Самостоятельная работа № 8
ТЕМА: РЕАЛИЗАЦИЯ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ.

1. **Цель (и) работы**: реализация модели угроз безопасности персональных данных при их обработке в информационных системах.

2. **Задачи:**
   - Изучение правовых, организационных и технических мер по обеспечению безопасности персональных данных.
   - Анализ угроз безопасности персональных данных при их обработке в информационных системах.
   - Разработка модели угроз безопасности персональных данных при их обработке в информационных системах.
   - Реализация модели угроз безопасности персональных данных в выбранном программном обеспечении.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - Изучить основы защиты персональных данных и законодательство в этой области.
   - Составить список угроз безопасности персональных данных в информационных системах.
   - Разработать модель угроз безопасности персональных данных при их обработке в информационных системах.
   - Применить модель к конкретной информационной системе для оценки уровня угроз безопасности персональных данных.
   - Разработать план по устранению выявленных угроз безопасности персональных данных.
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчетов и поиск информации.

5. **Критерии оценки**

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них
- Наличие анализа и выводов на основе представленной информации

Оценка 4 –

- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
- Грамотное использование терминов и понятий, но с некоторыми неточностями
- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

Обработка персональных данных требует высокого уровня защиты, чтобы гарантировать конфиденциальность и интегритет этих данных. Угрозы безопасности персональных данных могут возникать из различных источников, таких как несанкционированный доступ, утечка данных, вредоносное ПО, атаки на сеть и т.д.

Модели угроз безопасности персональных данных позволяют идентифицировать потенциальные угрозы и оценить их влияние на информационную систему. Они также могут помочь разработать эффективные меры безопасности для предотвращения и устранения этих угроз.

Реализация модели угроз безопасности персональных данных включает в себя оценку системы на наличие уязвимостей, выявление угроз безопасности, анализ и оценку влияния этих угроз на информационную систему, разработку мер по предотвращению и устранению угроз безопасности, и непрерывный мониторинг безопасности.

Самостоятельная работа № 9
ТЕМА: ПРОВЕДЕНИЕ АНАЛИЗА СЕТЕВЫХ РЕСУРСОВ ОРГАНИЗАЦИИ. ПРОВЕДЕНИЕ АНАЛИЗА СОТРУДНИКОВ ОРГАНИЗАЦИИ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННЫЙ БЕЗОПАСНОСТИ

1. **Цель (и) работы**: провести анализ сетевых ресурсов организации и сотрудников с точки зрения информационной безопасности.

2. **Задачи:**
   - Изучение существующих сетевых ресурсов организации, включая аппаратное и программное обеспечение, настройки и права доступа.
   - Определение уязвимостей в сетевой инфраструктуре организации и выработка мер по их устранению.
   - Анализ политики информационной безопасности организации и ее соответствия требованиям законодательства и стандартов.
   - Оценка компетенций сотрудников организации в области информационной безопасности и выявление слабых мест.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - Провести анализ безопасности сетевой инфраструктуры компьютерного класса или локальной сети на базе предоставленных средств и технологий, выявить уязвимости и разработать меры по их устранению.
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчетов и поиск информации.

5. **Критерии оценки**

Оценка 5 –
- Исчерпывающее изложение темы
- Четкая логика и последовательность изложения материала
- Грамотное и точное использование терминов и понятий
- Использование достаточного количества источников и ссылок на них
- Наличие анализа и выводов на основе представленной информации

Оценка 4 –
- Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
- Грамотное использование терминов и понятий, но с некоторыми неточностями

- Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
- Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –

- Среднее изложение темы с заметными недочетами в логике и последовательности изложения
- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

Анализ сетевых ресурсов и сотрудников является важной составляющей обеспечения информационной безопасности организации. Современные технологии и многочисленные угрозы, связанные с нарушением безопасности данных и сетей, требуют систематического анализа сетевых ресурсов и оценки компетенций сотрудников. Анализ сетевых ресурсов помогает выявить уязвимости и риски безопасности, а также разработать меры по их устранению. Анализ сотрудников позволяет определить уровень их знаний и навыков в области информационной безопасности и выявить слабые места, которые могут стать источником угроз для организации. Оценка политики информационной безопасности организации помогает убедиться в ее соответствии требованиям законодательства и стандартов.

Самостоятельная работа № 10
ТЕМА: РАБОТА С ОСНОВНЫМИ ПОНЯТИЯМИ СЛУЖЕБНОЙ ТАЙНЫ

3. **Цель (и) работы**: ознакомиться с основными понятиями служебной тайны и ее правовым регулированием в Российской Федерации..

4. **Задачи:**
   - Рассмотреть основные понятия служебной тайны и ее виды.
   - Изучить правовые основы регулирования служебной тайны в России.
   - Ознакомиться с порядком обращения с информацией, отнесенной к служебной тайне.
   - Разобраться в ответственности за нарушение режима служебной тайны.

3. **Подготовка к работе и порядок выполнения:**
   - изучить предложенную литературу;
   - Напишите эссе на тему "Значение служебной тайны для обеспечения безопасности государства".
   - составить отчет.

4. **Необходимое оборудование:**
   - Компьютер - необходимый инструмент для создания презентаций, докладов и рефератов. Рекомендуется использовать компьютер с достаточной производительностью, чтобы обеспечить плавность работы программ и быструю обработку данных.
   - Программное обеспечение - могут потребоваться различные программы, такие как Microsoft Word и другие.
   - Интернет-соединение - может потребоваться для загрузки дополнительной информации, изображений или видео.
   - Устройства хранения данных - USB-накопители, внешние жесткие диски или облачные сервисы могут использоваться для хранения презентаций и докладов.
   - Аксессуары - могут потребоваться дополнительные аксессуары, такие как мышь, клавиатура, стилус и т.д., чтобы облегчить создание отчетов и поиск информации.

5. **Критерии оценки**

Оценка 5 –
   - Исчерпывающее изложение темы
   - Четкая логика и последовательность изложения материала
   - Грамотное и точное использование терминов и понятий
   - Использование достаточного количества источников и ссылок на них
   - Наличие анализа и выводов на основе представленной информации

Оценка 4 –
   - Хорошее изложение темы, но с небольшими недочетами в логике и последовательности изложения
   - Грамотное использование терминов и понятий, но с некоторыми неточностями
   - Использование достаточного количества источников и ссылок на них, но не всегда полное и точное
   - Присутствие анализа и выводов, но не всегда полное и точное

Оценка 3 –
   - Среднее изложение темы с заметными недочетами в логике и последовательности изложения

- Не всегда грамотное использование терминов и понятий, существуют ошибки и неточности
- Использование недостаточного количества источников и ссылок на них
- Анализ и выводы отсутствуют или недостаточно полны и точны

Оценка 2 –

- Недостаточное и нечеткое изложение темы
- Частые ошибки и неточности в использовании терминов и понятий
- Отсутствие источников и ссылок на них
- Отсутствие анализа и выводов

6. Пояснения к работе

Краткие теоретические сведения

Служебная тайна - это информация, защищенная законом от разглашения, в том числе в интересах обеспечения безопасности государства, обороны страны, национального единства.

Служебная тайна является частью закона, который оговаривает конфиденциальность информации, полученной в рамках служебной деятельности. Служебная тайна имеет особый статус, который обеспечивает ее защиту от несанкционированного доступа и раскрытия.

Основные понятия, связанные со служебной тайной, включают следующее:

- Секреты государственной службы - конфиденциальная информация, касающаяся государственной политики, обороны и безопасности страны, а также реализации законов.
- Служебные сведения - информация, полученная в результате осуществления служебной деятельности, которая должна оставаться конфиденциальной.
- Служебная тайна - информация, которая содержится в служебных сведениях и не может быть разглашена без разрешения компетентных органов.

Список источников информации:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К.Баранова, А.В.Бабаш. — 3-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2020.
2. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.
3. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации): учебное пособие / В.К. Новиков. - Москва: Горячая Линия–Телеком, 2017.
4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2020.
5. Хабибулин, А. Г. Правовое обеспечение профессиональной деятельности: учебник для студ. учрежд. СПО/ А.Г. Хабибулин, К.Р. Мурсалимов. — 2-е изд., перераб. и доп. —