государственное автономное учреждение
Калининградской области
профессиональная образовательная организация
«КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА»

МЕТОДИЧЕСКАЯ РАЗРАБОТКА К ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ ПО ДИСЦИПЛИНЕ МДК 03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ»

для студентов профессии 09.01.02 Наладчик компьютерных сетей

Составил:
преподаватель
Красильникова И.А.

Калининград
2023

АННОТАЦИЯ

Методические разработки практических заданий для студентов по профессии 09.01.02 Наладчик компьютерных сетей содержат практические задания для студентов, предназначенных для выполнения практических работ по МДК.03.01 «Информационная безопасность персональных компьютеров и компьютерных сетей»
Методические разработки, включают практические задания, а также список литературных и других источников информации, необходимых для выполнения работ.

Содержание

Введение

С целью овладения профессиональными компетенциями обучающийся в ходе выполнения практических работ закрепляет теоретические знания о - видах угроз и методах защиты персональных компьютеров, серверов и корпоративных сетей от них;

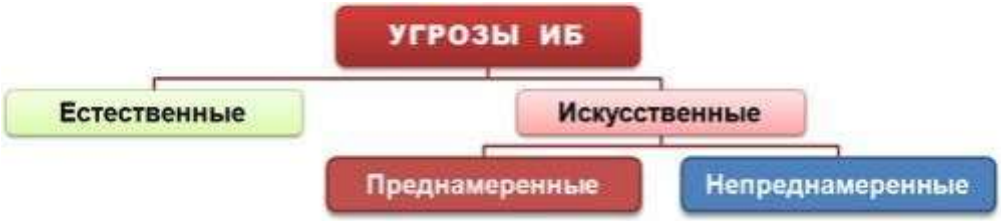
- аппаратных и программных средствах резервного копирования данных;
- методах обеспечения защиты компьютерных сетей от несанкционированного доступа; специализированных средствах для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами;

В состав методических рекомендаций входят практические задания к темам разделов №1 и №2.

Раздел 1. Информационная безопасность как часть инфраструктуры

1.1 Угрозы информационной безопасности и каналы утечки информации.

Важнейшей стороной обеспечения информационной безопасности является определение и классификация угроз. **Угрозы безопасности информации** — это некая совокупность факторов и условий, которые создают опасность в отношении защищаемой информации.
Для того чтобы определить угрозы, от которых необходимо обезопасить информацию, нужно определить объекты защиты. Ведь информация — это некоторые данные, носителями которых могут быть как материальные, так и нематериальные объекты. К примеру, носителями конфиденциальной информации могут быть документы, технические средства обработки и хранения информации и даже люди.
Документационными носителями информации могут быть проекты, бизнес-планы, техническая документация, контракты и договора, а также картотеки отдела кадров (персональные данные) и отдела по работе с клиентами. Отличительной их особенностью является зафиксированность данных на материальном объекте — бумаге.
Техническими средствами обработки и хранения информации являются персональные компьютеры, ноутбуки, серверы, сканеры, принтеры, а также съемные носители (переносные жесткие диски, флеш-карты, CD-диски, дискеты) и т.п. Информация в технических средствах хранится и обрабатывается в цифровом виде. Зачастую конфиденциальные данные отправляются через Интернет, например, по электронной почте. В сети они могут быть перехвачены злоумышленниками. Кроме того при работе компьютеров из-за их технических особенностей обрабатываемые данные преобразуются в электромагнитные излучения, распространяющиеся далеко за пределы помещения, которые также могут быть перехвачены и использованы в недобросовестных целях.
Люди также могут быть «носителями» информации. Например, сотрудники компании, которые имеют или могут иметь доступ к конфиденциальной информации. Таких людей называют инсайдерами. Инсайдер необязательно является злоумышленником, но в любой момент может им стать. Кроме того несанкционированный доступ к конфиденциальной информации могут получить посетители, клиенты или партнеры, а также обслуживающий персонал.
Теперь, когда мы понимаем, что нужно защищать, можно перейти непосредственно к рассмотрению угроз. Они могут заключаться как в нарушении конфиденциальности, так и в нарушении достоверности, целостности и доступности информации. Нарушением конфиденциальности является утечка данных, несанкционированный доступ или разглашение информации. Нарушение достоверности информации — это фальсификация данных или подделка документов. Искажение, ошибки при передаче информации, потери части данных являются нарушением целостности информации. А блокирование доступа к информации, выведение из строя средств связи, технических средств являются нарушением доступности.
По методам воздействия на информацию угрозы подразделяются на естественные и искусственные. В свою очередь искусственные угрозы состоят из преднамеренных и непреднамеренных.



Естественные угрозы:

- стихийные бедствия;

- пожары;
- наводнения;
- техногенные аварии;
- и другие явления, не зависящие от человека.

Искусственные преднамеренные угрозы:

- кража (копирование) документов;
- подслушивание переговоров;
- несанкционированный доступ к информации;
- перехват информации;
- внедрение (вербовка) инсайдеров;
- фальсификация, подделка документов;
- диверсии;
- хакерские атаки и т.п.

Искусственные непреднамеренные угрозы:

- ошибки пользователей;
- неосторожность;
- невнимательность;
- любопытство и т.п.

Естественно, наибольшую угрозу представляют преднамеренные действия злоумышленников, но и непреднамеренные и естественные угрозы нельзя сбрасывать со счетов, так как они в определенной степени также несут в себе серьезную опасность.

Задание: Привести примеры к каждой угрозе в классификации

1.2 Организационно-правовое обеспечение информационной безопасности

Международный стандарт ISO / IEC 17799 представляет собой набор рекомендаций *по* применению организационно-технических мер безопасности для эффективной защиты автоматизированных систем. В 2007 г. планируется принятие *ISO / IEC* 17799 в качестве ГОСТа. Стандарт состоит из одиннадцати разделов, каждый из которых описывает одну из областей *информационной безопасности*.

Дайте краткое описание разделам, указанным в таблице

№	Раздел стандарта	Описание раздела
1	"Политика*информационной безопасности*"	
2	"Организационные меры защиты"	
3	"*Безопасность персонала*"	
4	"Классификация и управление информационными ресурсами"	

1.3 Политика информационной безопасности

Ответьте на следующие вопросы:
1.Определение понятия «Политика информационной безопасности»
2.Опишите функции политики информационной безопасности
3.Опишите этапы разработки политики информационной безопасности

1.4. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности

Задание: Приведите примеры и краткую информацию по ним, и заполните таблицу

Программные средства защиты	
Аппаратные средства защиты	
Программно-аппаратные средства защиты	

Раздел 2. Резервное копирование данных

2.1 Резервное копирование. Программы для резервного копирования

Ответьте на следующие вопросы:
1.Что такое резервное копирование?
2.Для чего осуществляется резервное копирование?
3.Приведите примеры программ для резервного копирования?
4.Какая программа будет называться «агент» и для чего агент программам резервного копирования?

2.2 Типы резервного копирования. Хранение резервных копий. Восстановление данных

Задание: Разработайте собственную схему ротации резервных копий для реализации в рамках нашей лаборатории и обоснуйте ее целесообразность относительно классических схем.

2.3 Создание резервных копий.

Разработайте инструкцию по созданию резервной копии в любой известной вам программе резервного копирования

2.4 Восстановление данных

Приведите примеры мест хранения резервных копий и кратко поясните их достоинства

Пример	Пояснение
FTP	Хранение резервных копий на FTP сервере. Позволяет содержать резервные копии отдельно, не перегружая память рабочих станций в специализированном хранилище

Перечень рекомендуемых учебных изданий:

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2014. - 416 с.
2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.