

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»



УТВЕРЖДАЮ

Заместитель директора по УМР

Е.Ю. Кузнецов

«26» июня 2020 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ  
ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ И ПРАКТИЧЕСКИХ РАБОТ ПО  
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ  
СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ  
СРЕДСТВАМИ


по специальности 10.02.05 Обеспечение информационной безопасности  
автоматизированных систем

РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 7

« 27 » июня 20 20 г.

Председатель ПЦК  /Л.И.Логинова/

Разработчик: Пекунов Андрей Ананьевич, преподаватель, доцент кафедры ИВС ФГБОУ ВО «Поволжский государственный технологический университет».

Методические рекомендации предназначены для обучающихся по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и направлены на оказание практической помощи при выполнении внеаудиторной самостоятельной работы по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

## СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ
2. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
3. ТЕМАТИКА И СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ
4. КОНТРОЛЬ САМОСТОЯТЕЛЬНОЙ РАБОТЫ И КРИТЕРИИ ЕЕ ОЦЕНКИ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

## 1. ВВЕДЕНИЕ

Методические рекомендации предназначены в качестве методических материалов при проведении лабораторных и практических работ по дисциплине Защита информации в автоматизированных системах программными и программно-аппаратными средствами для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, составлены в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования.

Теоретический материал курса Защита информации в автоматизированных системах программными и программно-аппаратными средствами охватывает обширный круг актуальных вопросов по организации, ведению и управлению хозяйственной деятельности в организации. Методические указания позволяют улучшить усвоение учебного материала, изученного на лекционных занятиях. Обучающиеся смогут овладеть и свободно оперировать техническими категориями по различным областям деятельности организации. Решение практических задач, сформированных в данных методических указаниях, позволит студентам укрепить знания теоретического материала по указанной дисциплине.

Практические занятия проводятся после изучения соответствующих разделов и тем учебной дисциплины. Так как учебная дисциплина имеет прикладной характер, то выполнение обучающимися практических работ позволяет им понять, где и когда изучаемые теоретические положения, и практические умения могут быть использованы в будущей практической деятельности.

## 2.ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические рекомендации по выполнению лабораторных и практических работ разработаны в соответствии с рабочей программой учебной дисциплины Защита информации в автоматизированных системах программными и программно-аппаратными средствами специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Целью лабораторных и практических работ является закрепление теоретических знаний и приобретение практических умений по определению организационно-правовых форм организаций, расчету по принятой методике основных технических показателей деятельности организации, организации контроля на предприятии и др.

В результате выполнения лабораторных и практических работ по дисциплине ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами обучающийся должен овладеть предусмотренными ФГОС умениями, знаниями, которые формируют общие и профессиональные компетенции.

- 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 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
- ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
- ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
- ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
- ОК 09. Использовать информационные технологии в профессиональной деятельности.
- ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
- ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
- ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
- ПК 2.2. Обеспечивать защиту информации в автоматизированных системах

- отдельными программными, программно-аппаратными средствами.
- ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
- ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.
- ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
- ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

При выполнении лабораторной работы обучающийся должен иметь практический опыт:

- установки, настройки программных средств защиты информации в автоматизированной системе;
- обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;
- решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;
- применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;
- учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;
- работы с подсистемами регистрации событий;
- выявления событий и инцидентов безопасности в автоматизированной системе

должен уметь:

- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- применять программные и программно-аппаратные средства для защиты информации в базах данных;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- применять математический аппарат для выполнения криптографических преобразований;
- использовать типовые программные криптографические средства, в том

числе электронную подпись;

- применять средства гарантированного уничтожения информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных

а так должен знать:

- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
  - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
  - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
  - основные понятия криптографии и типовых криптографических методов и средств защиты информации;
  - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

### **3. Тематический план и содержание профессионального модуля ПМ. 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**

Наименование темы	лабораторная работа обучающихся	Количество часов
<b>РАЗДЕЛ 1 МОДУЛЯ. Применение программных и программно-аппаратных средств защиты информации</b>		
<b>МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b>		
<b>Раздел 1. Основные принципы программной и программно-аппаратной защиты информации</b>		
Тема 1.2. Стандарты безопасности	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.	6
Тема 1.3. Защищенная автоматизированная система	Учет, обработка, хранение и передача информации в АИС Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей Разграничение доступа.	10

	Регистрация событий (аудит). Контроль целостности данных Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности Криптографическая защита. Обзор программ шифрования данных Управление политикой безопасности. Шаблоны безопасности	
Тема 1.4. Управление памятью	Распределение каналов в соответствии с источниками воздействия на информацию	4
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Организация доступа к файлам Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	4
<b>Раздел 2. Защита автономных автоматизированных систем</b>		
Тема 2.3. Вредоносное программное обеспечение	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2
Тема 2.4. Защита программ и данных от несанкционированного копирования	Защита информации от несанкционированного копирования с использованием специализированных программных средств Защитные механизмы в приложениях (на примере MSWord, MSeXcel, MSPowerPoint)	4
Тема 2.5. Защита информации на машинных носителях	Применение средства восстановления остаточной информации на примере Foremost или аналога Применение специализированного программно средства для восстановления удаленных файлов Применение программ для безвозвратного удаления данных Применение программ для шифрования данных на съемных носителях	4
Тема 2.7. Системы обнаружения атак и вторжений	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2
<b>Раздел 3. Защита информации в локальных сетях</b>		
Тема 3.2. Средства организации VPN	Развертывание VPN	2
<b>Раздел 4. Защита информации в сетях общего доступа</b>		
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. Изучение различных способов закрытия "опасных" портов	4
Тема 5.1. Защита информации в базах данных	Изучение механизмов защиты СУБД MS Access Изучение штатных средств защиты СУБД MSSQL Server	4
<b>Раздел 6. Мониторинг систем защиты</b>		



Тема 6.1. Мониторинг систем защиты	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	4
Тема 6.2. Изучение мер защиты информации в информационных системах	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	6
Тема 6.3. Изучение современных программно-аппаратных комплексов.	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	6
Итого		62

### Лабораторная работа № 1

*Тема:* Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов

*Цель:* научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

*Количество часов:* 6

*Порядок работы:*

*Задание 1.* Определить нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

*Задание 2.* Изучить ФЗ «Об информации, информационных технологиях и о защите информации». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

*Задание 3.* Изучить приказ ФСТЭК России 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». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

*Задание 4.* Изучить типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для

обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством Центра ФСБ России 21.02.2008 №149/6/6-622. Выписать требования и рекомендации по защите информации программными и программно- аппаратными средствами.

### Лабораторная работа № 2

*Тема:* Учет, обработка, хранение и передача информации в АИС

Ограничение доступа на вход в систему.

Идентификация и аутентификация пользователей

Разграничение доступа.

Регистрация событий (аудит).

Контроль целостности данных

Уничтожение остаточной информации.

Управление политикой безопасности. Шаблоны безопасности

Криптографическая защита. Обзор программ шифрования данных

Управление политикой безопасности. Шаблоны безопасности

*Цель:* познакомиться со способами учета, обработки, хранения и передачи информации в АИС.

ознакомиться с процедурами создания учётных записей пользователей и управления их правами.

ознакомиться с механизмами идентификации и аутентификации пользователей;

освоение навыков управления доступом пользователей.

ознакомиться с механизмами регистрации событий.

получить навыки обнаружения фактов изменения данных, контроля целостности

данных с помощью механизма хэш-функций.

ознакомиться с механизмами уничтожения остаточной информации

ознакомиться с механизмами управления политикой безопасности

ознакомиться с программами шифрования данных

научиться работать с редактором шаблонов безопасности.

*Количество часов: 10*

*Порядок работы:*

**1.Задание 1.** Изучить технологии учета и хранения информации. Описать, как происходит сбор и регистрация данных. Назовите основные требования к сбору данных и к хранимым данным.

Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации.

Какие еще средства сбора информации вам известны?

**Задание 2.** Изучить технологический процесс обработки информации.

Перечислить и охарактеризовать технологические процессы процесса обработки информации. В чем заключается различие между централизованным и децентрализованным способами обработки информации?

Какие режимы обработки информации вам известны?

*Задание 3.* Изучить технологии передачи и представления информации. Описать, как происходит передача данных.

*Задание 4.* Выполнить задания:

- . набрать в одном из текстовых редакторов текст из 10 предложений на тему «Моя профессия»;
- . вставить в набранный текст рисунок;
- . сохранить текст на каких-либо носителях;
- . создать свою электронную почту;
- . отправить, набранную информацию по электронной почте;
- . получить информацию по электронной почте;
- . изменить полученный текст, введя диаграмму;
- . сохранить текст.

*Задание 5.* Продумать и создать технологию учета и обработки заявок на выполнение работ по ремонту компьютерной техники в салоне по ремонту компьютерного оборудования «Сервис- ТЕХНО». Результат выполнения задания оформить в виде таблицы.

*Задание 6.* Используя технологии поиска информации, найдите разницу между терминами “хранение” и “сохранение данных”.

*Задание 7.* Используя средства Интернета, перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

**2. Задание 1.** Ознакомиться с технологиями создания и управления учетными записями пользователей. Примените к созданной учётной записи настройки, указанные в варианте.

*Задание 2.* Создайте новую учетную запись пользователя с помощью командной строки.

*Задание 3.* Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем.

*Задание 4.* Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Прodelайте это двумя способами: через окно свойств группы и окно свойств пользователя.

**3. Задание 1.** Опишите параметры локальной политики безопасности операционной системы Windows:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на компьютере;
- включение и выключение записи действий пользователей или группы пользователей в журнале событий.

*Задание 2.* Опишите параметры и значения параметров Политики паролей. Заполните таблицу:

**4. Задание 1.** Выполните задания.

1. Создайте папку, в которую поместите текстовый файл и приложение в виде файла с

расширением exe, например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).

| Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.

| Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.

□ Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.

| Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.

| Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.

□ Составьте отчет о проведенных экспериментах.

*Задание 2.* Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

**5.Задание 1.** Опишите параметры и значения параметров Политики аудита. Заполнить таблицу.

*Задание 2.* Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале?

*Задание 3.* Включите аудит успеха и отказа всех параметров.

*Задание 4.* Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись.

*Задание 5.* Удалите ранее созданную учетную запись и зафиксируйте все события системного журнала, связанные с этим действием.

**6. Задание 1.** Создать несколько файлов, заполнить их данными. Сделать копии файлов и произвести для некоторых из них «незаметные» для пользователей изменения в файлах. К таким изменениям можно отнести, к примеру:

- изменение кода цвета объектов, в частности текста;
- замена символов на похожие символы с другими кодами символов;
- вставка объектов со 100 %-ной прозрачностью, отсутствующими цветами заливками или совпадающими с цветом фона;
- изменение текста до минимального, установка цвета текста под цвет фона;
- вставка текста с атрибутами «скрытый текст», опция «Шрифт» => «Видоизменение»;
- изменение рисунка (областей с мало отличимой палитрой цветов);
- изменение метаданных файлов (к примеру, вкладка «Подробно» с полями «Авторы», «Организация» и пр.); □ прочее.

*Задание 2.* Используя программную реализацию механизма хэш-функций, проверить целостность и неизменность файлов. Предоставить снимки экрана, описание действий и результатов. Прокомментировать детально результаты работы: когда совпадают, когда расходятся и почему.

*7. Задание 1.* Опишите причины возникновения остаточной информации.

*Задание 2.* Приведите примеры устройств уничтожения информации с магнитных носителей.

*Задание 3.* Изучите особенности современных методов ликвидации информации на магнитных носителях. Заполните таблицу.

*8. Задание 1.* Заданы документы с различным уровнем секретности, заданы пользователи с различным уровнем доступа (список документов и пользователей и их уровни доступа/секретности составить самостоятельно. Не менее 5 пользователей и 5 документов).

1. Для каждого пользователя составить список документов, доступных ему для работы при условии, что пользователь не понижает своего уровня допуска.

2. Для одного из пользователей составить список документов, доступных ему для работы при условии, что пользователь может понизить свой уровень доступа на один уровень.

3. Один из пользователей имеет возможность работать с несколькими документами. На основе этих документов он создает новый документ. Какой гриф секретности нужно присвоить этому документу?

4. Показать на примере одного из пользователей, что мандатная политика безопасности не может быть нарушена программой типа "Троянский конь".

*9. Задание 1.* Разработать алгоритм шифрования данных.

*Задание 2.* Привести примеры программ шифрования данных.

*Задание 3.* Провести сравнительный анализ программ шифрования данных.

*Задание 4.* Описать возможности одной из программ шифрования данных

*Задание 1.* Загрузите редактор Шаблона безопасности. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?

*Задание 2.* Отредактируйте шаблон безопасности и сохраните его под новым именем.

*Задание 3.* Опишите разделы, включаемые в стандартный Шаблон безопасности.

*Задание 4.* Опишите, какие параметры политики безопасности можно настроить с помощью шаблонов безопасности?

### Лабораторная работа № 3

*Тема:* Распределение каналов в соответствии с источниками воздействия на информацию.

*Цель:* ознакомиться с каналами несанкционированного получения информации.

*Количество часов:* 4

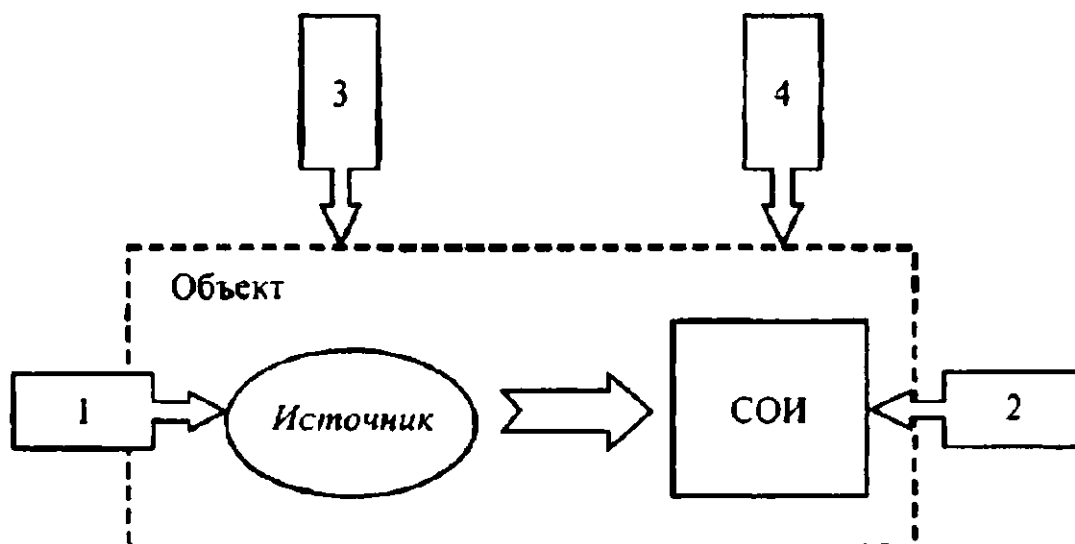
*Порядок работы:*

*Задание 1.* Заполнить таблицу:

Канал связи	Среда	Носитель сообщения	Процесс, используемый для передачи сообщения
Почта, курьеры			
Телефон, компьютерные сети			
Радио, телевидение			
Зрение			
Слух			
Обоняние, вкус			
Осязание			

*Задание 2.* Приведите конкретные примеры каналов несанкционированного получения информации каждого класса. Классы каналов несанкционированного получения информации:

- 1) от источника информации при несанкционированном доступе (НСД) к нему;
- 2) от средств обработки информации при НСД к ним;
- 3) от источника информации без НСД к нему;
- 4) от средств обработки информации без НСД к ним.



#### Лабораторная работа № 4

*Тема:* Организация доступа к файлам.

Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД.

*Цель:* научиться назначать разрешения файлов и папок NTFS учетным записям и группам.

ознакомиться с современными программными и программно-аппаратными средствами защиты от НСД.

Количество часов: 4

Порядок работы:

**1. Задание 1.** Планирование разрешений NTFS.

1. Спланируйте разрешения доступа к папкам и файлам. Затем реализуйте разрешения NTFS для файлов и папок вашего компьютера, а затем проверьте назначенные разрешения NTFS и убедитесь, что они работают должным образом.

Перед выполнением упражнений создайте следующие учетные записи и группы:

User81 (нет пароля) — член группы Managers;

User82 (нет пароля) — член группы Accounting;

User83 (нет пароля) — член группы Managers и группы Accounting;

User84 (нет пароля) — не является членом групп Accounting и Managers.

Создайте следующие папки:

C:\Public;

C:\Public\Library;

C:\Public\Manuals;

C:\Public\Library\Misc.

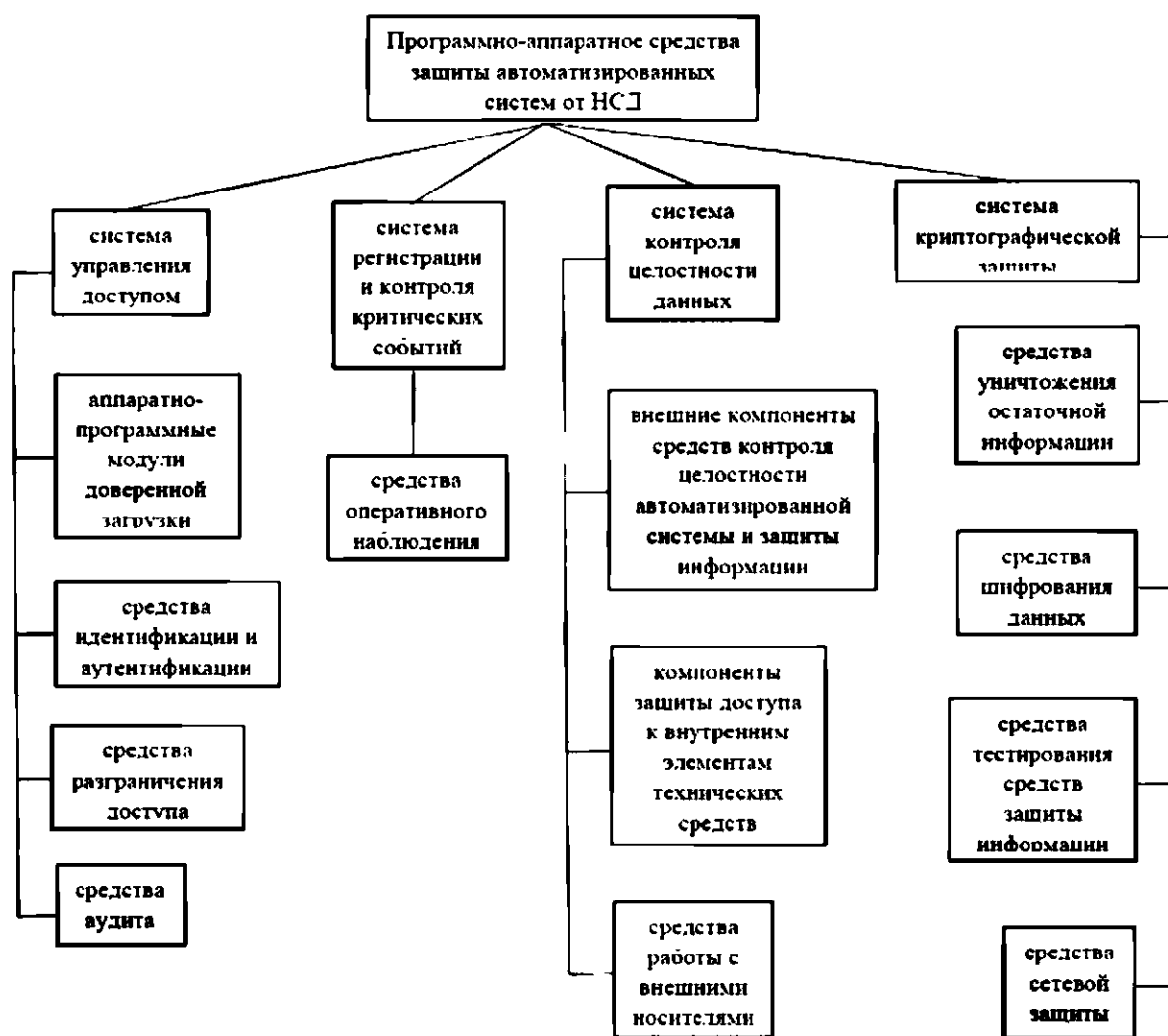
Можно использовать и свою структуру объектов, имеющихся на вашем компьютере.

2. Спланируйте назначение разрешений NTFS для файлов и папок:

3. Понятие приоритета и очереди процессов, особенности многопроцессорных систем.

Имя папки	Группа	Разрешения
Public	Users Administrators	Read & Execute Full Control
Public\Library	Users Administrators Manager	Read & Execute Full Control Modify
Public\Library\Misc	Users Administrators User82	Read & Execute Full Control Modify
Public\Manuals	Users Administrators Accounting	Read & Execute Full Control Modify

**2. Задание 1.** Охарактеризуйте программно-аппаратные средства защиты автоматизированных систем от НСД.



**Задание 2.** В качестве примеров отдельных программ, повышающих защищенность от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам DiskMonitor и др. Опишите одно из программных средств, повышающих защищенность от НСД.

**Задание 3.** В качестве примеров отечественных аппаратно-программных средств защиты можно привести системы «Аккорд-4», «DALLAS LOCK 3.1», «Редут», «ДИЗ-1». Опишите одно из программно-аппаратных средств защиты информации от НСД.

**Задание 4.** Приведите примеры современных систем защиты ПК от несанкционированного доступа к информации.

### Лабораторная работа № 5

**Тема:** Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО

**Цель:** ознакомиться с реестром Windows.

**Количество часов:** 2



*Порядок работы:*

*1.Задание 1.* Опишите разделы реестра Windows. Заполните таблицы.

HKEY_CURRENT_USER	
HKEY_USERS	
HKEY_LOCAL_MACHINE;	
HKEY_CLASSES_ROOT	
HKEY_CURRENT_CONFIG	

*Задание 2.* В каких разделах реестра хранится информация о выбранной политике безопасности.

*Задание 3.* Опишите возможности программы REGEDIT.EXE.

*Задание 4.* Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО.

### Лабораторная работа № 6

*Тема:* Защита информации от несанкционированного копирования с использованием специализированных программных средств

Защитные механизмы в приложениях (на примере MSWord, MSeXcel, MSPowerPoint).

*Цель:* ознакомиться с механизмами защиты информации от несанкционированного копирования с использованием специализированных программных средств. Ознакомиться с защитными механизмами в приложениях.

*Количество часов:* 4

*Порядок работы:*

*1.Задание 1.* Охарактеризуйте компоненты системы защиты от несанкционированного копирования.



**Задание 2.** Системы защиты от несанкционированного копирования можно классифицировать по способу внедрения защитного механизма:

- ☐ встроенная внедряется при создании программного продукта;
- ☐ пристыковочная подключается к уже готовому программному продукту.

Приведите достоинства и недостатки этих способов внедрения защитного механизма.

**Задание 3.** Опишите основные требования, предъявляемые к системе защиты от копирования.

**Задание 2.** Установить дистрибутив на компьютер.

Ответить на теоретические вопросы:

1. Утилиты для создания дистрибутивов Linux.
2. Этапы создания дистрибутива Linux.
3. Этапы установки дистрибутива Linux.

**2. Задание 1.** Создайте шаблон делового письма, содержащий текст шапки и подписи стандартного письма организации, с защищенными от изменения реквизитами. Средняя часть письма (содержание письма) доступно для изменения.

При этом в защищенных шапке и подпись письма следует предусмотреть возможность изменения следующих данных:

- исходящий номер и дата создания письма могут быть изменены (набраны) с клавиатуры;
- фамилия исполнителя может быть выбрана из списка.

Открытие файла письма должно быть защищено паролем.

*Задание 2.* В приложении MS Word создайте короткий опросник (анкету) с защищенным от изменения текстом вопросов для получения от пользователей различных данных. Сформулировать вопросы так, чтобы требовались:

- а) ответы в произвольной форме, подразумевающие ввод текста, (например, ФИО, какие-либо комментарии или пожелания, номер учебной группы, дата заполнения),
- б) выбор даты (дата дня рождения, начала сессии, рекомендуемая дата мероприятия или посещения и т.п.),
- с) выбор единственного варианта ответа из списка и с помощью переключателей (например, пол, возрастная группа, форма обучения, специальность),
- д) выбор нескольких вариантов с помощью флажков (например, знания, предпочтения, сферы интересов, участие в мероприятиях и т.п.)

### Лабораторная работа № 7

*Тема:* Применение средства восстановления остаточной информации на примере Foremost или аналога.

Применение специализированного программно средства для восстановления удаленных файлов.

Применение программ для безвозвратного удаления данных.

Применение программ для шифрования данных на съемных носителях.

*Цель:* Ознакомиться со средствами восстановления остаточной информации;

Ознакомиться со средствами восстановления удаленных файлов.

Ознакомиться с программами безвозвратного удаления файлов.

Ознакомиться с программами шифрования данных.

*Количество часов:* 4

*Порядок работы:*

*Задание 1.* Приведите примеры программ восстановления данных. Опишите их возможности.

Составьте сравнительную характеристику.

*Задание 2.* Опишите возможности программы восстановления данных Foremost. Как Foremost восстанавливает файлы? Опишите параметры запуска программы Foremost.

*Задание 3.* Создайте произвольный каталог и запишите туда данные каталога другого каталога. Удалите созданный каталог. С помощью Foremost восстановите данные.

*2. Задание 1.* Опишите назначение и возможности программы Easy Recovery Pro.

*Задание 2.* Создайте на рабочем столе файл. Удалите его в Корзину. Восстановите файл из Корзины.

*Задание 3.* Создайте текстовый файл на диске D: с именем Proba.txt, введите свою фамилию, закройте и сохраните файл. Удалите созданный файл. Очистите Корзину. Восстановите файл с

помощью программы Easy Recovery Pro.

*Задание 4.* Создайте на диске D:\ папку с именем Директория. Перепишите в созданную папку с диска C:\ файл Proba.txt. Удалите папку Директория. Очистите Корзину. Восстановите папку с помощью Easy Recovery Pro

**3.Задание 1.** Опишите программные механизмы удаления данных. Достоинства и недостатки.

На чем основаны программные методы гарантированного удаления информации?

*Задание 2.* Опишите механические механизмы удаления данных. Как работают аппаратные средства гарантированного удаления информации?

*Задание 3.* Сравните программные и аппаратные средства гарантированного удаления информации.

*Задание 4.* Проконтролируйте удаление файла с помощью стандартного метода удаления. Реализовать восстановление файла, после удаления стандартными средствами ОС.

*Задание 5.* Изучите методы уничтожения данных с электронных носителей путем многократной перезаписи.

**4. Задание 1.** Создайте на диске C:\Темп папку и скопируйте в нее любой файл. Зашифруйте файл вместе с папкой таким образом, чтобы все помещаемые в папку файлы тоже шифровались (если шифрование не удалось – дальнейшие действия с папкой делайте, как с зашифрованной).

Создайте на рабочем столе папку с вашей фамилией и добавьте в неё резервную копию зашифрованной вами папки (сохраняя шифрование).

*Задание 2.* Программа VeraCrypt позволяет создавать виртуальный зашифрованный диск, представляющий собой файл, который можно смонтировать в локальный диск. Программа NeoCrypt позволяет шифровать содержимое файла без изменения его расширения. Опишите возможности этих программ.

### Лабораторная работа № 8

*Тема:* Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений.

*Цель:* ознакомиться с инструментальными средствами обнаружения вторжений.

*Количество часов:* 6

*Порядок работы:*

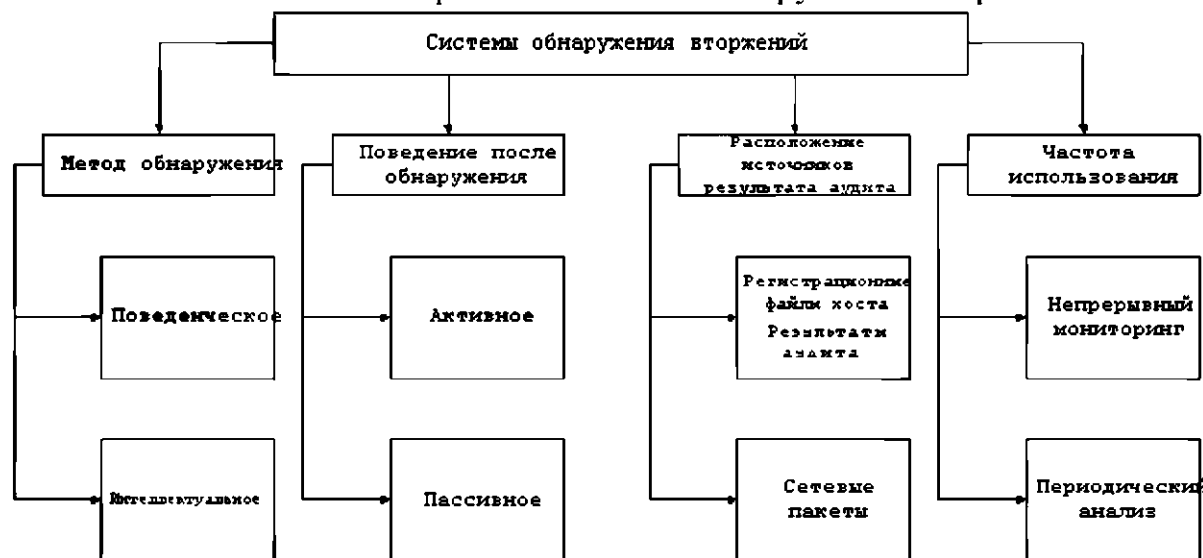
*Задание 1.* Выделяют следующие методы обнаружения вторжений:

- сигнатурный анализ;
- использование статистики Байеса;
- продукционные (экспертные) системы;
- анализ перехода системы из состояния в состояние и сети Петри;
- статистический анализ;
- относительная частота последовательностей;
- модель среднего значения и среднеквадратичного отклонения;

- операционная модель;
- модель временных серий.

Опишите один из методов обнаружения вторжений.

Задание 2. Поясните классификацию систем обнаружения вторжений.



### Лабораторная работа № 9

Тема: Развертывание VPN.

Цель: изучить технологии VPN.

Количество часов: 2

Порядок работы:

Задание 1. Дана БД предприятия, состоящая из трех таблиц.

Задание 2. Опишите этапы создания VPN сервера в Windows.

Задание 3. Опишите этапы создания VPN клиента в Windows.

Задание 4. Опишите технологии тестирования виртуальных сетей.

Задание 5. Представьте проект виртуальной сети для заданной организации.

### Лабораторная работа № 10

Тема: Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. Изучение различных способов закрытия "опасных" портов

Цель: изучение архитектур межсетевых экранов.

Количество часов: 4

Порядок работы:

Задание 1. Изучить основные типы архитектур мультихостовых Firewall: Dual Homed Host, Bastion Host, Perimetr, Demilitarized Zone.

Задание 2. Сравнить основные типы архитектур мультихостовых Firewall: Dual Homed Host, Bastion Host, Perimetr, Demilitarized Zone. Результаты представить с помощью таблицы, инициалах и учетном номере личного дела кассира в отделе кадров. Система позволяет вычислять денежный оборот за один или несколько дней, а также осуществлять поиск информации о сделках по номеру паспорта клиента.

## Лабораторная работа № 11

*Тема:* Изучение механизмов защиты СУБД MS Access.

Изучение штатных средств защиты СУБД MSSQL Server.

*Цель:* изучение механизмов защиты СУБД MS SQL Server.

*Количество часов:* 4

*Порядок работы:*

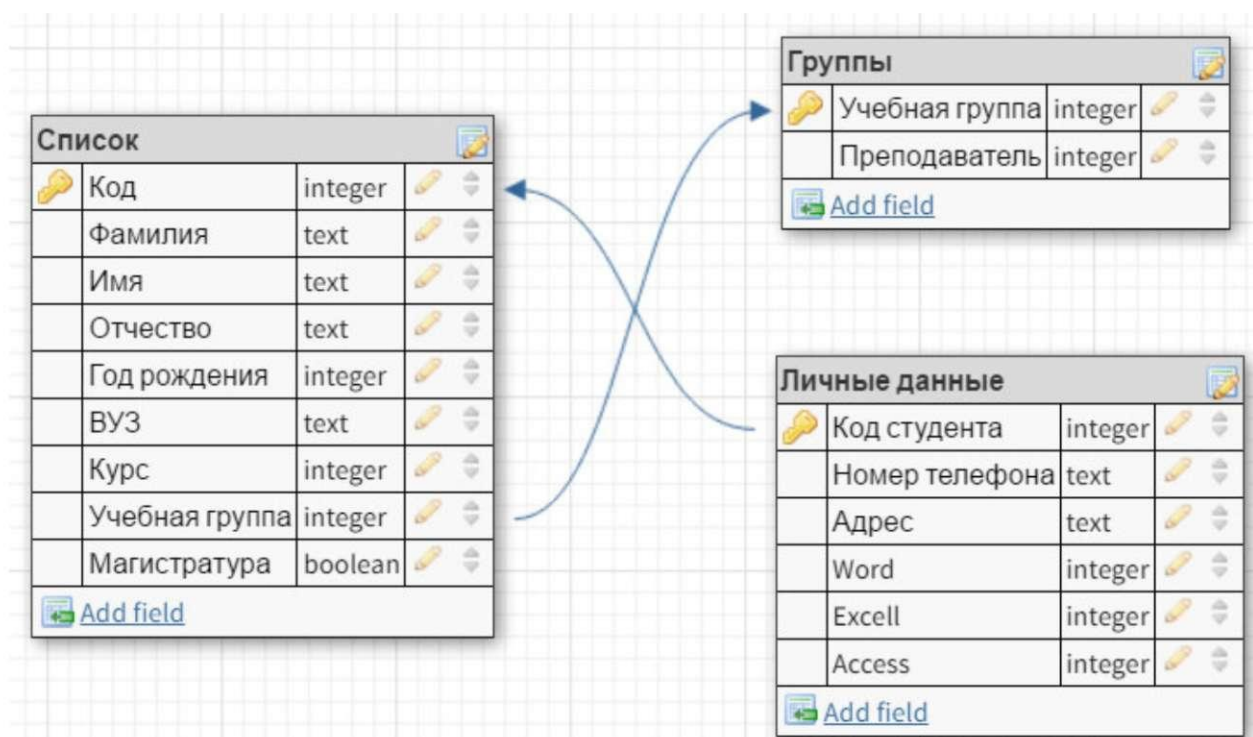
*Задание 1.* Создать базу данных для работы компьютерных курсов (рисунок 1).  
Заполнить таблицу несколькими записями.

*Задание 2.* Установите права на доступ к объектам базы данных.

*Задание 3.* Каким образом обеспечивается целостность данных?

*Задание 4.* Изучите операторы GRANT и REVOKE, используемые для предоставления и отмены привилегий соответственно.

*Задание 5.* Создайте резервную копию базы данных.



## Лабораторная работа № 12

*Тема:* Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов.

Проведение аудита ЛВС сетевым сканером.

*Цель:* изучение сетевых мониторов. Знакомство с сетевыми сканерами безопасности.

*Количество часов:* 4

*Порядок работы:*

*Задание 1.* Поясните структуру системы мониторинга информационной безопасности





*Задание 2.* Изучите назначение и основные возможности сетевых мониторов (RealSecure, SNORT, NFR или другие аналоги).

*Задание 3.* Проведите сравнительный анализ распространенных сетевых мониторов.

Результаты оформите с помощью таблицы.

*2. Задание 1.* Приведите примеры сканеров безопасности сетевых сервисов и протоколов.

*Задание 2.* Опишите возможности сетевого сканера безопасности Shadow Security Scanner или аналога. Основные команды.

*Задание 3.* Перечислите и охарактеризуйте стандартные правила, определяющие параметры.

сессии сканирования. На базе одного из них создайте собственное правило.

*Задание 4.* Проведите сканирование указанных преподавателем компьютеров в учебной лаборатории. При сканировании надо учитывать, что часть имеющихся уязвимостей может быть закрыта путем использования встроенного межсетевого экрана (брандмауэра Windows), появившегося в ОС семейства Windows, начиная Windows XP. Чтобы получить более полную информацию об исследуемых узлах, лучше провести одно сканирование при включенном, другое – при отключенном межсетевом экране (изменение настройки доступно через Панель управления → Брандмауэр Windows). Аналогичная ситуация возникает и при использовании других межсетевых экранов. Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров.

### Лабораторная работа № 13

*Тема:* Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.

*Цель:* знакомство с программными и программно-аппаратными средствами

защиты информации в информационных системах.

*Количество часов:* 4

*Порядок работы:*

*Задание 1.* Приведите примеры законодательных мер защиты информации в ИС.

*Задание 2.* Приведите примеры административных мер защиты информации в ИС.

*Задание 3.* Приведите примеры процедурных мер защиты информации в ИС.

*Задание 4.* Приведите примеры программно-технических мер защиты информации в ИС.

*Задание 5.* Разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты:

1. Общие положения.

1.2. Цели системы информационной безопасности.

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности.

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы.

3. Механизмы обеспечения информационной безопасности Предприятия.

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

#### Лабораторная работа № 14

*Тема:* Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов.

*Цель:* знакомство с приложением SecretNetStudio.

*Количество часов:* 6

*Порядок работы:*

*Задание 1.* Изучите учебную версию приложения SecretNetStudio.

*Задание 2.* Опишите возможности приложения SecretNetStudio. Какие задачи информационной безопасности решаются с помощью этого продукта?

*Задание 3.* Опишите уровни защиты информации с помощью приложения SecretNetStudio





Задание 4. Опишите варианты настройки приложения SecretNetStudio.

### 3. Тематический план и содержание профессионального модуля ПМ. 01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Наименование темы	лабораторная работа обучающихся	Количество часов
<b>РАЗДЕЛ 1 МОДУЛЯ. Применение программных и программно-аппаратных средств защиты информации</b>		
<b>МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b>		
<b>Раздел 3. Защита информации в локальных сетях</b>		
Тема 3.1. Основы построения защищенных сетей	Аутентификация, основанная на IP-адресе. Нетехнические меры защиты от внутренних угроз	4
<b>Раздел 6. Мониторинг систем защиты</b>		
Тема 6.1. Мониторинг систем защиты	Классификация инструментальных средств анализа уязвимостей	2
<b>Итого</b>		<b>6</b>

### Практическая работа № 1

*Тема:* Аутентификация, основанная на IP-адресе. Нетехнические меры защиты от внутренних угроз

*Цель:* Изучение способов защиты информации от вирусов на примере программы Антивирус Касперского.

*Количество часов:* 4

*Порядок работы:*

*Задание 1.* Настройте обновление сигнатур антивирусной программы и обновите их.

*Задание 2.* Изучите настройки Файлового, Почтового и Веб-антивируса.

*Задание 3.* Проверьте любой внешний носитель информации на вирусы.

*Задание 4.* Подготовьте доклад и презентацию на тему: «Общие сведения и особенности работы антивирусной программы [Название антивирусной программы]». Название антивирусной программы выбрать согласно своему варианту из вариантов заданий к работе. Объем доклада 4–5 страницы. Слайдов в презентации не менее пяти, по времени 7–10 минут. Варианты заданий

### Практическая работа № 2

*Тема:* Классификация инструментальных средств анализа уязвимостей

*Цель:* изучение функционала и областей применения DLP систем на примере InfoWatch Traffic Monitor или других аналогов.

*Количество часов:* 2

*Порядок работы:*

*Задание 1.* Опишите основные функции InfoWatch Traffic Monitor.

*Задание 2.* Опишите компоненты системы InfoWatch Traffic Monitor

*Задание 3.* Опишите варианты настройки приложения InfoWatch Traffic Monitor.

Наименование темы	лабораторная работа обучающихся	Количество часов
<b>РАЗДЕЛ 2 МОДУЛЯ. Применение криптографических средств защиты информации</b>		
<b>МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b>		
<b>Раздел 1. Математические основы защиты информации</b>		
Тема 1.1. Математические основы криптографии	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений Проверка чисел на простоту Решение задач с элементами теории чисел.	6
<b>Раздел 2. Классическая криптография</b>		
Тема 2.1. Методы криптографической защиты информации	Применение классических шифров замены Применение классических шифров перестановки Применение метода гаммирования	6
Тема 2.2. Криптоанализ	Криптоанализ шифра простой замены методом анализа частотности символов Криптоанализ классических шифров методом полного перебора ключей Криптоанализ шифра Вижинера	10

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	Применение методов генерации ПСЧ	2
<b>Раздел 3. Современная криптография</b>		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Кодирование информации Программная реализация классических шифров Изучение реализации классических шифров замены и перестановки в программе СтурTool или аналоге.	6
Тема 3.2. Симметричные системы шифрования	Изучение программной реализации современных симметричных шифров	4
Тема 3.3. Асимметричные системы шифрования	Применение различных асимметричных алгоритмов. Изучение программной реализации асимметричного алгоритма RSA	4
Тема 3.4. Аутентификация данных. Электронная подпись	Применение различных функций хеширования, анализ особенностей хешей Применение криптографических атак на хеш-функции. Изучение программно-аппаратных средств, реализующих основные функции ЭП	8
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	Применение протокола Диффи-Хеллмана для обмена ключами шифрования. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	4
Тема 3.7. Защита информации в электронных платежных системах	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	4
Тема 3.8. Компьютерная стеганография	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ Реализация простейших стеганографических алгоритмов	2
<b>Итого:</b>		<b>56</b>

### Лабораторная работа № 1

*Тема:* Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений. Проверка чисел на простоту Решение задач с элементами теории чисел.

*Цель:* научиться решать линейные диофантовые уравнения с двумя неизвестными, используя алгоритм Евклида. Научиться проверять числа на простоту. Решение задач с элементами теории чисел.

*Количество часов:* 6

*Порядок работы:*

*Задание 1.* Повторить алгоритм Евклида. Как с помощью алгоритма Евклида найти НОД двух чисел?

*Задание 2.* Приведите определение неопределенного уравнения.

*Задание 3.* Приведите определение диофантового уравнения.

*Задание 4.* Приведите примеры линейных диофантовых уравнений.

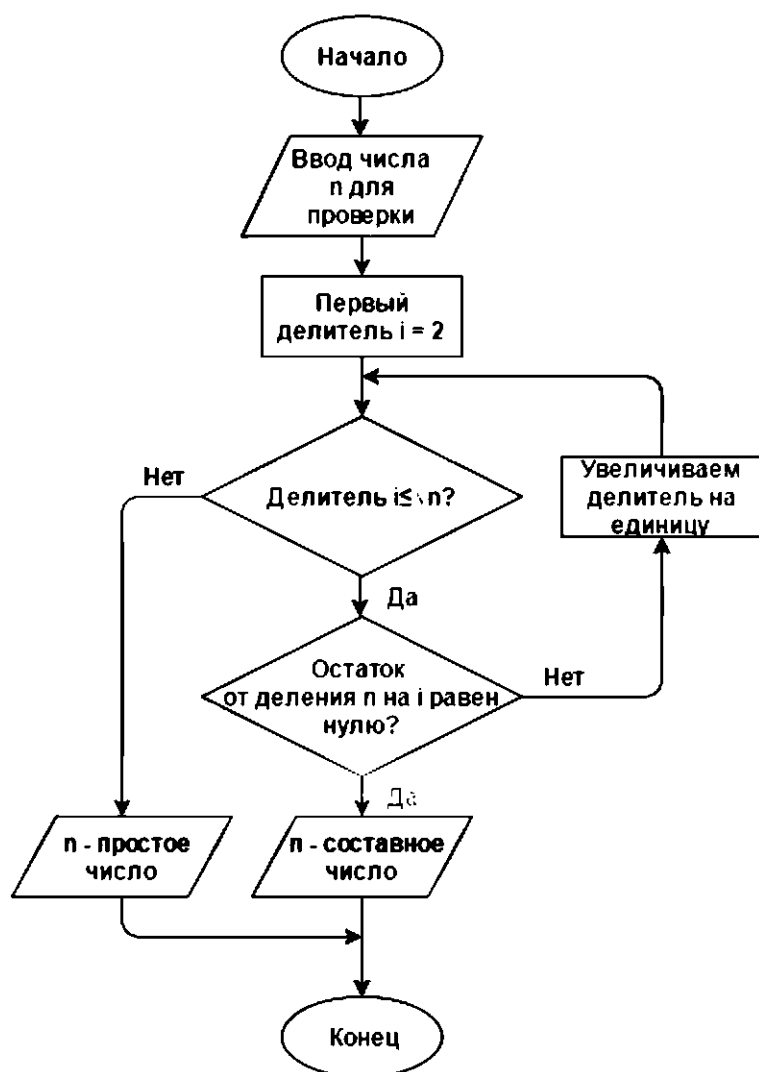
*Задание 5.* Изучите способ проверки числа на простоту «Пробное деление».

Словесное описание: способ состоит в последовательном делении числа на все нечетные числа, которые содержатся в интервале. Если в процессе деления получим целый результат, то число составное. Если же при переборе всех нечетных чисел из интервала разделить число на эти числа нацело нельзя, то число простое (рисунок 1).

Программная реализация на языке C++:

Рисунок

```
bool prime(long long n){  
    for(long long i=2;i<=sqrt(n);i++)  
        if(n%i==0)  
            return false;  
    return true;  
}
```



Задание 1. Найти все простые числа, не превосходящие 60.

Задание 2. Разложить на простые множители  $n = 29359$ .

Задание 3. При каких натуральных  $n$  число  $a = 2n + 1$  делится на 3?

Задание 4. Найти все делители числа 496 и сумму его собственных делителей.

Задание 5. Доказать, что если  $p > 4$  и взаимно просто с 6, то  $p^2 - 1$  делится на 24.

Задание 6. Найти НОД (1176, 315).

Задание 7. Решить систему сравнений.

## Лабораторная работа № 2

Тема: Применение классических шифров замены;

Применение классических шифров перестановки;

Применение метода гаммирования.

Цель: научиться применять классические шифры замены. Научиться применять классические шифры перестановки. Научиться применять метод гаммирования.

Количество часов: 6

*Порядок работы:*

**1. Задание 1.** Выбрать один из методов замены:

- а) шифр Атбаш;
- б) шифр Цезаря;
- в) шифр Полибианский квадрат;
- г) шифр Трисимуса;
- д) шифр многоалфавитной замены Вижинера;
- е) шифр биграммami;
- ж) шифр Гронсфельда.

Составить алгоритм программы шифрования по выбранному методу.

**Задание 2.** Составить программу шифрования по выбранному методу.

**Задание 3.** Составить алгоритм программы расшифрования по выбранному методу. Составить программу расшифрования по выбранному методу.

**2.Задание 1.** Выбрать один из методов перестановки:

- а) обратное написание текста;
- б) простая перестановка по таблице;
- в) одиночная перестановка по ключу по таблице;
- г) одиночная перестановка символов с пропусками по таблице;
- д) двойные перестановки столбцов и строк;
- е) шифр «Магический квадрат»;
- ж) шифр «Решетки» или «Трафареты».

Составить алгоритм программы шифрования по выбранному методу.

**Задание 2.** Составить программу шифрования по выбранному методу.

**Задание 3.** Составить алгоритм программы расшифрования по выбранному методу. Составить

программу расшифрования по выбранному методу.

**Задание 4.** Дешифровать сообщения:

- а) Бирои имч еыеес витсч арзки танет есарл лпюсп мотоо еипнф кйаои крслт мн;
- б) тиюоско нцрпоед иявдттж афэелиа ткокнбв еапанъг уитриоб;
- в) икинорткелэоидарждедлок.

**3.Задание 1.** Выбрать один из способов гаммирования:

- а) гаммирование по модулю K;
- б) двоичное гаммирование.

Составить алгоритм программы шифрования по выбранному методу.

**Задание 2.** Составить программу шифрования по выбранному методу.

**Задание 3.** Составить алгоритм программы расшифрования по выбранному методу. Составить программу расшифрования по выбранному методу.

### Лабораторная работа № 3

**Тема:** Криптоанализ шифра простой замены методом анализа частотности символов.

Криптоанализ классических шифров методом полного перебора ключей.

## Криптоанализ шифра Вижинера.

*Цель:* Научиться выполнять криптоанализ шифра простой замены методом анализа частотности символов; Научиться выполнять криптоанализ классических шифров методом полного перебора ключей; Научиться выполнять криптоанализ шифра Виженера.

*Количество часов:* 10

*Порядок работы:*

**Задание 1.** Получить от преподавателя текстовый файл, содержащий большой художественный текст на русском языке в открытом виде. Написать программу «Частота символов». Исследовать частотность символов открытого текста.

**Задание 2.** Получить от преподавателя текстовый файл, содержащий большой объем зашифрованного текста на русском языке. Исследовать частотность зашифрованного текста.

**Задание 3.** Сравнивая реальную частотность символов русского языка, полученную в пункте 1, с частотностями зашифрованного текста, составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст, реализовав программу дешифровки. Дешифровке подвергните только первые 15–20 символов, наиболее часто встречающиеся в шифротексте.

**Задание 4.** Выполнить эвристический анализ текста, полученного в результате дешифровки.

По смыслу текста выявить те замены, которые оказались неверными, и сформировать верные замены. Доведите результат дешифровки до приемлемого (удобочитаемого) вида.

**2.Задание 1.** Расшифровать фразу, зашифрованную столбцовой перестановкой:

- а) ОКЕСНВРП\_ЫРЕАДЕЫН\_В\_РСИКО;
- б) ДСЛИЕЗТЕА\_Ь\_ЛЮВМИ\_\_АОЧХК;
- в) НМВИАИ\_НЕВЕ\_СМСТУОРДИАНКМ;
- г) ЕДСЗЫНДЕ\_МУБД\_УЭ\_КРЗЕМНАЫ;
- е) СОНРЧОУО\_ХДТ\_ИЕИ\_ВЗКАТРРИ.

**Задание 2.** Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки):

- а) СЯСЕ\_ЛУНЫИАККННОГЯДУЧАТН;
- б) МСЕЫ\_ЛЫВЕНТОСАНТУЕИ\_РЛПОБ;
- в) АМНРИД\_УЕБСЫ\_ЕЙРСООКОТНВ\_;
- г) ОПЧУЛС\_БООНЕВ\_ОЖАЕОНЕЩЕИН;
- е) ЕШИАНИРЛПГЕЧАВРВ\_СЕЫНА\_ЛО.

**3. Задание 1.** Составить алгоритм шифрования и расшифрования методом Виженера.

**Задание 2.** Задан некоторый текст зашифрованный шифром Виженера, требуется определить ключевое слово и прочесть открытый текст.

Шифрованный текст

Влцдугжбюцхъяррмшбрхцэоэцгбрьцмйфктъяюьмшэяцпунуящэйтэъ  
дкцибрьцгбрпачкъяуцпъбъсэгкъягуушарцэъвърюуююэкаазбрняфукабъарпяъф

кьиьжяффнйояфывбнэнфуюгбрьсшьжэтбэёчюьюрьегофкбъчябашвёуъюадн  
чжчужцёэвлрнчулбюпцуруньъшсёюзкцхъяррнрювяспэмасчкпэужъжыатуфуя  
рюравртубурьпэшцлафоуфбюацмнубсюкйтаьэджюнооэгюожбгкбрънцэпотчмёо  
дзцвбцшщвщепчдчдрьюьскасэгьппэгюкдойрсрэвоопчщшоказръббнэугнялёкь  
србёуыэбдэулбюасшоуэтьшкрсдугэфлбубуьчнчтртпэгюкиугюэмэгюккьпэгя  
апуфуэзьрадзьжчюрмфцхраююанчёчюыхъцомэфьцпоирькншпэтэузуябашу  
шбаыэйчдфрпэцърьцыцпоилуфэдцойэдытррачкубуфнйтаьэдкцкрннцюабугюу  
убурьпйюэьжтгюркуюшоъуфъэгясуоичщщчдцсфырэдщэуяфшёчцюйрщвяхв  
мкршрпгюопэуццйтаьэдкцибрыцыяжтюрбуэтэбдуюцэубъибрювьежагибргаб  
рымпуноцшяжцечкфодщюъчжшйуьцхщвуэбдлдьэгясуахзцэбдэулькнъщбжяц  
эрьёдьвьовлрнуяфуоухфекьгцччгэьжтанопчынажпачкьюьмэнкйрэфшэьбд  
эндадьярёюэлэтчоубъцэфэвлнёгфдсэвэёкбсчоукгаутэыпуббцкпэгючсаьбэн  
эфьркацхёваетуфяепьрювьржадфёжбьфутощоявььгупчршуитеачйчирамчнюфч  
оуяюонкяжыкгсцбрысшчйотъьжрсщчл.

#### Лабораторная работа № 4

*Тема:* Применение методов генерации ПСЧ

*Цель:* изучение способов применения методов генерации ПСЧ.

*Количество часов:* 2

*Порядок работы:*

*Задание 1.* Написать программу, выполняющую задачу исследования ДСЧ для одного из следующих вариантов:

1. Исследовать равномерность датчика (проверить гипотезу о равномерности распределения совокупности ДСЧ).
2. Определить период ДСЧ для различных параметров.
3. Исследовать автокорреляцию совокупности ДСЧ для различных параметров на глубину 100 отсчетов.
4. Построить гистограмму частоты появления каждого возможного значения совокупности ДСЧ.

*Задание 2.* Разработать и отладить ПО для исследования датчика псевдослучайных чисел.

Представить результаты исследования в графическом виде eReader

#### Лабораторная работа № 5

*Тема:* Кодирование информации.

Программная реализация классических шифров.

Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.

*Цель:* изучение способов кодирования информации. Изучение способов кодирования информации. Ознакомиться с меню, возможностями программы CrypTool.



Количество часов: 6

Задание 1. Дана кодовая таблица азбуки Морзе:

А • –	Л • • •	Ц – • – •
Б – • • •	М – –	Ч – – – •
В • – –	Н – •	Ш – – – –
Г – – •	О – – –	Щ – – • –
Д – • •	П • – – •	Ъ • – – • – •
Е •	Р • – •	Ы – • – –
Ж • • • –	С • • •	Ь – • • –
З – – • •	Т –	Э • • – • •
И • •	У • • –	Ю • • – –
Й • – – –	Ф • • – •	Я • – • –
К – • –	Х • • • •	

Декодируйте сообщение:

Закодируйте с помощью азбуки Морзе слова ПАРОЛЬ, ЭКРАНИРОВАНИЕ, КОДИРОВАНИЕ

Задание 2. Средние века для шифрования перестановкой применялись и магические квадраты.

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила. Пример магического квадрата и его заполнения сообщением «Прилетаю восьмого» показан ниже (рисунок 3).

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером  $3 \times 3$  (если не учитывать его повороты). Количество магических квадратов  $4 \times 4$  составляет уже 880, а количество магических квадратов  $5 \times 5$  – около 250000.

Пользуясь изложенным способом создать программу, которая:

- а) зашифрует введенный текст и сохранит его в файл;
- б) считывает зашифрованный текст из файла и расшифрует данный текст.

Задание 3.. Ознакомиться с меню, возможностями программы CryptTool.

*Задание 4.* Перечислите классические алгоритмы шифрования, которые описаны и реализованы в программе CrypTool.

*Задание 5.* Зашифровать и расшифровать сообщение с помощью одного из имеющегося в программе CrypTool классического шифра замены и шифра перестановки.

#### Лабораторная работа № 6

*Тема:* Изучение программной реализации современных симметричных шифров

*Цель:* Ознакомиться с современными симметричными шифрами.

*Порядок работы:*

*Количество часов:* 4

*Задание 1.* Представьте алгоритм работы российского стандарта шифрования ГОСТ 28147-89.

*Задание 2.* Представьте алгоритм работы американского стандарта шифрования DES.

Сравните алгоритмы шифрования ГОСТ 28147-89 и DES.

*Задание 3.* Выполнить ручное шифрование исходного текста с помощью алгоритма DES,

алгоритма ГОСТ 28147-89.

*Задание 4.* Опишите особенности алгоритма AES. Сравните алгоритмы шифрования ГОСТ 28147-89 и AES.

*28147-89 и AES.*

#### Лабораторная работа № 7

*Тема:* Применение различных асимметричных алгоритмов.

Изучение программной реализации асимметричного алгоритма RSA

*Цель:* Ознакомиться с асимметричными алгоритмами. Ознакомиться с асимметричными алгоритмами.

*Количество часов:* 4

*Порядок работы:*

*Задание 1.* Опишите асимметричные алгоритмы шифрования.

Тип	Описание
RSA	
ЕСС (криптосистема на основе эллиптических кривых)	
Эль-Гамаль.	

**Задание 2.** Изучите процедуру создания ключей в алгоритме шифрования RSA на примере.

№ п/п	Описание операции	Пример
1	Выбираются два простых числа <sup>1</sup> <b>p</b> и <b>q</b> .	<b>p=7, q=13</b>
2	Вычисляется произведение <b>n</b> = <b>p * q</b> .	<b>n=91</b>
3	Вычисляется <b>функция Эйлера</b> <sup>2</sup> <b>φ(n)</b> .	<b>φ(n)=(7-1)(13-1)= 91-7-13+1 = 72</b>
4	Выбирается открытый ключ <b>e</b> , как произвольное число ( $0 < e < n$ ), взаимно простое <sup>3</sup> с результатом функции Эйлера ( $e \perp \phi(n)$ ).	<b>e=5</b>
5	Вычисляется секретный ключ <b>d</b> , как обратное число <sup>4</sup> к <b>e</b> по модулю <b>φ(n)</b> , из соотношения $(d * e) \bmod \phi(n) = 1$ .	<b>(d*5) mod 72 = 1, d = 29</b>
6	Публикуются открытый ключ ( <b>e, n</b> ) в специальном хранилище, где исключается возможность его подмены ( <b>общедоступном сертифицированном справочнике</b> ).	

Создайте открытый и секретный ключи для любой другой пары простых чисел.

**Задание 3** Разработать алгоритм шифрования RSA.

**Задание 4.** Разработать и отладить приложение, реализующее алгоритм асимметричного шифрования RSA.

Предлагаемый интерфейс приложения (рисунок 5).

Простые числа  

p =  q =

Зашифровать

Секретный ключ  

d =  n =

Расшифровать

## Лабораторная работа № 8

*Тема:* Применение различных функций хеширования, анализ особенностей хешей.

Применение криптографических атак на хеш-функции.

Изучение программно-аппаратных средств, реализующих основные функции ЭП

*Цель:* Ознакомиться с различными функциями хеширования; Научиться применять криптографические атаки на хеш-функции. Изучить программно-аппаратные средства, реализующие основные функции ЭП.

*Количество часов:* 8

**1 Задание 1.** Опишите функции хеширования.

Тип	Описание
MD2	
MD4	
MD5	
SHA (Secure Hash Algorithm)	

**Задание 2.** Опишите свойства хеш-функций.

**Задание 3.** Ознакомьтесь с алгоритмом работы хеш-функции MD5.

**Задание 4.** Программно реализовать алгоритм MD4 хеширования символьной строки. Хеш- код представить в виде 16-ричного числа.

**2.Задание 1.** Приведите примеры атак на функции хеширования.

**Задание 2.** Противник перехватил хеш  $H = H(M1)$ . Длина хеша  $n$  битов. Он хочет найти любое сообщение  $M2$ , для которого  $H(M1) = H(M2)$ , для чего генерирует  $k$  сообщений и вычисляет их хеши. Какова вероятность успеха?

**Задание 3.** Противник перехватил определенное число хешей разных сообщений. Длина хеша  $n$  битов. Сколько новых сообщений и их хешей надо сгенерировать, чтобы найти коллизию для 50 % перехваченных хешей?

**Задание 4.** Хэш-функция дает хеш длиной 64 бита. Сколько хешей надо сгенерировать, чтобы найти коллизию двух любых сообщений?

**3. Задание 1.** Разработать алгоритм реализации цифровой подписи RSA.

**Задание 2.** В чем отличие подписи RSA от алгоритма шифрования RSA?

**Задание 3.** Приведите примеры программно-аппаратных средств, реализующих основные функции электронной цифровой подписи.

### Лабораторная работа № 9

Тема: Применение протокола Диффи-Хеллмана для обмена ключами шифрования.

Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Цель: 1. Изучить протокол диффи-Хеллмана

Количество часов: 4

Порядок работы:

1. Задание 1. Для каких целей может применяться алгоритм Диффи-Хеллмана?

Задание 2. Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана.

Задание 3. На чём основывается безопасность обмена ключа по схеме Диффи-Хеллмана?

Задание 4. Доказать, что в схеме Диффи-Хеллмана  $K_A = K_B$ .

2. Задание 1. Опишите схему протокола Kerberos (рисунок 6).



Задание 2. Объясните механизм работы протокола Kerberos.

Задание 3. Реализация Kerberos в ОС Windows Server.

### Лабораторная работа № 10

Тема: Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей.

Цель: Ознакомиться с механизмом аутентификации по одноразовым паролям

Количество часов: 4

*Порядок работы:*

*Задание 1.* Приведите примеры устройств, используемых для генерации одноразовых паролей. Опишите алгоритм генерации одноразовых паролей.

*Задание 2.* Опишите способы защиты от атак на одноразовые пароли.

### Лабораторная работа № 11

Тема: Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ.

Реализация простейших стенографических алгоритмов

Цель: Изучить программное обеспечение, используемое для встраивания цифровых водяных знаков.

Изучить простейшие стенографические алгоритмы.

*Количество часов: 2*

*Порядок работы:*

*Задание 1.* Приведите примеры устройств, используемых для генерации одноразовых паролей. Опишите алгоритм генерации одноразовых паролей.

*Задание 2.* Проведите сравнительный анализ программ, используемых для создания цифровых водяных знаков: PhotoWatermark Professional, Image Tuner, EasyWatermark, CryptoFoto.

*Задание 3.* Опишите процесс создания печатного водяного знака в программе Image Tuner.

*Задание 4.* Рассмотреть работу двух программ, позволяющих проводить стеганографические преобразования.

*Задание 5.* Выбрать контейнер и выполнить внедрение в него некоторой информации.

*Задание 6.* Попробовать извлечь информацию из стегоконтейнера, созданного другой программой.

*Задание 7.* От чего зависит криптостойкость стеганографических систем?



## УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Критерии оценивания результатов выполнения практических работ, шкала оценивания

Критерии оценивания:

| умение самостоятельно выполнить работу (произвести расчеты, применить интеллектуальные и исследовательские приемы)

| качество выполнения работы и содержание информационного, расчётного, наглядного материала

□ умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала).

□ соответствие требованиям оформления письменной части

Шкала оценивания:

Результаты оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, если работа выполнена самостоятельно, произведена самооценка, продемонстрированы навыки самостоятельного использования оборудования, дидактического материала, ТСО; отличается новизной, нестандартным, творческим подходом к теме, решению задачи, оформлению; выполнена своевременно, отличается четким и грамотным выполнением в соответствии с рекомендациями преподавателя.

Оценка «хорошо» выставляется обучающемуся, если выполнение работы, самооценка, навыки самостоятельного использования оборудования, дидактического материала, ТСО происходят с посторонней помощью, исполнение работы частично соответствует рекомендациям преподавателя по оформлению, структуре, аккуратности исполнения, сдана в срок.

Оценка «удовлетворительно» выставляется обучающемуся, если в работе отсутствуют установленные рекомендациями порядок и структура работы, работа выполнена не самостоятельно, сдана с опозданием обозначенного срока, объем информации незначительный, из ограниченного числа источников

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ.

Баричев, С. Г. Основы современной криптографии: учебное пособие/ С. Г. Баричев, В. В. Гончаров, Р. Е. Серов — Санкт-Петербург : Лань, 2020.- 175 с.

Основы информационной безопасности [Текст] : учебное пособие : [по направлению подготовки "Информационные системы и технологии"] / [Ю. Ю. Громов и др.]. - Старый Оскол : ТНТ, 2017. - 381 с. : ил.

Мельников, В.П. Методы и средства хранения и защиты компьютерной информации [Текст] : учебник : [по направлениям "Автоматизация технологических процессов и производств", "Конструкторско-технологическое обеспечение машиностроительных производств"] / В. П. Мельников, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - Старый Оскол : ТНТ, 2017. - 399 с. : ил.

Белов Е.Б. Организационно-правовое обеспечение информационной безопасности/ Е.Б. Белов, В. Н. Пржегорлинский. –М.: Издательский центр «Академия». 2020 - 336 с.

Дополнительная литература

Никифоров, С. Н. Методы защиты информации. Пароли, сккрытие, шифрование [Текст : Электронный ресурс] : учебное пособие для вузов / С. Н. Никифоров. - 3-е изд., стер. - Санкт-Петербург : Лань, 2020. - 124 с. – Режим доступа: <https://e.lanbook.com/reader/book/146885/#1>

Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : 2018-06-07 / С. Н. Никифоров. - 1-е изд. - [Б. м.] : Лань, 2018. - 96 с. – Режим доступа: <https://e.lanbook.com/reader/book/107306/#1>