Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»

Стахановский инженерно-педагогический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Луганский государственный университет имени Владимира Даля»

Кафедра информационных систем

УТВЕРЖДАЮ:
Директор СИПИ (филиала)
ФГБОУ ВО «ЛГУ им. В. Даля»
_____ А.А. Авершин
(подпись)
«21» апреля 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

По направлению подготовки 44.03.04 Профессиональное обучение (по отраслям)
Профиль: «Информационные технологии и системы»

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Методы и средства защиты компьютерной информации» по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям). – 48 с.

Рабочая программа учебной дисциплины «Методы и средства защиты компьютерной информации» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям), утвержденным приказом Министерства образования и науки Российской Федерации от 22 февраля 2018 г. № 124 (с изменениями и дополнениями от 26 ноября 2020 г., 27 февраля 2023 г.)

СОСТАВИТЕЛИ:
ст.преп. Ганзенко И.В., канд. техн. наук, доцент Карчевский В.П.

Рабочая программа дисциплины утверждена на заседании кафедры информационных систем «18» апреля 2023 г., протокол № 9 .

Заведующий кафедрой
информационных систем _____ В.П. Карчевский

Переутверждена: «___» _____20___ г., протокол № _____ .

Переутверждена: «___» _____20___ г., протокол № _____ .

Рекомендована на заседании учебно-методической комиссии Стахановского инженерно-педагогического института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Луганский государственный университет имени Владимира Даля» «21» апреля 2023 г., протокол № 3 .

Председатель учебно-методической комиссии
СИПИ (филиала) ФГБОУ ВО «ЛГУ им. В. Даля» _____ Н.В. Банник

© Ганзенко И.В., Карчевский В.П., 2023 год
© ФГБОУ ВО «ЛГУ им. В. Даля», 2023 год

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Цель изучения дисциплины – формирование системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации;

Задачи: формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли; формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов; формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Методы и средства защиты компьютерной информации» относится к модулю «Предметно-содержательный». Основывается на базе дисциплин: «История развития техники. Техническое и методическое творчество», «Информатика и информационные технологии», «Архитектура компьютеров и информационных систем».

Содержание дисциплины является основой для изучения следующих дисциплин: «Робототехника. Основы теории управления», «Компьютерные технологии в учебном процессе», «Вычислительные системы, сети и телекоммуникации», «Компьютерные технологии в учебном процессе», выпускная квалификационная работа бакалавра.

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1. Демонстрирует умение находить и использовать необходимую для взаимодействия с другими членами общества информацию о культурных особенностях и традициях различных социальных и национальных групп УК-5.2. Соблюдает требования уважительного отношения к историческому наследию и культурным традициям различных национальных и социальных	Знать: закономерности и особенности социально-исторического развития различных культур в этическом и философском контексте
		Уметь: понимать и воспринимать разнообразие общества в социально-историческом, этическом и философском контекстах
		Владеть: простейшими методами адекватного восприятия межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах; навыками общения в мире культурного многообразия с использованием этических норм поведения

	групп в процессе межкультурного взаимодействия на основе знаний основных этапов развития России в социально-историческом, этическом и философском контекстах УК-5.3. Умеет выстраивать взаимодействие с учетом национальных и социокультурных особенностей	
ОПК-5. Способен осуществлять контроль и оценку формирования результатов образования обучающихся, выявлять и корректировать трудности в обучении	ОПК-5.1. Формулирует образовательные результаты обучающихся в рамках учебных предметов согласно освоенному (освоенным) профилю (профилям) подготовки ОПК-5.2. Осуществляет отбор диагностических средств, форм контроля и оценки Сформированности образовательных результатов обучающихся ОПК-5.3. Применяет различные диагностические средства, формы контроля и оценки сформированности образовательных результатов обучающихся ОПК-5.4. Формулирует выявленные трудности в обучении и корректирует пути достижения образовательных результатов	Знать: особенности контроля и оценки формирования результатов образования обучающихся в соответствии с образовательными стандартами; современные методы, средства и технологии контроля и оценивания предметных, метапредметных и личностных результатов образования. Уметь: определять характерные черты и особенности современных методов и технологий обучения и диагностики знаний и умений обучающихся; основные способы применения современных методов и технологий обучения и диагностики для контроля и оценки сформированности образовательных результатов обучающихся. Владеть: базовыми представлениями о современных методах и технологиях обучения и диагностики знаний и умений для выявления и корректировки трудности в обучении; практическими навыками применения современных методов и технологий для контроля и оценки качества образовательного процесса.
ПК–6. Способен применять технические средства обучения, компьютеры, гаджеты, информационные технологии, автоматизированные системы обучения, роботы для повышения эффективности обучения	ПК 6.1 – Владеет методологией использования технических средств обучения в учебном процессе ПК 6.2 – Умеет использовать компьютеры, всевозможные гаджеты, информационные технологии в профессиональной деятельности ПК 6.3 – Знает достоинства и характеристики автоматизированных систем обучения ПК 6.4 – Умеет разрабатывать и/или применять роботы, компьютерные программы в обучении.	Знать: виды угроз компьютерной информации; программные методы защиты информации; методы идентификации пользователей; кодирование информации в локальных сетях; назначение пакетов и их структура; стандарты информационной безопасности; законодательное регулирование информационной безопасности; анализ угроз сетевой безопасности; основы теории передачи информации в информационных сетях; аппаратные и программные средства, используемые при эксплуатации информационных сетей; современные международные технологии и протоколы передачи данных, применяемые в информационных сетях; современные международные стандарты передачи данных, применяемые в информационных сетях; принципы создания сетевых программных средств; основные понятия и задачи криптографии; криптографические протоколы; виды угроз компьютерной информации;

		законодательное регулирование информационной безопасности; теоретические основы по информационным технологиям и навыкам по применению ЭВМ в инженерных расчётах, достаточных для последующей самостоятельной работы со специальной литературой и изучения специальных дисциплин; базовые принципы работы с современными табличными процессорами; базовые понятия и определения, используемые в сфере информационной безопасности; методы и средства обеспечения информационной безопасности компьютерных систем; основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам; основные понятия и направления в защите компьютерной информации, принципы защиты информации; принципы классификации и примеры угроз безопасности компьютерным системам; современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности; основные инструменты обеспечения многоуровневой безопасности в информационных системах.
		Уметь: применять методы защиты компьютерной информации в различных предметных областях; иметь представление о направлении развития и перспективах защиты информации; формировать требования к локальной сети с учетом анализа угроз и несанкционированных воздействий; составлять функциональные схемы систем и сетей телекоммуникаций; проектировать протоколы передачи данных в информационных сетях; проводить анализ эффективности информационных сетей; осуществлять шифрование данных с использованием различных шифров; осуществлять дешифрование данных с использованием различных шифров; иметь представление о направлении развития и перспективах защиты информации; работать с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий (ИКТ); организовывать собственную информационную деятельность и планировать ее результаты; применять методы обработки табличных данных при помощи электронных таблиц для решения практических задач в любой области деятельности; составлять и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным; применять на практике собственные и классические алгоритмы криптографической защиты данных; конфигурировать встроенные средства безопасности в операционной системе; проводить анализ защищенности компьютера и

		сетевой среды с использованием сканера безопасности; устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; устанавливать и использовать один из межсетевых экранов; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настроить инструменты резервного копирования и восстановления информации.
		Владеть: методами использования основных положений теории информационной безопасности в различных информационных системах; информацией о направлении развития и перспективах защиты информации; навыками формирование общих требований к организации безопасности локальных сетей с учетом анализа угроз и различных групп нарушителей; законодательной базой регулирование информационной безопасности; навыками принятия решений; эксплуатации технических и программных средств информационных сетей; измерительных приборов и технологического оборудования; выбора критериев для формирования средств информационной сети; законодательной базой регулирование информационной безопасности; широкой общей подготовкой (базовыми знаниями) для решения практических задач в области информационных систем и технологий; способностью использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению; навыками постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей; методами аудита безопасности информационных систем; методами системного анализа информационных систем.

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (зач. ед.)**		
	Очная форма	**Очно-заочная форма**	**Заочная форма**
Объем учебной дисциплины (всего)	**72 (2 зач. ед)**	**-**	**72 (2 зач. ед)**
Обязательная аудиторная учебная нагрузка дисциплины (всего) в том	**48**	**-**	**36**

числе:			
Лекции	12	-	12
Семинарские занятия	-	-	-
Практические занятия	12	-	12
Лабораторные работы	24	-	12
Курсовая работа (курсовой проект)	-	-	-
Другие формы и методы организации образовательного процесса (*расчетно-графические работы, групповые дискуссии, ролевые игры, тренинг, компьютерные симуляции, интерактивные лекции, семинары, анализ деловых ситуаций и т.п.)*	-	-	-
Самостоятельная работа студента (всего)	**24**	**-**	**36**
Итоговая аттестация	зачет с оценкой	-	зачет с оценкой

4.2. Содержание разделов дисциплины

Раздел 1. Концептуальные основы информационной безопасности и защиты информации.

Тема 1.1. Значение информации и ее защиты.

Значение информации и ее защита. Основные понятия защиты информации и информационной безопасности. Способы и методы защиты информационных ресурсов. Классификация методов защиты данных. Информационная безопасность в современных системах управления базами данных.

Тема 1.2. Классификация компьютерных вирусов. Антивирусные программы. Работа с реестром.

Понятие «компьютерный вирус». История развития. Классификация компьютерных вирусов. Понятие «антивирусные программы». Классификация антивирусных программ.

Тема 1.3. Эволюция компьютерных сетей, их классификация. Место и роль локальных сетей. Топология сетей. Среды и типа передачи данных.

Виды компьютерных сетей. Протокол передачи данных. Методы передачи данных в компьютерных сетях. Топологии вычислительных сетей. Технологии передачи информации. Сетевые устройства и средства коммуникаций.

Тема 1.4. Назначение пакетов и их структура. Методы управления обменом. Эталонная модель OSI. Аппаратура локальных сетей.

Кодирование информации в локальных сетях. Код NRZI. Код RZ. Манчестерский код. Бифазный код. Назначение пакетов и их структура. Адресация пакетов. Управление обменом в сети с топологией шина. Управление обменом в сети с топологией кольцо. Управление обменом в сети с топологией шина. Эталонная модель OSI.

Раздел 2. Безопасность современных сетевых технологий

Тема 2.1. Стандартные сетевые программные средства. Сетевые

операционные системы. Адресация в IP-сетях. Технологии локальных сетей.

Стандартные сетевые протоколы. Стандартные сетевые программные средства. Сетевые операционные системы. Адресация в IP-сетях. Технологии локальных сетей.

Тема 2.2.Структура политики безопасности организации.

Стандарты информационной безопасности. Законодательное регулирование информационной безопасности.

Тема 2.3. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Обеспечение информационной безопасности сетей.

Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.

Раздел 3. Криптографические средства защиты информации.

Тема 3.1.Криптографические методы защиты информации. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернама.

Классификация криптографических методов. Системы подстановок. Подстановка Цезаря. Многоалфавитные системы. Системы одноразового использования. Системы шифрования Вижинера.

Тема 3.2. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; простые хэш-функции и хэш-функция MD5.

Основные понятия. MAC и хэш-функции. Простые хэш-функции. Хэш-функция MD5

Раздел 4. Симметричные и асимметричные криптосистемы.

Тема 4.1. Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ, режимы их выполнения. Основные понятия, относящиеся к алгоритмам симметричного шифрования. Определение устойчивости алгоритма. Сеть Фейштеля.

Принципы построения современных блочных алгоритмов. Понятие сети Фейстеля. Стандарт шифрования данных (DES). Режимы работы блочных шифров.

Тема 4.2. Асимметричные системы шифрования (системы с открытым ключом). RSA. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля. Схема RSA: алгоритм шифрования, его оборачиваемость, вопросы устойчивости.

Асимметричные системы шифрования (системы с открытым ключом). Схема RSA. Функции дискретного логарифмирования. Схема Эль-Гамаля.

Тема 4.3. Основные требования к цифровой подписи, прямая и арбитражная цифровые подписи, стандарты цифровой подписи ГОСТ 3410 и DSS.

Основные подходы к формированию цифровой подписи на основе различных алгоритмов с открытым ключом. Отечественные и зарубежные

стандарты на алгоритмы цифровой подписи, применяемые в настоящее время.

4.3. Лекции

4.3.1. Лекции 7-го семестра (очная форма), 8-го семестра (заочная форма)

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1	Значение информации и ее защиты. Классификация компьютерных вирусов. Антивирусные программы. Работа с реестром. Эволюция компьютерных сетей, их классификация. Место и роль локальных сетей. Топология сетей. Среды и типа передачи данных.	2	-	2
2	Назначение пакетов и их структура. Методы управления обменом. Эталонная модель OSI. Аппаратура локальных сетей.	2	-	2
3	Стандартные сетевые программные средства. Сетевые операционные системы. Структура политики безопасности организации. Угрозы и уязвимости проводных корпоративных сетей.	2	-	2
4	Криптографические методы защиты информации. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; простые хэш-функции и хэш-функция MD5.	2	-	2
5	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ, режимы их выполнения. Основные понятия, относящиеся к алгоритмам симметричного шифрования. Определение устойчивости алгоритма. Сеть Фейштеля.	2	-	2
6	Асимметричные системы шифрования (системы с открытым ключом). RSA. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля. Основные требования к цифровой подписи, прямая и арбитражная цифровые подписи, стандарты цифровой подписи ГОСТ 3410 и DSS.	2	-	2
Итого:		**12**	**-**	**12**

4.4. Лабораторные занятия

4.4.1. Лабораторные занятия 7-го семестра (очная форма), 8-го семестра (заочная форма)

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1	Защита данных на этапе ввода. Защита данных средствами MS Excel, средствами MS Access.	4	-	2

	Работа с программами архивации. Работа с реестром. Работа с антивирусами.			
2	Уровневая сетевая архитектура. Эталонная модель OSI. Формирование начальных умений для настройки IP-протокола. Изучение сетевых утилит командной строки Windows.	4	-	2
3	Шифр Цезаря. Алгоритмы блочного шифрования DES.	4	-	2
4	Алгоритмы асимметричного шифрования.	4	-	2
5	Алгоритм RSA	4	-	2
6	Алгоритм шифрования Эль Гамаль. Алгоритмы электронной цифровой подписи	4	-	2
Итого:		**24**	**-**	**12**

4.5. Практические занятия

4.5.1. Практические занятия 7-го семестра (очная форма), 8-го семестра (заочная форма)

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1	Средства ОС для защиты и восстановления данных. Утилиты обслуживания дисков и работы с реестром. Топологии компьютерных сетей. Разновидности кабелей. Расчеты задержки сигналов в кабеле.	2	-	2
2	Управление пользователями и группами. Работа с групповыми политиками. Групповые политики. Политики управления паролями	2	-	2
3	Расчет параметров локальных сетей. Управление Active Directory, создание профиля пользователя. Основы использования DHCP	2	-	2
4	Исследование шифров подстановки (замены)	2	-	2
5	Исследование шифров подстановки, многоалфавитных шифры	2	-	2
6	Исследование шифров подстановки. Исследование шифров перестановки.	2	-	2
Итого:		**12**	**-**	**12**

4.6. Самостоятельная работа студентов

4.6.1. Самостоятельная работа студентов 7-го семестра (очная форма), 8-го семестра (заочная форма)

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
1	Утечки информации: источники, правовые и	Подготовка к лабораторным и	1	-	2

	технологические аспекты борьбы.	практическим занятиям, к текущему и промежуточному контролю знаний и умений.			
2	Безопасность беспроводных технологий.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	1	-	2
3	Виртуальные частные сети (VPN) - технологии и средства организации.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	1	-	2
4	Биометрические системы аутентификации: принципы, технологии и перспективы.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	1	-	4
5	Средства взлома парольных систем и противодействие им.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	2	-	2
6	Защита персональных данных, типовые решения.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	2	-	2
7	Управление программным обеспечением, как аспект обеспечения информационной безопасности. Структура, требования, задачи.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	2	-	2
8	Алгоритмы генерации псевдослучайных последовательностей чисел.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	2	-	
9	Хэш-функции и	Подготовка к	2	-	4

	аутентификация сообщений. MD5, ГОСТ 3411.	лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.			
10	Электронная цифровая подпись (ЭЦП). стандарты ЭЦП: DSS, ГОСТ 3410.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	2	-	4
11	Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	2	-	4
12	Безопасность современных сетевых технологий. Протоколы аутентификации.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	2	-	4
13	Зачет с оценкой		4	-	4
Итого:			**24**		**36**

4.7. Курсовые работы/проекты по дисциплине «Методы и средства защиты компьютерной информации» не предполагаются учебным планом.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий: объяснительно-иллюстративного обучения (технология поддерживающего обучения, технология проведения учебной дискуссии), информационных технологий (презентационные материалы), развивающих и инновационных образовательных технологий.

Лабораторные и практические занятия проводятся с использованием развивающих, проблемных, проектных, информационных (использование электронных образовательных ресурсов (электронный конспект) образовательных технологий.

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы лектором и преподавателем (-ями), ведущими практические и лабораторные занятия по дисциплине в следующих формах*:* контрольные работы, лабораторные работы, практические занятия.

Промежуточная аттестации по результатам освоения дисциплины проходит в форме зачета с оценкой (включает в себя ответы на теоретические вопросы и ответы на тестовые задания). Студенты, выполнившие 75% текущих и контрольных мероприятий на «отлично», а остальные 25 % на «хорошо», имеют право на получение итоговой оценки.

В экзаменационную ведомость и зачетную книжку выставляются оценки по шкале, приведенной в таблице.

Шкала оценивания (экзамен)	Характеристика знания предмета и ответов	Зачеты
отлично (5)	Студент глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.	зачтено
хорошо (4)	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.	
удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.	
неудовлетворительно (2)	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы.	не зачтено

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974

2. Никифоров, С. Н. Методы защиты информации. Шифрование данных / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 160 с. — ISBN 978-5-507-44449-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/224672

3. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие для спо / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-7907-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167186

4. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699

б) дополнительная литература:

1. Келдыш, Наталья Всеволодовна Информационная безопасность. Защита информации на объектах информатизации. Учебное пособие – М.: Мир науки, 2022. – Сетевое издание. Режим доступа: https://izdmn.com/PDF/14MNNPU22.pdf

2. Васильева И.Н. Интеллектуальные системы защиты информации : учебное пособие / И.Н. Васильева, Д.Ю. Федоров. – СПб. : Изд-во СПбГЭУ, 2020.%– 119 с. ISBN 978-5-7310-4986-3. Режим доступа: https://infosec.spb.ru/wp-content/uploads/2020/12/intellektualnye-sistemy-zashhity-informaczii.pdf

3. Терентьев А.И. Основы информационной безопасности. Методы и средства защиты компьютерной информации [Текст] : учебное пособие / А.И. Терентьев. – М. : ИД Академии Жуковского, 2020. – 84 с. ISBN 978-5-907275-59-1. — URL: http://storage.mstuca.ru/xmlui/handle/123456789/8842

в) методическая литература:

1. Конспект лекций по дисциплине «Методы и средства защиты компьютерной информации» для студентов направления подготовки Профессиональное обучение (по отраслям), профиль «Информационные технологии и системы» (в 3-х частях). Часть 1. / Сост.: И.В.Ганзенко. – Стаханов: ГОУ ВО ЛНР «ЛГУ им. В. Даля», 2022. – 77 с.

2. Конспект лекций по дисциплине «Методы и средства защиты компьютерной информации» для студентов направления подготовки Профессиональное обучение (по отраслям), профиль «Информационные

технологии и системы» (в 3-х частях). Часть 2. / Сост.: И.В.Ганзенко. – Стаханов: ГОУ ВО ЛНР «ЛГУ им. В. Даля», 2022. – 76 с.

3. Конспект лекций по дисциплине «Методы и средства защиты компьютерной информации» для студентов направления подготовки Профессиональное обучение (по отраслям), профиль «Информационные технологии и системы» (в 3-х частях). Часть 3. / Сост.: И.В.Ганзенко. – Стаханов: ГОУ ВО ЛНР «ЛГУ им. В. Даля», 2023. – 50 с.

4. Карчевский В.П., Волков А.П., Чёрная Е.С., Авершина М.В., Тимошенко Д.С., Ганзенко И.В., Труфанова М.К., Владарский И.В. Исследование тенденций развития и инноваций в образовании с использованием искусственного интеллекта: учебное пособие для дополнительного изучения информационных технологий, робототехники и искусственного интеллекта в инженерно-педагогическом образовании для студентов очной и заочной форм обучения направления подготовки «Профессиональное обучение. Информационные технологии и системы» / В.П. Карчевский, А.П. Волков, Е.С. Чёрная, М.В. Авершина, Д.С. Тимошенко, И.В. Ганзенко, М.К. Труфанова, И.В. Владарский; под общ. редакцией В.П. Карчевского. – Луганск: СИПИМ ЛГУ им. В.ДАЛЯ, 2021. – 1024 с.

г) Интернет-ресурсы:

1. Министерство науки и высшего образования РФ – https://minobrnauki.gov.ru/
2. Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru/
3. Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru
4. Федеральный портал «Российское образование» – http://www.edu.ru/
5. Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/
6. Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru/

Электронные библиотечные системы и ресурсы

1. Электронно-библиотечная система «Консультант студента» – http://www.studentlibrary.ru/cgi-bin/mb4x
2. Электронная библиотека ФГБОУ ВО «ЮРГПУ (НПИ) имени М.И. Платова» «МегаПро» https://libweb.srspu.ru/MegaProWeb/Web.

Информационный ресурс библиотеки образовательной организации

Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru/

8. Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Методы и средства защиты компьютерной информации» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и

нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Программное обеспечение:

Функциональное назначение	Бесплатное программное обеспечение	Ссылки
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплейер	VLC	http://www.videolan.org/vlc/

9. Оценочные средства по дисциплине

Паспорт
оценочных средств по учебной дисциплине
«Методы и средства защиты компьютерной информации»

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине	Контролируемые темы учебной дисциплины, практики	Этапы формирования (семестр изучения)
	УК-5.	Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1. УК-5.2. УК-5.3.	Тема 1.1.	7 (очное), 8 (заочное)
				Тема 1.2.	7 (очное), 8 (заочное)
				Тема 1.3.	7 (очное), 8 (заочное)
				Тема 1.4.	7 (очное), 8 (заочное)
				Тема 2.1.	7 (очное), 8 (заочное)

				Тема 2.2.	7 (очное), 8 (заочное)
				Тема 2.3.	7 (очное), 8 (заочное)
				Тема 3.1.	7 (очное), 8 (заочное)
				Тема 3.2.	7 (очное), 8 (заочное)
				Тема 4.1.	7 (очное), 8 (заочное)
				Тема 4.2.	7 (очное), 8 (заочное)
				Тема 4.3.	7 (очное), 8 (заочное)
2	ОПК-5.	Способен осуществлять контроль и оценку формирования результатов образования обучающихся, выявлять и корректировать трудности в обучении	ОПК-5.1. ОПК-5.2. ОПК-5.3. ОПК-5.4.	Тема 1.1.	7 (очное), 8 (заочное)
				Тема 1.2.	7 (очное), 8 (заочное)
				Тема 1.3.	7 (очное), 8 (заочное)
				Тема 1.4.	7 (очное), 8 (заочное)
				Тема 2.1.	7 (очное), 8 (заочное)
				Тема 2.2.	7 (очное), 8 (заочное)
				Тема 2.3.	7 (очное), 8 (заочное)
				Тема 3.1.	7 (очное), 8 (заочное)
				Тема 3.2.	7 (очное), 8 (заочное)
				Тема 4.1.	7 (очное), 8 (заочное)
				Тема 4.2.	7 (очное), 8 (заочное)
				Тема 4.3.	7 (очное), 8 (заочное)
	ПК–6.	Способен применять технические средства обучения, компьютеры, гаджеты, информационные технологии, автоматизированные системы обучения, роботы для повышения эффективности обучения	ПК 6.1 ПК 6.2 ПК 6.3 ПК 6.4	Тема 1.1.	7 (очное), 8 (заочное)
				Тема 1.2.	7 (очное), 8 (заочное)
				Тема 1.3.	7 (очное), 8 (заочное)
				Тема 1.4.	7 (очное), 8 (заочное)
				Тема 2.1.	7 (очное), 8 (заочное)
				Тема 2.2.	7 (очное), 8 (заочное)
				Тема 2.3.	7 (очное), 8 (заочное)
				Тема 3.1.	7 (очное), 8 (заочное)
				Тема 3.2.	7 (очное), 8 (заочное)
				Тема 4.1.	7 (очное), 8 (заочное)
				Тема 4.2.	7 (очное), 8 (заочное)
				Тема 4.3.	7 (очное), 8 (заочное)

Показатели и критерии оценивания компетенций, описание шкал Оценивания

№ п/п	Код контроли-руемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов	Контроли-руемые темы учебной дисциплины	Наименование оценочного средства
1	УК-5.	УК-5.1. УК-5.2. УК-5.3.	Знать: о своих ресурсах и их пределах (личностных, ситуативных, временных и т.д.), для успешного выполнения порученной работы; Уметь: планировать перспективные цели собственной деятельности с учетом условий, средств, личностных возможностей; реализовывать намеченные цели деятельности с учетом условий, средств, личностных возможностей; Владеть: навыком составления плана последовательных шагов для достижения поставленной цели.	Тема 1.1. Тема 1.2. Тема 1.3.. Тема 1.4. Тема 2.1. Тема 2.2. Тема 2.3. Тема 3.1. Тема 3.2. Тема 4.1. Тема 4.2. Тема 4.3.	Вопросы для обсуждения (в виде докладов и сообщений), вопросы и задания к лабораторным и практическим работам, вопросы к контрольным работам, вопросы и задания к зачету с оценкой.
2	ОПК-5.	ОПК-5.1. ОПК-5.2. ОПК-5.3. ОПК-5.4.	Знать: особенности контроля и оценки формирования результатов образования обучающихся в соответствии с образовательными стандартами; современные методы, средства и технологии контроля и оценивания предметных, метапредметных и личностных результатов образования. Уметь: определять характерные черты и особенности современных методов и технологий обучения и диагностики знаний и умений обучающихся; основные способы применения современных методов и технологий обучения и	Тема 1.1. Тема 1.2. Тема 1.3.. Тема 1.4. Тема 2.1. Тема 2.2. Тема 2.3. Тема 3.1. Тема 3.2. Тема 4.1. Тема 4.2. Тема 4.3.	Вопросы для обсуждения (в виде докладов и сообщений), вопросы и задания к лабораторным и практическим работам, вопросы к контрольным работам, вопросы и задания к зачету с оценкой.

			диагностики для контроля и оценки сформированности образовательных результатов обучающихся. Владеть: базовыми представлениями о современных методах и технологиях обучения и диагностики знаний и умений для выявления и корректировки трудности в обучении; практическими навыками применения современных методов и технологий для контроля и оценки качества образовательного процесса.		
3	ПК–6.	ПК 6.1 ПК 6.2 ПК 6.3 ПК 6.4	Знать: виды угроз компьютерной информации; программные методы защиты информации; методы идентификации пользователей; кодирование информации в локальных сетях; назначение пакетов и их структура; стандарты информационной безопасности; законодательное регулирование информационной безопасности; анализ угроз сетевой безопасности; основы теории передачи информации в информационных сетях; аппаратные и программные средства, используемые при эксплуатации информационных сетей; современные международные технологии и протоколы передачи данных, применяемые в информационных сетях; современные международные стандарты передачи данных, применяемые в информационных сетях; принципы создания сетевых программных	Тема 1.1. Тема 1.2. Тема 1.3.. Тема 1.4. Тема 2.1. Тема 2.2. Тема 2.3. Тема 3.1. Тема 3.2. Тема 4.1. Тема 4.2. Тема 4.3.	Вопросы для обсуждения (в виде докладов и сообщений), вопросы и задания к лабораторным и практическим работам, вопросы к контрольным работам, вопросы и задания к зачету с оценкой.

			средств; основные понятия и задачи криптографии; криптографические протоколы; виды угроз компьютерной информации; законодательное регулирование информационной безопасности; теоретические основы по информационным технологиям и навыкам по применению ЭВМ в инженерных расчётах, достаточных для последующей самостоятельной работы со специальной литературой и изучения специальных дисциплин; базовые принципы работы с современными табличными процессорами; базовые понятия и определения, используемые в сфере информационной безопасности; методы и средства обеспечения информационной безопасности компьютерных систем; основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам; основные понятия и направления в защите компьютерной информации, принципы защиты информации; принципы классификации и примеры угроз безопасности компьютерным системам; современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-		

			безопасности; основные инструменты обеспечения многоуровневой безопасности в информационных системах. Уметь: применять методы защиты компьютерной информации в различных предметных областях; иметь представление о направлении развития и перспективах защиты информации; формировать требования к локальной сети с учетом анализа угроз и несанкционированных воздействий; составлять функциональные схемы систем и сетей телекоммуникаций; проектировать протоколы передачи данных в информационных сетях; проводить анализ эффективности информационных сетей; осуществлять шифрование данных с использованием различных шифров; осуществлять дешифрование данных с использованием различных шифров; иметь представление о направлении развития и перспективах защиты информации; работать с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий (ИКТ); организовывать собственную информационную деятельность и планировать ее результаты; применять методы обработки табличных данных при помощи электронных таблиц для решения практических задач в любой области		

			деятельности; составлять и решать схемотехнические задачи, связанные с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным; применять на практике собственные и классические алгоритмы криптографической защиты данных; конфигурировать встроенные средства безопасности в операционной системе; проводить анализ защищенности компьютера и сетевой среды с использованием сканера безопасности; устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; устанавливать и использовать один из межсетевых экранов; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настроить инструменты резервного копирования и восстановления информации. Владеть: методами использования основных положений теории информационной безопасности в различных информационных системах; информацией о направлении развития и перспективах защиты информации; навыками формирование общих требований к		

			организации безопасности локальных сетей с учетом анализа угроз и различных групп нарушителей; законодательной базой регулирование информационной безопасности; навыками принятия решений; эксплуатации технических и программных средств информационных сетей; измерительных приборов и технологического оборудования; выбора критериев для формирования средств информационной сети; законодательной базой регулирование информационной безопасности; широкой общей подготовкой (базовыми знаниями) для решения практических задач в области информационных систем и технологий; способностью использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению; навыками постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей; методами аудита безопасности информационных систем; методами системного анализа информационных систем.		

Оценочные средства по дисциплине «Методы и средства защиты компьютерной информации»

Вопросы к контрольным работам

7-й семестр (очная форма), 8-й семестр (заочная форма)

1. Понятие атрибутов доступа к файлам. Защита сетевого файлового ресурса на примерах организации доступа в различных операционных системах.
2. Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
3. Современные программно-аппаратные средства защиты компьютерной информации.
4. Несанкционированное копирование программ как тип несанкционированного доступа. Юридические аспекты несанкционированного копирования программ. Способы защиты от копирования.
5. Сравнительный анализ методов воздействия и противодействия в сети Internet.
6. Особенности построения защиты информации в телекоммуникационных сетях.
7. Методы и средства воздействия на безопасность телекоммуникационных сетей.
8. Направления по защите от враждебных воздействий на безопасность компьютерных сетей.
9. Необходимые и достаточные условия предотвращения разрушающего воздействия вируса.
10. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.
11. Аппаратные и программно-аппаратные средства криптозащиты данных.
12. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий.
13. Понятие атрибутов доступа к файлам. Организация доступа к файлам в различных операционных системах
14. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам
15. Организационно-правовая основа защиты информации в ФСИН России.
16. Методы и средства защиты данных от несанкционированного доступа.
17. Понятие и содержание информационной безопасности.
18. Необходимость, назначение и общее содержание организационно-правового обеспечения информационной безопасности.
19. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.
20. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки

21.Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД). Классы и виды НСД

22.Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки

23.Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты

24.Требования и показатели защищенности автоматизированных средств обработки информации.

25.Технические методы защиты информации.

26.Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.

27.Краткий обзор современных методов защиты информации.

28.Обеспечение информационной безопасности в каналах связи.

29.Меры противодействия информационной безопасности в автоматизированных системах обработки данных.

30.Особенности проблем защиты конфиденциальной информации.

31.Достоверность и целостность информации при передаче по каналам связи.

32.Понятие безопасности автоматизированных систем обработки информации.

33.Проблема удаленной аутентификации пользователей. Протоколы CHAP и S/KEY.

34.Электронные ключи HASP. Их классификации, архитектура.

35.Способы защиты от угроз нарушения конфиденциальности, целостности, доступности. Угрозы и уязвимости. Классификация защитных мер и их характеристика.

36.Шифр RSA.

37.Вирусы как класс разрушающих программных воздействий. Защита от вирусов.

38.Классификация технических каналов утечки.

39.Электронно-цифровая подпись и функции хеширования.

40.Проверка ПО на наличие недекларированных возможностей.

41.Защита информации от утечки по техническим каналам.

42.Алгоритм шифрования DES.

43.Классы защищенности АС и СВТ от НСД. Показатели защищенности,

44.требования.

45.Политики безопасности. Дискреционные и мандатные политики.

46.Симметричные и асимметричные криптосистемы.

47.Защита информации в компьютерных сетях.

48.Шифры гаммирования. Формирование гаммы шифра.

49.Сети VPN на основе шифрования.

50.Элементы теории чисел. Сравнимость по модулю.

51.Способы защиты от угроз нарушения конфиденциальности, целостности, доступности. Угрозы и уязвимости. Классификация защитных мер и их характеристика.

52.Шифры гаммирования. Формирование гаммы шифра.

53.Вирусы как класс разрушающих программных воздействий. Защита от вирусов.

54.Электронно-цифровая подпись и функции хеширования.

55.Политика безопасности Белла-ЛаПадулы.

56.Опишите суть метода контрольных сумм.

57.Опишите суть метода двойного ввода данных.

58.Что представляет собой компьютерный вирус?

59.К каким последствиям может привести действие компьютерного вируса?

60.Какими путями распространяется компьютерный вирус?

61.Какие средства защиты от вируса вы знаете?

62.Какие утилиты используются для очистки дисков? В чем отличия в их работе?

63.Что такое архивация данных? Для чего ее необходимо выполнять?

64.Как выполняется очистка реестра?

65.Какие утилиты для работы с дисками и реестром вам известны? Каковы их возможности?

66.Осветите понятия «узел», «линия связи», «топология сети.

67.Перечислите типовые и производные сетевые топологии.

68.Классификация компьютерных сетей по диаметру сети.

69.Что представляет собой кабель на основе витых пар?

70.Что такое эталонная модель ISO / OSI?

71.2. Какие функции выполняют каждые из уровней модели ИSO / OSИ?

72.3. Назовите аппаратуру локальных сетей.

73.Какие утилиты можно использовать для проверки правильности конфигурации TCP / IP?

74.2. Для чего утилита PING?

75.3. Как с помощью утилиты PING оценить пропускную способность сети?

76.Что такое групповая политика?

77.2. Назовите протокол передачи файлов?

78.3. Что такое конфигурация сети?

79.4. Какие вы знаете файловые системы?

80.5. Какие существуют методы перемещения данных?

81.Что такое Active Directory?

82.Что представляет собой рабочая станция?

83.На компьютере выполнена ручная настройка TCP/IP. Вы можете соединиться с любым узлом собственной подсети, но вам не удается соединиться с любым узлом в удаленной подсети. Какова причина проблемы и как ее устранить?

84.Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?

85.Для каких шифров простой замены используется составной ключ?

86.Какие угрозы существуют с точки зрения криптоаналитика? Как классифицируются атаки криптоаналитика?

87.Что является основным объектом криптографии? Какие требования предъявляются к криптографическому закрытию информации?

88.Приведите классификацию криптосистем.

89.Дайте определение хеш-функции?

90.2. Назовите различие между функцией аутентификации пользователя и функцией аутентификации сообщений?

91.Какая процедура является более производительной – асимметричное шифрование/ дешифрование или симметричное шифрование/дешифрование?

92.Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма Эль Гамаль?

93.Какая схема распределения открытых ключей абонентов может использоваться в системе связи, имеющей в своем составе центр сертификации открытых ключей?

Критерии и шкала оценивания по оценочному средству «контрольная работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Контрольная работа выполнена на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
4	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Контрольная работа выполнена на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Контрольная работа выполнена на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Задания к лабораторным и практическим работам

Раздел 1 «Концептуальные основы информационной безопасности и защиты информации»

1. Метод контрольных сумм. Перед вводом вся числовая информация суммируется по строкам и столбцам. Полученные результаты вносятся в бланк ввода данных в виде дополнительного столбца и строки. При вводе данных программным путем выполняется контрольное суммирование вводимых данных по строкам и столбцам. Полученные результаты сравниваются с введенными значениями контрольных сумм по строкам и столбцам. При обнаружении несовпадения введенного значения контрольной суммы и рассчитанного значения контрольной суммы выдается сообщение об ошибке. При наличии одной ошибки в сроке и столбце ошибочное число находится на пересечении строки и столбца, в которых выдано сообщение об ошибке.

2.Создайте базу данных с одной таблицей в приложении MS Access . В таблицу включите 15 полей.

2.1. Для 4-х полей, кроме поля счетчик (генерирующего свои собственные данные), сделать ввод данных обязательным.

2.2. Создайте в режиме Конструктор форму для ввода записей в таблицу.

В свойствах формы задайте источник записей – созданную таблицу. В форму включите 8 из 15 различных полей для ввода записей в таблицу в соответствии с вариантом задания. Проверьте работу масок ввода и заданных условий при вводе информации в таблицу с помощью формы.

2.3. Для текстовых полей определите маски ввода для ввода фамилии, инициалов, номера телефона, для заполнения поля справа налево, для ввода прописных и строчных символов и др.

2.4. Для текстовых полей создайте 3 маски ввода с использованием окна Создание масок.

2.4. Для одного текстового поля определите маску Пароль в окне Настройка масок ввода с количеством вводимых позиций - 3.

2.5. Для числовых полей определите маски ввода для ввода чисел без знака и со знаком, для ввода точно заданного числа позиций, для ввода чисел в пределах заданного числа позиций, для ввода целых и дробных чисел фиксированного и произвольного формата и др.

2.6. Для полей даты/времени определите маски ввода для различных форматов ввода (краткий формат, полный формат и т.д.). Заполнитель маски – символ *.

2.7. В соответствии с вашим вариантом для заданного числа полей установите Условие на значение. Условие на значение установите для текстовых, числовых полей и полей Дата/время.

2.7. В свойствах таблицы задайте Условие на значение для сравнения двух числовых полей.

3. Создайте в MS Access простую базу данных, содержащую 2 таблицы, 2 запроса, 2 формы и 2 отчета.

3.1. . Выполните шифрование созданной БД.

3.2. Выполните расшифровку базы данных.

3.3. Откройте последовательно созданную БД, зашифрованную БД и дешифрованную БД. Просмотрите содержимое всех этих баз данных. Запишите в отчет размеры этих файлов баз данных и вывод об эффективности использования шифрования БД для защиты данных.

4. Задайте пароль для открытия БД.

5. Ограничьте доступ пользователей к настройкам экрана Windows посредством изменения параметров реестра, находящихся в разделе HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Policies\System:

- сделайте недоступным диалог "Свойства: Экран";
- сделайте недоступной вкладку "Фон" диалога "Свойства: Экран";
- сделайте недоступной вкладку "Заставка";
- сделайте недоступным "Оформление";
- сделайте недоступной вкладку "Настройка".

6. Отмените просмотра списка дисков в My Computer.

7. Обеспечьте безопасность реестра:

- Добавьте 3 пользователей и 1 группу в список разрешений;
- Для созданных пользователей и групп назначьте разделу HKEY_CURRENT_USER\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Policies\System разрешения Чтение, Полный доступ и особые разрешения;

- добавьте пользователей и группу в список аудита;

- установите аудит всех попыток чтения, записи и удаления параметров из раздела реестра HKEY_CURRENT_USER\SOFTWARE\Microsoft\ Windows\ CurrentVersion\ Policies\System для разных пользователей.

8. С помощью стандартных утилит операционной системы для вашего компьютера выполнить

– проверку дисков;

– очистку дисков;

– дефрагментацию диска D:

– архивацию папки «Мои документы».

9. С помощью двух любых дополнительных утилит работы с дисками и реестром выполнить очистку и оптимизацию дисков и реестра вашего компьютера.

10. Рассчитайте задержку сигнала в кабеле.

Вариант	Фирма	Марка	Категория	Оболочка	NVP
1	AT&T	1010	3	non-plenum	0,67
2	AT&T	1041	4	non-plenum	0,70
3	AT&T	1061	5	non-plenum	0,70
4	AT&T	2010	3	plenum	0,70
5	AT&T	2041	4	plenum	0,75
6	AT&T	2061	5	plenum	0,75
7	Belden	1229A	3	non-plenum	0,69
8	Belden	1455A	4	non-plenum	0,72
9	Belden	1583A	5	non-plenum	0,72
10	Belden	1245A2	3	plenum	0,69
11	Belden	1457A	4	plenum	0,75
12	Belden	1585A	5	plenum	0,75
13	AT&T	1010	3	non-plenum	0,67
14	AT&T	1041	4	non-plenum	0,70
15	AT&T	1061	5	non-plenum	0,70
16	AT&T	2010	3	plenum	0,70
17	AT&T	2041	4	plenum	0,75
18	AT&T	2061	5	plenum	0,75
19	Belden	1229A	3	non-plenum	0,69
20	Belden	1455A	4	non-plenum	0,72
21	Belden	1583A	5	non-plenum	0,72
22	Belden	1245A2	3	plenum	0,69
23	Belden	1457A	4	plenum	0,75
24	Belden	1585A	5	plenum	0,75

25	AT&T	1010	3	non-plenum	0,67
26	AT&T	1041	4	non-plenum	0,70
27	AT&T	1061	5	non-plenum	0,70
28	AT&T	2010	3	plenum	0,70
29	AT&T	2041	4	plenum	0,75
30	AT&T	2061	5	plenum	0,75

11. Привести пример, демонстрирующий работу через стек протоколов двух объектов. Количество уровней не должно превышать 5-ти.

a. Описать область применения стека протоколов

b. Описать назначение каждого уровня;

c. Описать протоколы взаимодействия каждого уровня;

d. Описать интерфейсы между уровнями ..

12. Разработать собственную модель сетевого взаимодействия (стек протоколов) и организовать передачу между двумя узлами A и B. При последующих условиях:

a. Задано количество уровней;

b. Задано размер сообщений формирует узел A и B;

c. Возможна передача с различным способом.

Объяснить, как ваша сетевая модель соотносится с классической моделью ISO / OSI. Описать назначение каждого уровня.

Вариант	Кол-во уровней	Размер сообщения A	Размер сообщения B	Способ передачи
1	3	10	20	С подтверждением
2	4	30	15	Без подтверждения
3	5	15	5	С подтверждением
4	6	10	30	Без подтверждения
5	7	5	10	С подтверждением
6	3	10	20	Без подтверждения
7	4	15	5	С подтверждением
8	5	5	20	Без подтверждения
9	6	10	30	С подтверждением
10	7	20	15	Без подтверждения
11	3	15	20	С подтверждением
12	4	25	5	Без подтверждения
13	5	30	10	С подтверждением
14	6	5	25	Без подтверждения
15	7	10	15	С подтверждением
16	3	25	5	Без подтверждения
17	4	30	10	С подтверждением
18	5	25	15	Без подтверждения
19	6	15	20	С подтверждением
20	7	10	25	Без подтверждения
21	3	5	30	С подтверждением

22	4	25	5	Без подтверждения
23	5	30	10	С подтверждением
24	6	10	15	Без подтверждения
25	7	20	20	С подтверждением
26	3	5	25	Без подтверждения
27	4	15	30	С подтверждением
28	5	20	5	Без подтверждения
29	6	25	10	С подтверждением
30	7	30	15	Без подтверждения
31	3	20	20	С подтверждением
32	4	5	25	Без подтверждения
33	5	15	30	С подтверждением

13. Проверьте конфигурацию TCP / IP с помощью утилиты ipconfig.

Заполните таблицу:

IP-адрес	
маска подсети	
основной шлюз	
Используется DHCP (адрес DHCP-сервера)	
описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

Контрольные вопросы к лабораторным и практическим работам

1. Для чего необходима защита информации?
2. Какие тенденции защиты информации существуют в современном мире?
3. Какие основные понятия из области информационной безопасности вам известны? В чем их сущность?
4. Какие существуют методы защиты информации, для чего они используются?
5. Какие методы защиты применяются на этапе ввода данных в информационную систему?
6. Какие средства защиты существуют в современных системах управления базами данных?
7. Опишите суть метода контрольных сумм.
8. Опишите суть метода двойного ввода данных.
9. Перечислите ограничения и условия, которые можно наложить на вводимые данные.
10. Объясните, что такое шифрование базы данных?
11. Группа «Users» - это …

12. Файл рабочей группы - это …
13. Защищенная рабочая группа – это …
14. Учетная запись группы -это …
15. Учетная запись пользователя - это …
16. Группа «Admins» - это …
17. Учетная запись «Admin» - это …
18. Рабочая группа – это …
19. Что представляет собой компьютерный вирус?
20. К каким последствиям может привести действие компьютерного вируса?
21. Какими путями распространяется компьютерный вирус?
22. Какие средства защиты от вируса вы знаете?
23. Какие виды антивирусных программ вам известны?
24. Против всех видов вирусов может действовать рассмотрена вами антивирусная программа?
25. На каких носителях информации может обезвреживать вирусы антивирусная программа?
26. Как запускается антивирусная программа?
27. Какие действия может выполнять антивирусная программа?
28. Какие объекты могут проверять программа?
29. Как узнать результаты работы программы?
30. Для чего необходимо проводить проверку дисков?
31. Какие функции выполняет программа проверки дисков?
32. Что такое дефрагментация? Для чего ее надо выполнять?
33. Какими средствами можно выполнить дефрагментацию дисков компьютера?
34. Какие утилиты используются для очистки дисков? В чем отличия в их работе?
35. Что такое архивация данных? Для чего ее необходимо выполнять?
36. Как выполняется очистка реестра?
37. Какие утилиты для работы с дисками и реестром вам известны? Каковы их возможности?
38. Что представляет собой кабель на основе витых пар?
39. Как осуществляется передача информации из сети?
40. Какие вам известны виды кабелей?
41. Как осуществляется расчет задержки сигнала в кабеле?
42. Чем отличается non-plenum от plenum?
43. Что такое эталонная модель ISO / OSI?
44. Какие функции выполняют каждые из уровней модели ИSO / OSИ?
45. Назовите аппаратуру локальных сетей.
46. Что такое мосты?
47. Какая аппаратура служит для передачи информации?
48. Какие утилиты можно использовать для проверки правильности конфигурации TCP / IP?
49. Для чего утилита PING?
50. Как с помощью утилиты PING оценить пропускную способность сети?

51. Каким образом команда ping проверяет соединение с удаленным хостом?
52. Что такое хост?
53. Что такое петля маршрутизации?
54. Как выглядят правила маршрутизации, создают петлю?
55. Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равен 30?
56. Зачем нужна таблица ARP?
57. Объясните разницу во времени между обращениями к одному и тому же хосту по имени и IP адресу.
58. Как работает утилита tracert?

Задания к лабораторным и практическим работам
Раздел 2 «Безопасность современных сетевых технологий»

1. Задайте политику, согласно которой на уровне всего компьютера при установке пароля пользователя, потребовалось бы следующее:
   - длина пароля - не менее 8 символов;
   - пользователь не может установить ни один из трех предыдущих паролей;
   - пароль должен отвечать требованиям сложности;
   - максимальный срок действия пароля - 60 дней.

2. Задайте политику на уровне компьютера, выполняющего блокировки учетных записей на 5 минут в том случае, если подряд было сделано не менее трех ошибок входа в систему.

3. Найдите максимально допустимое расстояние Smax между наиболее удаленными станциями локальной сети Ethernet, если известны величины:

En, min = 512 бит - минимальная длина пакета (кадр)

VK = 10 Мбит / с - скорость передачи данных по коаксиальному кабелю;

Vc = 50000 км / с - скорость распространения сигнала в передающей среде;

Tn> 2Tc, max - время передачи пакета (Tn) должен быть более вдвое больше, чем время распространения сигнала (Tc, max) между наиболее удаленными станциями сети.

4. Определите максимальное время реакции на запрос пользователя Tp, пол в локальной сети с кольцевой топологией, где реализуется ППД типа "маркерное кольцо" без приоритетов, если заданные величины:

Npc = 25 - число рабочих станций в сети;

Vc = 50000 км/с - скорость распространения сигналов по коаксиальному кабелю (передающей среде)

Tc = 1500 мкс - время задержки маркера с кадром в одном узле (рабочей станции) сети;

Sk = 12,5 км - длина кольцевого моноканалу;

Ek = 512 байт - общая длина маркера и кадра;

Vk = 4 Мбит / с - скорость передачи данных по моноканалу, все абоненты

сети активные, то есть каждый из них готов к передаче своего кадра и выполняет эту операцию, когда подходит его очередь.

5. Определите максимальное время на передачу кадра от одной станции к другой в сети звездообразной топологии и эстафетной передачей маркера по логическому кольцу (маркер переходит от одной PC к другой в порядке возрастания их сетевых номеров), если заданы величины:

Spc = 0,5 км - расстояние между двумя PC сети (для всех PC оно принимается одинаковым)

Vc = 50000 км / с - скорость распространения сигнала в передающем среде (в коаксиальному кабелю)

Ek = 512 байт - длина кадра вместе с маркером;

Vk = 4 Мбит / с - скорость передачи данных в сети;

Tc = 1500 мкс - время задержки кадра в одном узле сети;

Npc = 32 - число рабочих станций в сети.

6. Создание смешанного профиля. Создать на сервере папку D: \ Profiles (открыть к ней полный общий доступ для группы "Пользователи домена"). Скопировать в эту папку локальный профиль.Установить на скопированный каталог и подкаталоги разрешения "Полный доступ" только для пользователя и группы "Администраторы" (Вкладка безопасность). В меню Active Directory - пользователи и группы, выделить пользователя и в свойствах на вкладке Профиль вписать путь к профилю. Создать сценарий входа пользователя. Файл сценария (например Scenario.bat), поместить в папку Scripts (сетевое имя NETLOGON). В меню Active Directory - пользователи и группы, выделите пользователя и в свойствах на вкладке Профиль в поле сценарий входа нужно вписать имя файла сценария.

7. Запустить виртуальные машины с контроллером домена и клиентской ОС. На клиентской машине создайте новое сетевое подключение и задайте режим автоматического получения IP-адреса. Активизируйте новое соединение и дождитесь окончания автоматической настройки. Убедитесь, что новое сетевое подключение получило IP-адрес из пула адресов DHCP-сервера. Отключите на время сервер DHCP с помощью оснастки DHCP. Повторите опыт с получением сетевого адреса новым сетевым соединением. Запишите, какой адрес присвоен соединению.С помощью службы помощи и поддержки определите, как называются адреса, получаемые клиентской машиной в случае недоступности сервера DHCP.

Контрольные вопросы к лабораторным и практическим работам

1. Что такое групповая политика?
2. Назовите протокол передачи файлов?
3. Что такое конфигурация сети?
4. Какие вы знаете файловые системы?
5. Какие существуют методы перемещения данных?
1. Основные этапы проектирования ЛВС.
2. Принципы проектирования ЛВС.

3. Метод анализа иерархий.
4. Что такое Active Directory?
5. Что представляет собой рабочая станция?
6. Что такое Сценарий входа?
7. Какие существуют виды политики безопасности?
8. Что такое Контроллер домена?
9. О каких проблемах в сети говорит факт получения вашим компьютером автоматического адреса вида 169.254.x.y.
10. Каково назначение маски подсети?
11. На компьютере выполнена ручная настройка TCP/IP. Вы можете соединиться с любым узлом собственной подсети, но вам не удается соединиться с любым узлом в удаленной подсети. Какова причина проблемы и как ее устранить?

Задания к лабораторным и практическим работам
Раздел 3 «Криптографические средства защиты информации»

1. разработать программы для шифрования и расшифровывания русскоязычного текста при помощи шифра перестановки и шифра замены. Программы должны обеспечивать:

- шифрование информации, находящейся в текстовом файле, с записью результата в другой файл;
- шифрование информации, вводимой с клавиатуры, с записью в файл только зашифрованного текста;
- ввод ключа шифрования/расшифрования с клавиатуры без отображения его на экране;
- расшифровку текста, содержащегося в файле, с выводом результатов на экран или в другой файл (ключ расшифровывания вводится с клавиатуры без эха).

1.2. При помощи созданной программы подготовить зашифрованный русский текст объемом не менее 2000 символов.

2. В соответствии со своим вариантом разработать программы для шифрования и расшифровывания русскоязычного текста при помощи шифра, представленного в таблице. Программы должны обеспечивать:

- шифрование информации, находящейся в текстовом файле, с записью результата в другой файл;
- шифрование информации, вводимой с клавиатуры, с записью в файл только зашифрованного текста;
- ввод ключа шифрования/расшифрования с клавиатуры без отображения его на экране;
- расшифровку текста, содержащегося в файле, с выводом результатов на экран или в другой файл (ключ расшифровывания вводится с клавиатуры без эха).

2.1. При помощи созданной программы подготовить зашифрованный русский текст объемом не менее 2000 символов.

Варианты заданий

№ варианта	Шифры
1	Шифр скитала, шифр Трисемуса
2	Шифр скитала, шифр Цезаря
3	Шифр скитала, шифр Цезаря с ключевым словом
4	Шифр скитала, шифр Вижиненра
5	Простая шифрующая таблица, шифр Трисемуса
6	Простая шифрующая таблица перестановки, шифр Цезаря
7	Простая шифрующая таблица перестановки, шифр Цезаря с ключевым словом
8	Простая шифрующая таблица перестановки, шифр Вижиненра
9	Одиночная перестановка по ключу, шифр Трисемуса
10	Одиночная перестановка по ключу, шифр Цезаря
11	Одиночная перестановка по ключу, шифр Цезаря с ключевым словом
12	Одиночная перестановка по ключу, шифр Вижиненра
13	Двойная перестановка по ключу, шифр Трисемуса
14	Двойная перестановка по ключу, шифр Цезаря
15	Двойная перестановка по ключу, шифр Цезаря с ключевым словом
16	Двойная перестановка по ключу, шифр Вижиненра

3. Зашифруйте открытый текст «Криптография – это наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей» биограммным шифром и с помощью магического квадрата 4×4

4. Зашифруйте открытый текст «Криптография – это наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей» с помощью полибианского квадрата и шифром Виженера, секретный ключ задайте сами.

5. Зашифруйте открытый текст «Криптография – это наука о методах и способах преобразования информации с целью ее защиты от незаконных пользователей» шифром Цезаря со сдвигом 7 и простейшего шифра замены, для которого ключ задайте сами.

6. Зашифруйте открытый текст «Система DES – это блочный шифр» с помощью шифра OTP, используя таблицу ASCII, получите двоичный код для заданного текста и преобразуйте его в символы; и зашифруйте открытый текст используя простейший шифр перестановки

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
5	7	30	21	4	9	1	8	29	14	22	2	20	3	11	17	23	25	10	26

21	22	23	24	25	26	27	28	29	30
28	18	12	27	16	24	13	19	15	6

7. Зашифруйте открытый текст «Система DES – это блочный шифр» шифром Цезаря со сдвигом 5 и полибианским квадратом.

8. Зашифруйте открытый текст «Система DES – это блочный шифр» биограммным шифром и с помощью магического квадрата 5×5

9. Зашифруйте открытый текст «Любой шифр может быть вскрыт, если только в этом есть настоятельная необходимость и информация, которую предлагается получить, стоит затраченных средств, усилий и времени. – Норберт Винер» шифром Виженера, секретный ключ задайте сами и шифром полибианский квадрат.

10. Зашифруйте открытый текст «Любой шифр может быть вскрыт, если только в этом есть настоятельная необходимость и информация, которую предлагается получить, стоит затраченных средств, усилий и времени. – Норберт Винер» шифром Цезаря со сдвигом 6 и магическим квадратом 4×4

11. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество. Выполнить проверку, расшифровав полученное сообщение.

Вариант

1 Простая перестановка

2 Одиночная перестановка

3 Двойная перестановка

4 Магический квадрат

5 Шифр Цезаря

6 Полибианский квадрат

7 Шифр Гронсфельда

8 Многоалфавитная замена

9 Простая перестановка

10 Одиночная перестановка

11 Двойная перестановка

12 Магический квадрат

13 Шифр Цезаря

14 Полибианский квадрат

15 Шифр Гронсфельда

16 Многоалфавитная замена

17 Простая перестановка

18 Одиночная перестановка

19 Двойная перестановка

20 Магический квадрат

21 Шифр Цезаря

22 Полибианский квадрат

23 Шифр Гронсфельда

24 Многоалфавитная замена

25 Простая перестановка

26 Одиночная перестановка

27 Двойная перестановка

28 Магический квадрат

29 Одиночная перестановка

30 Шифр Гронсфельда

12. Зашифровать текст при помощи таблицы Вижинера (см. таблицу), используя ключевое слово. Обменяться с партнером зашифрованными тестами и ключевыми словами. Расшифровать текст.

Номер варианта	Текст	Ключевое слово
1.	СТЕГАНОГРАФИЯ СЛУЖИТ ДЛЯ ПЕРЕДАЧИ СЕКРЕТОВ В ДРУГИХ СООБЩЕНИЯХ	АБОНЕНТ
2.	КАК ПРАВИЛО ОТПРАВИТЕЛЬ ПИШЕТ КАКОЕ-НИБУДЬ НЕПРИМЕТНОЕ СООБЩЕНИЕ	СИСТЕМА
3.	ПРИЕМЫ ВКЛЮЧАЮТ НЕВИДИМЫЕ ЧЕРНИЛА, МАЛОПРИМЕТНЫЕ ПОМЕТКИ У БУКВ	РЕШЕНИЕ
4.	В НАСТОЯЩЕЕ ВРЕМЯ ЛЮДИ НАЧАЛИ ПРЯТАТЬ СЕКРЕТЫ В ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЯХ	ТЕХНИКА
5.	В ПЕРЕСТАНОВОЧНОМ ШИФРЕ МЕНЯЕТСЯ НЕ ОТКРЫТЫЙ ТЕКСТ, А ПОРЯДОК СИМВОЛОВ	ПАРТНЕР
6.	КРИПТОГРАФИЯ РЕШАЕТ ПРОБЛЕМЫ СЕКРЕТНОСТИ, ПРОВЕРКИ ПОДЛИННОСТИ, ЦЕЛОСТНОСТИ	ФИНАНСЫ
7.	ПРОТОКОЛ - ЭТО ПОРЯДОК ДЕЙСТВИЙ, ПРЕДПРИНИМАЕМЫХ ДВУМЯ ИЛИ БОЛЕЕ СТОРОНАМИ	АУКЦИОН
8.	ДЕЙСТВИЕ ДОЛЖНО ВЫПОЛНЯТЬСЯ В СВОЮ ОЧЕРЕДЬ И ПОСЛЕ ОКОНЧАНИЯ ПРЕДЫДУЩЕГО	УСЛОВИЕ
9.	КАЖДЫЙ УЧАСТНИК ПРОТОКОЛА ДОЛЖЕН СОГЛАСИТЬСЯ СЛЕДОВАТЬ ПРОТОКОЛУ	ДЕВУШКА
10.	КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ - ЭТО ПРОТОКОЛ, ИСПОЛЬЗУЮЩИЙ КРИПТОГРАФИЮ	ПРИНЦИП
11.	ПОНЯТИЕ ОДНОНАПРАВЛЕННОЙ ФУНКЦИИ ЯВЛЯЕТСЯ ЦЕНТРАЛЬНЫМ В КРИПТОГРАФИИ	ЭКСПЕРТ
12.	ЗНАЮЩИЙ КОМБИНАЦИЮ ЧЕЛОВЕК МОЖЕТ ОТКРЫТЬ	ПОЛИЦИЯ

	СЕЙФ, ПОЛОЖИТЬ В НЕГО ДОКУМЕНТ	
13.	ВСКРЫТИЕ С ВЫБРАННЫМ ОТКРЫТЫМ ТЕКСТОМ МОЖЕТ БЫТЬ ОСОБЕННО ЭФФЕКТИВНЫМ	БУДУЩЕЕ
14.	ИЗ-ЗА НЕДОСТАТКОВ СИСТЕМЫ СИНХРОНИЗАЦИЯ ЧАСОВ МОЖЕТ БЫТЬ НАРУШЕНА	УГЛЕКОП
15.	ОБЫЧНАЯ КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ ИСПОЛЬЗУЕТ ДВА КЛЮЧА	НАПИТОК
16.	ХАКЕР НЕ ПРЕНЕБРЕГАЕТ ОПЕРАТИВНО-ТЕХНИЧЕСКИМИ И АГЕНТУРНЫМИ МЕТОДАМИ	БОТИНОК
17.	ЕСЛИ ВНЕДРЕНИЕ ЗАКЛАДКИ ПРОХОДИТ УСПЕШНО, ВТОРАЯ АТАКА УЖЕ НЕ ТРЕБУЕТСЯ	ДЕРЗКИЙ
18.	ХАКЕР ЗАРАНЕЕ ПРОДУМЫВАЕТ ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ НЕУДАЧИ	СИМПТОМ
19.	ПРОГРАММНАЯ ЗАКЛАДКА, ВНЕДРЕННАЯ В СИСТЕМУ, ЗАМЕТНА ТОЛЬКО ХАКЕРУ	ЧЕМОДАН
20.	С ТОЧКИ ЗРЕНИЯ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМА РАБОТАЕТ КАК ОБЫЧНО	ЭСКУЛАП
21.	ЕСЛИ АТАКА НЕ УДАЛАСЬ, ХАКЕР СТАРАЕТСЯ ОСТАВИТЬ ЛОЖНЫЙ СЛЕД	ВПАДИНА

13. Получите индивидуальное задание у преподавателя. Реализуйте программный модуль в соответствии с полученным заданием. При реализации необходимо учесть следующие моменты:

– предусмотреть возможность задания пользователем параметров шифра;

– предусмотреть визуализацию всех пользовательских настроек;

– для удобства тестирования и взаимодействия с другими модулями реализовать файловый ввод исходных данных и файловый вывод результата криптографического преобразования.

После реализации программного модуля выполните статистический анализ текста по биграммам до криптографического преобразования и после него.

Варианты заданий

– Модуль для шифрования текста с помощью решёток Кардано.

– Модуль для расшифровывания текста с помощью решёток Кардано.

– Модуль для шифрования текста по алгоритму двойной перестановки.

– Модуль для расшифровывания текста по алгоритму двойной перестановки.

Контрольные вопросы к лабораторным и практическим работам

1. Что собой представляют шифры подстановки (замены)? Приведите примеры таких шифров.
2. Что собой представляют шифры перестановки? Приведите примеры таких шифров.
3. Что такое односторонняя функция и функция с «лазейкой»? Приведите примеры таких функций.
4. Дайте определения шифру, ключу, криптосистеме.
5. Сформулируйте основную задачу криптографии.
6. В чем особенность шифров простой замены?
7. Чем отличаются система шифрования Цезаря и аффинная система подстановок Цезаря?
8. Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?
9. Для каких шифров простой замены используется составной ключ?
10. Каким образом заполняется таблица подстановок для шифрования с использованием системы Трисемуса?
11. Дайте характеристику Шифру замены
12. Дайте характеристику Полибианский квадрат
13. Дайте характеристику Шифрование биграммами
14. Дайте характеристику Многоалфавитные шифры замены
15. Дайте характеристику Шифр One – Time – Pad (OTP)
16. Дайте характеристику Шифрование с автоключом. Алгоритм «Crypto»
17. Какие угрозы существуют с точки зрения криптоаналитика? Как классифицируются атаки криптоаналитика?
18. Что является основным объектом криптографии? Какие требования предъявляются к криптографическому закрытию информации?
19. Приведите классификацию криптосистем.
20. Что собой представляет модель Шеннона криптосистемы с секретным ключом?
21. На каких принципах реализуется шифр одноразового блокнота?
22. Оцените количество возможных простых перестановок текста, состоящего из 5 символов? Из 10 символов? Из n символов?
23. Чем принципиально отличаются шифры перестановки от шифров замены?
24. Возможно ли применение статистических методов криптоанализа к перестановочным шифрам?

Задания к лабораторным и практическим работам
Раздел 4 «Симметричные и асимметричные криптосистемы»

1. Разработать приложение для шифрования, позволяющее выполнять следующие действия:

– шифруемый текст должен храниться в одном файле, а ключ шифрования-в другом;

– зашифрованный текст должен сохраняться в файл;

– в процессе шифрования предусмотреть возможность просмотра и изменения ключа, шифруемого и зашифрованного текстов в шестнадцатеричном и символьном виде;

– программа должна показывать время шифрования.

2. Реализовать приложение для дешифрования, позволяющее выполнять следующие действия:

– зашифрованный текст должен храниться в одном файле, ключ – в другом;

– расшифрованный текст должен сохраняться в файл;

– в процессе дешифрования предусмотреть возможность просмотра и изменения ключа, зашифрованного и расшифрованного текстов в шестнадцатеричном и символьном виде.

3. Разработать приложение согласно варианта задания:

1. Зашифровать и дешифровать файл с использованием алгоритма Рабина с идентификацией сообщения по контрольной сумме на ключе не менее 128 бит.

2. Зашифровать и дешифровать файл с использованием алгоритма Рабина с идентификацией сообщения по добавленной метке на ключе не менее 128 бит.

3. Зашифровать и дешифровать файл с использованием алгоритма экспоненциального ключевого обмена Диффи-Хелмана на 2-х участников и блочного шифра TEA в режиме OFB с ключами не менее 128 бит.

4. Зашифровать и дешифровать файл с использованием алгоритма экспоненциального ключевого обмена Диффи-Хелмана на 3-х участников и блочного шифра IDEA в режиме CFB с ключами не менее 128 бит.

5. Зашифровать и дешифровать файл с использованием алгоритма Меркла-Хеллмана с использованием массива весов не менее 100 чисел.

6. Зашифровать и дешифровать файл с использованием алгоритма Месси-Омуры с ключами не менее 128 бит.

4. Разработать приложение, совмещающие в себе достоинства симметричных и асимметричных методов шифрования. Реализовать приложение для шифрования, позволяющее вычислять открытый и закрытый ключи для алгоритма RSA.

5. Рассмотреть общие математические принципы организации процедуры шифрования/дешифрования при использовании метода Эльт-Гамаля.

6. Рассмотреть принцип организации процедуры шифрования и обмена ключами с использованием эллиптических кривых.

7. Реализовать программно алгоритм Эль-Гамаля. Провести шифрование открытого текста, выбранного согласно варианту, указанному преподавателем, и его последующее восстановление.

8. Разработать и реализовать алгоритм электронной цифровой подписи. На контрольном примере проверить правильность работы алгоритма.

Контрольные вопросы к лабораторным и практическим работам

1. Общая схема алгоритма шифрования DES.

2. Почему длина ключа для алгоритма DES равна 56 бит?
3. Как соотносятся между собой матрицы и в алгоритме DES?
4. Как происходит шифрование функции (( ) ( )) в алгоритме DES?
5. Алгоритм получения раундовых ключей ( ) в алгоритме DES.
6. В чём заключается процесс расшифрования данных в DES?
7. Что представляет собой функция () в алгоритме ГОСТ?
8. Как используется заданный ключ при шифровании в алгоритме ГОСТ?
9. Общие черты и отличия алгоритмов ГОСТ и DES.
10. Критерии оценки свойств лавинного эффекта.
11. Перечислите достоинства и недостатки асимметричных алгоритмов в сравнении с симметричными.
12. Перечислите основные трудновычисляемые задачи, использующиеся в современной асимметричной криптографии.
13. Предложите алгоритм укладки рюкзака по сверхвозрастающей последовательности.
14. Каким образом можно идентифицировать зашифрованное сообщение в алгоритме Рабина при дешифрации?
15. Приведите схему ключевого обмена Диффи-Хеллмана на 3-х участников.
16. Докажите обратимость процедур шифрации и дешифрации в алгоритме Меркла-Хеллмана.
17. Какие ограничения накладываются на размер блока шифруемого сообщения в алгоритме Месси-Омуры?
18. Какая процедура является более производительной – асимметричное шифрование/ дешифрование или симметричное шифрование/дешифрование?
19. К какому типу криптоалгоритма (с точки зрения его устойчивости к взлому) и почему относится алгоритм RSA?
20. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма RSA?
21. Опишите принцип шифрования с помощью схемы Эль –Гамаля.
22. На чем основана криптостойкость алгоритма Эль-Гамаля?
23. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма Эль Гамаль?
24. Что называется электронной цифровой подписью?
25. Для чего используется электронная цифровая подпись?
26. Что такое хэш-функция?
27. Что такое дайджест сообщения?

Критерии и шкала оценивания по оценочному средству «лабораторная и практическая работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Задание выполнено на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Задание выполнено на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)
3	Задание выполнено на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Задание выполнено на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

Оценочные средства для промежуточной аттестации (зачет с оценкой – 7-й семестр (очное), 8-й семестр (заочное))

Теоретические вопросы

1. Общие понятия защиты информации.
2. Криптографическая защита информации. Основные понятия.
3. Симметричные алгоритмы шифрования.
4. Потоковые шифры. Шифр Цезаря.
5. Генерация ключей. Генераторы случайных чисел.
6. Алгоритм шифрования DES. Общая схема.
7. Стандарт шифрования ГОСТ 28147-89. Общая схема шифрования.
8. Формирование ключей в алгоритме шифрования ГОСТ 28147-89.
9. Функция преобразования f (R, X) в алгоритме ГОСТ 28147-89.
10. Алгоритм расшифрования ГОСТ 28147-89. Общая схема.
11. Асимметричные алгоритмы шифрования.
12. Алгоритм шифрования RSA.
13. Комбинированные методы шифрования.
14. Функция хеширования. Ее свойства.
15. Электронная цифровая подпись. Классическая схема.
16. Схема цифровой подписи RSA.
17. Основные задачи службы защиты информации предприятия.
18. Что такое информационная безопасность? Понятия и определения в информационной безопасности
19. Пользователи и злоумышленники в Internet.

20. Причины уязвимости сети Internet.
21. Основные закономерности возникновения и классификация угроз информационной безопасности.
22. Пути и каналы утечки информации.
23. Удаленные атаки на интрасети.
24. Классификация "компьютерных вирусов".
25. Файловые вирусы.
26. Загрузочные вирусы.
27. Макровирусы.
28. Сетевые вирусы.
29. Источники "компьютерных вирусов".
30. Основные правила защиты от "компьютерных вирусов".
31. Антивирусные программы.
32. Восстановление пораженных объектов.
33. Стандарт США "Оранжевая книга".
34. Разграничение и контроль доступа к информации.
35. Идентификация и установление подлинности объекта (субъекта).
36. Методы и средства защиты информации от случайного воздействия.
37. Методы защиты информации от аварийных ситуаций.
38. Организационные мероприятия по защите информации.
39. Законодательные меры по защите информации.
40. Обеспечение информационной безопасности в Internet.
41. Архитектура телекоммуникационных систем.
42. Модели безопасности, политика безопасности.
43. Способы хищения информации.
44. Методы идентификации и аутентификации пользователей.
45. Методы простой замены.
46. Методы сложной замены.
47. Шифры перестановки.
48. Шифрование методом гаммирования
49. Основные режимы работ алгоритма DES.

Практические задания

1. Задание определить время перебора всех паролей, состоящих из 6 цифр.

2. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.

3. Допустим, требуется зашифровать сообщения, состоящие из определенных символов. Например, исходный текст состоит из цифры от 0 до 9

(представленных в программе в виде символов) и других знаков и имеет длину в 15 символов. В шифровке на место цифр подставляются соответствующие им знаки, на место всех остальных символов дополнительный 11-й знак.

4. Для шифрования каждой буквы используются двузначные числа. Известно, что буква «е» закодирована числом 20. Среди слов «елка», «полка», «поле», «пока», «кол» есть слова, кодируемые последовательностями цифр 11321220, 20121022.

Выясните код слова «колокол».

5. Для пяти букв алфавита заданы их двоичные коды (для некоторых букв – из двух бит, для некоторых – из трех). Эти коды представлены в таблице:

Определите, какой набор букв закодирован двоичной строкой *1100000100110*.

00	10	1	01	0

6. С помощью двух любых дополнительных утилит работы с дисками и реестром выполнить очистку и оптимизацию дисков и реестра вашего компьютера. Дать сравнительную характеристику работе рассмотренных вами утилит.

7. Используя шифр Цезаря, зашифруйте свои данные: Фамилию Имя Отчество.

8. Функция хеширования. Найти хеш–образ своей Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где n = pq, где p = 13 и q = 19.

9. Электронная цифровая подпись. Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

10. Необходимо зашифровать сообщение по методу Цезаря. Исходное сообщение: «Криптография». Ключ: 3

11. Шифр Гронсфельда. Исходный текст: «шифр гронсфельда». Ключ 15382

12. Зашифруем методом Цезаря с ключом k=7 слово «*шифр*».

13. Зашифровать пословицу: От умного научишься, от глупого разучишься с помощью шифра перестановки с ключом. Ключ слово «*информация*».

14. Код Хаффмана. Для кодирования букв О, В, Д, П, А решили использовать двоичное представление чисел 0, 1, 2, 3 и 4 соответственно (с сохранением одного незначащего нуля в случае одноразрядного представления). Если закодировать последовательность букв ВОДОПАД таким способом и результат за-

писать восьмеричным кодом, то получится:

1) 22162

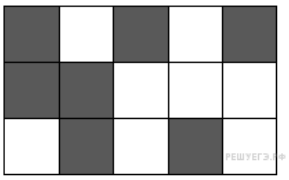
2) 1020342

3) 2131453

4) 34017

Укажите правильный ответ и объясните почему?

15. Код Хаффмана. Черно-белое растровое изображение кодируется построчно, начиная с левого верхнего угла и заканчивая в правом нижнем углу. При кодировании 1 обозначает черный цвет, а 0 – белый.



16. Для компактности результат записали в восьмеричной системе счисления. Выберите правильную запись кода.

1) 57414

2) 53414

3) 53412

4) 53012

Укажите правильный ответ и объясните почему?

17. Построить оптимальный код, пользуясь алгоритмом Хаффмана, найти стоимость кода. a1 − 0,31; a2 − 0,26; a3 − 0,24; a4 − 0,18; a5 − 0,01.

Критерии и шкала оценивания по оценочному средству промежуточный контроль («зачет с оценкой»)

Шкала оценивания (интервал баллов)	Критерий оценивания
отлично (5)	Студент глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
хорошо (4)	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.

удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
неудовлетворительно (2)	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)