

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное бюджетное образовательное учреждение  
высшего образования**

**«Луганский государственный университет имени Владимира Даля»**

**Краснодонский факультет инженерии и менеджмента (филиал)  
Кафедра информационных технологий и транспорта**

УТВЕРЖДАЮ

Директор Краснодонского факультета  
инженерии и менеджмента

  
Панайотов К.К.  
(подпись)

«22» марта 2023 г.



**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**«ТЕОРИЯ АЛГОРИТМОВ»**

По направлению подготовки: 09.03.01 – Информатика и вычислительная техника

Профиль: «Компьютерные системы и сети»

Краснодон 2023

## Лист согласования РПУД

Рабочая программа учебной дисциплины «Защита информации» по направлению подготовки 09.03.01 «Информатика и вычислительная техника» – 33 с.

Рабочая программа учебной дисциплины «Защита информации» составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 «Информатика и вычислительная техника», утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 года № 918.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

ст. преп. Крупица О.В.

Рабочая программа учебной дисциплины утверждена на заседании кафедры информационных технологий и транспорта «\_\_» \_\_\_\_\_ 202\_\_ года, протокол № \_\_.

Заведующий кафедрой информационных технологий и транспорта \_\_\_\_\_

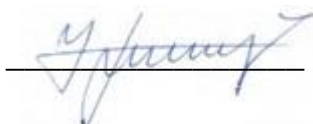


Бихдрикер А.С.

Переутверждена: «\_\_» \_\_\_\_\_ 202\_\_ года, протокол № \_\_\_\_\_

Согласована (для обеспечивающей кафедры):

Директор факультета \_\_\_\_\_



Панайотов К.К.

Рекомендована на заседании учебно-методической комиссии Краснодарского факультета инженерии и менеджмента «04» сентября 2019 года, протокол № 1.

Председатель учебно-методической комиссии Краснодарского факультета инженерии и менеджмента \_\_\_\_\_



Замота О.Н.

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

Рабочая программа по дисциплине «Защита информации» составлена в соответствии с требованиями государственного образовательного стандарта по направлению 09.03.01 – Информатика и вычислительная техника и относится к циклу профессиональных дисциплин (БЗ)

Целями дисциплины является формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, овладение основами методологии обеспечения информационной безопасности.

Задачи: освоить методы и средства защиты информации; изучить документы в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальности информации.

## **2. Место дисциплины в структуре ООП**

Курс «Защита информации» входит в вариативную часть профессионального цикла дисциплин подготовки студентов по направлению подготовки 09.03.01 Информатика и вычислительная техника

Дисциплина реализуется кафедрой инженерных дисциплин.

Основывается на базе дисциплин: теория информации и кодирования; программирование; практикум по программированию.

Является основой для изучения следующих дисциплин: администрирование баз данных; веб-программирование; проблемно-ориентированные вычислительные системы.

### 3. Требования к результатам освоения содержания дисциплины

Студенты, завершившие изучение дисциплины «Защита информации», должны:

**знать:**

- понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;
- стандартные программные средства набора текста и баз данных;
- правовые акты в области защиты государственной тайны и информационной безопасности;
- правовые основы организации защиты государственной тайны и конфиденциальной информации;
- основные понятия информационной безопасности;
- основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках;
- возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ;
- основные принципы организации и алгоритмы функционирования операционных систем и оболочек;
- проблемы и направления развития системных программных средств.

**уметь:**

- использовать программные и аппаратные средства персонального компьютера;
- ориентироваться в современной системе источников информации;
- использовать современные информационные технологии в своей профессиональной деятельности;
- применять средства антивирусной защиты;
- анализировать информационную безопасность многопользовательских систем;
- пользоваться программными средствами, реализующими основные криптографические функции системы публичных ключей, цифровую подпись, разделение доступа;
- видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи.

**владеть:**

- применения аппаратных и программных средств обеспечения информационной безопасности;
- противостояния типовым удаленным атакам
- обеспечения безопасной работы на компьютере;
- поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами;
- современной терминологией и методологией в области информационной безопасности.

Перечисленные результаты образования являются основой для формирования следующих компетенций (в соответствии с ГОС ВО 09.03.01 Информатика и вычислительная техника и требованиями к результатам освоения основной образовательной программы (ООП):

**общекультурных:**

способность к самоорганизации и самообразованию (ОК-7)

**общепрофессиональных:**

способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности(ОПК-5)

**профессиональных:**

способность разрабатывать модели компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно-вычислительная машина"( ПК-1)

способность проверять техническое состояние вычислительного оборудования и оборудования и осуществлять необходимые профилактические процедуры(ПК-7)

способность составлять инструкции по эксплуатации оборудования(ПК-8)

## 4. Структура и содержание дисциплины

### 4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов	
	Очная форма	Заочная форма
<b>Общая учебная нагрузка (всего)</b>	<b>180</b>	<b>180</b>
<b>Обязательная аудиторная учебная нагрузка (всего)</b>	<b>63</b>	<b>7</b>
в том числе:		
Лекции	34	6
Семинарские занятия	-	-
Практические занятия	-	-
Лабораторные работы	34	6
Курсовая работа (курсовой проект)	5	5
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)	117	173
Итоговая аттестация	зачет	зачет

### 4.2. Содержание разделов дисциплины

#### **ТЕМА 1 КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.**

Понятие угроз безопасности. Классификация угроз информационной безопасности. Основная классификация угроз: угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения доступности информации. Методы перечисления угроз. Случайные и преднамеренные угрозы. Технологические возможности злоумышленников по преодолению систем защиты информации. Признаки угрозы безопасности информации в распределенных вычислительных системах (РВС): по характеру воздействия; по цели воздействия; по условию начала осуществления воздействия; по наличию

обратной связи с атакуемым объектом; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие.

### **Лабораторная работа № 1 Аудит реестра в операционной системе Windows**

## **ТЕМА 2. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

Понятие стандарта. Классификация стандартов в области информационной безопасности.

«Оранжевая книга», ее структура и группы классов защищенности. Руководящие документы Гостехкомиссии России.

Понятие несанкционированного доступа (НСД). Направления защиты от НСД. Основные способы НСД. Принципы защиты от НСД.

### **Лабораторная работа № 2 Получение информации о настройках протокола TCP/IP и выполнение его настройки**

## **ТЕМА 3. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. УПРАВЛЕНИЕ РИСКАМИ. ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

Уровни защиты информации. Ключевые понятия информационной безопасности - политика безопасности и программа безопасности. Структура соответствующих документов, меры по их разработке и сопровождению. Этапы жизненного цикла информационных систем и меры безопасности. Методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств. Оценка рисков: выбор анализируемых объектов и уровня детализации их рассмотрения; выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий, выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска.

### **Лабораторная работа № 3 Разграничение прав пользователей в защищенных версиях операционной системы Windows.**

## **ТЕМА 4. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ, УПРАВЛЕНИЕ ДОСТУПОМ.**

Техническое обеспечение информационной безопасности. Понятие сервиса безопасности. Понятие архитектурной безопасности. Классификация сервисов безопасности. Средства идентификации и аутентификации пользователей. Идентификация и аутентификация, управление доступом. Парольная аутентификация. Одноразовые пароли. Система S/KEY компании Bellcore. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Матрица доступа. Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом.



Ограничивающий интерфейс. Ролевое управление доступом. Статическое разделение обязанностей. Динамическое разделение обязанностей.

**Лабораторная работа № 4 Реализация политики безопасности в защищенных версиях операционной системы Windows.**

## **ТЕМА 5. МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ.**

Основные понятия и классификация средств криптографической защиты информации. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Основные свойства асимметричных криптосистем.

Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Основные свойства хэш-функций. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамала. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи. Схемы неоспоримой подписи. Защита информации при работе в сети

**Лабораторная работа № 5 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.**

## **ТЕМА 6. ПРОТОКОЛИРОВАНИЕ И АУДИТ, КОНТРОЛЬ ЦЕЛОСТНОСТИ.**

Протоколирование и аудит, их место в общей архитектуре безопасности. Активный аудит. Подозрительная активность. Сигнатура атаки. Функциональные компоненты, входящие в состав средств активного аудита. Применение аудита в ОС семейства Windows для отслеживания деятельности пользователей. Настройка политики аудита. Аудит в Windows Server 2008/2012.

**Лабораторная работа № 6 Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов.**

## **ТЕМА 7. ЭКРАНИРОВАНИЕ, АНАЛИЗ ЗАЩИЩЕННОСТИ. ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ. ТУННЕЛИРОВАНИЕ.**

Понятие демилитаризованной зоны. Механизмы защиты, реализуемые межсетевым экраном (МЭ): фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам (наиболее распространённым); управление списками доступа на маршрутизаторах. Типы МЭ. Пакетные фильтры. Шлюзы уровня соединения. Шлюзы прикладного уровня.

Технологии Proxy и Stateful inspection. Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей.

Два вида средств поддержания высокой доступности: обеспечение отказоустойчивости (нейтрализация отказов, живучесть) и обеспечение безопасного и быстрого восстановления после отказов (обслуживаемость).

**Лабораторная работа № 7 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.**

## **ТЕМА 8. ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВИРУСОВ И ВРЕДОНОСНЫХ ПРОГРАММ**

Классификация компьютерных вирусов и вредоносных программ. Файловые, загрузочные и сетевые вирусы. Методы и средства борьбы с вирусами и вредоносными программами. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения. Механизмы распространения вирусов. Каналы распространения вирусов. Классические компьютерные вирусы. Макровирусы. Троянские программы. Сетевые черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.

**Лабораторная работа № 8 Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности при использовании глобальных вычислительных сетей.**

### 4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Тема 1 Классификация и характеристика угроз безопасности информации.	4	2
2	Тема 2. Стандарты и спецификации в области информационной безопасности.	4	2
3	Тема 3. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности.	4	2
4	Тема 4. Идентификация и аутентификация, управление доступом.	4	
5	Тема 5. Методы криптографической защиты информации. Электронная цифровая подпись.	4	
6	Тема 6. Протоколирование и аудит, контроль целостности.	4	
7	Тема 7. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование.	6	
8	Тема 8. Защита компьютерных систем от вирусов и вредоносных программ	4	
Итого:		34	6

### 4.4. Практические (семинарские) занятия

Практические занятия не предусмотрены.

#### 4.5. Лабораторные работы

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Лабораторная работа № 1 Аудит реестра в операционной системе Windows	2	2
2	Лабораторная работа № 2 Получение информации о настройках протокола ТСР/ІР и выполнение его настройки	2	2
3	Лабораторная работа № 3 Разграничение прав пользователей в защищенных версиях операционной системы Windows.	4	2
4	Лабораторная работа № 4 Реализация политики безопасности в защищенных версиях операционной системы Windows.	4	
5	Лабораторная работа № 5 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.	4	
6	Лабораторная работа № 6 Использование программной системы РGP для обеспечения конфиденциальности и целостности информационных ресурсов.	4	
7	Лабораторная работа № 7 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.	4	
8	Лабораторная работа № 8 Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности при использовании глобальных вычислительных сетей.	10	
Итого:		34	6

#### 4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	Заочная форма
1	Тема 1 Классификация и характеристика угроз безопасности информации.	подготовка лабораторным работам оформление отчетов, к и	14	22
2	Тема 2. Стандарты и спецификации в области информационной безопасности.	подготовка лабораторным работам оформление отчетов, к и	14	20
3	Тема 3. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности.	подготовка лабораторным работам оформление отчетов, к и	14	20
4	Тема 4. Идентификация и аутентификация, управление доступом.	подготовка лабораторным работам оформление отчетов, к и	13	20
5	Тема 5. Методы криптографической защиты информации. Электронная цифровая подпись.	подготовка лабораторным работам оформление отчетов, к и	13	20
6	Тема 6. Протоколирование и аудит, контроль целостности.	подготовка лабораторным работам оформление отчетов, к и	13	21
7	Тема 7. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование.	подготовка лабораторным работам оформление отчетов, к и	13	20
8	Тема 8. Защита компьютерных систем от вирусов и вредоносных программ	подготовка лабораторным работам оформление отчетов, к и	13	20
Итого:			107	163

#### 4.7. Курсовые работы/проекты.

1. Защита систем трансляции, передачи сообщений и электропитания.
2. Защита помещения от утечки акустической информации через акустоэлектрические преобразователи телефонной цепи и аппарата.
3. Акустопреобразовательные элементы с передачей информативного сигнала радиоизлучением.

4. Акустоэлектрические преобразователи, технические характеристики акустопреобразовательного канала.
5. Криптографическая защита телефонных сообщений.
6. Активные способы защиты телефонных линий.
7. Пассивные способы защиты телефонных линий.
8. Телефонная линия как канал утечки информации, индуктивный и бесконтактный съём информации с телефонной линии.
9. Комбинированные способов технической защиты телефонных линий.
10. Способы технической защиты в IP телефонии.
11. Радиозакладные устройства.
12. Сетевые закладные устройства.
13. Средства и способы обнаружения радиозакладных устройств.
14. Комплексы мониторинга технических каналов утечки информации.
15. Активное противодействие закладным радиоустройствам.
16. Акустические устройства перехвата информации.
17. Защита конфиденциальной акустической информации от несанкционированной аудио записи.
18. Портативные средства аудиозаписи, способы и средства противодействия.
19. Переносные средства аудиозаписи, способы и средства противодействия.
20. Способы и средства проверки звукоизоляции помещений.
21. Средства контроля эффективности акустической защиты.
22. Аппаратно-программные комплексы виброакустических измерений.
23. Пассивные способы защиты акустической информации.
24. Активные способы защиты акустической информации.
25. Комплексные системы защиты акустической информации.
26. Защита конфиденциальной информации от несанкционированной видео записи.
27. Портативные средства видеозаписи, способы и средства противодействия.
28. Переносные средства видеозаписи, способы и средства противодействия.
29. Технические каналы утечки информации.
30. Технические средства информационной разведки и промышленного шпионажа.

## 5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- традиционные объяснительно-иллюстративные технологии, которые обеспечивают доступность учебного материала для большинства студентов, системность, отработанность организационных форм и привычных методов, относительно малые затраты времени;

- технологии проблемного обучения, направленные на развитие познавательной активности, творческой самостоятельности студентов и предполагающие последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешение которых позволяет студентам активно усваивать знания (используются поисковые методы; постановка познавательных задач);

- технологии развивающего обучения, позволяющие ориентировать учебный процесс на потенциальные возможности студентов, их реализацию и развитие;

- технологии концентрированного обучения, суть которых состоит в создании максимально близкой к естественным психологическим особенностям человеческого восприятия структуры учебного процесса и которые дают возможность глубокого и системного изучения содержания учебных дисциплин за счет объединения занятий в тематические блоки;

- технологии модульного обучения, дающие возможность обеспечения гибкости процесса обучения, адаптации его к индивидуальным потребностям и особенностям обучающихся (применяются, как правило, при самостоятельном обучении студентов по индивидуальному учебному плану);

- технологии дифференцированного обучения, обеспечивающие возможность создания оптимальных условий для развития интересов и способностей студентов, в том числе и студентов с особыми образовательными потребностями, что позволяет реализовать в культурно-образовательном пространстве университета идею создания равных возможностей для получения образования

- технологии активного (контекстного) обучения, с помощью которых осуществляется моделирование предметного, проблемного и социального содержания будущей профессиональной деятельности студентов (используются активные и интерактивные методы обучения) и т.д.

- Максимальная эффективность педагогического процесса достигается путем конструирования оптимального комплекса педагогических технологий и (или) их элементов на личностно-ориентированной, деятельностной, диалогической основе и использования необходимых современных средств обучения.

## 6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы лектором и преподавателем, ведущим лабораторные работы по дисциплине в следующих формах:

- собеседование (устный или письменный опрос);
- контрольные работы.

Фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить результаты текущей и промежуточной аттестации обучающихся по данной дисциплине, помещаются в приложении к рабочей программе в соответствии с «Положением о фонде оценочных средств».

Форма аттестации по результатам освоения дисциплины проходит в форме устного экзамена (включает в себя ответ на теоретические вопросы и решение задач). Студенты, выполнившие 75% текущих и контрольных мероприятий на «отлично», а остальные 25 % на «хорошо», имеют право на получение итоговой отличной оценки.

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

Национальная шкала	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	не зачтено



	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.	
--	---	--

## **7. Учебно-методическое и программно-информационное обеспечение дисциплины:**

### **а) основная литература:**

1. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. - М.: Форум : ИНФРА-М, 2014.
2. Мельников В. П. Информационная безопасность и защита информации. - М.: Академия, 2008.
3. Информационная безопасность открытых систем. - М.: Горячая линия-Телеком, 2008.

### **б) дополнительная литература:**

1. Леванский В.А. Моделирование в социально-правовых исследованиях. М.: Наука, 1986. 160 с.
2. Наумов В.Б. Право и Интернет: Очерки теории и практики. - М.: Книжный дом «Университет», 2002.
3. Норткатт С., Новак Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу, Москва - Лори, 2001.
4. Овчинский А.С. Информация и оперативно-розыскная деятельность. –М.: Инфра-М, 2002. 97 с.

### **в) интернет-ресурсы:**

Министерство образования и науки Российской Федерации – <http://минобрнауки.рф/>

Федеральная служба по надзору в сфере образования и науки – <http://obrnadzor.gov.ru/>

Министерство образования и науки Луганской Народной Республики – <https://minobr.su>

Народный совет Луганской Народной Республики – <https://nslnr.su>

Портал Федеральных государственных образовательных стандартов высшего образования – <http://fgosvo.ru>

Федеральный портал «Российское образование» – <http://www.edu.ru/>

Информационная система «Единое окно доступа к образовательным ресурсам» – <http://window.edu.ru/>

Федеральный центр информационно-образовательных ресурсов – <http://fcior.edu.ru/>

### **Электронные библиотечные системы и ресурсы**

Электронно-библиотечная система «Консультант студента» – <http://www.studentlibrary.ru/cgi-bin/mb4x>

Электронно-библиотечная система «StudMed.ru» –  
<https://www.studmed.ru>

**Информационный ресурс библиотеки образовательной организации**

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

1. Электронная библиотечная система «Лань». Режим доступа:  
<http://e.lanbook.com>

2. Университетская библиотека ONLINE. Режим доступа:  
<http://biblioclub.ru/>

3. [ru.wikipedia.org/](http://ru.wikipedia.org/)

4. <http://clubreaders.ru/kompyuternaya-literatura/zhelezo/>

**8. Материально-техническое обеспечение дисциплины**

Освоение дисциплины «Защита информации» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее:

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;

- для проведения лекционных занятий требуется аудитория на курс, оборудованная мультимедийным проектором с экраном;

- для проведения лабораторных работ требуется компьютерный класс, подключенный к Интернет.

Программное обеспечение:

Функциональное назначение	Бесплатное программное обеспечение	Ссылки
Офисный пакет	Libre Office 6.3.1	<a href="https://www.libreoffice.org/">https://www.libreoffice.org/</a> <a href="https://ru.wikipedia.org/wiki/LibreOffice">https://ru.wikipedia.org/wiki/LibreOffice</a>
Операционная система	UBUNTU 19.04	<a href="https://ubuntu.com/">https://ubuntu.com/</a> <a href="https://ru.wikipedia.org/wiki/Ubuntu">https://ru.wikipedia.org/wiki/Ubuntu</a>
Браузер	Firefox Mozilla	<a href="http://www.mozilla.org/ru/firefox/fx">http://www.mozilla.org/ru/firefox/fx</a>
Браузер	Opera	<a href="http://www.opera.com">http://www.opera.com</a>
Почтовый клиент	Mozilla Thunderbird	<a href="http://www.mozilla.org/ru/thunderbird">http://www.mozilla.org/ru/thunderbird</a>
Файл-менеджер	Far Manager	<a href="http://www.farmanager.com/download.php">http://www.farmanager.com/download.php</a>
Архиватор	7Zip	<a href="http://www.7-zip.org/">http://www.7-zip.org/</a>

Графический редактор	GIMP (GNU Image Manipulation Program)	<a href="http://www.gimp.org/">http://www.gimp.org/</a> <a href="http://gimp.ru/viewpage.php?page_id=8">http://gimp.ru/viewpage.php?page_id=8</a> <a href="http://ru.wikipedia.org/wiki/GIMP">http://ru.wikipedia.org/wiki/GIMP</a>
Редактор PDF	PDFCreator	<a href="http://www.pdfforge.org/pdfcreator">http://www.pdfforge.org/pdfcreator</a>
Аудиоплеер	VLC	<a href="http://www.videolan.org/vlc/">http://www.videolan.org/vlc/</a>

**Показатели и критерии оценивания компетенций, описание шкал оценивания**

№ п/п	Код контролируемой компетенции	Показатель оценивания (знания, умения, навыки)	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1.	ОК-7	<p>Знать: методы организации работы над программным проектом в команде.</p> <p>Уметь: создавать компоненты программного обеспечения.</p> <p>Владеть: навыками документирования процесса разработки.</p>	Тема 1,Тема 2	Собеседование (устный или письменный опрос), контрольная работа.
2.	ОПК-5	<p>Знать: типы и классы информационных систем и технологий для различных прикладных областей информационных технологии решения прикладных задач методологию проектирования информационных систем с использованием инновационных инструментальных средств</p> <p>Уметь: выбирать типы и классы информационных систем и технологий для решения задач прикладной области использовать инструментальные средства информационных систем и технологий решать прикладные задачи с использованием информационных систем и информационных технологий</p> <p>Владеть: практическими навыками использования информационных систем и информационных технологий практическими навыками разработки</p>	Тема 2,Тема 3	Собеседование (устный или письменный опрос), контрольная работа.

		информационных систем практическими навыками интеграции информационных систем и технологий для решения прикладных задач предметной области.		
3.	ПК-1	<p>Знать: специализированный язык работы с БД; современные модели построения БД; психологические аспекты человекомашинного взаимодействия; принципы создания интерфейсов; уровни представления структур данных и их особенности.</p> <p>Уметь: обоснованно выбирать, проектировать и модифицировать структуры данных и алгоритмы при решении практических задач разработки программного обеспечения; проектировать интерфейсы прикладных программ; проектировать БД, строить запросы к БД, правильно выбирать модели построения БД; строить проектные модели ПО и ИС с использованием диаграмм визуальной нотации UML.</p> <p>Владеть: практическими навыками проектирования баз знаний и интеллектуальных систем с интегрированными базами знаний практическими навыками разработки интеллектуальных систем; практическими навыками реализации структур данных; навыками пошагового построения проекта ПО как последовательного набора UML диаграмм в инструментальном CASE</p>	Тема 2	Собеседование (устный или письменный опрос), контрольная работа.

		<p>средстве; навыками реализации лучших практик разработки программного обеспечения, включая построения компонентной архитектуры ПО и применение архитектурных механизмов анализа.</p>		
4.	ПК-7	<p>Знать: основные понятия и методы тестирования; условия применения тестирования; приемы тестирования на разных фазах разработки качественного программного продукта; построение, методы доступа, протоколы локальных вычислительных сетей; технологии корпоративных сетей, включая протоколы TCP/IP.</p> <p>Уметь: разрабатывать тестовые программы и тестовые наборы в программном проекте; разрабатывать проектную документацию для этапа тестирования; тестировать программное обеспечение разработанных проектов; использовать двоичную арифметику; выполнять настройку локальных сетей масштаба малого предприятия.</p> <p>Владеть: средствами тестирования и мониторинга работы сетей; основными методиками тестирования программного обеспечения; одним либо несколькими прикладными программами по тестированию ПО; навыками разработки и отладки программ на алгоритмических языках</p>	Тема 1	Собеседование (устный или письменный опрос), контрольная работа.

		<p>программирования;          принципами и методами          администрирования баз          данных, стандартами,          соглашениями и          рекомендациями в области          информационных систем.</p>		
5.	ПК-8	<p>Знать: принципы          обоснования принимаемых          проектных решений;          методику постановки и          выполнения          экспериментов по проверке          их          корректности и          эффективности.</p> <p>Уметь: выбирать элементы          ВМ при ее сборке и          проектировании;          использовать базовые          алгоритмы          обработки информации;          эксплуатировать          программно-аппаратные          средства в          информационных          системах.</p> <p>Владеть: основными          методами и средствами          анализа вычислительных          узлов и блоков; базовыми          алгоритмами обработки          информации; навыками          конфигурирования          локальных сетей.</p>	Тема 6, Тема 7, Тема 8	Собеседование (устный или письменный опрос), контрольная работа.

## Фонды оценочных средств по дисциплине «Защита информации»

### Перечень вопросов (для проведения собеседования (устный или письменный опрос))

1. Стандарты в области информационной безопасности.
2. Международные стандарты информационного обмена.
3. Понятие угрозы, атаки.
4. Понятие нарушителя информационной безопасности.
5. Понятие государственной, коммерческой, личной тайны.
6. Основные нормативные документы в этой области.
7. Порядок рассекречивания документов.
8. Уровень тайны.
9. Понятие угрозы нарушения режима безопасности.
10. Причины нарушения информационной безопасности.
11. Предпосылки угроз
12. Аудит событий в рамках информационной системы.
13. Реализация законодательного уровня защиты информации в РФ.

#### Конституция.

14. Закон об информатизации.
15. Закон о цифровой подписи.
16. Уголовный кодекс РФ о незаконном использовании объектов авторского права и смежных прав.
17. Международные и отечественные требования по защите информации и их стандартизация.
18. Уровни безопасности информации. Требования к криптографическим алгоритмам и системам.

#### Критерии и шкала оценивания по оценочному средству собеседование (устный или письменный опрос)

Шкала оценивания (интервал баллов)	Критерий оценивания
5	собеседование (устный или письменный опрос) прошел на высоком уровне (студент в полном объеме осветил рассматриваемый вопрос, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	собеседование (устный или письменный опрос) прошел на среднем уровне (студент в целом осветил рассматриваемый вопрос, владеет профильным понятийным (категориальным) аппаратом и т.п.)
3	собеседование (устный или письменный опрос) на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	собеседование (устный или письменный опрос) прошел на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)



## Задания к контрольным работам

1 Используя алгоритмы двойной перестановки строк и столбцов выполнить шифрование следующих фраз (ключ выбрать самостоятельно, номер варианта выбрать по номеру в списке группы):

1. Он досрочно завалил экзамен.
2. Закон суров, но это закон.
3. Умному легче доказать, что он дурак.
4. И у дурака вырастает зуб мудрости.
5. Свободу симулировать нельзя.
6. Подумай, прежде чем подумать.
7. Каждый век имеет свое средневековье.
8. Брюки протираются даже на троне.
9. Окно в мир можно закрыть газетой.
10. Чаще всего выход там, где был вход.
11. Безграмотные вынуждены диктовать.
12. Хлеб открывает любой рот.
13. Деньги не пахнут, но улетучиваются.
14. Сны зависят от положения спящего.
15. Труднее всего поджечь ад.
16. Ужасен кляп, смазанный медом.
17. Не пиши кредо на заборе.
18. Беззубым многое легче выговаривать.
19. И регалии звенят по разному.
20. Лицемерный палач ослабляет петлю.
21. Интеллектуальная узость ширится.
22. Вписывайся во влиятельные круги.
23. Иные ступени карьеры ведут на виселицу.
24. И маятник идет в ногу со временем.
25. И ненужные постоянно нужны.

2 Используя алгоритмы двойной перестановки строк и столбцов выполнить дешифрование шифрограмм, приведенные в таблице 3.1 (номер варианта выбрать по последней цифре номера шифра). В шифротексте следует обратить внимание на наличие пробелов в тексте, длина текста по всем вариантам равняется 25 символам:

Номер вар-та	Шифротекст	Ключ 1	Ключ 2
1	<b>В ОН , Т ОЭЗКНОА УОРСЗКНОА</b>	КРУТО	СТУЖА
2	<b>ЗВАОЛИ ЛАН ОДОРОНЧСАЧТЕЗ</b>	ВЕСНА	ОСЕНЬ
3	<b>ПАЙРДЕЕЖ М ЧЕДАТУМЬДУПОМ</b>	ОСЕНЬ	ДОСУГ
4	<b>ДОВХЫМА Т ЕД Г ДО ХВ ИИЩ</b>	ТРАВА	ДОСУГ
5	<b>!Т РОЙОЛЮБ БХЛЕ ТВАЕЫРОТК</b>	ПРАВО	ТРАВА
6	<b>Ь ДА ОЖЧЕДТУНДРЕ СВЕЕОП Г</b>	КРУТО	ПРАВО
7	<b>ЕН ПОЕРД ЕОБР!ЗАН А ШИИК</b>	СПОРТ	КРУТО
8	<b>Е ВГОБЫ-М БЕУЗЗ ЛЧЕГОРЬИТ</b>	ВЕТЕР	СПОРТ
9	<b>ГАЛЕР ЗВИИОМУНЗЯТ НЕ РАОП</b>	СТУЖА	ВЕТЕР
10	<b>СЯТООН ОН УЫЖННЫПЕН ЕЖННУ</b>	ДРЕВО	СТУЖА

3 Используя магический квадрат (таблица 3.2) расшифровывать следующие шифрограммы (шифрограммы приведены в таблице 3.3, номер варианта выбрать по числу букв в фамилии):

11	24	7	20	3
4	12	25	8	16
17	5	13	21	9
10	18	1	14	22
23	6	19	2	15

Вариант	Шифротекст
1	ОЛ ЕЛ ОДУЛА-СЕЛЯС МЕЛЙДГ
2	ВТТЙЕБА КЛЮ Е РЫБХТРОООЛ
3	ОЕР Д ТОАЛОЗЗЧНИОААЧСЛНВ
4	УЗУНОБЛЯСВАОИЕИМТСРЛЬДВО
5	ЕТЙДДУЖЬ ЧЕМДУПРМПЕМАА О
6	ЕАЕЕУДГД ПОНОЧВСДТ Ъ ЕЖР
7	КРШЗ РЕИ НПЕА АНДБОИ ЕО
8	ОНЫ НУСЫЕННЖТН ПОНОУЖН ЕЯ
9	ЕМИАГАНУ ПОЛЯЗЗВ РТНОИРЕ
10	НУУ З Е!ДЛЪТ РА КБТЫБРОЕО

4 Используя шифр многоалфавитной замены шифровать фразу из п. 3.2.1 (исключив пробелы и знаки препинания), используя в качестве ключа «Ключ 1» из пункта 3.2.2. Для шифрования использовать алфавит замены из таблицы 3.5.

5 Используя шифр многоалфавитной замены дешифровать фразу, используя «Ключ» (шифрограммы и ключи приведены в таблице 3.4, номер варианта выбрать по последней цифре суммы числа букв в имени и фамилии).

Номер вар-та	Шифротекст	Ключ
1	РПКЮВОНЕЩОИТЯФАМХМЯЪЕШТТРО	ВЕСНА
2	ПЦМРМОЭУЯЙЦЗИЙВЧЙТЙХНЧОЪУЕЯШ	ОСЕНЬ
3	ЩЦЦФСЦШБОЕДУГЮБЕЪГСЦ	ДОСУГ
4	ГЭЫЙАФШСБТАВПРЛАЦЕПИСБПЩЧУО	ТРАВА
5	РХЗЙБРЛМОЫЭУОЗЩФУЧЗРКУОДОЯШВВАЛ	ПРАВО
6	ХШЙЧЪПААНЧЩРЮГЕШЕЮТПХПЩДЭПВЮР	КРУТО
7	ЩЪАХЭЪФШВЕСЪКЭТРВХЮГГЛЖШВЩЕЯП	СПОРТ
8	ДФЫЦЛДЕЫЩПДУФРШВЧЧРМПАЧПАХИЪ	ВЕТЕР
9	УБЫЧЫУТЬЧЯУАХСИРДШСЪЮНШРРДХЫ	СТУЖА
10	МЪЕБАСШПКТЙВЭПЪЗГЦРРФХСЗЫЙЪ	ДРЕВО



## Оценочные средства для промежуточной аттестации (зачет) Теоретические вопросы

1. Свойства защищаемой информации.
2. Доступность.
3. Конфиденциальность.
4. Целостность
5. Понятие Информационной безопасности и безопасности информации.
6. Понятие защита информации.
7. Виды носителей информации.
8. Угрозы защищаемой информации по видом носителей.
9. Возможные предпосылки нарушений свойств информационной безопасности.
10. Возможные злоумышленники.
11. Каналы утечки информации.
12. Анализ угроз защищаемой информации по видам носителей.
13. Понятие криптография
14. Понятие криптоанализ
15. Понятие стеганография
16. Шифрование
17. Дешифрование
18. Кодирование
19. Обзор основных методов шифрования и дешифрования
20. Обзор основных методов кодирования
21. Обзор основных методов криптоанализа
22. Обзор основных методов стеганографии
23. Симметричные системы шифрования с одним ключом.
24. Достоинства и недостатки шифров с одним ключом.
25. Создание шифров на основе блочных алгоритмом перестановки.
26. Стандарты шифрования DES, 3DES и ГОСТ.
27. Стандарт шифрования AES
28. Асимметричные системы шифрования с открытым ключом.
29. Достоинства и недостатки шифров с открытым ключом.
30. Способы передачи секретного ключа.
31. Создание ключа на основе псевдослучайных последовательностей.
32. Примеры шифров на основе алгоритма Эль-Гамала и алгоритма RSA.
33. Аутентификация (подмена данных, хэш-функция, защита от подмены данных).
34. Цифровая подпись (создание цифровой подписи, атаки и защита цифровой подписи).
35. Стандарты на электронно-цифровую подпись: DSS и ГОСТ Р 34.10-94.

36. Цифровая подпись на базе шифра RSA и шифра Эль-Гамала.
37. Системы по отпечаткам пальцев. На основании каких физических характеристик пальца можно
38. составить биометрический шаблон?
39. Преимущества и недостатки метода отпечатка пальцев.
40. Системы по голосу. Какие физические характеристики входят в основу шаблона? Преимущества
41. и недостатки.
42. Системы по радужной оболочке глаза. Преимущества и недостатки.
43. Основные подсистемы системы идентификации по радужной оболочки глаза. Статистические
44. характеристики метода.
45. Системы идентификации и аутентификации по изображению лица. Классификация методов.
46. Системы идентификации и аутентификации по 2-d изображению лица. Преимущества и
47. недостатки.
48. Особенности систем по 3-d распознаванию лица. Классификация систем и особенности.
49. 64. Системы идентификации по геометрии руки. Виды систем. Преимущества и недостатки метода.
50. Метод распознавания по сетчатке глаза. Статистические показатели. Преимущества и недостатки.
51. Метод аутентификации и идентификации по венозному рисунку руки. Статистические
52. показатели.
53. Классификация методов распознавания по почерку. Преимущества и недостатки.
54. Система электронного носа.
55. Система распознавания по форме ушной раковины.
56. Перспективные методы БСЗИ.
57. Применение биометрии в подсистемах безопасности и ИБ.
58. Механизм генерации ЭП с помощью биометрии.
59. Система BioLink Cl.
60. Применение технологий БСЗИ в картах Государственных систем социального обеспечения.
61. Возможности видеоаналитики в мониторинговых системах.
62. Компьютерная система.
63. Основные угрозы безопасности информации в компьютерной системе.
64. Основные механизмы защиты информации в компьютерных системах.
65. Защита компьютерной системы на физическом уровне.
66. Идентификация и аутентификация пользователей.

67. Парольная аутентификация
68. Атрибутивная аутентификация
69. Биометрическая аутентификация
70. Разграничение доступа пользователей к ресурсам.
71. Дискретная модель.
72. Мандатная модель.
73. Верификационная модель.
74. Проблемы безопасности сетей.
75. Уровни безопасности сетевых систем.
76. Источники угроз в сетях.
77. Виды сетевых угроз и противодействие им.
78. Атаки на сетевые системы.
79. ПЭМИН каналов связи.
80. Удаленные атаки через сеть Internet.
81. Уязвимости протоколов и служб Internet.
82. Задачи и уровни защиты в сетях передачи данных.
83. Механизмы современной защиты информации в каналах связи.
84. Организационные мероприятия по защите информации в сетях.
85. Политика сетевой безопасности.
86. Методы и средства защиты информации от побочного электромагнитного излучения и наводок
87. информации.
88. Управление доступом к информации в сетях передачи данных.
89. Межсетевые экраны (МЭ). Компоненты МЭ.
90. Основные схемы защиты на базе МЭ. Модули МЭ.
91. Программные методы защиты, реализуемые МЭ.
  - а. Антивирусная защита
92. Системы обнаружения сетевых вторжений.
93. Принципы построения СЗИ в АС.
94. Уровни защиты информации в ИС
95. Физический уровень
96. Уровень данных
97. Уровень программ
98. Уровень локальной сети
99. Межсетевой уровень
100. Организационный уровень.
101. Методы проектирования СЗИ.
102. План-график проектирования СЗИ.
103. Инструментарий для разработки проектов СЗИ в ИС по уровням.

### Критерии и шкала оценивания к промежуточной аттестации «экзамен»

Национальная шкала	Характеристика знания предмета и ответов
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)