МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ»
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ)

Физико-математический факультет
Кафедра вычислительной математики и информационных технологий

Согласовано
деканом физико-математического факультета
« 19 »_____03_____ 2025 г.
_____
/Кулешова Ю.Д./

Рабочая программа дисциплины

Основы информационной безопасности и защиты информации

Направление подготовки
44.04.01 Педагогическое образование

Программа подготовки:
Современные информационные образовательные технологии

Квалификация
Магистр

Форма обучения
Очно-заочная

Согласовано учебно-методической комиссией
физико-математического факультета
Протокол «19»_____03_____2025 г. №_7_
Председатель УМКом_____
/Кулешова Ю.Д./

Рекомендовано кафедрой
вычислительной математики и
информационных технологий
Протокол от «19»_____03_____2025 г. №_10_
Зав. кафедрой_____
/Шевчук М.В./

Москва
2025

Авторы-составители:
Шевчук М. В. кандидат физико-математических наук, доцент
Костякова В. Г. кандидат педагогических наук, доцент

Рабочая программа дисциплины «Основы информационной безопасности и защиты информации» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.04.01 Педагогическое образование, утверждённого приказом МИНОБРНАУКИ России от 22.02.2018 г. № 126.

Дисциплина входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» и является обязательной для изучения.

Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

Год начала подготовки (по учебному плану) 2025

СОДЕРЖАНИЕ

1. Планируемые результаты обучения ……..... 4
2. Место дисциплины в структуре образовательной программы …..... 4
3. Объем и содержание дисциплины ……..……...……. 5
4. Учебно-методическое обеспечение самостоятельной работы обучающихся ……. 13
5. Фонд оценочных средств для проведения текущей и промежуточной аттестации по дисциплине ……..……..….... 16
6. Учебно-методическое и ресурсное обеспечение дисциплины …..... 24
7. Методические указания по освоению дисциплины …….…. 26
8. Информационные технологии для осуществления образовательного процесса по дисциплине ……... 26
9. Материально-техническое обеспечение дисциплины …..…… 27

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1. Цель и задачи дисциплины

Целью освоения дисциплины является изучение основных вопросов криптографии и стеганографии, необходимых для обеспечения компьютерной безопасности информации, защиты информации от несанкционированного допуска и обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, рассмотрение математических основ современных криптосистем и методов их криптоанализа.

Задачи дисциплины:

- формирование представлений о методах и алгоритмах шифрования;
- изучение математических основ криптографии;
- формирование и развитие компетенций, знаний, практических навыков и умений в области систем криптографии и шифрования;
- изучение стандартов, протоколов и алгоритмов шифрования.

1.2. Планируемые результаты обучения

В результате освоения данной дисциплины у обучающихся формируются следующие компетенции:

СПК-2. Способен к преподаванию учебных курсов, дисциплин (модулей) по образовательным программам в образовательных организациях соответствующего уровня образования.

СПК-4. Способен к разработке учебно-методического обеспечения для реализации образовательных программ в образовательных организациях соответствующего уровня образования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» и является обязательной для изучения.

Компетенции, знания, навыки и умения, полученные в ходе изучения дисциплины, должны всесторонне использоваться и развиваться студентами в процессе последующей профессиональной деятельности при использовании языков программирования, системного и прикладного программного обеспечения для решения профессиональных задач.

3. ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем дисциплины

Показатель объема дисциплины	**Форма обучения**
	Очно-заочная
Объем дисциплины в зачетных единицах	3
Объем дисциплины в часах	108(100)[1]
Контактная работа:	14,2
Лекции	4(4)[2]

[1] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий
[2] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий

Лабораторные занятия	10(10)[3]
Контактные часы на промежуточную аттестацию:	0,2
Зачет с оценкой	0,2
Самостоятельная работа	86(86)[4]
Контроль	7,8

Форма промежуточной аттестации: зачет с оценкой во 2 семестре.

3.2. Содержание дисциплины

Для очной формы обучения

Наименование разделов (тем) дисциплины с кратким содержанием	Количество часов	
	Лекции	Лабораторные занятия
Тема 1. Введение в информационную безопасность Информационная безопасность. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. Методы информационной безопасности: физические, организационно-правовые и технические средства защиты. Сервисы информационной безопасности: аутентификация, авторизация и аудит. Угрозы информационной безопасности. Классификация угроз информационной безопасности: по природе возникновения, по степени преднамеренности, по месторасположению, по степени вреда, наносимого информационной системе. Понятие защищенных операционных систем. Уровни защищенности операционных систем. Профили защиты на операционных системах. Виды, классы, типы операционных систем в соответствии с профилями защиты. Различие типов операционных систем по принципу работы и функциональному предназначению. Обзор существующих защищенных операционных систем. Практическое применение различных функций защиты информации, реализованных в защищенной операционной системе. Сравнение функциональных возможностей операционных систем.	1	
Тема 2. Средства антивирусной защиты и межсетевые экраны Понятие средства антивирусной защиты. Профили защиты в средствах антивирусной защиты. Виды, классы, типы средств антивирусной защиты в соответствии с профилями защиты. Различие типов средств антивирусной защиты по принципу работы и функциональному предназначению. Обзор существующих средств антивирусной защиты. Работа со средствами антивирусной защиты типа «Г». Практическое	1	

[3] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий
[4] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий

применение различных функций защиты информации, реализованных в средствах антивирусной защиты. Сравнение функциональных возможностей средств антивирусной защиты. Понятие межсетевого экрана. Профили защиты в межсетевых экранах. Виды, классы, типы межсетевых экранов в соответствии с профилями защиты. Различие типов межсетевых экранов по принципу работы и функциональному предназначению. Обзор существующих межсетевых экранов. Межсетевые экраны типа «В». Сравнение функциональных возможностей межсетевых экранов.		
Тема 3. Системы обнаружения вторжений и анализы защищённости Понятие системы обнаружения вторжений. Профили защиты в системах обнаружения вторжений. Виды, классы, типы систем обнаружения вторжений в соответствии с профилями защиты. Различие типов систем обнаружения вторжений по принципу работы и функциональному предназначению. Обзор существующих систем обнаружения вторжений. Работа с системами обнаружения вторжений типа «уровень узла». Практическое применение различных функций защиты информации, реализованных в системах обнаружения вторжений. Понятие средства анализа защищенности. Различие средств анализа защищенности по принципу работы и функциональному предназначению. Обзор существующих средств анализа защищенности. Практическое применение различных функций защиты информации, реализованных в средствах анализа защищенности. Сравнение функциональных возможностей средств анализа защищенности.	1	
Тема 4. Защищенные системы виртуализации и резервного копирования Понятие защищенных систем виртуализации. Различие защищенных систем виртуализации по принципу работы и функциональному предназначению. Обзор существующих защищенных систем виртуализации. Практическое применение различных функций защиты информации, реализованных в защищенных системах виртуализации. Сравнение функциональных возможностей защищенных систем виртуализации. Понятие систем резервного копирования. Различие систем резервного копирования по принципу работы и функциональному предназначению. Обзор существующих систем резервного копирования. Практическое применение различных функций защиты информации, реализованных в системах резервного копирования.	1	
Тема 5. Механизмы дискреционного управления доступом Дискреционное управление доступом. Учетные записи пользователей и групп. Аутентификация пользователей. Файлы, каталоги и дискреционные права доступа к ним. Особенности моделирования дискреционного доступа. Управление учетными записями пользователей. Организация совместной работы с файлами и каталогами с помощью общей группы, списков управления доступом. Использование дополнительных атрибутов файловой системы и привилегий для ограничения производимых с файлами операций. Использование различных механизмов для расширения возможностей администрирования дискреционного управления доступом.		4
Тема 6. Мандатный контроль целостности Общий подход к реализации мандатного контроля целостности. Администрирование параметров мандатного контроля целостности.		6

Описание состояний системы. Описание правил перехода из состояния в состояние. Доказательство выполнения условий безопасности. Использование мандатной целостности для администрирования ОССН. Организация файловой системы в рамках мандатного контроля целостности. Использование мандатного и дискреционного управления доступом для организации совместной работы с файлами и каталогами. Использованием привилегий для восстановления данных из архивов. Настройка ОССН для безопасной работы.		
Итого	4(4)[5]	10(10)[6]

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самостоятельной работы	Методические обеспечения	Формы отчетности
1. Классические криптосистемы.	Основные понятия. Области применения.	8	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
2. Блочные шифры.	Основные понятия. Области применения.	8	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
3. Элементы алгебраической геометрии.	Основные понятия. Области применения.	8	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
4. Системы RSA.	Основные понятия. Области применения.	8	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
5. Шифрование с открытым ключом.	Основные понятия. Области применения.	8	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
6. Электронно-цифровая подпись.	Основные понятия. Области применения.	10	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
7. Алгебраические методы криптоанализа.	Основные понятия. Области применения.	10	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
8. Информационная безопасность и защита информации в	Основные понятия. Способы защиты.	14	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект

[5] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий
[6] Реализуется в формате электронного обучения с применением дистанционных образовательных технологий

отечественных операционных системах					
9. Механизмы дискреционного управления доступом	Основные понятия. Области применения.	6	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
10. Мандатный контроль целостности	Основные понятия. Области применения.	6	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Итого		86			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

5.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и наименование компетенции	Этапы формирования
СПК-2. Способен к преподаванию учебных курсов, дисциплин (модулей) по образовательным программам в образовательных организациях соответствующего уровня образования	1. Работа на учебных занятиях. 2. Самостоятельная работа.
СПК-4. Способен к разработке учебно-методического обеспечения для реализации образовательных программ в образовательных организациях соответствующего уровня образования	1. Работа на учебных занятиях. 2. Самостоятельная работа.

5.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
СПК-2	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	Знать: структуру образовательных программ в образовательных организациях соответствующего уровня образования	Лабораторная работа Конспект Тестирование	Шкала оценивания лабораторной работы Шкала оценивания конспекта Шкала оценивания

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
			Уметь: применять полученные знания на практике		тестирования
	Продвинутый	1. Работа на учебных занятиях 2. Самостоятельная работа	Знать: структуру образовательных программ в образовательных организациях соответствующего уровня образования Уметь: применять полученные знания на практике Владеть: способностью к преподаванию учебных курсов, дисциплин (модулей) по образовательным программам в образовательных организациях соответствующего уровня образования	Лабораторная работа Конспект Тестирование	Шкала оценивания лабораторной работы Шкала оценивания конспекта Шкала оценивания тестирования
СПК-4	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	*Знать*: - методы и средства разработки учебно-методического обеспечения образовательных программ *Уметь*: - сопровождать разработку учебно-методического обеспечения образовательных программ	Лабораторная работа Конспект Тестирование	Шкала оценивания лабораторной работы Шкала оценивания конспекта Шкала оценивания тестирования
	Продвинуты	1. Работа на	*Знать*:	Лаборатор	Шкала

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
	й	учебных занятиях 2. Самостоятельная работа	- методы и средства разработки учебно-методического обеспечения образовательных программ *Уметь*: - сопровождать разработку учебно-методического обеспечения образовательных программ *Владеть*: - навыками разработки учебно-методического обеспечения для реализации образовательных программ	ная работа Конспект Тестирование	оценивания лабораторной работы Шкала оценивания конспекта Шкала оценивания тестирования

Шкала оценивания лабораторной работы

Критерий оценивания	Баллы
Задание выполнено полностью, оформлено по образцу, соответствует предъявляемым требованиям (к каждому заданию предъявляются свои требования, прописанные перед каждым заданием в электронном курсе)	3
Задание выполнено полностью, но есть неточности в оформлении материала или совсем не соответствует требованиям, предъявляемым к оформлению	2
Задание выполнено не полностью или есть неточности в выполнении, есть неточности в оформлении материала или совсем не соответствует требованиям, предъявляемым к оформлению	1
Максимальное количество баллов	3

Шкала оценивания конспекта

Критерии оценивания	Баллы
Текст конспекта логически выстроен и точно изложен, ясен весь ход рассуждения	0,5
Даны ответы на все поставленные вопросы, изложены научным языком, с применением терминологии	0,5
Ответ на каждый вопрос заканчиваться выводом, сокращения слов в тексте	0,5

отсутствуют (или использованы общепринятые)	
Оформление соответствует образцу. Представлены необходимые таблицы и схемы	0,5
Максимальное количество баллов	2

Шкала оценивания тестирования

Критерии оценивания	Баллы за один правильны й ответ
На вопрос дан правильный ответ	2
На вопрос дан неправильный ответ	0
Максимальное количество баллов за тест (15 вопросов)	30

5.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Пример тестового задания

1. Уровень защищенности «Усиленный» («Воронеж») подходит для
a. работы с общедоступной информацией в ИТ-системах различных организаций, а также для защиты информации в государственных информационных системах 3 класса защищенности
b. обработки и защиты информации ограниченного доступа, не составляющей государственную тайну, в том числе в ГИС, ИС ПД и значимых объектов КИИ любого класса защищенности
c. защиты информации, содержащей государственную тайну любой степени секретности и предназначен для обработки информации любой категории доступ

2. Уровень защищенности «Максимальный» («Смоленск») подходит для
a. обработки и защиты информации ограниченного доступа, не составляющей государственную тайну, в том числе в ГИС, ИС ПД и значимых объектов КИИ любого класса защищенности
b. защиты информации, содержащей государственную тайну любой степени секретности и предназначен для обработки информации любой категории доступа
c. работы с общедоступной информацией в ИТ-системах различных организаций, а также для защиты информации в государственных информационных системах 3 класса защищенности

3. Метка безопасности назначается?
a. каждому диску системы
b. каждому разделу системы
c. каждому объекту системы
d. каждому пользователю системы

4. Категория конфиденциальности служит для?
a. разделения доступа к информации одного уровня конфиденциальности
b. разделения доступа к информации на разных уровнях конфиденциальности
c. разделения доступа к информации одного уровня защищенности
d. разделения доступа к информации на разных уровнях защищенности

5. Создана учетная запись пользователя student с использованием политики приватной первичной группы. Какое имя получила первичная группа пользователя?
a. users
b. student

c. root
d. astra-admin

Пример лабораторной работы

Лабораторная работа №1. Управление учетными записями пользователей и групп.
Цель работы: получение навыков управления учетными записями и паролями пользователей, приобретение знаний об атрибутах учетных записей пользователей и формате файлов, хранящих локальную базу данных этих записей.

Порядок выполнения работы:

1. Войти в систему, используя учетную запись администратора.
2. Создать учетную запись пользователя с помощью консольных утилит useradd, adduser.
3. Создать учетную запись пользователя с помощью графической утилиты fly-admin-smc.
4. Сменить пароль существующей учетной записи.
5. Изменить фамилию.

Отчет по работе:

1. Название лабораторной работы.
2. Цель работы.
3. Теоретическая часть.
4. Краткое описание последовательности выполняемых действий.

Примерные вопросы к зачету с оценкой

1. Информационная безопасность. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.
2. Методы информационной безопасности: физические, организационно-правовые и технические средства защиты.
3. Сервисы информационной безопасности: аутентификация, авторизация и аудит.
4. Угрозы информационной безопасности. Классификация угроз информационной безопасности: по природе возникновения, по степени преднамеренности, по месторасположению, по степени вреда, наносимого информационной системе.
5. Понятие защищенных операционных систем. Уровни защищенности операционных систем.
6. Профили защиты на операционных системах. Виды, классы, типы операционных систем в соответствии с профилями защиты.
7. Различие типов операционных систем по принципу работы и функциональному предназначению.
8. Обзор существующих защищенных операционных систем.
9. Практическое применение различных функций защиты информации, реализованных в защищенной операционной системе.
10. Сравнение функциональных возможностей операционных систем.
11. Понятие средства антивирусной защиты. Профили защиты в средствах антивирусной защиты.
12. Виды, классы, типы средств антивирусной защиты в соответствии с профилями защиты.
13. Различие типов средств антивирусной защиты по принципу работы и функциональному предназначению.
14. Обзор существующих средств антивирусной защиты.
15. Работа со средствами антивирусной защиты типа «Г».
16. Практическое применение различных функций защиты информации, реализованных в средствах антивирусной защиты.

17. Сравнение функциональных возможностей средств антивирусной защиты.
18. Понятие межсетевого экрана. Профили защиты в межсетевых экранах.
19. Виды, классы, типы межсетевых экранов в соответствии с профилями защиты.
20. Различие типов межсетевых экранов по принципу работы и функциональному предназначению.
21. Обзор существующих межсетевых экранов.
22. Межсетевые экраны типа «В».
23. Сравнение функциональных возможностей межсетевых экранов.
24. Понятие системы обнаружения вторжений. Профили защиты в системах обнаружения вторжений.
25. Виды, классы, типы систем обнаружения вторжений в соответствии с профилями защиты.
26. Различие типов систем обнаружения вторжений по принципу работы и функциональному предназначению.
27. Обзор существующих систем обнаружения вторжений.
28. Работа с системами обнаружения вторжений типа «уровень узла».
29. Практическое применение различных функций защиты информации, реализованных в системах обнаружения вторжений.
30. Понятие средства анализа защищенности.
31. Различие средств анализа защищенности по принципу работы и функциональному предназначению.
32. Обзор существующих средств анализа защищенности.
33. Практическое применение различных функций защиты информации, реализованных в средствах анализа защищенности.
34. Сравнение функциональных возможностей средств анализа защищенности.
35. Понятие защищенных систем виртуализации. Различие защищенных систем виртуализации по принципу работы и функциональному предназначению.
36. Обзор существующих защищенных систем виртуализации.
37. Практическое применение различных функций защиты информации, реализованных в защищенных системах виртуализации.
38. Сравнение функциональных возможностей защищенных систем виртуализации.
39. Понятие систем резервного копирования. Различие систем резервного копирования по принципу работы и функциональному предназначению.
40. Обзор существующих систем резервного копирования.
41. Практическое применение различных функций защиты информации, реализованных в системах резервного копирования.
42. Учетные записи пользователей и групп. Аутентификация пользователей.
43. Файлы, каталоги и дискреционные права доступа к ним. Особенности моделирования дискреционного доступа.
44. Управление учетными записями пользователей.
45. Организация совместной работы с файлами и каталогами с помощью общей группы, списков управления доступом.
46. Использование дополнительных атрибутов файловой системы и привилегий для ограничения производимых с файлами операций.
47. Использование различных механизмов для расширения возможностей администрирования дискреционного управления доступом.
48. Общий подход к реализации мандатного контроля целостности.
49. Администрирование параметров мандатного контроля целостности.
50. Описание состояний системы.
51. Описание правил перехода из состояния в состояние. Доказательство выполнения условий безопасности.
52. Использование мандатной целостности для администрирования ОССН.

53. Организация файловой системы в рамках мандатного контроля целостности.
54. Использование мандатного и дискреционного управления доступом для организации совместной работы с файлами и каталогами.
55. Использованием привилегий для восстановления данных из архивов.

5.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Требования к зачету с оценкой

На зачет с оценкой выносится материал, излагаемый в лекционном курсе и рассматриваемый на лабораторных занятиях. Для получения зачета с оценкой необходимо правильно ответить на несколько поставленных вопросов. В затруднительных ситуациях (в отдельных случаях) допускается на зачете с оценкой воспользоваться тетрадью с записью материалов лекций в присутствии преподавателя. При этом преподаватель может убедиться, в какой степени студент ориентируется в «своих» материалах, и по ряду дополнительных вопросов (по тетради).

Структура оценивания зачета с оценкой

Критерии оценивания	**Баллы**
Ставится, если студент обнаруживает всестороннее, систематическое и глубокое знание программного материала по дисциплине; обстоятельно анализирует структурную взаимосвязь рассматриваемых тем и разделов дисциплины; усвоил основную и знаком с дополнительной литературой, рекомендованной программой, а также усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии; проявил творческие способности в понимании, изложении и использовании учебного материала.	26-30
Ставится, если студент, обнаруживает полное знание программного материала, успешно выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей образовательной деятельности.	21-25
Ставится, если студент обнаруживает знание основного программного материала в объеме, необходимом для дальнейшего обучения и профессиональной деятельности; справляется с выполнением заданий, предусмотренных программой; знаком с основной литературой, рекомендованной программой; допускает погрешности непринципиального характера в ответе на экзамене.	15-20
Ставится в том случае, если студент обнаруживает пробелы в знаниях основного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий.	0-14

Итоговая шкала оценивания результатов освоения дисциплины

Итоговая оценка по дисциплине формируется из суммы баллов по результатам текущего контроля и промежуточной аттестации и выставляется в соответствии с приведенной ниже таблицей.

Оценка по 100-балльной системе	Оценка по традиционной системе

81 – 100	отлично
61 - 80	хорошо
41 - 60	удовлетворительной
0 - 40	неудовлетворительно

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — URL : https://urait.ru/bcode/567915
2. Чернова, Е. В. Информационная безопасность человека : учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — URL : https://urait.ru/bcode/566457
3. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — URL : https://urait.ru/bcode/567672

6.2. Дополнительная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2025. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — URL : https://urait.ru/bcode/561077
2. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — URL : https://urait.ru/bcode/561313
3. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — URL : https://urait.ru/bcode/569267
4. Рабчевский, А. Н. Основы информационного противоборства: сетевая наука : учебник для вузов / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2025. — 202 с. — (Высшее образование). — ISBN 978-5-534-19085-4. — URL : https://urait.ru/bcode/569038
5. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — URL : https://urait.ru/bcode/560426
6. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — URL : https://urait.ru/bcode/560977
7. Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2025. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — URL : https://urait.ru/bcode/568708
8. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — URL : https://urait.ru/bcode/560516
9. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебник для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2025. — 170 с. —

(Высшее образование). — ISBN 978-5-534-17153-2. — URL : https://urait.ru/bcode/568566

10. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2025. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — URL : https://urait.ru/bcode/561432

11. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2025. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL : https://urait.ru/bcode/560804

12. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — URL : https://urait.ru/bcode/536453

13. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2025. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — URL : https://urait.ru/bcode/563862

14. Панарина, М. М. Корпоративная безопасность. Управление рисками и комплаенс в эпоху цифровизации : учебное пособие для вузов / М. М. Панарина. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 181 с. — (Высшее образование). — ISBN 978-5-534-17777-0. — URL : https://urait.ru/bcode/559219

15. Новожилов, О. П. Информатика в 2 ч. Часть 1 : учебник для вузов / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 320 с. — (Высшее образование). — ISBN 978-5-534-09964-5. — URL : https://urait.ru/bcode/564565

16. Новожилов, О. П. Информатика в 2 ч. Часть 2 : учебник для вузов / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 302 с. — (Высшее образование). — ISBN 978-5-534-09966-9. — URL : https://urait.ru/bcode/564566

17. Трофимов, В. В. Глобальные и локальные сети : учебник для вузов / В. В. Трофимов, М. И. Барабанова, В. И. Кияев. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 151 с. — (Высшее образование). — ISBN 978-5-534-20428-5. — URL : https://urait.ru/bcode/568695

6.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Интернет-Университет Информационных Технологий [Электронный ресурс]. - Режим доступа: http://www.intuit.ru
2. МООК Государственного университета просвещения. - Режим доступа: https://online.eduprosvet.ru/mod/page/view.php?id=18795
3. Сайт Министерства науки и высшего образования РФ [Электронный ресурс]. - Режим доступа: https://minobrnauki.gov.ru/
4. Электронная версия журнала «Вестник образования» Электронный ресурс]. - Режим доступа: www.vestnik.edu.ru

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Методические рекомендации по подготовке к практическим занятиям.
2. Методические рекомендации по организации самостоятельной работы магистрантов.

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Лицензионное программное обеспечение:
Microsoft Windows
Microsoft Office
Kaspersky Endpoint Security

Информационные справочные системы:
Система ГАРАНТ
Система «КонсультантПлюс»

Профессиональные базы данных
fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования
pravo.gov.ru - Официальный интернет-портал правовой информации
www.edu.ru – Федеральный портал Российское образование

Свободно распространяемое программное обеспечение, в том числе отечественного производства
ОМС Плеер (для воспроизведения Электронных Учебных Модулей)
7-zip
Google Chrome

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя:
- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения: учебной мебелью, доской, демонстрационным оборудованием, персональными компьютерами, проектором;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключением к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде.