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
«26» 03 2024 г.
_____
/Кулешова Ю.Д./

Рабочая программа дисциплины

Основы информационной безопасности и защиты информации

Направление подготовки
44.04.01 Педагогическое образование

Профиль:
Современные информационные образовательные технологии

Квалификация
Магистр

Формы обучения
Очная, очно-заочная, заочная

Согласовано учебно-методической комиссией физико-математического факультета
Протокол «26» 03 2024 г. № 7
Председатель УМКом_____
/Кулешова Ю.Д./

Рекомендовано кафедрой вычислительной математики и информационных технологий
Протокол от «13» 03 2024 г. № 11
Зав. кафедрой_____
/Шевчук М.В./

Мытищи
2024

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.

Год начала подготовки (по учебному плану) 2024

СОДЕРЖАНИЕ

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		
	Очная	Очно-заочная	Заочная
Объем дисциплины в зачетных единицах	3	3	3
Объем дисциплины в часах	108	108	108
Контактная работа:	18,2	14,2	6,2
Лекции	4	4	2
Лабораторные занятия	14	10	4
Контактные часы на промежуточную аттестацию:	0,2	0,2	0,2
Зачет с оценкой	0,2	0,2	0,2
Самостоятельная работа	82	86	94
Контроль	7,8	7,8	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 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.	1	
Тема 3. Системы обнаружения вторжений и анализы защищённости Понятие системы обнаружения вторжений. Профили защиты в системах	1	

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.		
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.		6
Тема 6. Мандатный контроль целостности Общий подход к реализации мандатного контроля целостности. Администрирование параметров мандатного контроля целостности. 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.		8
Итого	4	14

Для очно-заочной 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 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.	1	
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	1	

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.		
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. 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.		6
Итого	4	10

Для заочной 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.	0,5	
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 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.	0,5	
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.	0,5	

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.		
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.	0,5	
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.		2
Тема 6. Мандатный контроль целостности Общий подход к реализации мандатного контроля целостности. Администрирование параметров мандатного контроля целостности. 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.		2
Итого	2	4

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Для очной формы обучения

Темы для самостоятельного	Изучаемые вопросы	Кол-во часов	Формы самостоятель-	Методические обес-	Формы отчетнос

изучения			ной работы	печения	ти
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 отечественных операционных системах	Основные понятия. Способы защиты.	12	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
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.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Итого		82			

Для очно-заочной формы обучения

Темы для самостоятельного	Изучаемые вопросы	Кол-во часов	Формы са-мостоятель-	Методиче-ские обес-	Формы отчетнос

изучения			ной работы	печения	ти
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 отечественных операционных системах	Основные понятия. Способы защиты.	14	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
9. Механизмы дискреционного управления доступом	Основные понятия. Области применения.	8	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
10. Мандатный контроль целостности	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Итого		86			

Для заочной формы обучения

Темы для самостоятельного	Изучаемые вопросы	Кол-во часов	Формы самостоятель-	Методические обес-	Формы отчетнос

изучения			ной работы	печения	ти
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.	10	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.	10	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.	12	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
7. Алгебраические методы криптоанализа.	Основные понятия. Области применения.	12	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
8. Информационная безопасность и защита информации в отечественных операционных системах	Основные понятия. Способы защиты.	14	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
9. Механизмы дискреционного управления доступом	Основные понятия. Области применения.	8	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
10. Мандатный контроль целостности	Основные понятия. Области применения.	4	Работа с литературой и сетью Интернет.	Рекомендуемая литература. Ресурсы Интернет.	Конспект
Итого		94			

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 Уметь: применять полученные знания на практике	Лабораторная работа Конспект Тестирование	Шкала оценивания лабораторной работы Шкала оценивания конспекта Шкала оценивания 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	Лабораторная работа Конспект Тестирование	Шкала оценивания лабораторной работы Шкала оценивания конспекта Шкала оценивания тестирования

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
			преподаванию учебных курсов, дисциплин (модулей) по образовательным программам в образовательных организациях соответствующего уровня образования		
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
	Продвинутый	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 *Владеть*: - навыками разработки учебно-методического обеспечения для реализации	Лабораторная работа Конспект Тестирование	Шкала оценивания лабораторной работы Шкала оценивания конспекта Шкала оценивания тестирования

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
			образовательных программ		

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 отсутствуют (или использованы общепринятые)	0,5
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).

Шкала 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	26-30

Критерии оценивания	Баллы
также усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии; проявил творческие способности в понимании, изложении и использовании учебного материала.	
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. Никифоров, С.Н. Методы защиты информации: защита от внешних вторжений: учеб.пособие / С. Н. Никифоров. - 2-е изд.,стереотип. - СПб. : Лань, 2019. - 96с. – Текст: непосредственный.

2. Мельников, В.П. Защита информации: учебник для вузов / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М. : Академия, 2014. - 304с. – Текст: непосредственный.

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 07.02.2023).

6.2. Дополнительная литература

1. Гашков С.Б., Применко Э.А., Черепнев М.А., Криптографические методы защиты информации. [Текст] - М.: Издательство «Академия», 2010. – 304 с.

2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И., Защита информации. Учебное пособие. [Текст] - М.: Издательство «РИОР», 2013. – 392 с.

3. Мельников, В.П. Информационная безопасность и защита информации: учеб.пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 4-е изд.,стереотип . - М. : Академия, 2009. - 336с. – Текст: непосредственный.

4. 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, 2023. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138 (дата обращения: 07.02.2023).

5. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2023. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511890 (дата обращения: 07.02.2023).

6. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520063 (дата обращения: 07.02.2023).

7. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1898839 (дата обращения: 07.02.2023). – Режим доступа: по подписке.

8. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016 (дата обращения: 07.02.2023). – Режим доступа: по подписке.

9. Малюк, А. А. Теория защиты информации / Малюк А. А. - Москва : Горячая линия - Телеком, 2012. - 184 с. - ISBN 978-5-9912-0246-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991202466.html (дата обращения: 07.02.2023). - Режим доступа : по подписке.

10. Баричев С.Г., Гончаров В.В., Серов Р.Е., Основы современной криптографии. [Текст] - М.: Издательство «Горячая линия-Телеком», 2011. – 175 с.

11. Дождиков В.Г., Салтан М.И., Краткий энциклопедический словарь по информационной безопасности. [Текст] - М.: Издательство «Энергия», 2012. – 240 с.

12. Заика А.А., Компьютерная безопасность. [Текст] - М.: Издательство «Рипол КЛассик», 2010. – 304 с.

13. Музыкантский А.И., Фурин В.В., Лекции по криптографии. [Текст] - М.: Издательство «МЦНМО», 2011. – 68 с.

14. Рябко Б.Я., Фионов А.Н., Криптографические методы защиты информации. [Текст] - М.: Издательство «Горячая линия-Телеком», 2012. – 229 с.

15. Рябко Б.Я., Фионов А.Н., Основы современной криптографии и стеганографи. [Текст] - М.: Издательство «Горячая линия-Телеком», 2013. – 232 с.

16. Смирнов А.А., Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза. [Текст] - М.: Издательство «РИОР», 2012. – 159 с.

17. Таранников Ю.В., Комбинаторные свойства дискретных структур и приложения к криптологии. [Текст] - М.: Издательство «МЦНМО», 2011. – 152 с.

18. Чечета С., Введение в дискретную теорию информации и кодирования. Учебное пособие. [Текст] - М.: Издательство «МЦНМО», 2011. – 224 с.

6.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Интернет-Университет Информационных Технологий [Электронный ресурс]. - Режим доступа: http://www.intuit.ru

2. Информационно-образовательная среда «Открытый класс» [Электронный ресурс]. - Режим доступа: http://www.openclass.ru/

3. Конференция «Информационные технологии в образовании» [Электронный ресурс]. - Режим доступа: http://ito.bitpro.ru

4. Методология и технология электронного обучения (обзоры, статьи и др.) [Электронный ресурс]. - Режим доступа: http://cnit.ssau.ru/do/

5. Сайт Министерства образования и науки РФ [Электронный ресурс]. - Режим доступа: www.ed.gov.ru

6. 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 по дисциплинам.

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.