МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

02.12.2025 г.

протокол № 3

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель Карх Д.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Методы и средства информационной безопасности
Направление подготовки	38.03.05 Бизнес-информатика
Профиль	Цифровой бизнес
Форма обучения	очно-заочная
Год набора	2026

Разработана:
Доцент, к.ф.-м.н.
Тюлюкин В.А.

Ст. преподаватель
Змеева Н.Ю.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 38.03.05 Бизнес-информатика (приказ Минобрнауки России от 29.07.2020 г. № 838)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Методы и средства информационной безопасности» является формирование у студентов теоретических и практических знаний в области информационной безопасности, принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем и сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 6						
Экзамен	144	20	8	12	115	4

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Шифр и наименование компетенции	Индикаторы достижения компетенций
аналитический	

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-1.ПК-3 Знать: Возможности имеющейся у исполнителя методологической и технологической инфраструктуры анализа больших данных Предметная область анализа Теоретические и прикладные основы анализа больших данных Современные методы и инструментальные средства анализа больших данных Современный опыт использования анализа больших данных Типы больших данных: метаданные, полуструктурированные, структурированные, неструктурированные Виды источников данных: созданные человеком, созданные машинами Источники информации, в том числе информации, необходимой для обеспечения деятельности в предметной области заказчика исследования Методы извлечения информации и знаний из гетерогенных, мультиструктурированных, неструктурированных источников, в том числе при потоковой обработке Российские и международные стандарты информационной безопасности Современная технологическая инфраструктура высокопроизводительных и распределенных вычислений Режимы получения и обработки данных, поддержка режима реального времени Технологии хранения и обработки больших данных в организации: базы данных, хранилища данных, распределенная и параллельная обработка данных, вычисления в оперативной памяти Облачные технологии, облачные сервисы Методы оценки временных и стоимостных характеристик технологий больших данных Технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии Правила деловой переписки
	ИД-2.ПК-3 Уметь: Определять требования к поставщикам данных из гетерогенных источников Осуществлять взаимодействие с внутренними и внешними поставщиками данных из гетерогенных источников Разрабатывать и оценивать модели больших данных Использовать инструментальные средства для извлечения, преобразования, хранения и обработки данных из разнородных источников, в том числе в режиме реального времени Производить очистку данных для проведения аналитических работ Проводить интеграцию и преобразование больших объемов данных Оценивать соответствие наборов данных задачам анализа больших данных Оценивать стоимость данных для проведения аналитических работ

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-3.ПК-3 Иметь практический опыт: Определение источников больших данных для анализа, идентификация внешних и внутренних источников данных для проведения аналитических работ Получение и фильтрация больших объемов данных из гетерогенных источников Извлечение, проверка и очистка больших объемов данных из гетерогенных источников Агрегация и разработка представления больших объемов данных из гетерогенных источников Оценка соответствия набора данных предметной области и задачам аналитических работ

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 6		135					
Тема 1.	Информационная безопасность: законодательные и нормативно-правовые основы. Виды информационных ресурсов по категориям доступа (ПК-3)	33	1			32	
Тема 2.	Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации (ПК-3)	13	2	2		9	
Тема 3.	Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации (ПК-3)	16	2			14	
Тема 4.	Защита информации от утечки по техническим каналам (ПК-3)	15	1			14	
Тема 5.	Защита информации в компьютерных системах (ПК-3)	21	1	6		14	
Тема 6.	Криптографические методы защиты (ПК-3)	17	1	2		14	
Тема 7.	Вопросы управления ИБ (ПК-3)	20		2		18	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			

Тема 1. Информационная безопасность: законодательные и нормативно-правовые основы. Виды информационных ресурсов по категориям доступа	Контрольная работа №1 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации
Тема 2. Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации	Тест (Приложение 4)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Оценивается знание изученного материала.
Тема 3. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации	Контрольная работа №2 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.

Тема 4. Защита информации от утечки по техническим каналам	Контрольная работа №3 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.
Тема 5. Защите информации в компьютерных системах	Контрольная работа №4 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.
Тема 6. Криптографические методы защиты	Контрольная работа №5 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.
Промежуточная аттестация(Приложение 5)			
6 семестр (Эк)	Билет для экзамена (приложение 5)	в билете 2 теоретических вопроса и 1 практический	0-100 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроля и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущий контроль.Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения профессиональных задач
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Информационная безопасность: законодательные и нормативно-правовые основы. Виды информационных ресурсов по категориям доступа (ПК-3)
Введение: предмет, содержание и задачи дисциплины, ее место среди других дисциплин учебного плана, формы отчетности, основная и дополнительная литература.
Место информационной безопасности в общей системе безопасности государства. Концепция информационной безопасности. Структура и основные положения нормативных правовых актов в области информационной безопасности. Государственные стандарты, используемые в области информационной безопасности.

Тема 2. Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации (ПК-3)
Понятие государственной системы защиты информации. Принципы функционирования государственной системы защиты информации. Правовые основы деятельности государственной системы защиты информации. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Цели и задачи государственной системы защиты информации. Организационная и функциональная структура государственной системы защиты информации. Стандартизация в области обеспечения информационной безопасности. Пользование стандартами информационной безопасности.
Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима. Регламентация доступа персонала к информационным и вычислительным ресурсам. Организация работы с конфиденциальными документами. Требования и рекомендации по защите конфиденциальной информации. Учет, хранение, использование и уничтожение документов (носителей) с конфиденциальной информацией. Организация контроля за соблюдением исполнителями должностных инструкций. Правовое регулирование в сфере информационных отношений. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности. Пользование стандартами информационной безопасности. Международные и отечественные нормативные и руководящие документы, связанные с информационной безопасностью. Руководящие документы Гостехкомиссии РФ.

Тема 3. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации (ПК-3)
Система лицензирования на право проведения работ и оказания услуг в области защиты информации с ограниченным доступом. Нормативные документы, определяющие порядок лицензирования в области защиты конфиденциальной информации. Условия лицензирования деятельности по защите конфиденциальной информации. Общие принципы лицензирования в области защиты конфиденциальной информации. Лицензионные требования для получения лицензии на деятельность в области технической защиты конфиденциальной информации. Перечень документов, представляемых для получения лицензий в области защиты конфиденциальной информации. Система сертификации средств защиты информации. Структура средств защиты информации, подлежащих сертификации. Аттестация объектов информатизации на соответствие требованиям безопасности информации. Объекты, подлежащие аттестации. Перечень основных нормативных документов, определяющих порядок и объём аттестационных испытаний объектов информатизации. Общие требования по аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации. Порядок проведения аттестации объектов информатизации.

Тема 4. Защита информации от утечки по техническим каналам (ПК-3)
Общая характеристика и классификация технических каналов утечки информации (ТКУИ). Элементарная модель канала утечки информации. Основные и вспомогательные технические средства и системы. Контролируемая зона. Основные виды ТКУИ. Технические каналы утечки информации обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ): электромагнитные; электрические; параметрические. Технические каналы утечки акустической (речевой) информации: воздушные; вибрационные; акустоэлектрические; параметрические; оптико-электронный (лазерный). Технические каналы перехвата информации при ее передаче по каналам связи. Технические каналы утечки видовой информации.
Инженерно-технические средства и системы охраны объектов. Охранная сигнализация. Телевизионные системы видеоконтроля. Идентификация и аутентификация лиц, допускаемых на объект. Основные виды технических каналов и источников утечки информации. Противодействие наблюдению в оптическом диапазоне. Защита от прослушивания акустических сигналов. Средства борьбы с закладными подслушивающими устройствами. Защита речевой информации, передаваемой по каналам связи. Пассивные и активные методы защиты информации от утечки в результате электромагнитных излучений и наводок.
Комплексное обеспечение защиты информации от утечки по техническим каналам. Методика принятия решения на защиту от утечки информации в организации. Возможные виды квалификации злоумышленников. Оценка возможностей вероятных злоумышленников. Оценка своей организации как возможного источника информации для злоумышленников. Порядок организации защиты информации на этапе определения задач защиты. Порядок выбора целесообразных мер и средств защиты. Критерии оценки уровня защиты. Организационные способы защиты.

Тема 5. Защита информации в компьютерных системах (ПК-3)
Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Угрозы безопасности в компьютерных системах. Классификация способов несанкционированного доступа к информации в компьютерных системах. Модель поведения потенциального нарушителя. Алгоритм подготовки и реализации атаки нарушителем. Атака на политику безопасности. Атака на сменные элементы системы безопасности. Атака на протоколы информационного взаимодействия. Анализ способов нарушений информационной безопасности.
Противодействие несанкционированного доступа к информации в компьютерных системах. Требования к системе защиты информации. Принципы и правила организации защиты информации от несанкционированного доступа к информации в компьютерных системах. Этапы развития систем информационной безопасности. Средства защита информации в компьютерных системах. Система защиты информации на базе программно-аппаратного комплекса. Подсистемы защиты информации. Состав типового комплекса защиты от несанкционированного доступа к информации. Механизмы работы комплекса защиты от несанкционированного доступа к информации.
Многоуровневая модель защиты объектов информатизации. Способы защиты информации от утечки за счет ПЭМИН. Активные устройства защиты от утечки по каналам ПЭМИН.
Международные стандарты информационного обмена. Аппаратно-технические средства для организации технической защиты в сфере международного информационного обмена. Технологии защиты информации. Аппаратные межсетевые экраны. Рекомендации Microsoft по безопасному подключению почтового сервера к интернет. Безопасность браузеров. Схема подключения брандмауэров или файлволлов или межсетевого экрана. Брандмауэр Agnitum Outpost Firewall Pro. Защита локальный вычислительных сетей брандмауэром с одним сетевым интерфейсом. Средства защиты информации eToken, Symantec Antivirus for Ms Exchange, Symantec Antivirus client. Электронная цифровая подпись, порядок функционирования. Гипотетическая (гетерогенная) вычислительная сеть. Комплексный план технической защиты информации. Алгоритм создания системы информационной безопасности. Совершенствование организационных мероприятий, меры противодействия взлому защиты. Логическая архитектура информационно-вычислительного комплекса.
Защита информации в компьютерных системах от случайных угроз. Создание и управление учетными записями пользователей. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS. Аудит ресурсов и событий системы защиты. Настройка системных параметров безопасности. Настройка параметров безопасности подключения к Интернет. Повышение безопасности информации встроенными средствами. Шифрования операционной системы. Архивация и восстановление данных.
Понятия о видах вирусов. Классификация вирусов: по среде обитания; по способу заражения; по степени опасности деструктированных воздействий; по алгоритму функционирования. Механизм работы вирусов. Способы внедрения потенциально опасных программ. Методы обнаружения вирусов: сканирование; обнаружение изменений; эвристический анализ; использование резидентных сторожей; вакцинирование программ; аппаратно-программная защита. Антивирусные программы: Norton AntiVirus; McAfee; Dr. Web; Kaspersky Anti-Virus; Антивирус Касперского OEM. Профилактика заражения вирусами компьютерных систем. Сущность комплексного подхода к безопасности информации в компьютерных системах.

Тема 6. Криптографические методы защиты (ПК-3)
Введение в криптологию. Исторический обзор. Криптография и криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования. Ключи и алгоритмы шифрования. Методы шифрования с симметричным ключом. Методы замены (подстановки) и перестановки. Гаммирование. Шифрование, использующее генераторы (датчики) псевдослучайных последовательностей. Системы блочного шифрования на основе отечественного ГОСТа и стандарта DES (США). Системы несимметричного шифрования: с открытым ключом для шифрования и закрытым - для дешифрования. Односторонние функции. Криптографическая система RSA. Электронная цифровая подпись на основе криптографического преобразования. Особенности стандартизации и сертификации криптографических средств.

7.2 Содержание практических занятий и лабораторных работ

Тема 5. Защита информации в компьютерных системах (ПК-3) Противодействие несанкционированного доступа к информации в компьютерных системах. Требования к системе защиты информации. Принципы и правила организации защиты информации от несанкционированного доступа к информации в компьютерных системах. Этапы развития систем информационной безопасности. Средства защита информации в компьютерных системах. Система защиты информации на базе программно-аппаратного комплекса. Подсистемы защиты информации. Состав типового комплекса защиты от несанкционированного доступа к информации. Механизмы работы комплекса защиты от несанкционированного доступа к информации.
Тема 6. Криптографические методы защиты (ПК-3) Проверка криптостойкости шифров
Тема 7. Вопросы управления ИБ (ПК-3) Изучение современных подходов к обеспечению безопасности коммерческой информации.

7.3. Содержание самостоятельной работы

Тема 2. Структура, задачи и основные функции государственной системы защиты информации. Организационно-правовое обеспечение защиты информации (ПК-3) Изучение литературы по теме
Тема 3. Лицензирование деятельности в области защиты информации, сертификация средств защиты информации и аттестация объектов информатизации (ПК-3) Изучение литературы по теме
Тема 4. Защита информации от утечки по техническим каналам (ПК-3) Изучение литературы по теме
Тема 5. Защита информации в компьютерных системах (ПК-3) Изучение литературы по теме
Тема 6. Криптографические методы защиты (ПК-3) Изучение литературы по теме

Тема 7. Вопросы управления ИБ (ПК-3)
Вопросы управления ИБ

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
не предусмотрено

7.4. Электронное портфолио обучающегося
не предусмотрено

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
не предусмотрено

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2025. - 337 – Режим доступа: https://znanium.com/catalog/product/2199796

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО&#65533;, 2025. - 336 – Режим доступа: https://znanium.com/catalog/product/2178344

Дополнительная литература:

2. Фисун В. В. Искусственный интеллект управления информационной безопасностью объектов критической информационной инфраструктуры:монография. - Москва: РУСАЙНС, 2023. - 358

3. Бабаш А.В., Баранова Е.К. Моделирование системы защиты информации: Практикум [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО&#65533;, 2025. - 355 – Режим доступа: https://znanium.com/catalog/product/2173934

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии -Без ограничения срока.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии -Без ограничения срока.

Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без ограничения срока.

Astra Linux Common Edition. Договор №0417-ПО/2019 от 08.05.2019, Акт №Sk000343 от 24.05.2019 и Контракт № 35-У/2018 от 13.06.2018, Акт № УТ213 от 17.12.2018. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену

К экзамену

1. Понятие информационных угроз.
2. Информационные войны.
3. Информационные угрозы безопасности РФ. Доктрина информационной безопасности РФ.
4. Виды противников. Хакеры.
5. Компьютерные вирусы. История. Определение по УК РФ.
6. Виды, принципы действия вирусов, демаскирующие признаки.
7. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
8. Угрозы ресурсам компьютерной безопасности. Угрозы, реализуемые на уровне локальной компьютерной системы. Человеческий фактор.
9. Угрозы компьютерной информации, реализуемые на аппаратном уровне.
10. Удаленные атаки на компьютерные системы. Причины уязвимостей компьютерных сетей.
11. Правовое урегулирование защиты информации.
12. Роль, задачи и обязанности администратора безопасности КС.
13. Защита данных криптографическими методами. Методы шифрования.
14. Защита данных криптографическими методами. Алгоритмы шифрования.
15. Требования к шифрам. Сравнение DES и ГОСТ 28147-89
16. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак.
17. Политика безопасности и ее составляющие.
18. Модели защиты информации в КС.
19. Технологии защиты и разграничения доступа.
20. Стандарты ИБ.

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену

Компетенция ПК-3

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных

Задания закрытого типа

1. Что такое шифрование?

a. Процесс преобразования понятного текста в зашифрованный текст

b. Процесс преобразования зашифрованного текста в понятный текст

c. Метод атаки на сеть, использующий множество компьютеров

d. Название определенного типа вируса

2. Что такое файрвол?

a. Программа, которая защищает компьютер от несанкционированного доступа

b. Программа, которая создает вирусы

c. Устройство, которое используется для хранения данных

d. Метка, которая идентифицирует устройство в сети

3. Что означает термин "фишинг" в контексте информационной безопасности?

A. Кража паролей и логинов с уязвимых сайтов

B. Отправка ложных сообщений с целью обмана пользователей

C. Незаконный доступ к защищенным данным

D. Использование вредоносного ПО для получения доступа к системе

4. Как называется процесс обнаружения и устранения уязвимостей в системе информационной безопасности?

A. Анализ угроз

B. Криптография

C. Проверка безопасности

D. Резервное копирование

5. Какие из перечисленных ниже паролей наиболее надежны?

A. 123456

B. qwerty

C. 5f9d8bf45c1900a0

D. password

6. Что такое двухфакторная аутентификация?

A. Ввод логина и пароля

B. Использование отпечатка пальца для входа в систему

C. Использование смарт-карты и пароля для входа в систему

D. Использование нескольких различных методов для подтверждения личности пользователя

7. Каким образом можно защитить себя от вирусов и вредоносного ПО?

A. Использовать сложные пароли

B. Резервирование данных

C. Установка антивирусного программного обеспечения

D. Использование облачного хранилища данных

8. Что такое SSL-шифрование?

A. Защита от вирусов и вредоносного ПО

B. Протокол безопасного соединения для передачи данных через Интернет

C. Формат шифрованного пароля

D. Система контроля доступа к защищенным данным

9. Что такое "фишинг"?

a. Тип злонамеренного ПО

b. Тип мошенничества, основанный на обмане пользователя

c. Аппаратное обеспечение, защищающее от взломов

d. Алгоритм шифрования данных

10. Что такое "вредоносное ПО"?

a. Программное обеспечение, разработанное для защиты от хакеров

b. Программное обеспечение, предназначенное для обхода защиты

c. Программное обеспечение, которое наносит вред компьютеру или другому устройству

d. Программное обеспечение, которое автоматически обновляет систему без разрешения пользователя

Задания открытого типа (приводится хотя бы один пример, допускаются отклонения от приведенных ниже определений)

1. **Что такое шифрование данных? Приведите пример алгоритмов шифрования.**
2. **Что такое VPN? Приведите пример популярных VPN-сервисов.**
3. **Что такое межсетевой экран?**
4. **Каковы основные принципы криптографии и как они используются для обеспечения информационной безопасности? Приведите пример алгоритмов криптографии.**
5. **Что такое ботнеты и как они используются для проведения кибератак? Приведите пример ботнетов.**

6. **Какие существуют методы защиты от SQL-инъекций? Приведите пример инструментов для защиты от SQL-инъекций.**
7. **Каковы основные уязвимости, связанные с безопасностью IoT-устройств? Приведите пример конкретных устройств и типов атак на них.**
8. **Что такое анализ угроз и как он используется для определения уровня риска в информационной безопасности? Приведите пример инструментов для проведения анализа угроз.**
9. **Что такое безопасность веб-сервисов и как она обеспечивается? Приведите пример уязвимостей веб-сервисов и методов их защиты.**
10. **Как работает система защиты информации на уровне операционной системы? Приведите пример операционных систем и методов защиты информации на уровне ОС.**
11. **Что такое защита от DDoS-атак и как она реализуется? Приведите пример инструментов и технологий для защиты от DDoS-атак.**
12. **Какие существуют методы защиты от фишинга и социальной инженерии? Приведите пример инструментов и технологий для защиты от фишинга и социальной инженерии.**
13. **Как работает система управления доступом и как она обеспечивает безопасность в информационных системах? Приведите пример инструментов для управления доступом и методов их применения.**
14. **Что такое целостность данных и как она обеспечивается? Приведите пример методов обеспечения целостности данных.**
15. **Что такое пароль? Приведите пример типов паролей.**
16. **Какие существуют методы аутентификации пользователей? Приведите пример каждого метода.**
17. **Что такое SSL-сертификат? Приведите пример сертификатов.**
18. **Какие существуют типы атак на веб-приложения? Приведите пример каждого типа атак.**
19. **Что такое фишинг? Приведите пример разновидностей фишинга.**
20. **Что такое DoS-атака? Приведите пример методов проведения DoS-атак.**
21. **Что такое DDoS-атака? Приведите пример методов проведения DDoS-атак.**
22. **Что такое SQL-инъекция? Приведите пример типов SQL-инъекций.**
23. **Что такое защита периметра? Приведите пример инструментов защиты периметра.**
24. **Какие существуют типы бэкапов данных? Приведите пример каждого типа бэкапов.**
25. **Что такое многофакторная аутентификация? Приведите пример методов реализации многофакторной аутентификации.**

26. **Какие существуют типы вредоносного ПО? Приведите пример каждого типа вредоносного ПО.**
27. **Что такое антивирус? Приведите пример популярных антивирусов.**
28. **Что такое фаервол? Приведите пример популярных фаерволов.**
29. **Что такое вирус-шифровальщик? Приведите пример известных вирусов-шифровальщиков.**
30. **Что такое брутфорс? Приведите пример ситуаций, когда используется брутфорс.**