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.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Программно-аппаратные средства защиты информации
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2026

Разработана:
Профессор, д.э.н.
Назаров Д.М.

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 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Данный курс нацелен ознакомление студентов с современными средствами защиты информации в компьютерных системах, овладение методами решения профессиональных задач, а также на выработку навыков и получение знаний у обучающихся, необходимых для выполнения работ по установке, настройке и обслуживания программных, программно-аппаратных средств защиты информации, умению ориентироваться в продуктах и тенденциях развития средств защиты информационных технологий.

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 5						
Зачет	108	48	24	24	60	3
Семестр 6						
Экзамен	144	32	0	32	85	4
	252	80	24	56	145	7

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
эксплуатационный	

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-1.ПК-1 Знать: Архитектура и принципы построения операционных систем Программные интерфейсы операционных систем Виды политик управления доступом и информационными потоками применительно к операционным системам Архитектура подсистем защиты информации в операционных системах Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы Состав типовых конфигураций программно-аппаратных средств защиты информации Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам Порядок реализации методов и средств антивирусной защиты в операционных системах Программно-аппаратные средства и методы защиты информации в операционных системах Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-1 Уметь: Формулировать политики безопасности операционных систем Настраивать политики безопасности операционных систем Оценивать угрозы безопасности информации операционных систем Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах Настраивать антивирусные средства защиты информации в операционных системах Устанавливать обновления программного обеспечения и средств антивирусной защиты Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-3.ПК-1 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в операционных системах Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах Формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах Установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации Конфигурирование программно-аппаратных средств защиты информации в операционных системах Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах Управление антивирусной защитой операционных систем в соответствии с действующими требованиями
ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-1.ПК-2 Знать: Принципы построения компьютерных сетей Стек сетевых протоколов операционных систем Стек протоколов сетевого оборудования Порядок реализации методов и средств межсетевого экранирования Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы Виды политик управления доступом и информационными потоками в компьютерных сетях Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации Программно-аппаратные средства и методы защиты информации в компьютерных сетях Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации

ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-2.ПК-2 Уметь: Оценивать угрозы безопасности информации в компьютерных сетях Настраивать правила фильтрации пакетов в компьютерных сетях Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях
	ИД-3.ПК-2 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях Настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-1.ПК-3 Знать: Архитектура подсистем защиты информации в операционных системах Принципы построения систем управления базами данных Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их эксплуатации Виды и формы функционирования вредоносного программного обеспечения Характерные признаки наличия вредоносного программного обеспечения Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-3 Уметь: Анализировать угрозы безопасности информации программного обеспечения Формулировать правила безопасной эксплуатации программного обеспечения Обосновывать правила безопасной эксплуатации программного обеспечения Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-3.ПК-3 Иметь практический опыт: Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения Выполнение работ по обнаружению вредоносного программного обеспечения Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования Формулирование требований к встроенным средствам защиты информации программного обеспечения

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 5		108					
Тема 1.	Уязвимость компьютерных систем (ПК-1, ПК-2, ПК-3)	47	8	8		31	
Тема 2.	Средства и методы ограничения доступа к информации (ПК-2)	61	16	16		29	
Семестр 6		117					
Тема 3.	Понятие штрих-кода. Принципы построения системы контроля управления доступом (СКУД) (ПК-2)	36		8		28	
Тема 4.	Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения (ПК-2)	36		12		24	
Тема 5.	Средства, системы и комплексы защиты программного обеспечения (ПК-2)	45		12		33	

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	Тест (Приложение 4)	Состоит из 15 вопросов, каждый вопрос по 7 баллов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<105 -5
Тема 2	Контрольная работа (Приложение 4)	Состоит из одной комплексной задачи	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5

Тема 3	Ситуационная задача (Приложение 4)	Включает описание ситуации и задание на компьютерную реализацию	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Промежуточная аттестация(Приложение 5)			
5 семестр (За)	Творческое задание (Приложение 5)	20 тем творческих заданий	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
6 семестр (Эк)	Билеты для экзамена (Приложение 5)	Билет включает 2 теоретических вопроса и один и практический	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5

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. Уязвимость компьютерных систем (ПК-1, ПК-2, ПК-3) Особенности современных компьютерных систем как объекта защиты
Тема 2. Средства и методы ограничения доступа к информации (ПК-2) Методы и технологии мониторинга несанкционированные действий

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Средства и методы ограничения доступа к информации (ПК-2) Методы и технологии защиты данных и информации
Тема 3. Понятие штрих-кода. Принципы построения системы контроля управления доступом (СКУД) (ПК-2) Основные элементы СКУД. Режимы работы СКУД. Штрих-код.
Тема 4. Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения (ПК-2) Практические аспекты ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Тема 5. Средства, системы и комплексы защиты программного обеспечения (ПК-2) Классификация аппаратных компонентов средств защиты программ

7.3. Содержание самостоятельной работы

Тема 2. Средства и методы ограничения доступа к информации (ПК-2) Принципы достаточности защиты информации. Хэш-функции.
Тема 3. Понятие штрих-кода. Принципы построения системы контроля управления доступом (СКУД) (ПК-2) Интеграция СКУД. Эксплуатация СКУД
Тема 4. Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения (ПК-2) ОБЕСПЕЧЕНИЕ ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Тема 5. Средства, системы и комплексы защиты программного обеспечения (ПК-2) Программные и технические средства защиты

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
Курсовые работы не предусмотрены

7.4. Электронное портфолио обучающегося
Материалы не размещаются

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. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 592 – Режим доступа: https://znanium.com/catalog/product/1843022

3. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения [Электронный ресурс]:учебник и практикум для вузов. - Москва: Юрайт, 2022. - 312 с – Режим доступа: https://urait.ru/bcode/491249

Дополнительная литература:

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:

Nmap security scanner.Лицензия GPL v2. Срок действия лицензии - без ограничения срока.

Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.

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

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

Вопросы к зачету

1. Цели и средства защиты информации. Типичный набор функциональных
2. подсистем.
3. Основные принципы организации защиты информации от НСД и обеспечения ее
4. конфиденциальности.
5. Понятие Защищенной системы обработки информации. Стандарты информационной безопасности и их роль.
6. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
7. Защита компьютерной системы от «взлома». Программные закладки.
8. Методы уничтожения информации, хранимой на энергонезависимых носителях.
9. Уровни степеней надежности.
10. Защита программного обеспечения.
11. Превентивные меры защиты.
12. Средства собственной защиты.
13. Защита программного обеспечения.
14. Средства защиты в составе вычислительной системы.
15. Защита программного обеспечения.
16. Средства защиты с запросом информации.
17. Защита программного обеспечения.
18. Средства активной защиты.
19. Защита программного обеспечения.
20. Средства пассивной защиты.
21. Технология защиты информации на основе: электронных ключей, смарт-карт, персональных идентификаторов.
22. Принципы и методы создания защищенной операционной системы.

Вопросы к экзамену

1. Основные направления, методы и средства технического противодействия закладным устройствам.
2. Оптико-электронный канал утечки речевой информации.
3. Лазерные микрофоны интерферометрического и дифференциально-интерферометрического принципов действия.
4. Понятие о демаскирующих признаках объекта.
5. Демаскирующие признаки сигналов.
6. Механизм (методика, принцип) обнаружения и классификации опасных сигналов.
7. Методы локализации закладных устройств.
8. Метод энергетического зондирования.
9. Метод акустической и радиолокационной триангуляции.
10. Атрибуты и признаки потенциально опасного сигнала закладных устройств.
11. Государственная система (иерархия) в области технических средств защиты информации.
12. Основные руководящие, нормативные и методические документы.
13. Технический контроль эффективности мер по защите информации.
14. Общая методика проведения технического контроля (ПЭМИН, акустических и виброакустических каналов утечки).

15. Средства защиты с запросом информации.
16. Защита программного обеспечения.
17. Средства активной защиты.
18. Защита программного обеспечения.
19. Средства пассивной защиты.
20. Технология защиты информации на основе: электронных ключей.
21. Технология защиты информации на основе: смарт-карт,
22. Технология защиты информации на основе: персональных идентификаторов.
23. Принципы и методы создания защищенной операционной системы

Приложение 2
к рабочей программе

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

ЗАДАНИЯ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

10.03.01 Информационная безопасность

Дисциплина: Программно-аппаратные средства защиты информации

Компетенция ПК-1; ПК-2; ПК-3

ПК-1: Администрирование подсистем защиты информации в операционных системах

ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях

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

ПК-1: Администрирование подсистем защиты информации в операционных системах

Открытые задания (краткий ответ):

1. Назовите команду Windows для отображения списка сеансов пользователей.
2. Объясните, что имеется в виду под словами «права доступа». Какая команда в Linux используется для изменения прав доступа к файлам?
3. Дайте определение лога. В какой файл Linux заносятся системные журналы (логи)?
4. Дайте определение учетной записи администратора. Укажите имя встроенной учетной записи администратора в ОС Windows.
5. Перечислите три способа ограничения доступа к файлам в ОС Linux. Приведите пример, описывающий один способ ограничения доступа к файлам в ОС Linux

Закрытые задания (тест с 4 вариантами):

Какой командой в Windows можно создать нового пользователя?

A) usercreate

B) newuser

C) net user

D) winadd

Какой файл в Linux содержит информацию о паролях пользователей?

A) /etc/passwd

B) /etc/group

C) /etc/shadow

D) /etc/security

Какая утилита используется в Windows для управления групповыми политиками?

A) gpedit.msc

B) regedit.exe

C) services.msc

D) devmgmt.msc

Какой тип прав доступа не является стандартным в UNIX-системах?

A) Чтение

B) Запись

C) Исполнение

D) Архивация

Какой механизм безопасности встроен в современные версии Windows для защиты целостности ядра ОС?

A) BitLocker

B) UAC

C) Secure Boot

D) Windows Defender

ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях

Открытые задания (краткий ответ):

1. Дайте определение протокола. Назовите основной протокол, обеспечивающий защищённую передачу данных в интернете.
2. Дайте определение порта. Какой порт обычно используется для HTTPS?
3. Дайте определение межсетевого экрана. Перечислите два типа межсетевых экранов.
4. Дайте определение технологии обнаружения вторжений. Приведите пример одной из таких технологий.
5. Дайте определение протокола. Укажите назначение протокола IPsec.

Закрытые задания (тест с 4 вариантами):

Какой протокол используется для защищенного обмена ключами?

A) TCP

B) UDP

C) SSH

D) SSL/TLS

Какая из перечисленных технологий относится к программным средствам защиты сети?

A) Маршрутизатор

B) Межсетевой экран

C) Сетевой кабель

D) Коммутатор

Какой порт используется по умолчанию для SSH?

A) 21

B) 22

C) 23

D) 25

Что означает аббревиатура IDS?

A) Internal Data Security

B) Internet Data Service

C) Intrusion Detection System

D) International Defense Standard

Какой компонент СЗИ отвечает за фильтрацию сетевых пакетов?

A) Сканер уязвимостей

B) Криптомодуль

C) Маршрутизатор

D) Фаервол

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

Открытые задания (краткий ответ):

1. Дайте определение большим данным. Назовите один из форматов файлов, применяемых для хранения больших объемов данных.
2. Перечислите этапы очистки данных. Опишите один из этапов очистки данных.
3. Какая библиотека Python или R чаще всего используется для обработки таблиц?
4. Дайте понятие пропущенного значения. Как называется процесс замены пропущенных значений?
5. Что означает термин «нормализация данных»?

Закрытые задания (тест с 4 вариантами):

Какой формат не предназначен для хранения табличных данных?

A) CSV

B) JSON

C) DOCX

D) XLSX

Какая библиотека Python используется для анализа данных?

A) requests

B) pandas

C) pygame

D) tkinter

Какой метод может использоваться для удаления пропущенных значений?

A) dropna()

B) fillzero()

C) cleardata()

D) emptyrow()

Что такое нормализация данных?

A) Сортировка строк

B) Преобразование данных в диапазон от 0 до 1

C) Удаление дубликатов

D) Сжатие таблиц

Какой из этапов анализа данных идёт после загрузки данных?

A) Хранение

B) Очистка

C) Архивирование

D) Шифрование