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	Управление антивирусной защитой
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2026

Разработана:
Ассистент
Ковтун Д.Б.

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

Целью освоения учебной дисциплины 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 предприятия.

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						
Экзамен	216	96	48	48	93	6

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		189					
Тема 1.	Общие сведения о компьютерных вирусах (ПК-1, ПК-2)	31	6			25	
Тема 2.	Загрузочные вирусы (ПК-1, ПК-2)	14	6	8			
Тема 3.	Файловые вирусы в Windows (ПК-1, ПК-	12	8	4			
Тема 4.	Макровирусы (ПК-1, ПК-2, ПК-3)	14	8	6			
Тема 5.	Сетевые и почтовые вирусы и черви (ПК-1, ПК-2, ПК-3)	28	8	20			
Тема 6.	Распространение вирусов (ПК-1, ПК-2, ПК-3)	20	4			16	
Тема 7.	Обнаружение вирусов (ПК-1, ПК-2)	14	4	10			
Тема 8.	Структура антивирусного программного обеспечения (ПК-1, ПК-2)	30	4			26	
Тема 9.	Применение типового антивирусного программного обеспечения (ПК-1, ПК-2)	26				26	

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	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 2.	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5

Тема 3.	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 4.	Тест	Состоит из 10 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 5.	Тест	Состоит из 10 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 6.	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 7.	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 8.	Тест	Состоит из 10 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Тема 9.	Тест	Состоит из 5 вопросов	менее 30 - 2 31<...<60 - 3 61<...<85 - 4 86<...<100 -5
Промежуточная аттестация(Приложение 5)			
5 семестр (Эк)	Экзаменационные билеты (приложение 5)	В билете 2 теоретических вопроса и 1 практический	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. Общие сведения о компьютерных вирусах (ПК-1, ПК-2) Введение в компьютерную вирусологию. Основные понятия о компьютерных вирусах.
Тема 2. Загрузочные вирусы (ПК-1, ПК-2) Общая информация о загрузочных компьютерных вирусов. Загрузка с винчестера. Загрузочные вирусы в Windows. Методы борьбы с загрузочными вирусами
Тема 3. Файловые вирусы в Windows (ПК-1, ПК-2) Системная организация Windows. Специфика вирусов для Windows. Полиморфные вирусы.
Тема 4. Макровирусы (ПК-1, ПК-2, ПК-3) Вирусы в MS Word и MS Excel. Общие сведения о макросах. Полиморфные макровирусы.
Тема 5. Сетевые и почтовые вирусы и черви (ПК-1, ПК-2, ПК-3) Архитектуру современных сетей. Типовая структура и поведение программы-червя. Механизм заражения ЭВМ программой-червем.
Тема 6. Распространение вирусов (ПК-1, ПК-2, ПК-3) Методы обнаружения программ деструктивного воздействия
Тема 7. Обнаружение вирусов (ПК-1, ПК-2) Методы защиты от программ деструктивного воздействия
Тема 8. Структура антивирусного программного обеспечения (ПК-1, ПК-2) Архитектура современного антивирусного пакета

7.2 Содержание практических занятий и лабораторных работ

Тема 3. Файловые вирусы в Windows (ПК-1, ПК-2) Анализ и нейтрализация конкретного вирусы
Тема 4. Макровирусы (ПК-1, ПК-2, ПК-3) Анализ и удаление конкретного макровируса
Тема 5. Сетевые и почтовые вирусы и черви (ПК-1, ПК-2, ПК-3) Обнаружение, исследование и удаление программы-червя
Тема 7. Обнаружение вирусов (ПК-1, ПК-2) Обнаружение вирусной активности, лечение зараженного компьютера, ликвидация вредоносного кода

7.3. Содержание самостоятельной работы

Тема 6. Распространение вирусов (ПК-1, ПК-2, ПК-3) Изучение принципов инфекции файлов
Тема 8. Структура антивирусного программного обеспечения (ПК-1, ПК-2) Выбор антивирусного комплекса методом функциональной полноты
Тема 9. Применение типового антивирусного программного обеспечения (ПК-1, ПК-2) Установка и использование антивирусного программного пакета

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
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
Материалы не предусмотрены

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. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2021. - 416 – Режим доступа: https://znanium.com/catalog/product/1189327

3. 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

4. Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2024. - 357 – Режим доступа: https://urait.ru/bcode/555950

5. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения [Электронный ресурс]:учебник и практикум для вузов. - Москва: Юрайт, 2024. - 312 – Режим доступа: https://urait.ru/bcode/538066

6. Казарин О. В., Шубинский И. Б. Надежность и безопасность программного обеспечения [Электронный ресурс]:учебное пособие для вузов. - Москва: Юрайт, 2024. - 342 – Режим доступа: https://urait.ru/bcode/539995

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:

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

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без ограничения срока.

ОС "Альт Образование" 8. Договор № ДС-010-2018 от 12.04.2018, Акт к договору от 07.05.2018. Срок действия лицензии - без ограничения срока.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. 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. Компьютерные вирусы. Основные определения.
2. Классификация компьютерных вирусов.
3. Обзор способов заражения компьютерных систем и сетей.
4. Макровирусы.
5. Основные принципы полиморфизма на примере макровирусов.
6. Почтовые черви.
7. Троянские программы. Общие принципы работы. Типы троянских программ.
8. Троянские программы типа Backdoor, алгоритм, структура.
9. Вирусы, поражающие com-файлы.
10. Вирусы, поражающие exe-файлы MS DOS.
11. Загрузочные (boot) вирусы.
12. Резидентные вирусы в системе MS DOS.
13. Полиморфные вирусы.
14. Stealth-вирусы.
15. Вирусы, работающие в системе Windows XP/7/2003/2008, принципы работы.
16. Методы борьбы с вирусами.
17. Антивирусные программы. Типы, примеры.
18. Антивирусные комплексы. AVP. DrWeb. EsetNod32
19. Выбор антивирусного программного средства.
20. Принципы организации антивирусной защиты предприятия.

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: Управление антивирусной защитой

Компетенция ПК-1; ПК-2; ПК-3

ПК-1 Администрирование подсистем защиты информации в операционных система

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

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

Задания закрытого типа

1. Какой тип угрозы безопности данных может привести к потере данных, если вы не сделаете резервную копию?

a) Хакерские атаки
b) Вирусы
c) Кража личной информации
d) Ошибка пользователя

2. Что означает термин "социальная инженерия"?

a) Атака на базу данных
b) Хакерский взлом
c) Использование обмана для получения доступа к системе
d) Использование программного обеспечения для взлома паролей

3. Какой тип кибератаки пытается перегрузить веб-сервер, отправляя большое количество запросов?

a) Фишинг
b) DDoS
c) Кросс-сайтовый скриптинг
d) SQL-инъекция

4. Какое программное обеспечение защищает компьютеры от вредоносных программ?

a) Антивирус
b) Фаервол
c) VPN
d) Интранет

5. Что такое пароль?

a. Символьная строка, используемая для доступа к устройству или приложению
b. Метка, которая идентифицирует устройство в сети
c. Физическое устройство, которое используется для хранения данных
d. Название компании, которая разработала операционную систему

6. Что такое антивирусное программное обеспечение?

a. Программа, которая защищает компьютер от вирусов
b. Программа, которая создает вирусы
c. Программа, которая удаляет важные файлы с компьютера
d. Программа, которая ускоряет работу компьютера

7. Что такое бэкап?

a. Копия важных данных, созданная в случае их потери
b. Ошибка в работе программного обеспечения
c. Программа, которая удаляет все данные с жесткого диска
d. Устройство, которое используется для хранения данных

8. Что такое фишинг?

a. Мошенничество, направленное на получение личной информации пользователя
b. Программа, которая защищает компьютер от вирусов
c. Метод атаки на сеть, использующий множество компьютеров
d. Название определенного типа вируса

9. 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

10. 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

Задания открытого типа

1. Что такое пароль? Приведите пример типов паролей.
2. Какие существуют методы аутентификации пользователей? Приведите пример каждого метода.
3. Что такое SSL-сертификат? Приведите пример сертификатов.
4. Какие существуют типы атак на веб-приложения? Приведите пример каждого типа атак.
5. Что такое фишинг? Приведите пример разновидностей фишинга.
6. Что такое DoS-атака? Приведите пример методов проведения DoS-атак.
7. Что такое DDoS-атака? Приведите пример методов проведения DDoS-атак.
8. Что такое SQL-инъекция? Приведите пример типов SQL-инъекций.
9. Что такое защита периметра? Приведите пример инструментов защиты периметра.
10. Какие существуют типы бэкапов данных? Приведите пример каждого типа бэкапов.

11.Что такое многофакторная аутентификация? Приведите пример методов реализации многофакторной аутентификации.

12.Какие существуют типы вредоносного ПО? Приведите пример каждого типа вредоносного ПО.

13.Что такое антивирус? Приведите пример популярных антивирусов.

14.Что такое фаервол? Приведите пример популярных фаерволов.

15.Что такое вирус-шифровальщик? Приведите пример известных вирусов-шифровальщиков.

16.Что такое брутфорс? Приведите пример ситуаций, когда используется брутфорс.

17.Что такое хакер? Приведите пример разновидностей хакеров.

18.Что такое спам? Приведите пример типов спама.

19.Что такое социальная инженерия? Приведите пример методов социальной инженерии.

20.Что такое шифрование данных? Приведите пример алгоритмов шифрования.

21.Что такое VPN? Приведите пример популярных VPN-сервисов.

22.Что такое межсетевой экран?

23.Каковы основные принципы криптографии и как они используются для обеспечения информационной безопасности? Приведите пример алгоритмов криптографии.

24.Что такое ботнеты и как они используются для проведения кибератак? Приведите пример ботнетов.

25.Какие существуют методы защиты от SQL-инъекций? Приведите пример инструментов для защиты от SQL-инъекций.

26.Каковы основные уязвимости, связанные с безопасностью IoT-устройств? Приведите пример конкретных устройств и типов атак на них.

27.Что такое анализ угроз и как он используется для определения уровня риска в информационной безопасности? Приведите пример инструментов для проведения анализа угроз.

28.Что такое безопасность веб-сервисов и как она обеспечивается? Приведите пример уязвимостей веб-сервисов и методов их защиты.

29.Как работает система защиты информации на уровне операционной системы? Приведите пример операционных систем и методов защиты информации на уровне ОС.

30.Что такое защита от DDoS-атак и как она реализуется? Приведите пример инструментов и технологий для защиты от DDoS-атак.