

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.14
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации от вредоносного программного обеспечения (спец. курс)
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 33Е

Распределение часов дисциплины по семестрам

Семестр	6	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	16	16
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,25	0,25
Контактная работа	48,25	48,25
Самостоятельная работа	59,75	59,75
Контроль	-	-
Итого	108	108

Рабочую программу составил(и):

доцент ИИиЭБ, к.т.н. Полякова Е.В.

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы до 31 декабря 2031 года

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 1 от «01» сентября 2025 г.).

1. Цель освоения дисциплины

Целью освоения учебной дисциплины является формирование у студентов знаний и представлений о смысле, целях и задачах защиты от различных видов опасной компьютерной информации, включая вредоносные программы.

Приобретенные знания позволят студентам правильно строить систему антивирусной безопасности организации, выступить в роли эксперта при расследовании компьютерных преступлений, предотвращать проникновение и распространение вредоносных программ, а также концепциям, инструментам и методам распознавания вредоносных программ, и общим элементам анализа вредоносного ПО, тестирования и аттестации безопасности ПО и ОС.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Компьютерные сети;
- Основы управления информационной безопасностью.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:

- Информационная безопасность компьютерных сетей;
- Техническая защита информации;
- Аудит защищенности информационных систем.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-11 Способен противодействовать угрозам безопасности информации с использованием средств защиты информации операционных систем и сетей, включая средства криптографической защиты информации	ПК-11.7 Использует знания типов вредоносного ПО, их принцип действия и каналы проникновения в инфраструктуру	Знать: - типы вредоносного ПО, их принцип действия и каналы проникновения в инфраструктуру;
		Уметь: - фиксировать при проведении следственных действий криминалистически значимую компьютерную информацию, в том числе осуществлять ее копирование; - определять признаки вредоносности компьютерных программ, - уметь разрабатывать шелл-коды и эксплойты в целях проведения всестороннего анализа защищенности
		Владеть

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		<ul style="list-style-type: none"> - навыками настройки и проверки систем защиты от вредоносного ПО
	ПК-11.8 Умеет самостоятельно проводить простые диагностические экспертизы и исследования в сфере компьютерных технологий	Знать: - методы анализа защищенности программных систем от потенциальных угроз, связанных с ошибками и недоработками программного кода.
		Уметь: - самостоятельно проводить простые диагностические экспертизы и исследования в сфере компьютерных технологий;
		Владеть - навыками настройки и проверки систем, для обеспечения защиты от применения наиболее распространенных пэйлоадов
	ПК-11.9 Владеет навыками поиска и нейтрализации вредоносного ПО	Знать: - уязвимости, присутствующие в ОС и ПО; - способы борьбы с вредоносным ПО и уязвимостями
		Уметь: - обнаруживать присутствие вредоносного программного кода в статическом и динамическом режимах
		Владеть - навыками поиска и нейтрализации вредоносного ПО

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек 1	Тема 1 Введение в анализ вредоносных программ Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Классификация программ по степени опасности для защищаемой информации и компьютерной системы. Деструктивные функции вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Понятие потенциально нежелательного ПО. Правила именования и поглощения вредоносного ПО. Признаки присутствия вредоносного ПО в ИС. Каналы проникновения вредоносного ПО. Уязвимые места программного обеспечения ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ.	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 1	Тема 1 Введение в анализ вредоносных программ Исследование деструктивных возможностей потенциально опасных программ и команд	6	2	2		Практическое задание 1
Модуль 1	Лек 2	Тема 2 Вредоносное ПО как средство совершения компьютерных преступлений Понятие компьютерных преступлений. Понятие киберпреступник и хакер. Классификация	6	2	-	-	Банк тестовых заданий/ Устный опрос

		хакеров. Понятие хакерской атаки. Классификация хакерских атак. Хакерские группировки. Понятие анонимность в сети Интернет. Средства достижения анонимности.					
Модуль 1	Пр 2	Тема 2 Вредоносное ПО как средство совершения компьютерных преступлений Исследование возможностей скрытого внедрения и запуска опасных программ	6	2	2		Практическое задание 2
Модуль 1	Пр 3	Тема 2 Вредоносное ПО как средство совершения компьютерных преступлений Исследование возможностей скрытого внедрения и запуска опасных программ	6	2	2		Практическое задание 2
Модуль 1	Лек 3	Тема 3 Изучение функциональных возможностей вредоносных программ Основные признаки и возможности макровирусов, сетевых «червей», программ «удаленного администрирования». Возможности программ-«руткитов». Изучение функциональных возможностей вредоносных программ. Рекомендации по дизассемблированию и исследованию программного кода. Трассировка программ. Возможности программ типа EkeScore и OllyDebugger.	6	2	-		Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 4	Тема 3 Изучение функциональных возможностей вредоносных программ Исследование интерпретируемых вредоносных программ (командных файлов, макросов и сценариев)	6	2	2		Практическое задание 3
Модуль 1	Пр 5	Тема 3 Изучение функциональных возможностей вредоносных программ Исследование интерпретируемых вредоносных программ (командных файлов, макросов и сценариев)	6	2	2		Практическое задание 3

Модуль 1	Лек 4	Тема 4 Статический анализ Определение типа файла. Сличение информации с помощью цифровых отпечатков. Хэш функции. Извлечение строк. Структура памяти процесса. Стековые кадры. Передача параметров функции. Соглашения о вызове функций. Переполнение буфера. Опасные конструкции языка C. Однобайтовое переполнение. Динамическое выделение памяти. Куча. Структура участков кучи. Алгоритм работы функции free. Структура подставных участков при переполнении кучи	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 6	Тема 4 Статический анализ Исследование уязвимости переполнения кучи	6	2	2		Практическое задание 4
Модуль 1	Пр 7	Тема 4 Статический анализ Исследования уязвимости переполнения стека	6	2	2		Практическое задание 5
Модуль 1	Пр 8	Тема 4 Статический анализ Классификация вредоносных программ с использованием YARA	6	2	2		Практическое задание 6
Модуль 1	Лек 5	Тема 5 Динамический анализ Обзор тестовой среды. Инструменты динамического анализа (мониторинга). Захват сетевого трафика с помощью Wireshark. Этапы динамического анализа. Анализ динамически подключаемой библиотеки (DLL). Анализ DLL с помощью rundll32.exe. Анализ DLL с помощью проверки процессов.	6	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 9	Тема 5 Динамический анализ Анализ исполняемого файла вредоносного ПО	6	2	2		Практическое задание 7
Модуль 1	Лек 6	Тема 6 Анализ на практике	6	2	-		Банк тестовых заданий/

		Приложение для генерирования трафика: SuperFunkyChat. Курс анализа с помощью Wireshark. Определение структуры пакета. Парсинг пакета сообщения.					Устный опрос
Модуль 1	Пр 10	Тема 6 Анализ на практике Анализ протокола с помощью Python.	6	2	2		Практическое задание 8
Модуль 1	Пр 11	Тема 6 Анализ на практике Анализ протокола с помощью Python.	6	2	2		Практическое задание 8
Модуль 1	Лек 7	Тема 7 Обратная разработка приложения Компиляторы, интерпретаторы и ассемблеры. Архитектура x86. Статический и динамический обратный инжиниринг. Обратное проектирование управляемого кода.	6	2	-		Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 12	Тема 7 Обратная разработка приложения Декомпилирование приложения.	6	2	2		Практическое задание 9
Модуль 1	Пр 13	Тема 7 Обратная разработка приложения Декомпилирование приложения.	6	2	2		Практическое задание 9
Модуль 1	Лек 8	Тема 8 Защита ИС от вредоносного ПО Принцип борьбы с вредоносным ПО. Аппаратные средства защиты. Программные средства защиты. Антивирусные средства. Средства защиты от НСД. Средства анализа трафика. Средства предотвращения утечки информации. Средства мониторинга и анализа процессов. Средства преодоления защиты. Алгоритм поиска вредоносного ПО в зараженной ИС. Понятие дефекта ПО. Определение уязвимостей. Понятие метрики. Система оценки уязвимостей. Понятие взлома ПО. Виды взлома ПО. Защита от взлома ПО. Техника защиты от взлома ПО	6	2	-		Банк тестовых заданий/ Устный опрос

Модуль 1	Пр 14	Тема 8 Защита ИС от вредоносного ПО Внедрение удаленного исполняемого файла или шелл-кода.	6	2	2		Практическое задание 10
Модуль 1	Пр 15	Тема 8 Защита ИС от вредоносного ПО Внедрение удаленного исполняемого файла или шелл-кода.	6	2	62		Практическое задание 10
Модуль 1	Ср	Самостоятельное изучение материала, не вошедшего в курс лекций	6	59,75	-		Банк тестовых заданий
	ПА	Промежуточная аттестация	6	0,25	-	-	Вопросы к зачету
	Псц	Посещаемость	6	-	10	-	
	Пр 16	Итоговое тестирование	6	2	100	-	Тестовые
		Бонусные баллы	6	-	20	-	
Итого:				108			

Схема расчета итогового балла

Обучающийся получает до 90 баллов за выполнение практических заданий, до 10 баллов за посещаемость и проходит итоговое тестирование, оцениваемое от 0 до 100 в зависимости от успешности его прохождения. Итоговый балл за курс рассчитывается, как сумма баллов за выполнение практических заданий, баллов за посещаемость и баллов, набранных в ходе тестирования, после чего вся сумма делится на 2. Бонусные баллы выставляются студенту за участие в олимпиадах, конференциях, форумах.

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.

6. Методические указания по освоению дисциплины

Изучение дисциплины предусматривает чтение лекций, проведение практических занятий, самостоятельное изучение специальной литературы по вопросам лекций.

Изучение теоретического материала определяется рабочей учебной программой дисциплины, включенным в нее перечнем литературы. Рекомендуется при подготовке к занятиям повторить материал предшествующих тем лекций.

При подготовке к практическому занятию необходимо изучить материалы лекции, рекомендованную литературу. Изученный материал следует проанализировать в соответствии с планом занятия, затем проверить степень усвоения содержания вопросов.

Виды самостоятельной работы обучающихся:

1. Повторение пройденного лекционного материала, чтение рекомендованной литературы.

2. Подготовка к практическим занятиям.

3. Работа с электронными источниками.

4. Подготовка к сдаче зачета.

Самостоятельная работа обучающихся заключается в изучении литературы, дополняющей материал, излагаемый в лекционной части курса. Необходимо овладеть навыками библиографического поиска, в том числе в сетевых Интернет-ресурсах, научиться сопоставлять различные точки зрения и определять методы исследований.

При подготовке к зачету следует руководствоваться перечнем вопросов для подготовки к итоговому контролю по курсу. При этом необходимо уяснить суть основных понятий дисциплины.

Предполагается, что, прослушав лекцию, обучающийся должен ознакомиться с рекомендованной литературой из основного списка, осуществить поиск и критическую оценку материала на сайтах Интернет, собрать необходимую информацию

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-11	Тестовые задания. Вопросы к зачету № 1-60. Практические задания № 1-10

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Практическое задание

(наименование оценочного средства)

Практическое задание 1. Исследование деструктивных возможностей потенциально опасных программ и команд.

Практическое задание 2. Исследование возможностей скрытого внедрения и запуска опасных программ.

Практическое задание 3. Исследование интерпретируемых вредоносных программ (командных файлов, макросов и сценариев).

Практическое задание 4. Исследование уязвимости переполнения кучи.

Практическое задание 5. Исследования уязвимости переполнения стека.

Практическое задание 6. Классификация вредоносных программ с использованием YARA.

Практическое задание 7. Анализ исполняемого файла вредоносного ПО

Практическое задание 8. Анализ протокола с помощью Python.

Практическое задание 9. Декомпилирование приложения

Практическое задание 10. Внедрение удаленного исполняемого файла или шелл-кода.

Типовой(ые) пример(ы) задания(ий)

Цель: Сформировать практические навыки выявления, безопасного воспроизведения и анализа деструктивного воздействия потенциально опасных программ и системных команд, а также освоить механизмы их ограничения в изолированной среде.

Задание:

1. Студент разворачивает виртуальную машину или контейнер с отключённым сетевым доступом.
2. В задании моделируются безопасные аналоги деструктивных сценариев: истощение процессорного времени (fork-бомбы), переполнение дискового пространства, блокировка ресурсов файловых систем и рекурсивное удаление данных.
3. С помощью инструментов мониторинга (strace, auditd, htop, iotop) фиксируется влияние команд на ядро ОС и планировщик процессов.
4. После базового воспроизведения применяются механизмы контроля: ulimit, cgroups v2, sssomr, политики выполнения. Проводится повторный запуск, фиксируется срабатывание ограничений.
5. Результаты оформляются в виде отчёта с логами трассировки, графиками потребления ресурсов и матрицей «вектор → уязвимость → механизм защиты».

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

Формы текущего контроля	Критерии и нормы оценки
Отчет по практическим работам № 1-10	2 балла – задание выполнено в полном объеме без замечаний - 2 балла – задание не выполнено
Устный опрос	41-62 балла – дан полный, развернутый, аргументированный ответ на 2 вопроса 31-40 баллов – дан неполный ответ на 2 вопроса 21-30 баллов – дан полный, развернутый, аргументированный ответ на 1 вопрос 1-20 баллов – дан неполный ответ на 1 вопрос 0 баллов – не дан ни один ответ на 2 вопроса
Посещаемость	10 баллов - обучающийся посещает все занятия. Для обучающихся с менее чем 100% посещаемостью оценка рассчитывается пропорционально количеству посещенных занятий

7.2.2. Типовой пример тестового задания

Типовой пример тестовых заданий

Как называется тип атаки, при котором злоумышленник выдает себя за сотрудника технической поддержки для получения доступа к системе?

Выберите один из 4 вариантов ответа:

- 1) Фишинг
- 2) Вишинг
- 3) Спуфинг
- 4) Смишинг

Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 6

№ п/п	Вопросы к зачету
1.	Раскройте эволюцию вредоносного программного обеспечения: от первых экспериментальных вирусов до современных целевых атак. Какие технологические и экономические факторы обусловили усложнение структуры и функционала вредоносных программ?

2.	Дайте развёрнутое определение термина «вредоносное программное обеспечение». Опишите основные критерии классификации (по цели, способу распространения, степени автономности, уровню требуемых привилегий).
3.	Объясните различие между вирусами, сетевыми червями, троянскими программами, программами-шифровальщиками, шпионским ПО и удалёнными административными инструментами. Приведите примеры реальных представителей каждого класса.
4.	Опишите архитектурные особенности современных многокомпонентных вредоносных программ (загрузчик, модуль закрепления, модуль эксфильтрации, клиент командного центра). Зачем используется модульная архитектура и как она влияет на живучесть угрозы?
5.	Раскройте понятие «индикаторы компрометации». Какие типы индикаторов используются при анализе вредоносного ПО и как они применяются в системах проактивной защиты?
6.	Объясните концепцию «жизненного цикла вредоносной программы». Как этапы доставки, выполнения, закрепления, повышения привилегий, бокового перемещения и эксфильтрации соотносятся с моделью MITRE ATT&CK?
7.	Охарактеризуйте влияние легитимных системных утилит на развитие вредоносных технологий. Как злоумышленники используют административные инструменты операционных систем для сокрытия активности?
8.	Раскройте содержание понятия «файл-дроппер» и «файл-лоадер». В чём их принципиальное отличие и как они используются в многоэтапных цепочках заражения?
9.	Объясните, почему современные вредоносные программы активно используют шифрование, упаковку и обфускацию. Какие методы применяются для каждого из этих механизмов сокрытия?
10.	Опишите роль изолированных сред исследования в анализе вредоносного ПО. Какие ограничения виртуальной машины необходимо учитывать при динамическом анализе, чтобы избежать детектирования образцом?
11.	Раскройте основные механизмы сохранения доступа в операционных системах Windows и Linux. Как злоумышленники используют системный реестр, запланированные задачи, службы и конфигурационные файлы?
12.	Объясните принцип работы механизма захвата загрузки библиотек. Какие условия необходимы для успешной эксплуатации данной техники и как можно защититься от неё на уровне конфигурации приложений?
13.	Опишите методы скрытия процессов, файлов и сетевых соединений в современных операционных системах. Как используются технологии руткитов на уровне ядра и пользовательского пространства?
14.	Раскройте понятие «инъекция в процесс». Опишите техники внедрения динамических библиотек, вырезания процесса и рефлексивной загрузки. В чём их преимущества для атакующего?
15.	Объясните, как вредоносные программы обходят механизмы контроля учётных записей в Windows. Какие техники обхода наиболее распространены и как они маскируются под легитимные действия?
16.	Охарактеризуйте методы обхода антивирусного сканирования. Как используются полиморфизм, метаморфизм, шифрование полезной нагрузки и временные задержки выполнения?
17.	Раскройте содержание понятия «вредоносное ПО без файлов». Как выполняется исполнение кода в оперативной памяти без записи на диск и какие артефакты остаются в системе после такой атаки?
18.	Объясните механизмы сокрытия сетевой активности вредоносных программ. Как используются туннелирование через протокол доменных имён, шифрование трафика и легитимные облачные сервисы?

19.	Опишите техники антиотладки и антианализа, применяемые в современных образцах вредоносного ПО. Как реализуются проверки наличия отладчика, виртуальной машины и изолированной среды?
20.	Раскройте влияние механизмов безопасной загрузки и контроля целостности начального загрузчика на возможности закрепления вредоносного кода на ранних этапах инициализации операционной системы.
21.	Объясните природу уязвимости переполнения стека вызовов. Как происходит перезапись адреса возврата и что необходимо для успешной эксплуатации в современных условиях с включёнными механизмами защиты?
22.	Раскройте особенности уязвимости переполнения динамической памяти. Чем отличается управление памятью в куче от стека и как используются фрагментация, атаки на связные списки и техники работы с кэшем распределения?
23.	Опишите концепцию программирования, ориентированного на возврат. Как формируются цепочки фрагментов кода и для чего они применяются при обходе механизмов запрета исполнения данных?
24.	Объясните принципы работы уязвимостей типа «использование после освобождения» и «двойное освобождение». Как они эксплуатируются для получения произвольного чтения или записи памяти?
25.	Раскройте содержание понятия «удалённое выполнение кода». Какие векторы доставки и условия необходимы для реализации данного типа уязвимости в веб-приложениях и сетевых сервисах?
26.	Опишите структуру и этапы разработки шелл-кода. Как обеспечивается его позиционно-независимое исполнение и обход ограничений на использование нулевых байт?
27.	Объясните механизмы обхода современных защитных флагов компилятора и операционной системы. Какие техники позволяют снизить эффективность рандомизации адресного пространства, канареек стека и контроля потока выполнения?
28.	Раскройте особенности эксплуатации уязвимостей в интерпретаторах и виртуальных машинах выполнения. Как происходит выход из изолированной среды интерпретатора и получение контроля над хост-системой?
29.	Охарактеризуйте уязвимости формата документов и медиафайлов. Как используются макросы, встраиваемые объекты, парсеры шрифтов и декодеры изображений для доставки полезной нагрузки?
30.	Объясните роль автоматизированного фаззинг-тестирования в поиске уязвимостей. Какие типы генераторов входных данных существуют и как они интегрируются в процесс разработки безопасного программного обеспечения?
31.	Раскройте алгоритм проведения статического анализа исполняемого файла. Какие инструменты используются для анализа структур заголовков, таблиц импорта и экспорта, строк и ресурсов?
32.	Объясните методику динамического анализа вредоносного ПО. Как настраивается изолированная среда, какие системные вызовы и прикладные интерфейсы мониторятся, как фиксируется сетевая активность?
33.	Опишите процесс распаковки исполняемых файлов. Какие признаки указывают на наличие упаковщика и как восстанавливается оригинальный код в оперативной памяти?
34.	Раскройте принципы декомпиляции и дизассемблирования. В чём различие между этими подходами и какие ограничения возникают при восстановлении логики из машинного кода?
35.	Объясните назначение и структуру отчёта по анализу вредоносного образца. Какие разделы обязательны для передачи информации аналитикам центров мониторинга безопасности и разработчикам средств защиты?

36.	Охарактеризуйте методы анализа обфусцированных скриптов и макросов. Как восстанавливается исходная логика при использовании кодировок, конкатенации строк и динамического выполнения?
37.	Раскройте содержание понятия «сигнатурный и поведенческий анализ». Как современные системы защиты конечных точек комбинируют оба подхода для детектирования неизвестных угроз?
38.	Объясните роль программных отладчиков в исследовании вредоносного ПО. Как устанавливаются точки останова, анализируются регистры процессора и модифицируется поток выполнения?
39.	Опишите методику анализа вредоносных документов. Как извлекаются встроенные объекты, анализируются встроенные скрипты и восстанавливаются цепочки загрузки полезной нагрузки?
40.	Раскройте особенности анализа вредоносного программного обеспечения для мобильных платформ. Как исследуются пакеты приложений, деконструируется промежуточный код и анализируются запрашиваемые разрешения?
41.	Объясните механизмы выполнения вредоносных макросов в офисных документах. Как обходятся настройки безопасности и режим защищённого просмотра?
42.	Раскройте особенности командной оболочки PowerShell как инструмента атаки и защиты. Как используются механизмы обхода встроенного мониторинга, ограничения политик выполнения и техники автоматической загрузки кода?
43.	Охарактеризуйте угрозы, связанные с интерпретируемыми языками программирования. Как обеспечивается скрытность выполнения и обход средств мониторинга процессов?
44.	Объясните принципы работы вредоносных скриптов автозапуска в различных операционных системах. Как они интегрируются в легитимные процессы системного администрирования?
45.	Раскройте методы детектирования и блокировки интерпретируемых угроз на уровне хоста и сети. Какие политики выполнения и ограничения применяются в корпоративных информационных системах?
46.	Объясните назначение и синтаксис правил классификации вредоносного ПО. Как комбинируются строковые, байтовые и условные выражения для точной идентификации семейств угроз?
47.	Раскройте методику разработки и тестирования классифицирующих правил. Как минимизируются ложные срабатывания и обеспечивается покрытие полиморфных и метаморфных образцов?
48.	Охарактеризуйте возможности автоматизации анализа вредоносного ПО с использованием языка Python. Как применяются библиотеки для разбора исполняемых файлов, дизассемблирования, классификации и анализа сетевых пакетов?
49.	Объясните принципы анализа сетевых протоколов при исследовании вредоносной активности. Как реконструируются сессии, извлекается полезная нагрузка и детектируются каналы связи с командными центрами?
50.	Раскройте содержание понятия «сетевая сигнатура». Как создаются правила для систем обнаружения вторжений с целью блокировки известных паттернов вредоносного трафика?
51.	Объясните архитектуру и функции современных систем защиты конечных точек с расширенным детектированием и реагированием. Как обеспечивается сбор телеметрии, корреляция событий и автоматизированное реагирование на инциденты?
52.	Раскройте принципы построения системы мониторинга безопасности в корпоративной сети. Какие источники журналов событий необходимы для детектирования вредоносной активности на ранних стадиях?
53.	Охарактеризуйте процесс реагирования на инциденты, связанные с вредоносным программным обеспечением. Как организуется изоляция заражённых узлов, сбор цифровых артефактов и восстановление систем?

54.	Объясните роль данных об угрозах в защите от вредоносного ПО. Как используются платформы обмена индикаторами компрометации и внутренние базы данных для проактивной защиты?
55.	Раскройте содержание понятия «уязвимость нулевого дня». Какие стратегии применяются для защиты от неизвестных эксплойтов до выхода официальных исправлений?
56.	Опишите методы безопасной эксплуатации уязвимостей в тестовых средах. Как обеспечивается изоляция, контроль ресурсов и предотвращение латерального перемещения в лабораторных сетях?
57.	Объясните влияние современных механизмов защиты ядра операционной системы на возможности руткитов и вредоносных драйверов. Какие ограничения накладываются на модификацию структур ядра?
58.	Раскройте особенности защиты виртуализированных сред и контейнеров от вредоносного программного обеспечения. Какие риски возникают при атаках выхода из изоляции и как они нейтрализуются?
59.	Охарактеризуйте нормативно-правовые требования к защите от вредоносного ПО в организациях. Какие стандарты и руководящие документы регламентируют организационные и технические меры защиты?
60.	Объясните этические и юридические аспекты исследования вредоносного программного обеспечения. Какие ограничения установлены законодательством Российской Федерации и как обеспечивается соблюдение академической честности при выполнении лабораторных и исследовательских работ?

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
6	Зачет (по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Прохорова О. В.	Информационная безопасность и защита информации	учебник	2025	эбс-Лань
2	Баранова Е. К.	Информационная безопасность и защита информации	учебное пособие	2026	эбс-ZNANIUM

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Шаньгин В. Ф.	Информационная безопасность и защита информации	учебное пособие	2019	эбс-IPRbooks
2	Глинская Е. В.	Информационная безопасность конструкций ЭВМ и систем	учебное пособие	2021	эбс-ZNANIUM
	Ревнивых А. В.	Информационная безопасность в организациях	учебное пособие	2021	эбс-IPRbooks

8.3. Перечень профессиональных баз данных и информационных справочных систем

1. FREEDOM COLLECTION (Полнотекстовая коллекция электронных журналов Elsevier B.V.) <https://www.sciencedirect.com/> неизвестный
2. Nano Database <http://nano.nature.com/> база данных
3. Springer Materials <http://materials.springer.com/> база данных
4. Springer Nature Protocols and Methods <https://experiments.springernature.com/sources/springer-protocols> база данных
5. zbMath <https://zbmath.org/> база данных
6. Springer Nature (Полнотекстовая коллекция журналов) <https://www.springernature.com/gp/products> неизвестный
7. Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature) <https://link.springer.com/> неизвестный
8. ORBIT INTELLIGENCE (Патентная база компании QUESTEL) <http://www.orbit.com/> база данных
9. CSD-ENTERPRISE (База данных компании CAMBRIDGE CRYSTALLOGRAPHIC DATA CENTER) <https://www.ccdc.cam.ac.uk/structures/> база данных
10. ELIBRARY.RU (электронная библиотека научных публикаций) <http://elibrary.ru> неизвестный
11. "Гарант" <https://www.garant.ru/> ИСС
12. "КонсультантПлюс" <https://www.consultant.ru/> ИСС
13. "Кодекс" <https://kodeks.ru/> ИСС
14. Техэксперт <https://cntd.ru/> ИСС

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Помещение для самостоятельной работы обучающихся Д -409	Стол-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы,

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
		компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф
2	Помещение для самостоятельной работы обучающихся УЛК-105	Столы, стулья, стеллажи (в т.ч. выставочные) с книгами, персональные компьютеры, мобильные рабочие места
3	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
4	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-402	Столы ученические двухместные , стулья, стол преподавательский , стул преподавательский , доска аудиторная (меловая) , кафедра напольная, проектор, экран выкатной.