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 от вредоносного программного обеспечения
(наименование дисциплины)

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

Форма обучения: очная

Год набора: 2023

Общая трудоемкость:3 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**6**	**Итого**
Форма контроля **Вид занятий**	**зачет**	
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):

Власов Игорь Анатольевич

(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 дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

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.

Полученные знания используются при изучении следующих дисциплин:
- Безопасность компьютерных сетей;
- Техническая защита информации.

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 криминалистический 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 - 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

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		- 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	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		-	
Модуль 1	Пр	Тема 1 Введение в анализ вредоносных программ Исследование деструктивных возможностей потенциально опасных программ и команд	6	4			Отчет по практическому занятию №1
Модуль 1	Ср	Тема 1 Введение в анализ вредоносных программ Понятие шелл-кода. Библиотеки шелл-кодов. Пакет эксплойтов Metasploit Framework для анализа защищенности. Основы ассемблера платформы IA-32 и IA-64. Механизм системных вызовов, его применение при написании шелл-кода.	6	8			

		Привязывающий шелл-код. Обратный шелл-код.					
Модуль 1	Лек	Тема 2 Вредоносное ПО как средство совершения компьютерных преступлений Понятие компьютерных преступлений. Понятие киберпреступник и хакер. Классификация хакеров. Понятие хакерской атаки. Классификация хакерских атак. Хакерские группировки. Понятие анонимность в сети Интернет. Средства достижения анонимности.	6	2		-	
Модуль 1	Пр	Тема 2 Вредоносное ПО как средство совершения компьютерных преступлений Исследование возможностей скрытого внедрения и запуска опасных программ	6	4			Отчет по практическому занятию №2
Модуль 1	Ср	Тема 2 Вредоносное ПО как средство совершения компьютерных преступлений Реферат	6	8			
Модуль 1	Лек	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 ExeScope и OllyDebugger.	6	2			
Модуль 1	Пр	Тема 3 Изучение функциональных возможностей вредоносных программ Исследование интерпретируемых вредоносных программ (командных файлов, макросов и сценариев)	6	4			Отчет по практическому занятию №3
Модуль 1	Ср	Тема 3 Изучение функциональных возможностей вредоносных программ Исследование защитных механизмов ОС и прикладного ПО	6	8			

Модуль 1	Лек	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 С. Однобайтовое переполнение. Динамическое выделение памяти. Куча. Структура участков кучи. Алгоритм работы функции free. Структура подставных участков при переполнении кучи	6	2		-	
Модуль 1	Пр	Тема 4 Статический анализ Исследование уязвимости переполнения кучи	6	4			Отчет по практическому занятию №4
Модуль 1	Пр	Тема 4 Статический анализ Исследования уязвимости переполнения стека	6	4			Отчет по практическому занятию №5
Модуль 1	Пр	Тема 4 Статический анализ Классификация вредоносных программ с использованием YARA	6	4			Отчет по практическому занятию №6
Модуль 1	Ср	Тема 4 Статический анализ Структура стекового кадра в данном случае. Спецификаторы формата. Семейство функций для работы с форматными строками. Чтение содержимого памяти при помощи форматных строк. Передача управления при помощи форматных строк.	6	8			
Модуль 1	Лек	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	6	2		-	

		помощью проверки процессов.					
Модуль 1	Пр	Тема 5 Динамический анализ Анализ исполняемого файла вредоносного ПО	6	4			Отчет по практическому занятию №7
Модуль 1	Ср	Тема 5 Динамический анализ Реферат	6	7			
Модуль 1	Лек	Тема 6 Анализ на практике Приложение для генерирования трафика: SuperFunkyChat. Курс анализа с помощью Wireshark. Определение структуры пакета. Парсинг пакета сообщения.	6	2			
Модуль 1	Пр	Тема 6 Анализ на практике Анализ протокола с помощью Python.	6	4			Отчет по практическому занятию №8
Модуль 1	Ср	Тема 6 Анализ на практике	6	7			
Модуль 1	Лек	Тема 7 Обратная разработка приложения Компиляторы, интерпретаторы и ассемблеры. Архитектура x86. Статический и динамический обратный инжиниринг. Обратное проектирование управляемого кода.	6	2			
Модуль 1	Пр	Тема 7 Обратная разработка приложения Декомпилирование приложения.	6	4			Отчет по практическому занятию №9
Модуль 1	Ср	Тема 7 Обратная разработка приложения	6	7			
Модуль 1	Лек	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	6	2			

		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					
Модуль 1	Пр	Тема 8 Защита ИС от вредоносного ПО Внедрение удаленного исполняемого файла или шелл-кода.	6	4			Отчет по практическому занятию №10
Модуль 1	Ср	Тема 8 Защита ИС от вредоносного ПО Понятие дефекта ПО. Определение уязвимостей ПО.Типы уязвимостей. Классификация уязвимостей. Понятие метрики. Система оценки уязвимостей. Понятие взлома ПО. Виды взлома ПО. Защита от взлома ПО. Техника защиты от взлома ПО. Тестирование безопасности ПО.	6	2			
Модуль 1	Ср	Тема 8 Защита ИС от вредоносного ПО Проверка во время исполнения. LibsafePlus и TIED. Алгоритм Jones-Kelley. Применение OOB (out-of-bound) объектов. Рандомизация пространства адресов. ASLR. Статический анализ уязвимости переполнения буфера. Предотвращение TOCTTOU атак. Средства контроля потока исполнения.	6	6,75			
	ПА	Сдача зачета (итоговый тест/сдача зачета устно (письменно)	6	0,25		-	Банк тестовых заданий /Вопросы к зачету

Итого:	**108**			

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.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-11	Протоколы практических заданий №1-10
		Вопросы к зачету №№1-45 Оценка рефератов

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

Реферат Встроенные аппаратные средства защиты от вредоносного ПО
Реферат Средства мониторинга и анализа процессов ПО

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Исследование деструктивных возможностей потенциально опасных программ и команд
2	Исследование возможностей скрытого внедрения и запуска опасных программ
3	Исследование интерпретируемых вредоносных программ (командных файлов, макросов и сценариев)
4	Исследование уязвимости переполнения кучи
5	Исследования уязвимости переполнения стека
6	Классификация вредоносных программ с использованием YARA
7	Анализ исполняемого файла вредоносного ПО
8	Анализ протокола с помощью Python
9	Декомпилирование приложения
10	Внедрение удаленного исполняемого файла или шелл-кода.

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты исследуют деструктивные возможности потенциально опасных программ и команд, внедрения и запуска опасных программ, различного типа уязвимостей, анализируют программными средствами исполняемый файл, писать и внедрять шелл –код.

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:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.2. Типовой пример тестового задания

Типы шелл-кода:

Выберите два из 4 вариантов ответа:
1. Локальный
2. Удаленный
3. Выполняемый
4. Критичный

Критерии оценки:

Минимальное количество баллов 1. 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.	Понятия об информационных и компьютерных преступлениях.
2.	Компьютерная система как средство совершения преступления и хранилище информации о преступной деятельности
3.	Вредоносный программный код документов офисных приложений и его возможности. Методы вирусного копирования
4.	Реализация защиты от вредоносного программного кода в приложениях офисного пакета. Нейтрализация вредоносных макросов с целью их исследования.
5.	Механизмы статического скрытия вредоносного программного кода

6.	Классификация и основные особенности различных видов вредоносных программ
7.	Внедрение и запуск вредоносных программ на этапах самотестирования компьютера и загрузки операционной системы. Способы автоматического запуска вредоносных программ
8.	Виды компьютерных инфекций. Сущность вирусного заражения и жизненный цикл компьютерного вируса
9.	Возможности и особенности сетевых вредоносных программ
10.	Виды нарушений работы ЭВМ со стороны вредоносных программ.
11.	Виды несанкционированного блокирования и модификации компьютерной информации вредоносными программами.
12.	Определение компьютерного червя. Принцип действия. Принцип активации. Принцип распространения. Типы компьютерных червей.
13.	Определение троянской программы. Принцип действия. Принцип активации. Принцип распространения. Типы троянских программ.
14.	Определение вредоносной утилиты. Принцип действия. Принцип активации. Принцип распространения. Типы вредоносных утилит
15.	Каналы проникновение ВПО в операционную систему (на ЭВМ)
16.	Наносимый ущерб ВПО (основной и второстепенный)
17.	Признаки присутствия ВПО в ИС. Виды проявлений
18.	Понятие киберпреступности. Виды киберпреступностей. Перечень компьютерных правонарушений
19.	Понятие и принцип действия Хакинга
20.	Понятие защиты от ВПО. Применение защиты в ИС. Виды средств защиты
21.	Аппаратные средства защита (АСЗ) от ВПО в ИС. Виды аппаратных средств. Построение защиты ИС на основе АСЗ
22.	Программные средства защита (ПСЗ) от ВПО в ИС. Принцип построение защиты ИС на основе ПСЗ
23.	Понятие антивируса. Цели и задачи антивируса. Структура антивируса. Принцип работы. Функционал
24.	Антивирусный комплекс для защиты рабочих станций. Принцип организации антивирусной защиты
25.	Антивирусный комплекс для защиты почтовых систем. Принцип организации антивирусной защиты
26.	Методы обнаружения и устранения вредоносного ПО в Windows-подобных ОС
27.	Методы обнаружения и устранения вредоносного ПО в Linux-подобных ОС
28.	Организационные средства защита (ОСЗ) от ВПО в ИС. Принцип построение защиты ИС на основе организационных средств. Виды ОСЗ
29.	Понятие защиты от ВПО в ПО. Понятие дефекта. Типы дефектов. Причины дефектов. Устранение дефектов
30.	Типы уязвимостей. Источники появления уязвимостей. Устранение уязвимостей
31.	Определение шелл-кода. Типы шелл-кода

32.	Понятие «Кучи». Принцип организации и защиты от переполнения кучи
33.	Понятие «Стэк». Принцип организации и защиты от переполнения стэка
34.	Понятие технических методов защиты ПО. Виды технических методов защиты ПО
35.	Понятие организационных методов защиты ПО. Виды организационных методов защиты ПО
36.	Испытания программных средств на наличие вредоносного ПО (ГОСТ Р 51188)
37.	Статический анализ исходного кода
38.	Динамический анализ исходного кода
39.	Средства анализа трафика
40.	Средства предотвращения утечки информации
41.	Средства мониторинга и анализа процессов
42.	Аттестация программного обеспечения на отсутствие недекларированных возможностей
43.	Сертификационные испытания программных средств
44.	Порядок поиска доказательной информации в памяти ЭВМ
45.	Требования к экспертному заключению

7.3.2. Критерии и нормы оценки

Семестр	**Форма проведения промежуточной аттестации**	**Критерии и нормы оценки**	
6	Зачет (письменно/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	учебное пособие	2022	
2	Форшоу Д.	Атака сетей на уровне протоколов	учебное пособие	2022	

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	Поляков А.М.	Безопасность Oracle глазами аудитора: нападение и защита	учебное пособие	2019	https:// e.lanbook.com/book/ 1121
2	Монаппа К.А.	Анализ вредоносных программ	учебное пособие	2019	

8.3. Перечень профессиональных баз данных и информационных справочных систем

Интернет-портал для ИТ-специалистов - http://www.habrahabr.ru/
Интернет-портал ресурсов по информационной безопасности - http//www.all-ib.ru
Консультант Плюс - http://www.consultant.ru/
Официальный портал правовой информации - http://pravo.gov.ru/
Официальный сайт Федеральной службы по техническому и экспортному контролю - http://www.fstec.ru/
Государственная публичная научно-техническая библиотека. www.gpntb.ru/

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	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.
2	"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	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.

№ 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
	аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф