

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

Б1.В.12
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Аудит защищенности информационных систем
(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: 5 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	7	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	16	16
Лабораторные		
Практические	64	64
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,25	0,25
Контактная работа	80,25	80,25
Самостоятельная работа	99,75	99,75
Контроль	-	-
Итого	180	180

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

Цель освоения дисциплины – изучение основ проведения тестирования на проникновение методом черного ящика, имитируя внешнего и внутреннего нарушителя. Слушатели познакомятся с основным инструментарием, который применяется при проведении тестирования на проникновение, изучат основные виды уязвимостей и способы их эксплуатации.

В курсе рассматриваются следующие темы:

- веб-технологии;
- веб-уязвимости;
- методика проведения тестирования на проникновение;
- активная и пассивная разведка;
- автоматизированное и ручное сканирование сети на наличие уязвимостей;
- устройство домена и уязвимости в протоколах;
- тестирование Wi-Fi сетей;
- защита от проникновения.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Технологии и методы социальной инженерии;
- Компьютерные сети.

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

- Информационная безопасность автоматизированных систем;
- Защита информационных процессов;
- Информационная безопасность компьютерных сетей.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-6 Способен производить оценку эффективности применения программно-аппаратных средств защиты информации, осуществлять мониторинг функционирования программно-аппаратных средств защиты информации	ПК-6.9 Использует методику и проведение комплексного аудита, средства и инструменты анализа защищенности	Знать: - методику и проведение комплексного аудита; - основы программирования; - основы веб-технологий; - протоколы передачи файлов; - виды уязвимостей ИС.
		Уметь: - организовать аудит информационных систем; - разрабатывать политику безопасности; - эксплуатировать уязвимости ИС;
		Владеть: - основами социальной инженерии; - методами обнаружения компьютерных атак;

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		.
	ПК-6.10 Применяет инструменты для пентеста	Знать: - средства и инструменты анализа защищенности
		Уметь: - применять инструменты для пентеста
		Владеть: - методами проведения пентеста
	ПК-6.11 Умеет разрабатывать политику безопасности, эксплуатировать уязвимости, расследовать компьютерные инциденты	Знать: - законодательство РФ - нормативные акты регуляторов
		Уметь: - расследовать компьютерные инциденты - моделировать угрозы
		Владеть: - навыками разработки ОРД
	ПК-6.12 Владеет основами социальной инженерии, методами обнаружения компьютерных атак, инструментарием QSINT	Знать: - основы социальной инженерии
		Уметь: - получать информацию от сетевых сервисов
		Владеть: - инструментарием QSINT

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы
Модуль 1	Лек	Тема 1 Введение в аудит ИБ. Методология аудита. 1. Сущность аудита ИБ 2. Нормативные акты по аудиту 3. Цели и задачи аудита 4. Этапы аудита 5. Как провести аудит законно 6. Внешний и внутренний аудит 7. Методология аудита 8. Документирование результатов аудита 9. Классификация мероприятий аудита. 10. Тестирование как один из основных типов аудита. 11. Тестирование на основе моделей. 12. Тестирование специальными средствами и способами 13. Нормативное обоснование тестирования на проникновение	7	2	
Модуль 1	Пр	Тема 1 Введение в аудит ИБ. Методология аудита. Разработка этапов и мероприятий аудита	7	4	
Модуль 1	Ср	Тема 1 Введение в аудит ИБ. Методология аудита.	7	12	
Модуль 1	Лек	Тема 2 Проведение аудита 1. Анализ защищенности информационных систем с применением технических средств, направленный на выявление потенциальных уязвимостей в инфраструктуре вычислительной сети. 2. Обследование и аудит ключевых бизнес-систем и бизнес-процессов финансово-хозяйственной деятельности. 3. Аудит процессов информационной безопасности. 4. Аудит технической защиты конфиденциальной информации. 5. Аудит соответствия обработки персональных данных требованиям законодательства.	7	2	
Модуль 1	Пр	Тема 2 Проведение аудита Тестирование инфраструктуры на основе моделей. Тестирования реальных систем и их прототипов с использованием специальных средств и способов.	7	4	
Модуль 1	Пр	Тема 2 Проведение аудита Аудит активов и бизнес процессов	7	4	
Модуль 1	Пр	Тема 2 Проведение аудита Моделирование угроз и действий нарушителя	7	4	
Модуль 1	Ср	Тема 2 Проведение аудита	7	12	
Модуль 1	Лек	Тема 3 Экспертная оценка результатов	7	2	

		аудита 1.Экспертная проверка состояния защищенности информации и информационных систем. 2.Оценка соответствия систем и мер информационной безопасности на предмет соответствия стандартам и требованиям законодательства			
Модуль 1 Тема 3 Экспертная оценка результатов аудита	Пр	Тема 3 Экспертная оценка результатов аудита Аудит соответствия обработки персональных данных требованиям законодательства	7	4	
Модуль 1 Тема 3 Экспертная оценка результатов аудита	Пр	Тема 3 Экспертная оценка результатов аудита Оценка защищенности ИС	7	4	
Модуль 1 Тема 3 Экспертная оценка результатов аудита	Ср	Тема 3 Экспертная оценка результатов аудита	7	12	
Модуль 1	Лек	Тема 4 Методология взлома 1. Этапы разведки и проникновения 2.Разведка и сбор информации различными методами. 3. Пассивная, полупассивная разведка. 4. Получение информации от сетевых сервисов 5. Получение информации из открытых и закрытых источников	7	2	
Модуль 1	Пр	Тема 4 Методология взлома Анализ сетевого трафика	7	4	
Модуль 1	Пр	Тема 4 Методология взлома Пассивная разведка ИС организации	7	4	
Модуль 1	Ср	Тема 4 Методология взлома		12	

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы
Модуль 1	Лек	Тема 5 Фазинг директорий веб-сайта. Поиск открытых портов 1. Инструментарий для фазинга директорий веб-приложения. 2. Сканирование сети на наличие открытых портов с помощью nmap. 3.Исследование веб-приложения с помощью Burp Suite.	7	4	
Модуль 1	Пр	Тема 5 Фазинг директорий веб-сайта. Поиск открытых портов Мониторинг активности в сети. Использование инструментария фазинга для проверки открытых портов	7	4	
Модуль 1	Пр	Тема 5 Фазинг директорий веб-сайта. Поиск открытых портов Исследование веб-приложения	7	4	
Модуль 1	Ср	Тема 5 Фазинг директорий веб-сайта. Поиск открытых портов	7	12	
Модуль 1	Лек	Тема 6 Поиск уязвимостей в	7	2	

		приложениях и на хостах сети 1. Изучение различных сканеров по поиску уязвимостей. 2. Банки уязвимостей и угроз 3. Классификация уязвимостей 4. Ручной поиск уязвимостей 5. Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС. Функции, методика использования			
Модуль 1	Пр	Тема 6 Поиск уязвимостей в приложениях и на хостах сети XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС Функции, методика использования	7	4	
Модуль 1	Ср	Тема 6 Поиск уязвимостей в приложениях и на хостах сети	7	12	
Модуль 1	Лек	Тема 7 Эксплуатация уязвимостей. 1. Работа с фреймворком Metasploit. 2. Понятие exploit, CVSS.	7	4	
Модуль 1	Пр	Тема 7 Эксплуатация уязвимостей. Работа с фреймворком Metasploit	7	4	
Модуль 1	Пр	Тема 7 Эксплуатация уязвимостей. Google dork для поиска информации	7	4	
Модуль 1	Ср	Тема 7 Эксплуатация уязвимостей.	7	12	
Модуль 1	Лек	Тема 8 Защита информационных систем от атак и вторжений 1. Политики безопасности, стандарты, процедуры 2. Защита от утечек информации 3. Системы обнаружения вторжений IDS 4. Брэндмауэры 5. Виртуальные защищенные сети	7	4	
Модуль 1	Пр	Тема 8 Защита информационных систем от атак и вторжений Создание VPN из компонентов с открытым исходным кодом	7	4	
Модуль 1	Пр	Тема 8 Защита информационных систем от атак и вторжений Проведение фишинговой атаки	7	4	
Модуль 1	Пр	Тема 8 Защита информационных систем от атак и вторжений Построение IDS и проектирование системы защиты от утечек информации	7	4	
Модуль 1	Ср	Тема 8 Защита информационных систем от атак и вторжений	7	15,75	
	ПА	Сдача зачета	7	0,25	
Итого:				180	

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	Наглядные, словесные, практические.

	домашнее задание.	
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. Подготовка 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
7	ПК-6	Протоколы практических заданий №1-16
		Вопросы к зачету №№1-100
		Банк тестовых заданий №1-350

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

7.2.1. Выполнение практических заданий

№	Тема
1	Разработка этапов и мероприятий аудита
2	Тестирование инфраструктуры на основе моделей. Тестирования реальных систем и их прототипов с использованием специальных средств и способов.
3	Аудит активов и бизнес процессов
4	Моделирование угроз и действий нарушителя
5	Аудит соответствия обработки персональных данных требованиям законодательства
6	Оценка защищенности ИС
7	Анализ сетевого трафика
8	Пассивная разведка ИС организации
9	Мониторинг активности в сети. Использование инструментария фазинга для проверки открытых портов
10	Исследование веб-приложения
11	XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС Функции, методика использования
12	Работа с фреймворком Metasploit
13	Google dork для поиска информации
14	Создание VPN из компонентов с открытым исходным кодом
15	Проведение фишинговой атаки
16	Построение IDS и проектирование системы защиты от утечек информации

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты организуют мероприятия по аудиту бизнес-процессов организации, моделируют угрозы нарушителей, проводят Оценку защищенности ИС, исследуют веб-приложения, учатся имитировать фишинговые атаки для повышения осведомленности пользователей, применяют на практике инструментарий аудитора.

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. Тестирование для дисциплин 1-6 семестров

Типовой пример тестового задания

Информация, необходимая для анализа любого вида производственной деятельности, может включать следующие моменты:

Выберите один из 4 вариантов ответа:

- 1) образование работника
- 2) технологический процесс
- 3) длительность и частота выполнения работ;
- 4) средства коллективной защиты

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 7

№ п/п	Вопросы к зачету
1.	Определение аудита информационной безопасности
2.	Цели и задачи аудита.
3.	Этапы проведения аудита.
4.	Концептуальные основы аудита
5.	Тестирование как один из основных типов аудита
6.	Тестирование на основе моделей
7.	Тестирование специальными средствами и способами
8.	Порядок анализа состояния ИБ объекта аудита
9.	Регистрация, сбор и проверка статистических данных и результатов инструментальных измерений уязвимостей и угроз
10.	Сущность оценки результатов проверки
11.	Критерии нарушения ИБ
12.	Порядок разработки модели угроз
13.	Аудит на основе анализа рисков
14.	Аудит на основе анализа стандартов ИБ
15.	Аудит на основе экспериментальных исследований системы или ее прототипа
16.	Сущность процессного подхода к аудиту
17.	Классификация мероприятий аудита
18.	Основания, по которым могут быть классифицированы мероприятия аудита ИБ объекта
19.	Пассивный аудит

20.	Активный аудит
21.	Внешний аудит
22.	Внутренний аудит
23.	Экспертный аудит
24.	Что такое Оценка соответствия
25.	Что такое аттестация объекта
26.	Сканирование портов, цель, осуществление, инструменты
27.	Атаки на веб-приложения, цель, способы
28.	Виды веб-уязвимостей
29.	Социальная инженерия, цели, задачи
30.	Фишинг
31.	Типы атак
32.	Как осуществляется перехват информации
33.	Системы обнаружения атак
34.	Вредоносные программы, типы, способы внедрения
35.	Metasploit Framework, назначение, применение
36.	Эксплоиты, полезная нагрузка
37.	Атаки, направленные на переполнение буфера
38.	Системы обнаружения вторжения (IDS)
39.	Политики, стандарты аудита защищенности
40.	Брэндмауэры, назначение
41.	Этапы разведки и проникновения
42.	Разведка и сбор информации различными методами.
43.	Пассивная, полупассивная разведка.
44.	Получение информации от сетевых сервисов
45.	Получение информации из открытых и закрытых источников
46.	Как провести аудит законно?
47.	Этапы взлома системы
48.	Получение информации из открытых источников
49.	Получение информации о домене
50.	Определение активных хостов
51.	Получение информации от DNS-сервера
52.	Поиск уязвимостей
53.	Атаки на веб-приложения, SQL - инъекции, XSS
54.	Методы социальной инженерии
55.	Сущность фишинга
56.	Методы защиты от фишинга
57.	Social-Engineer Toolkit
58.	Перехват информации в беспроводных сетях
59.	Методы защиты информации в беспроводных сетях
60.	Пассивный перехват трафика
61.	Активный перехват трафика
62.	Инструменты перехвата трафика и их использование
63.	Системы обнаружения атак
64.	Вредоносные программы
65.	Методы распространения вредоносных программ
66.	Методика выявления вредоносных программ
67.	Использование Metasploit Framework
68.	Протоколы передачи файлов их отличие в использовании
69.	Перенаправление портов, туннелированные

70.	Атаки, направленные на переполнение буфера
71.	Стандарт выполнения тестов на проникновение
72.	Компоненты виртуальной частной сети
73.	Защита виртуальных сетей
74.	Системы обнаружения вторжений, компоненты SOV
75.	Защита от утечек информации
76.	Политики безопасности, стандарты, процедуры
77.	Google dork, способы применения
78.	Методы обнаружения активности в сети
79.	Регистрация и анализ инцидентов
80.	Сущность процессного подхода
81.	Сущность теоретического подхода
82.	Мероприятия аудита
83.	Классификация мероприятий аудита
84.	Сущность и содержание внутреннего аудита
85.	Сущность экспертного аудита
86.	Тестирование как один из основных типов аудита
87.	Виды тестирований и их сущность
88.	Тестирование на основе моделей
89.	Тестирование специальными средствами и способами
90.	Базовые понятия социальной инженерии
91.	Системно-функциональный подход к моделированию
92.	Порядок обследования процессов ИБ
93.	Порядок обследования информационной инфраструктуры
94.	Порядок обследования подсистем защиты информации
95.	Порядок составления отчетности по результатам аудита
96.	Порядок организации проведения пентеста
97.	Цели и задачи пентеста. Bug bounty.
98.	Методика определения вероятности проведения атаки, а также уровней ущерба
99.	Что включает в себя регламент обследования ИС?
100.	Перечень ОРД, проверяемой при аудите

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
7	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	Н.В. Скабцов	Аудит безопасности информационных систем	учебно-методическое пособие	СПб.: Питер, 2020	
2	С.А. Петренко	Аудит безопасности	учебно-методическое пособие	Академия АиТи: ДМК Пресс, 2022	
3	Алешкин А. С., Лесько С. А., Жуков Д. О.	Аппаратные и программные средства поиска уязвимостей	Учебное пособие	2020	https://e.lanbook.com/book/167600?category=1545

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	А. И. Бирюков	Информационная безопасность: защита и нападение 2-е изд.)	учебно-методическое пособие	2019	
2	А.А. Лихоносов , Д.А.	Основы аудита информационной	учебно-	Москва:	

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
	Денисов	безопасности	методическое пособие	МФПА, 2019	

8.3. Перечень профессиональных баз данных и информационных справочных систем

- Securitylab.ru Адрес ресурса: <https://www.securitylab.ru>
- Информационная безопасность. Защита информации Адрес ресурса: <http://all-ib.ru/>
- Ассоциация по вопросам защиты информации BISA Адрес ресурса: <http://bis-expert.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