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

ФТД.01
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Этичный хакинг
(наименование дисциплины)

по направлению подготовки
09.04.03 Прикладная информатика

направленность (профиль)
Информационные системы и технологии корпоративного управления

Форма обучения: Очная

Год набора: 2019

Общая трудоемкость: 2ЗЕ

Распределение часов дисциплины по семестрам

Семестр	2	**Итого**
Форма контроля / **Вид занятий**	Зачет	
Лекции	8	8
Лабораторные		
Практические	8	8
Руководство: курсовые работы (проекты) / РГР		
Промежуточная аттестация	0,25	0,25
Контактная работа	16,25	16,25
Самостоятельная работа	55,75	55,75
Контроль	0	0
Итого	72	72

Рабочую программу составил: профессор, доцент, д.техн.наук, Мкртычев С.В.

(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

09.04.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31 августа 2021г.

УТВЕРЖДЕНО

На заседании кафедры

Прикладная математика и информатика

(протокол заседания № 1 от «30» 08 2018 г.).

1. Цель освоения дисциплины

Цель освоения дисциплины – формирование у студентов теоретических знаний и практических навыков выявления и устранения проблем безопасности в компьютерных сетях.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: Корпоративные информационные системы.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: Методологии создания и внедрения корпоративных информационных систем.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-1 - Способен управлять ИТ-проектами: взаимодействовать с заказчиками ИТ-проектов, организовывать и оптимизировать проектную деятельность	ПК-1.1 Знает основные принципы и методы управления ИТ-проектами, организации и оптимизации проектной деятельности; имеет представление о правилах ведения деловых переговоров ПК-1.2 Умеет управлять ИТ-проектами, инновациями, инвестициями, проводить анализ данных при управлении ИТ-проектами, проводить деловые переговоры ПК-1.3 Имеет навыки управления ИТ-проектами, организации и оптимизации проектной деятельности, проведения деловых переговоров.	Знать: основные принципы и методы управления ИТ-проектами, организации и оптимизации проектной деятельности по управлению информационными процессами
		Уметь: управлять ИТ-проектами, организации и оптимизации проектной деятельности по управлению информационными процессами
		Владеть: навыками управления ИТ-проектами, организации и оптимизации проектной деятельности по управлению информационными процессами
ПК-6 Способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления	ПК-6.1Знает методы научных исследований и инструментарий в области проектирования и управления информационными системами в прикладных	Знать: методы выявления и устранения проблем безопасности в компьютерных сетях
		Уметь: использовать методы выявления и устранения проблем безопасности в компьютерных сетях

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
информационными системами в прикладных областях	областях ПК-6.2 Умеет использовать методы научных исследований и инструментарий в области проектирования и управления информационными системами в прикладных областях ПК-6.3 Владеет навыками применения методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях	Владеть: практическими навыками выявления и устранения проблем безопасности в компьютерных сетях

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. Методы выявления проблем безопасности в компьютерных сетях	Лек	Тема 1. Этапы хакинга и типы хакерских атак. Компьютерные вирусы	2	2	-	-	
	Лек	Тема 2. Методологии и технологии сканирования уязвимостей компьютерных сетей	2	2	-	-	
	Пр	1 Программные средства для анализа защищенности ОС Windows 2. Сканирование уязвимости сетевого	2	4	-	-	Отчеты по практическим работам №1,2
	Ср	Темы модуля 1	2	27,75	-	-	
Модуль 2. Методы устранения проблем безопасности в компьютерных сетях	Лек	Тема 3. Методы защиты компьютерной сети от хакерских атак	2	2	-	-	
	Лек	Тема 4. Методы защиты компьютерной сети от вирусов	2	2	-	-	
	Пр	3. Программно-аппаратные методы защиты от удаленных атак 4. Установка, настройка и использование антивирусной программы	2	4	-	-	Отчеты по практическим работам №3,4
	Ср	Темы модуля 2	2	28	-		
	ПА		2	0,25	--	-	
Итого:				**72**			

5. Образовательные технологии

В рамках учебного курса предусмотрены следующие образовательные технологии:

– технология традиционного обучения: лекции и практические работы, самостоятельная работа;

– технология проектного обучения: реализация и защита отчетов по практическим работам.

6. Методические указания по освоению дисциплины

6.1. Рекомендации по подготовке к лекционным занятиям

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет.

В ходе лекционных следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсовых и выпускных квалификационных работ.

6.2. Рекомендации по подготовке к практическим занятиям

Студентам следует доводить каждую практическую работу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по рассмотренному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться студентом на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

По результатам выполнения работы составляется отчет, который при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что выполнение каждой работы должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

6.3. Рекомендации по подготовке к зачету

Подготовка к зачету способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к зачету, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На зачете студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
2	ПК-1	Отчеты по практическим работам №1,2
2	ПК-6	Отчеты по практическим работам №3,4

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

7.2.1. Отчеты по практическим работам
(наименование оценочного средства)

Типовые примеры заданий

Практическая работа 1. Программные средства для анализа защищенности ОС Windows.

Форма отчета по практической работе № 1. В отчет по практической работе должны быть включены следующие пункты:

- титульный лист;
- цель работы;
- краткие теоретические сведения;
- описание хода выполнения работы;
- результаты выполненной работы;
- ответы на контрольные вопросы.

Практическая работа 2. Сканирование уязвимости сетевого сервера.

Форма отчета по практической работе № 3. В отчет по практической работе должны быть включены следующие пункты:

- титульный лист;
- цель работы;
- краткие теоретические сведения;
- описание хода выполнения работы;
- результаты выполненной работы.

Критерии оценки за отчеты по практическим работам по модулю**:**

- отметка «зачтено» ставится студенту, который продемонстрировал результаты выполнения практической работы, соответствующие поставленным задачам, и ответил на контрольные вопросы;
- отметка «не зачтено» ставится студенту, который не продемонстрировал результаты выполнения практической работы и не ответил на контрольные вопросы.

Темы письменных работ

Учебным планом не предусмотрено.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр_____2_____

№ п/п	Вопросы к зачету
1.	Обзор концепций информационной безопасности
2.	Угрозы информационной безопасности и векторы атак
3.	Понятия хакинга
4.	Этапы хакинга
5.	Типы атак
6.	Управление обеспечением информационной безопасности (ИБ) предприятия
7.	Модель угроз ИБ
8.	Политики, процедуры и процессы обеспечения ИБ
9.	Методы оценки защищенности - аудит, анализ уязвимостей и тестирование на проникновение
10.	Планирование и проведение тестирования на проникновение
11.	Угрозы утечки информации об информационной системе организации
12.	Методологии сбора информации из открытых источников
13.	Средства сбора информации
14.	Меры противодействия утечкам информации
15.	Тестирование на предмет получения информации об информационной системе организации
16.	Обзор возможностей сканирования сети
17.	Методология сканирования
18.	Техники обнаружения открытых портов
19.	Техника скрытого сканирования
20.	Техники уклонения от систем обнаружения вторжений
21.	Анализ баннеров
22.	Сканирование уязвимостей
23.	Подготовка прокси-сервера
24.	Техники туннелирования
25.	Анонимайзеры
26.	Спуфинг IP адреса и меры противодействия
27.	Сканирование сети как этап тестирования на проникновение
28.	Мониторинг TCP/IP соединения
29.	Концепции инвентаризации
30.	Инвентаризация SMTP
31.	Инвентаризация DNS
32.	Меры противодействия инвентаризации
33.	Инвентаризации ресурсов как этап тестирования на проникновение
34.	Получение доступа на основе стандартных паролей
35.	Цели взлома системы

36.	Методология взлома системы
37.	Последовательность хакинга системы
38.	Взлом паролей
39.	Повышение привилегий
40.	Выполнение приложений
41.	Сокрытие файлов
42.	Сокрытие следов
43.	Тестирование на предмет взлома системы
44.	Классификация вредоносного ПО -трояны, вирусы и черви
45.	Пути проникновения вредоносного ПО
46.	Методы и средства анализа вредоносного ПО
47.	Методы обнаружения вредоносного ПО
48.	Антивирусные программы
49.	Угрозы веб-приложениям

7.3.2. Критерии и нормы оценки

Семестр	**Форма проведения промежуточной аттестации**	**Критерии и нормы оценки**	
2	Зачет (устно)	«зачтено»	Выставляется студенту, проявившему знания по дисциплине, усвоившему литературу, рекомендуемую программой и показавшему систематический характер знаний. В изложении материала и ответах на дополнительные вопросы допускаются небольшие неточности.
		«не зачтено»	выставляется студенту, который обнаружил пробелы в знаниях по дисциплине. При ответе студент допустил принципиальные ошибки (вопросы не раскрыты). На дополнительные вопросы ответы даны не были или содержали серьезные ошибки.

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	Никифоров С. Н.	Защита информации. Защита от внешних вторжений	учеб. пособие	2017	ЭБС "IPRbooks"
2	Петренко С. А.	Политики безопасности компании при работе в Интернет	учеб. пособие	2017	ЭБС "IPRbooks"

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	Мэйволд Э.	Безопасность сетей	учеб. курс	2016	ЭБС "IPRbooks"
2	Джонс К. Д..	Инструментальные средства обеспечения безопасности	курс лекций	2016	ЭБС "IPRbooks"

8.3. Перечень профессиональных баз данных и информационных справочных систем

– Web of Science[Электронный ресурс] : мультидисциплинарная реферативная база данных. – Philadelphia: ClarivateAnalitics, 2016– . – Режим доступа : apps.webofknowledge.com. – Загл. с экрана. – Яз. рус., англ.

Scopus [Электронный ресурс] : реферативная база данных. – Netherlands: Elsevier, 2004– . – Режим доступа : scopus.com. – Загл. С экрана. – Яз. рус., англ.

Elibrary [Электронный ресурс] : научная электронная библиотека. – Москва : НЭБ, 2000– . – Режим доступа : elibrary.ru. – Загл. с экрана. – Яз. рус., англ.

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	2013г., № 00179-40183-81808-AAOEM, бессрочный
2	Microsoft Office 13	№61935138 от 28.05.2012 (бессрочный)

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
	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. 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. (УЛК-408)	Компьютер (монитор 17”, системный блок Intel (R) Celeron (R) 2,66 GHz / 1 Gb / 80 Gb), маршрутиза-тор 2801 Router, коммутатор Catalyst, экран/интерактивная доска Smart Board TB, проектор Acer P1303W., стол преподавательский, стол ученический, стол компьютерный, стул, доска аудиторная (маркерная).
	Компьютерный класс. Помещение для самостоятельной работы. 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 (Г-401)	Столы ученические, стулья ученические, ПК с выходом в сеть Интернет