

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

ФТД.01
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Этичный хакинг

(наименование дисциплины)

по направлению подготовки (специальности)

09.04.03 Прикладная информатика

(код и наименование направления подготовки, специальности в соответствии с ФГОС ВПО/ ФГОС ВО)

Информационные системы и технологии корпоративного управления

(направленность (профиль)/специализация)

Форма обучения: заочная

Год набора: 2019

Распределение часов дисциплины по семестрам и видам занятий (по учебному плану)

Количество ЗЕТ	2								
Часов по РУП	72								
Виды контроля в семестрах (на курсах):	Экзамены		Зачеты			Курсовые проекты		Курсовые работы	Контрольные работы (для заочной формы обучения)
			2						
	№№ курса								
	1	2	3	4	5	6	Итого		
ЗЕТ по семестрам		2				2			
Лекции		8				8			
Лабораторные									
Практические		8				8			
ПА		0,25				0,25			
Контактная работа		16,25				16,25			
Сам. работа		52				52			
Контроль		3,75				3,75			
Итого		72				72			

Тольятти, 2019

Рабочая программа составлена на основании ФГОС ВО и учебного плана направления подготовки 09.04.03 Прикладная информатика
(код и наименование направления подготовки, специальности в соответствии с с ФГОС ВПО/ ФГОС ВО)

Рецензирование рабочей программы дисциплины:



Отсутствует



Учебная (рабочая) программа одобрена на заседании кафедры «Прикладная математика и информатика» (протокол заседания № 6 от «13» февраля 2019 г.).



Рецензент

(должность, ученое звание, степень)

« » 20 г.

(подпись)

(И.О. Фамилия)

Срок действия рабочей программы дисциплины до « 25 » мая 2022 г.

Информация об актуализации рабочей программы дисциплины:

Протокол заседания кафедры № 1 от «09» сентября 2019 г.

Протокол заседания кафедры № 1 от « 28 » августа 2020 г.

Протокол заседания кафедры № от « » 20 г.

Протокол заседания кафедры № от « » 20 г.

УТВЕРЖДАЮ

Заведующий кафедрой

Прикладная математика и информатика
(разработавшей РПД)

« » 20 г.

(подпись)

А.В. Очеповский
(И.О. Фамилия)

)

АННОТАЦИЯ

дисциплины (учебного курса)

ФТД.01 Этичный хакинг

(индекс и наименование дисциплины (учебного курса))

1. Цель и задачи изучения дисциплины (учебного курса)

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

Задачи:

1. Сформировать знания о методах выявления и устранения проблем безопасности в компьютерных сетях.
2. Сформировать знания о типичных уязвимостях сетевых протоколов, операционных систем и приложений.
3. Обучить практическим навыкам выявления и устранения проблем безопасности в компьютерных сетях.

2. Место дисциплины (учебного курса) в структуре ОПОП ВО

Данная дисциплина (учебный курс) относится к Блоку ФТД «Факультативы» (вариативная часть).

Дисциплины, учебные курсы, на освоении которых базируется данная дисциплина (учебный курс):

- Корпоративные информационные системы.

Дисциплины, учебные курсы, для которых необходимы знания, умения, навыки, приобретаемые в результате изучения данной дисциплины (учебного курса):

- Методологии создания и внедрения корпоративных информационных систем.

3. Планируемые результаты обучения по дисциплине (учебному курсу), соотнесенные с планируемыми результатами освоения образовательной программы

Формируемые и контролируемые компетенции	Планируемые результаты обучения
ПК-1 Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	Знать: современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
	Уметь: применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
	Владеть: практическими навыками применения современных методов и инструментальных средств прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
ПК-6 Способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях	Знать: методы выявления и устранения проблем безопасности в компьютерных сетях
	Уметь: использовать методы выявления и устранения проблем безопасности в компьютерных сетях
	Владеть: практическими навыками выявления и устранения проблем безопасности в компьютерных сетях

Тематическое содержание дисциплины (учебного курса)

Раздел, модуль	Подраздел, тема
Модуль 1. Методы выявления проблем безопасности в компьютерных сетях	Тема 1.1 Этапы хакинга и типы хакерских атак. Компьютерные вирусы
	Тема 1.2 Методологии и технологии сканирования уязвимостей компьютерных сетей
Модуль 2. Методы устранения проблем безопасности в компьютерных сетях	Тема 2.1 Методы защиты компьютерной сети от хакерских атак
	Тема 2.2 Методы защиты компьютерной сети от вирусов

Общая трудоемкость дисциплины (учебного курса) – 2 ЗЕТ

Разработчик программы:

Профессор, д.т.н., доцент
(должность, степень, ученое звание)

(подпись)

С.В. Мкртычев
(И.О. Фамилия)

4. Структура и содержание дисциплины (учебного курса) Этичный хакинг

(наименование дисциплины (учебного курса))

Курс изучения 2

Раздел, модуль	Подраздел, тема	Виды учебной работы						Необходимые материально- технические ресурсы	Текущий кон- троль		Реко- мендуе- мая ли- терату- ра (№)	
		Аудиторные занятия (в часах)					Самостоятельная работа					
		всего			в т.ч. в интерактив- ной форме	Формы проведения лекций, лабораторных, практических занятий, методы обучения, реал- изующие применяе- мую образовательную технологию	в часах		формы организации самостоятельной работы			
		лекций	лабораторных	практических								
Модуль 1. Методы выявления проблем безопасности в компьютерных сетях	1.1 Этапы ха- кинга и типы хакерских атак. Компьютерные вирусы	2				Лекции электронного учебника с консульта- цией преподавателя на фо- руме	5	Самостоятельное изу- чение материалов электронного учебни- ка с разделением на лекции и с тестами для самоконтроля по каж- дой лекции, анализ поведения обучаю- щихся при помощи LRS-системы и Experience API, анализ текущей успеваемости при помощи БРС- рейтинга	LMS-система на основе Moodle, компьютер либо планшет либо смартфон	Проме- жуточ- ный тест	12	1,2
	1.2 Методоло- гии и техноло- гии сканирова- ния уязвимо- стей компью- терных сетей	2				Лекции электронного учебника с консульта- цией преподавателя на фо- руме	5	Самостоятельное изу- чение материалов электронного учебни- ка с разделением на лекции и с тестами для самоконтроля по каж- дой лекции, анализ	LMS-система на основе Moodle, компьютер либо планшет либо смартфон	Проме- жуточ- ный тест	13	1,2

								поведения обучающихся при помощи LRS-системы и Experience API, анализ текущей успеваемости при помощи БРС-рейтинга				
				4		Выполнение практических заданий с консультацией преподавателя на форуме и через комментарии в заданиях	13	Самостоятельное выполнение практических заданий, контроль смены IP-адресов, анализ текущей успеваемости при помощи БРС-рейтинга	LMS-система на основе Moodle, компьютер либо планшет либо смартфон	Отчет по заданию 1	5	1,2
Модуль 2. Методы устранения проблем безопасности в компьютерных сетях	2.1 Методы защиты компьютерной сети от хакерских атак	2				Лекции электронного учебника с консультацией преподавателя на форуме	5	Самостоятельное изучение материалов электронного учебника с разделением на лекции и с тестами для самоконтроля по каждой лекции, анализ поведения обучающихся при помощи LRS-системы и Experience API, анализ текущей успеваемости при помощи БРС-рейтинга	LMS-система на основе Moodle, компьютер либо планшет либо смартфон	Промежуточный тест	12	1,2
	2. 2 Методы защиты компьютерной сети от вирусов	2				Лекции электронного учебника с консультацией преподавателя на форуме	10	Самостоятельное изучение материалов электронного учебника с разделением на лекции и с тестами для самоконтроля по каждой лекции, анализ поведения обучающихся при помощи LRS-системы и Experience API, анализ текущей успеваемости	LMS-система на основе Moodle, компьютер либо планшет либо смартфон	Промежуточный тест	13	1,2

								при помощи БРС-рейтинга					
				4		Выполнение практических заданий с консультацией преподавателя на форуме и через комментарии в заданиях	14	Самостоятельное изучение материалов электронного учебника с разделением на лекции и с тестами для самоконтроля по каждой лекции, анализ поведения обучающихся при помощи LRS-системы и Experience API, анализ текущей успеваемости при помощи БРС-рейтинга	LMS-система на основе Moodle, компьютер либо планшет либо смартфон	Отчет по заданию 2	5	1,2	
Контроль							3,75	Самостоятельное изучение материалов электронного учебника с разделением на лекции и с тестами для самоконтроля по каждой лекции, анализ поведения обучающихся при помощи LRS-системы и Experience API, анализ текущей успеваемости при помощи БРС-рейтинга	LMS-система на основе Moodle, компьютер либо планшет либо смартфон	Итоговый тест	40	1,2	
ПА							0,25						
Итого:		8		8			56						
		72											

5. Критерии и нормы текущего контроля и промежуточной аттестации

Формы текущего контроля	Условия допуска	Критерии и нормы оценки
Промежуточный тест	Допускаются все	Максимальное количество баллов – 13 б. (баллы студенту начисляются автоматически пропорционально выполненным тестовым заданиям)
Отчет по заданиям 1,2	Допускаются все	5 баллов – задание выполнено в полном объеме без замечаний 4 балла – задание выполнено в полном объеме, присутствует 1 замечание по выполнению задания 3 балла – задание выполнено в полном объеме, присутствуют 2 замечания по выполнению задания 2 балла – задание выполнено не в полном объеме, присутствует 1 замечание по выполнению задания 1 балла – задание выполнено не в полном объеме, присутствуют 2 замечания по выполнению задания 0 баллов – задание не выполнено
Итоговое тестирование	Допускаются все	Максимальное количество баллов - 40 б. (баллы студенту начисляются автоматически пропорционально выполненным тестовым заданиям)
Итого		Максимальное количество баллов – 100 б.

Форма проведения промежуточной аттестации	Условия допуска	Критерии и нормы оценки	
Зачёт (по накопительному рейтингу)	Допускаются все	«зачтено»	Студент набрал от 40 до 100 баллов по накопительному рейтингу
		«не зачтено»	Студент набрал 39 и менее баллов по накопительному рейтингу

6. Критерии и нормы оценки курсовых работ (проектов)

Учебным планом не предусмотрено.

7. Примерная тематика курсовых работ

Учебным планом не предусмотрено.

8. Вопросы к зачету

№ п/п	Вопросы
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.	Соккрытие файлов
42.	Соккрытие 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
50.	Методология атаки на веб-приложения
51.	Инструменты взлома веб-приложений
52.	Меры противодействия взлому веб-приложений
53.	Инструменты защиты веб-приложений
54.	Основы хакинга мобильных платформ
55.	Инструменты и рекомендации по защите мобильных устройств

9. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

9.1. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Модули 1,2 по курсу «Этичный хакинг»	ПК-1, ПК-6	Промежуточные тесты по модулям 1,2
			Отчеты по заданиям 1,2

9.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

9.2.1. Фонд тестовых заданий (примеры)

Модуль 1. Методы выявления проблем безопасности в компьютерных сетях.

1. Чем может быть вызван отказ в обслуживании на веб-сервере?

- Специально подготовленными HTTP запросами
- Специально подготовленными SMB запросами ИТ-консультант

- Большим количеством обычных HTTP запросов
- Ошибкой пользователя в URL сайта

2. Наиболее часто используемые методы, охватывающие больший спектр вредоносных программ – это...

- ☐ сканирование
- ☐ эвристический анализ
- ☐ обнаружение изменений
- ☐ проверка протоколов

3. Какие бывают виды сканирования?

- ☐ Сканирование IP адресов
- ☐ Сканирование портов
- ☐ Сканирование на наличие уязвимостей
- ☐ Сканирование на проникновение

Модуль 2. Методы устранения проблем безопасности в компьютерных сетях.

4. Назовите метод защиты от компьютерных вирусов:

- отключение компьютера от электросети при малейшем подозрении на вирус
- перезагрузка компьютера
- вызов специалиста по борьбе с вирусами
- установка на компьютер антивирусной программы

5. К антивирусным программам относится

- Avast
- Word
- CorelDraw
- WinRAR

6. IP-спуфинг-это...

- вид атаки, когда злоумышленник выдаёт себя за санкционированного пользователя
- сетевой протокол
- компьютерный вирус
- защита от хакеров

Критерии оценки за пройденный тест по теме:

Максимальное количество баллов – 13 б. (баллы студенту начисляются автоматически пропорционально выполненным тестовым заданиям).

9.2.2. Комплект отчетов по заданиям, проверяемым вручную (примеры)

Задание 1. Программные средства для анализа защищенности ОС Windows.

Форма отчета по заданию 1. В отчет должны быть включены следующие пункты:

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

- результаты выполненной работы;
- ответы на контрольные вопросы.

Задание 2. Современные антивирусные программы.

Форма отчета по заданию 2. В отчет следующие пункты:

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

Критерии оценки за отчеты по заданиям, проверяемым вручную:

Формы текущего контроля	Критерии и нормы оценки
Отчет по заданиям 1,2	5 баллов – задание выполнено в полном объеме без замечаний 4 балла – задание выполнено в полном объеме, присутствует 1 замечание по выполнению задания 3 балла – задание выполнено в полном объеме, присутствуют 2 замечания по выполнению задания 2 балла – задание выполнено не в полном объеме, присутствует 1 замечание по выполнению задания 1 балла – задание выполнено не в полном объеме, присутствуют 2 замечания по выполнению задания 0 баллов – задание не выполнено

10. Образовательные технологии и методические указания по освоению дисциплины (учебного курса)

При изучении дисциплины (учебного курса) используются дистанционные образовательные технологии.

10.1. Рекомендации по подготовке к тестированию по темам курса

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов.

При самостоятельной подготовке к тестированию студенту необходимо:

а) готовясь к тестированию, проработайте информационный материал по дисциплине. Проконсультируйтесь с преподавателем по вопросу выбора учебной литературы;

б) четко выясните все условия тестирования заранее. Вы должны знать, сколько тестов Вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.;

в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;

г) в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

д) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.

е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

Тестирование - позволяет оценить знание фактического материала, умение логически мыслить, способность к рефлексии и творчески подходить к решению поставленной задачи.

10.2. Рекомендации по выполнению практических заданий

Основные задачи выполняемой работы:

- 1) закрепление полученных ранее теоретических знаний;
- 2) выработка навыков самостоятельной работы;
- 3) выяснение подготовленности студента к будущей практической работе;

Весь процесс написания работы можно условно разделить на следующие этапы:

- а) выбор темы и составление предварительного плана работы;
- б) сбор научной информации, изучение литературы;
- в) анализ составных частей проблемы, изложение темы;
- г) обработка материала в целом.

Подготовку выполнения работы следует начинать с повторения соответствующего раздела учебника, учебных пособий по данной теме. Приступать к выполнению работы без изучения основных положений и понятий науки, не следует, так как в этом случае студент, как правило, плохо ориентируется в материале, не может отграничить смежные вопросы и сосредоточить внимание на основных, первостепенных проблемах рассматриваемой темы.

11. Учебно-методическое и информационное обеспечение дисциплины (учебного курса)

11.1. Обязательная литература

№ п/п	Библиографическое описание	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, аудио-, видео-пособия и др.)	Количество в библиотеке
1.	Никифоров С. Н. Защита информации. Защита от внешних вторжений [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Санкт-Петербург : СПбГАСУ, 2017. - 83 с. : ил. - ISBN 978-5-9227-0757-2.	Учебное пособие	ЭБС "IPRbooks"
2.	Петренко С. А. Политики безопасности компании при работе в Интернет [Электронный ресурс] : [учеб. пособие] / С. А. Петренко, В. А. Курбатов. - Саратов : Профобразование, 2017. - 400 с. : ил. - ISBN 978-5-4488-0082-5.	Учебное пособие	ЭБС "IPRbooks"

11.2. Дополнительная литература и учебные материалы (аудио-, видеопособия и др.)

№ п/п	Библиографическое описание	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, аудио-, видеопособия и др.)	Количество в библиотеке
1.	Мэйволд Э. Безопасность сетей [Электронный ресурс] : [учеб. курс] / Э. Мэйволд. - 2-е изд., испр. - Москва : ИНТУИТ, 2016. - 572 с. : ил. - (Шаг за шагом). - ISBN 5-9570-0046-9.	Учебный курс	ЭБС "IPRbooks"
2.	Джонс К. Д. Инструментальные средства обеспечения безопасности [Электронный ресурс] : [курс лекций] / К. Д. Джонс, М. Шема, Б. С. Джонсон. - 2-е изд., испр. - Москва : ИНТУИТ, 2016. - 915 с. : ил.	Курс лекций	ЭБС "IPRbooks"

СОГЛАСОВАНО

Директор научной библиотеки _____
(подпись)

А.М. Асаева
(И.О. Фамилия)

«__» _____ 201_ г.

МП

11.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

- Антивирусная защита компьютерных систем [Электронный ресурс]. – Режим доступа <https://www.intuit.ru/studies/courses/2259/155/info>
- Хакер этичный – хакерство на благо [Электронный ресурс]. – Режим доступа <http://inetrab.ru/poisk-raboty/interesnaya-professiya/xaker-etichnyj-xakerstvo-na-bлаго>
- Методология объектно-ориентированного анализа и проектирования [
- Информационная безопасность [Электронный ресурс]. – Режим доступа <http://www.itsec.ru/main.php>

11.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Количество лицензий	Реквизиты договора (дата, номер, срок действия)
1.	Windows	1398	Бессрочная
2.	Office Standard	1398	Бессрочная

11.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

№ п/п	Наименование оборудованных учебных каби- нетов, лабора- торий, мастер- ских и др. объ- ектов для про- ведения прак- тических и ла- бораторных за- нятий	Перечень основно- го оборудования	Фактический ад- рес учебных ка- бинетов, лабора- торий, мастер- ских и др.	Площадь, м ²	Количество посадочных мест
----------	---	--------------------------------------	--	-------------------------	-------------------------------

1.	<p>Аудитория веб-конференций.</p> <p>Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.</p>	<p>Экран телевизионный, ширмы, проектор на штативе. стол преподавательский, стулья преподавательские., Транспарант-перетяжка, системный блок .</p>	<p>445020, Самарская обл., г. Тольятти, ул. Белорусская, 16В, УЛК-807</p>	17,1	1
----	---	--	---	------	---