МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

СОГЛАСОВАНО
Руководитель ОП

Р.И. Дремлюга

«17» июня .2019 г.

УТВЕРЖДАЮ
Директор Школы цифровой экономики

_____ И.Г. Мирин

«17» _____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ТЕСТИРОВАНИЕ УЯЗВИМОСТЕЙ ЗАЩИЩЕННЫХ СИСТЕМ»
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

курс 2 семестр 3
лекции 18 час.
практические занятия 18 час.
лабораторные работы 0 час.
всего часов аудиторной нагрузки 36 час.
самостоятельная работа 18 час.
контрольные работы программой не предусмотрены
курсовая работа/проект – не предусмотрено
зачет не предусмотрено учебным планом
экзамен – 3 семестр

Рабочая программа составлена в соответствии составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 918.

Рассмотрена и утверждена на заседании Дирекции Школы цифровой экономики «17» июня 2019 года (протокол № 124-01-07-05).

Составитель: С.С. Зотов

Оборотная сторона титульного листа РПД

•

I. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

АННОТАЦИЯ
Б1.В.01.02 ТЕСТИРОВАНИЕ УЯЗВИМОСТЕЙ ЗАЩИЩЕННЫХ СИСТЕМ

Рабочая программа учебной дисциплины «Тестирование уязвимостей защищенных систем» предназначена для студентов, обучающихся по направлению подготовки 09.04.01 Информатика и вычислительная техника (уровень магистратуры), профиль «Кибербезопасность».

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Дисциплина реализуется на 2 курсе в 3 семестре.

Семестр	Аудиторные занятия			Самостоя-тельная работа	Форма Контроля	Всего по дисциплине	
	Лекции	Лабораторные работы	Всего			Часы	Зачетные единицы
3 семестр	18	-	36	18	Экзамен	108	3
Всего	**18**	**-**	**36**	**18**		**108**	**3**

Изучение дисциплины «Тестирование уязвимостей защищенных систем» базируется на следующих дисциплинах бакалавриата: «Информатика», «Экономика», «Высшая математика».

Цель: формирование у студентов совокупности знаний и представлений о том, что такое безопасность информационной системы, какие существуют возможности компрометации системы, какие существуют методы нарушения безопасности системы и каким образом проверять ее на защищенность.

Задачи:

1. Формирование знаний, умений и навыков в области создания защищенной информационной системы;
2. Изучение рисков безопасности информационной системы;
3. Изучение методов нарушения безопасности информационной системы;

4. Изучение методов тестирования безопасности информационной системы.

В результате данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**
ПК-1 Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-1.1 Знает: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; нормативно-правовые акты; национальные и международные стандарты в области защиты информации ПК-1.2 Умеет: определять параметры функционирования программно-аппаратных средств защиты информации; разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации; анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия ПК-1.3 Владеет: методами и средствами оценки корректности и эффективности программных реализаций алгоритмов защиты информации; методами оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации; методами анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей
ПК-5 Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-5.1 Знает: форматы хранения информации в анализируемой компьютерной системе; особенности хранения конфигурационной и системной информации в компьютерных системах; уязвимости компьютерных систем и сетей; порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; нормы уголовного и административного права в сфере компьютерной информации; характеристики правонарушений в области связи и информации; виды преступлений в сфере компьютерной информации; порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с

	учетом нормативных правовых актов ПК-5.2 Умеет: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; выявлять возможные траектории состояний функционирования системы и несоответствия имеющейся информации ее расположению в системе ПК-5.3 Владеет: технологиями поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; навыками прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов; способами обнаружения и нейтрализации последствий вторжений в компьютерные системы; методами анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов; методами анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении
ПК-6 Способен разрабатывать и тестировать средств защиты информации компьютерных систем и сетей	ПК-6.1 Знает: принципы проектирования антивирусного программного обеспечения; виды атак и механизмы их реализации в компьютерных системах; принципы построения систем защиты информации компьютерных систем; методологии и технологии разработки программного и аппаратного обеспечения; криптографические алгоритмы и особенности их программной реализации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации ПК-6.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга

	защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-6.3 Владеет методами и средствами получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях; защиты информации в компьютерных сетях, операционных системах и системах управления базами данных; анализа безопасности компьютерных систем

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Модуль 1. Безопасность информационной системы (10 час.)

Тема 1. Понятие безопасности информационной системы, системы защиты системы, компоненты этой системы, модель безопасности (2 час.)

Тема 2. Классификация угроз и рисков безопасности, виды атак, векторы атак. (2 час.)

Тема 3. Уязвимости информационной системы и способы их эксплуатации (4 час.)

Тема 4. Процесс тестирования безопасности информационной системы (2 час.)

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (16 час.)

Лабораторная работа 1: «Сканеры веб-уязвимостей» (4 часа)

Лабораторная работа 2: «Инструменты мониторинга трафика» (4 часа)

Лабораторная работа 3: «Инструменты шифрования» (4 часа)

Лабораторная работа 4: «Сканеры портов» (4 часа)

Практические занятия (10 час.)

Практическое занятие 1: «Веб-уязвимости» (2 час.)

Практическое занятие 2: «Мониторинг трафика» (2 час.)

Практическое занятие 3: «Сканеры портов» (2 час.)

Практическое занятие 4: «Инструменты для эксплуатации уязвимостей» (2 час.)

Практическое занятие 5: «Инструменты криминалистики» (2 час.)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Тестирование уязвимостей защищенных систем» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Электрон. текстовые данные. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 242 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62945.html

2. Методологические основы построения защищенных автоматизированных систем [Электронный ресурс] : учебное пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий [и др.]. — Электрон. текстовые данные. — Воронеж: Воронежский государственный университет инженерных технологий, 2013. — 260 c. — 978-5-89448-981-0. — Режим доступа: http://www.iprbookshop.ru/47427.html

3. Креопалов, В. В. Технические средства и методы защиты информации [Электронный ресурс] : учебное пособие / В. В. Креопалов. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2011. — 278 c. — 978-5-374-00507-3. — Режим доступа: http://www.iprbookshop.ru/10871.html

4. Защита от хакеров Web-приложений [Электронный ресурс] / Д. Форристал [и др.]. — Электрон. дан. — Москва : ДМК Пресс, 2008. — 496 с. — Режим доступа: https://e.lanbook.com/book/1116

Дополнительная литература

1. Ахмад Д.М., Дубравский И., Флинн Х., Гранд Д. - Защита от хакеров корпоративных сетей. Издательство: "ДМК Пресс", Год: 2008. https://e.lanbook.com/book/1120?category=1545,

2. , Бирюков А.А. - Информационная безопасность: защита и нападение; Издательство: "Машиностроение", Год: 2013, Издание: Второе издание, исправленное и дополненное, Объем:172 стр. https://e.lanbook.com/book/93278?category=1545

3. Титов А.А. «Инженерно-техническая защита информации» , Учебное пособие, Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники). - Год: 2010. - Объем: 197 стр. - http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4959

4. А.А. Варфоломеев «Основы информационной безопасности» М.: РУДН, 2008;

5. В.Г. Грибунин «Комплексная система защиты информации на предприятии» М.: Академия, 2009;

6. J. Faircloth «Penetration Tester's Open Source Toolkit», Elsevier Inc., 2010.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Тестирование уязвимостей защищенных систем», составляет 36 часов. На самостоятельную работу – 72 часа. При этом аудиторная нагрузка состоит из 10 лекционных часов, 16 лабораторных часов и 10 часов практических занятий.

В рамках указанной дисциплины итоговой формы аттестации является зачет. Самостоятельная работа при подготовке к зачету включает изучение

теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения данной дисциплины необходима аудитория, оснащенная презентационной техникой, компьютерный класс с программным обеспечением и возможностью использования Интернет-ресурсов и виртуализации, учебные и методические пособия (учебники, программы, сборники упражнений и т.д.), расходные материалы (бумага, картридж).

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине
«ТЕСТИРОВАНИЕ УЯЗВИМОСТЕЙ ЗАЩИЩЕННЫХ СИСТЕМ»
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка практических заданий.	32	Отчет по самостоятельной работе
2	1-18 неделя обучения	Подготовка лабораторных работ	30	Отчет по лабораторной работе
3	Сессия	Подготовка к зачету	20	Зачет

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.
4. Текущее тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;

- умение сформировать свою позицию, оценку и аргументировать ее

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	**Оценка**
От 95% до 100%	отлично
От 76% до 95%	хорошо
От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по практическим занятиям и лабораторным работам.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
«ТЕСТИРОВАНИЕ УЯЗВИМОСТЕЙ ЗАЩИЩЕННЫХ СИСТЕМ»
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции
ПК-1 Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-1.1 Знает: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; нормативно-правовые акты; национальные и международные стандарты в области защиты информации ПК-1.2 Умеет: определять параметры функционирования программно-аппаратных средств защиты информации; разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации; анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия ПК-1.3 Владеет: методами и средствами оценки корректности и эффективности программных реализаций алгоритмов защиты информации; методами оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации; методами анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей
ПК-5 Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-5.1 Знает: форматы хранения информации в анализируемой компьютерной системе; особенности хранения конфигурационной и системной информации в компьютерных системах; уязвимости компьютерных систем и сетей; порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; нормы уголовного и административного права в сфере компьютерной информации; характеристики правонарушений в области связи и информации; виды преступлений в сфере компьютерной информации; порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов ПК-5.2 Умеет: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства

	события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; выявлять возможные траектории состояний функционирования системы и несоответствия имеющейся информации ее расположению в системе ПК-5.3 Владеет: технологиями поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; навыками прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов; способами обнаружения и нейтрализации последствий вторжений в компьютерные системы; методами анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов; методами анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении
ПК-6 Способен разрабатывать и тестировать средств защиты информации компьютерных систем и сетей	ПК-6.1 Знает: принципы проектирования антивирусного программного обеспечения; виды атак и механизмы их реализации в компьютерных системах; принципы построения систем защиты информации компьютерных систем; методологии и технологии разработки программного и аппаратного обеспечения; криптографические алгоритмы и особенности их программной реализации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации; национальные, межгосударственные и международные стандарты в области защиты информации ПК-6.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-6.3 Владеет методами и средствами получения, обработки

	и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях; защиты информации в компьютерных сетях, операционных системах и системах управления базами данных; анализа безопасности компьютерных систем

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Модуль 1. Безопасность информационной системы	ПК-1, ПК-5, ПК 6	знает	ПР-1	1-10
			умеет	ПР-1	10-20
			владеет	ПР-1	20-36

Оценочные средства для промежуточной аттестации
Список вопросов на зачет

1. Модель безопасности информационной системы, ее компоненты
2. Модель угроз информационной системы
3. Классификация векторов атак
4. Классификация уязвимостей
5. Методы и инструменты тестирования безопасности
6. Процесс тестирования безопасности информационной системы
7. Мониторинг трафика
8. Тестирование на проникновение
9. Инструменты криминалистики
10. Инструменты брутфорса
11. Веб уязвимости
12. Инструменты эксплуатации уязвимостей