

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ  
КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**  
**АНАЛИЗ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ**

Направление подготовки  
(специальность)

[1] 10.03.01 Информационная безопасность

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/ В СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП	
8	3-5	108- 180	20	0	40		21-84	0	Э
Итого	3-5	108- 180	20	0	40	20	21-84	0	

## АННОТАЦИЯ

Цель дисциплины – изучение основ проведения тестирования на проникновение методом черного ящика, имитируя внешнего и внутреннего нарушителя. Студенты 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;
- социальная инженерия.

### 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение основ проведения тестирования на проникновение методом черного ящика, имитируя внешнего и внутреннего нарушителя.

### 2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные знания используются при изучении следующих дисциплин:

- Моделирование систем защиты информации;
- Аудит информационных технологий и систем обеспечения безопасности;
- Информационная безопасность открытых систем;
- Защита информации в банковских системах;
- Разработка и эксплуатация защищенных автоматизированных систем;
- Защищенный электронный документооборот в кредитно-финансовой сфере.

### 3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1.4 [1] – Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	З-ОПК-1.4 [1] – знать нормативными и корпоративными требованиями по безопасности компьютерных систем и сетей У-ОПК-1.4 [1] – уметь применять нормативные и корпоративные требования по безопасности компьютерных систем и сетей В-ОПК-1.4 [1] – владеть методами оценки уровня безопасности компьютерных систем и сетей

--	--

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

<b>Задача профессиональной деятельности (ЗПД)</b>	<b>Объект или область знания</b>	<b>Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)</b>	<b>Код и наименование индикатора достижения профессиональной компетенции</b>
эксплуатационный			
эксплуатация технических и программно-аппаратных средств защиты информации	программно-аппаратные средства защиты информации	ПК-1 [1] - способен устанавливать, настраивать и проводить техническое обслуживание средств защиты информации  <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-1[1] - знать требования к проведению технического обслуживания средств защиты информации ; У-ПК-1[1] - уметь устанавливать, настраивать и проводить техническое обслуживание средств защиты информации; В-ПК-1[1] - владеть навыками проведения технического обслуживания средств защиты информации
эксплуатация технических и программно-аппаратных средств защиты информации	программно-аппаратные средства защиты информации	ПК-1.3 [1] - способен проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей  <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-1.3[1] - знать способы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей; У-ПК-1.3[1] - уметь проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей; В-ПК-1.3[1] - владеть принципами проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей

#### 4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (B18)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (B19)	1.Использование воспитательного потенциала дисциплин/практик «Научно-исследовательская работа», «Проектная практика», «Научный семинар» для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2.Использование воспитательного потенциала дисциплин "История науки и инженерии", "Критическое мышление и основы научной коммуникации", "Введение в специальность", "Научно-исследовательская работа", "Научный семинар" для: - формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед; - формирования критического мышления, умения рассматривать различные исследования с экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок

		появления тех или иных открытий и теорий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)	<p>1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий.</p> <p>2. Использование воспитательного потенциала дисциплины "Проектная практика" для формирования культуры решения изобретательских задач, развития логического мышления, путем погружения студентов в научную и инновационную деятельность института и вовлечения в проектную работу.</p> <p>3. Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях.</p> <p>4. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для</p>

		<p>формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий.</p> <p>5.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования системного подхода по обеспечению информационной безопасности и кибербезопасности в различных сферах деятельности посредством исследования и перенятия опыта постановки и решения научно-практических задач организациями-партнерами.</p>
--	--	---

## 5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары )/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>8 Семестр</i>						
1	Первый раздел	1-3			25	КИ-4	З-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-1.3, У-

							ПК-1.3, В-ПК-1.3
2	Второй раздел	4-6			25	КИ-8	3-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, 3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-1.3, У-ПК-1.3, В-ПК-1.3
	<i>Итого за 8 Семестр</i>		20/0/40		50		
	<b>Контрольные мероприятия за 8 Семестр</b>				50	АттР	3-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, 3-ПК-1, У-ПК-1, В-ПК-1, 3-ПК-1.3, У-ПК-1.3, В-ПК-1.3

\* – сокращенное наименование формы контроля

\*\* – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
АТР	Аттестация разделов
КИ	Контроль по итогам
Э	Экзамен

### КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	<i>8 Семестр</i>	20	0	40
<b>1-3</b>	<b>Первый раздел</b>	10		20
1	<b>Введение в информационные технологии</b> Основы веб-технологий. Принцип работы веб-приложений. Различия в методах проведения тестирования на проникновение.	Всего аудиторных часов		
		3		6
		Онлайн		
2	<b>Первые этапы проведения тестирования на проникновение</b> Разведка и сбор информации о компании различными методами. Пассивная, полупассивная разведка. Знакомство с инструментарием и ручной поиск информации. Лабораторная работа на пассивный рекон по компании	Всего аудиторных часов		
		3		6
		Онлайн		
3	<b>Веб-уязвимости</b> Веб-уязвимости. OWASP TOP 10. Лабораторная работа на поиск и эксплуатацию уязвимостей из OWASP TOP 10.	Всего аудиторных часов		
		4		8
		Онлайн		
<b>4-6</b>	<b>Второй раздел</b>	10		20
4	<b>Фазинг директорий веб-сайта. Поиск открытых портов</b> Различный инструментарий для фазинга директорий веб-приложения. Сканирование сети на наличие открытых портов с помощью nmap. Исследование веб-приложения с помощью Burp Suite. Лабораторная работа на работу с инструментарием для фазинга и наличие открытых портов.	Всего аудиторных часов		
		3		6
		Онлайн		
5	<b>Автоматизированное сканирование на наличие уязвимостей</b> Изучение различных автоматизированных сканеров по поиску уязвимостей. Различия между ними. Ручной поиск уязвимостей Лабораторная работа на сравнение различных сканеров уязвимостей	Всего аудиторных часов		
		3		6
		Онлайн		
6	<b>Эксплуатация уязвимостей. Социальная инженерия</b> Работа с фреймворком Metasploit. Понятие exploit. CVSS Лабораторная работа на работу с фреймворком Metasploit.	Всего аудиторных часов		
		4		8
		Онлайн		



	Различные виды социальной инженерии			
--	-------------------------------------	--	--	--

Сокращенные наименования онлайн опций:

Обозначение	Полное наименование
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

## 6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основными образовательными технологиями в освоении дисциплин профессионального цикла являются традиционные технологии лекций и лабораторных работ. Интерактивные методики обеспечиваются решением индивидуальных задач студентами и коллективным обсуждением результатов и методов решения.

## 7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	Индикаторы освоения	Аттестационное мероприятие (КП 1)
ОПК-1.4	З-ОПК-1.4	АттР, КИ-4, КИ-8
	У-ОПК-1.4	АттР, КИ-4, КИ-8
	В-ОПК-1.4	АттР, КИ-4, КИ-8
ПК-1	З-ПК-1	АттР, КИ-4, КИ-8
	У-ПК-1	АттР, КИ-4, КИ-8
	В-ПК-1	АттР, КИ-4, КИ-8
ПК-1.3	З-ПК-1.3	АттР, КИ-4, КИ-8
	У-ПК-1.3	АттР, КИ-4, КИ-8
	В-ПК-1.3	АттР, КИ-4, КИ-8

## Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-

балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – «отлично»	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «хорошо»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «удовлетворительно»	E	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64			
Ниже 60	2 – «неудовлетворительно»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства приведены в Приложении.

## 8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Комментарии к Доктрине информационной безопасности Российской Федерации. : , Москва: Горячая линия -Телеком, 2018

2. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Москва: Горячая линия -Телеком, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

<https://online.mephi.ru/>

<http://library.mephi.ru/>

## **9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ**

загружено

## **10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ**

загружено

Автор(ы):

Хачинян Ольга Владимировна

Семцова Ольга Владимировна