Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № 4/1/2023

от 25.04.2023 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	108	20	0	40		21	0	Э
Итого	3	108	20	0	40	20	21	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 требованиями по безопасности компьютерных систем и сетей В-ОПК-1.4 [1] – владеть методами оценки уровня безопасности компьютерных систем и сетей

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

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
	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 *Основание:* 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 *Основание:* 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
эксплуатация	программно-	ПК-4.3 [1] - способен	З-ПК-4.3[1] - знать

технических и программно-аппаратных средств защиты информации	аппаратные средства защиты информации	проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей *Основание:* Профессиональный стандарт: 06.032	способы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей; У-ПК-4.3[1] - уметь проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей; В-ПК-4.3[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 (В18)	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 (В19)	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)	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. 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. 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. 4.Использование воспитательного потенциала дисциплин " "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий. 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.

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
	8 Семестр						
1	Первый раздел	1-3	10/0/20		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, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3
2	Второй раздел	4-6	10/0/20		25	КИ-8	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, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3
	Итого за 8 Семестр		20/0/40		50		
	Контрольные мероприятия за 8 Семестр				50	Э	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, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3

* – 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**
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	8 Семестр	20	0	40
1-3	**Первый раздел**	10	0	20
1	**Введение в информационные технологии** Основы веб-технологий. Принцип работы веб-приложений. Различия в методах проведения тестирования на проникновение.	Всего аудиторных часов		
		3	0	6
		Онлайн		
		0	0	0
2	**Первые этапы проведения тестирования на проникновение** 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	0	6
		Онлайн		
		0	0	0
3	**Веб-уязвимости** Веб-уязвимости. OWASP TOP 10. Лабораторная работа на поиск и эксплуатацию уязвимостей из OWASP TOP 10.	Всего аудиторных часов		
		4	0	8
		Онлайн		
		0	0	0
4-6	**Второй раздел**	10	0	20
4	**Фазинг директорий веб-сайта. Поиск открытых портов** 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	0	6
		Онлайн		
		0	0	0
5	**Автоматизированное сканирование на наличие уязвимостей** Изучение различных автоматизированных сканеров по поиску уязвимостей. Различия между ними. Ручной поиск уязвимостей Лабораторная работа на сравнение различных сканеров уязвимостей	Всего аудиторных часов		
		3	0	6
		Онлайн		
		0	0	0
6	**Эксплуатация уязвимостей. Социальная инженерия** Работа с фрейморком Metasploit. Понятие exploit. CVSS Лабораторная работа на работу с фреймворком Metasploit. Различные виды социальной инженерии	Всего аудиторных часов		
		4	0	8
		Онлайн		
		0	0	0

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

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	Темы занятий / Содержание
	8 Семестр
	Изучение уязвимостей систем, приводящих к атакам SQL-injection • ознакомление с уязвимостями, способствующими реализации SQL-инъекций, путем практической реализации этих атак и понимания методов ее предотвращения
	Изучение уязвимостей систем, приводящих к атакам XSS • ознакомление с уязвимостями, способствующими реализации атак XSS, путем практической реализации этих атак и понимания методов ее предотвращения
	Межсетевое экранирование. Трансляция сетевых адресов • изучение и практическое применение межсетевого экрана ОС Linux Netfiler/iptables
	Стандартные сетевые утилиты. Сетевой сканер Nmap. Анализатор трафика tcpdump • получить практические навыки работы со стандартными сетевыми утилитами: ping, traceroute, nc (netcat); • получить практические навыки работы с сетевым сканером nmap и анализатором трафика tcpdump

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, влючают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятиий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы.

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	Э, КИ-4, КИ-8
	У-ОПК-1.4	Э, КИ-4, КИ-8
	В-ОПК-1.4	Э, КИ-4, КИ-8
ПК-1	З-ПК-1	Э, КИ-4, КИ-8
	У-ПК-1	Э, КИ-4, КИ-8
	В-ПК-1	Э, КИ-4, КИ-8
ПК-1.3	З-ПК-1.3	Э, КИ-4, КИ-8
	У-ПК-1.3	Э, КИ-4, КИ-8
	В-ПК-1.3	Э, КИ-4, КИ-8
ПК-4.3	З-ПК-4.3	Э, КИ-4, КИ-8
	У-ПК-4.3	Э, КИ-4, КИ-8
	В-ПК-4.3	Э, 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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>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.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2"></td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала,</td></tr>
<tr><td>60-64</td><td>E</td></tr>
</table>

			но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
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.

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. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций и семинарских занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время семинарских занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

При необходимости в конце лекции преподаватель оставляет время для того, чтобы студенты имели возможность задать вопросы по изучаемому материалу.

Лекции нацелены на освещение основополагающих положений теории алгоритмов и теории функций алгебры логики, наиболее трудных вопросов, как правило, связанных с доказательством необходимых утверждений и теорем, призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого семинара.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе лекций, аудиторных практических занятий, лабораторных и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции. В лекционном курсе главное место отводится общетеоретическим проблемам.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Семцова Ольга Владимировна