Приложение № 4
к образовательной программе высшего образования – программе магистратуры
по направлению подготовки 09.04.01 Информатика и вычислительная техника
(направленность (профиль) «Разработка и управление
критической информационной инфраструктурой»)

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 7835bcdac1c89a3da835a18f6045494f3f404337
Владелец: Некрасова Людмила Андреевна
Действителен: с 08.07.2026 до 08.07.2027

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Практика наступательной информационной безопасности»

1. Трудоемкость дисциплины (модуля): 3 з.е.

2. Место дисциплины (модуля) в учебном плане:
Факультативная дисциплина (модуль), реализуется во 2 семестре.

3. Цель дисциплины (модуля): формирование у обучающихся практических навыков выявления, анализа и эксплуатации уязвимостей в информационных системах и программном обеспечении, а также освоение методологии этичного хакинга и проведения тестирований на проникновение в контексте обеспечения безопасности объектов критической информационной инфраструктуры.

4. Задачи дисциплины (модуля):

– сформировать представление о методологиях тестирования на проникновение (PTES, OWASP, MITRE ATT&CK), правовых и этических аспектах наступательной безопасности, а также об этапах проведения пентеста;

– обеспечить владение практическим инструментарием разведки, сканирования, эксплуатации уязвимостей, постэксплуатации и подготовки отчётной документации;

– научить применять техники эксплуатации веб-уязвимостей, сетевых атак, повышения привилегий и обхода средств защиты для оценки защищённости систем и разработки рекомендаций по устранению обнаруженных недостатков.

5. Перечень разделов (тем) дисциплины (модуля) и их краткое содержание:

Наименование раздела (темы) дисциплины (модуля)	Краткое содержание
Раздел 1. Введение в наступательную безопасность и разведка	Понятие этичного хакинга. Правовые основы и стандарты пентеста. Фазы тестирования на проникновение. Пассивная и активная разведка: сбор информации о цели из открытых источников (OSINT), WHOIS, DNS-разведка, анализ метаданных. Инструменты: Maltego, theHarvester, Shodan, Recon-ng.
Раздел 2. Сканирование и идентификация уязвимостей	Сетевое сканирование: обнаружение хостов, портов и сервисов (Nmap, Masscan). Баннер-граббинг и определение версий ПО. Сканеры уязвимостей: OpenVAS, Nessus, Nikto. Анализ результатов сканирования, приоритизация уязвимостей, устранение ложных срабатываний.
Раздел 3. Эксплуатация уязвимостей и постэксплуатация	Поиск и адаптация эксплойтов (Exploit-DB, SearchSploit). Фреймворк Metasploit: основные модули, полезные нагрузки, создание обратных соединений. Эксплуатация веб-уязвимостей: SQL-инъекции, XSS, CSRF, command injection (Burp Suite, sqlmap). Повышение привилегий в

Наименование раздела (темы) дисциплины (модуля)	Краткое содержание
	Linux/Windows, закрепление в системе, сбор данных и lateral movement.
Раздел 4. Тестирование веб-приложений и беспроводных сетей	Методология OWASP Top 10. Ручное и автоматизированное тестирование веб-приложений. Атаки на механизмы аутентификации и авторизации. Основы тестирования безопасности Wi-Fi сетей: перехват рукопожатий, атаки на WPA/WPA2.
Раздел 5. Обход средств защиты и отчётность	Методы обхода антивирусов, межсетевых экранов и систем обнаружения вторжений. Техники туннелирования и проксирования трафика. Написание профессионального отчёта о тестировании на проникновение: структура, описание уязвимостей, оценка рисков, рекомендации по устранению.

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-3. Способен анализировать и обеспечивать безопасность компьютерных сетей, включая распределенные, облачные и высоконагруженные системы	ИПК-3.1. Знает основные принципы компьютерной сетевой безопасности и методы анализа уязвимостей в локальных сетях и распределенных системах
	ИПК-3.2. Умеет исследовать компьютерные сети, распределенные, облачные и высоконагруженные системы, выявлять и устранять в них уязвимости
	ИПК-3.3. Владеет методами обеспечения безопасности компьютерных сетей, распределенных, облачных и высоконагруженных систем с помощью методов мониторинга и обнаружения инцидентов
ПК-5. Способен анализировать и реагировать на угрозы информационной безопасности	ИПК-5.1. Знает основы анализа и классификации угроз информационной безопасности, виды вредоносного программного обеспечения
	ИПК-5.2. Умеет выявлять и устранять угрозы информационной безопасности, а также обнаруживать и реагировать на вредоносное программное обеспечение

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
	ИПК-5.3. Владеет методами оперативного реагирования на угрозы, включая обнаружение и устранение вредоносного программного обеспечения, а также способен создавать собственные методологии для обеспечения защиты информационной безопасности