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)

«Локальный и сетевой анализ защищенности»

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 навыков анализа и обеспечения безопасности локальных и сетевых систем, умения проводить аудит и диагностику уязвимостей сетевой инфраструктуры; изучение методов обеспечения безопасности сетевой инфраструктуры, включая мониторинг сетевого трафика, обнаружение и реагирование на инциденты безопасности.

4. Задачи дисциплины (модуля):
– сформировать представление об уязвимостях локальных и сетевых систем, методах их выявления и классификации;
– обеспечить владение средствами анализа защищенности и сканирования сетевой инфраструктуры;
– научить проводить аудит защищенности, выявлять уязвимости и формировать рекомендации по их устранению.

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

Наименование раздела (темы) дисциплины (модуля)	**Краткое содержание**
Раздел 1. Постановка задачи анализа защищенности компьютерной системы	Корпоративная сеть как объект защиты. Событие безопасности. Понятие и классификация уязвимостей. Источники информации об уязвимостях.
Раздел 2. Методы выявления уязвимостей и системы анализа защищенности	Основные приемы выявления уязвимостей. Выявление известных уязвимостей. Системы анализа защищенности. Примеры средств анализа.
Раздел 3. Сетевые сканеры безопасности и сбор информации о сети	Размещение сетевых агентов сканирования. Способы сбора информации о сети. Предварительное изучение цели. Инвентаризация ресурсов.
Раздел 4. Идентификация сетевых объектов и настроек	Использование протоколов ICMP и ARP. Идентификация узлов. Сканирование портов TCP и UDP. Определение сервисов и операционных систем.
Раздел 5. Выявление уязвимостей с помощью тестов	Эксплойты и их разновидности. Техники запуска кода. Удаленный подбор и оценка стойкости паролей. Тестирование на проникновение.
Раздел 6. Специализированные средства анализа защищенности	Классификация сканеров безопасности по назначению. Угрозы и уязвимости СУБД и веб-приложений. Особенности анализа их защищенности. Формирование отчета.

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
	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
ПК-6. Способен проектировать и реализовывать объекты критической информационной инфраструктуры для различных операционных систем и облачных платформ	ИПК-6.1. Знает принципы проектирования информационных систем и объектов критической инфраструктуры, особенности различных операционных систем и облачных платформ
	ИПК-6.2. Умеет реализовывать объекты критической инфраструктуры для различных операционных систем и облачных платформ, учитывая их специфику
	ИПК-6.3. Владеет методами проектирования и реализации объектов критической инфраструктуры, включая установку, настройку и обеспечение их работоспособности с учетом специфики работы в

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
	различных операционных системах и облачных платформах