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)

«Анализ вредоносного программного обеспечения»

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

2. Место дисциплины (модуля) в учебном плане:
Факультативная дисциплина (модуль), реализуется в 3 семестре.

3. Цель дисциплины (модуля): формирование навыков анализа и обнаружения вредоносного программного обеспечения с использованием технологий со свободной лицензией и открытым исходным кодом, навыков реагирования на инциденты безопасности и проведения расследований в области кибербезопасности; изучение методов обнаружения угроз информационной безопасности и классификации вредоносных программ.

4. Задачи дисциплины (модуля):
– сформировать представление о видах вредоносного программного обеспечения, методах его распространения и классификации;
– обеспечить владение методами и инструментами статического и динамического анализа вредоносного ПО;
– научить выявлять вредоносное ПО, реагировать на инциденты и проводить расследования в безопасной среде.

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

Наименование раздела (темы) дисциплины (модуля)	**Краткое содержание**
Раздел 1. Вредоносное программное обеспечение: виды и классификация	Понятие и виды вредоносного ПО. Способы распространения и заражения. Классификация и таксономия угроз. Жизненный цикл вредоносной программы.
Раздел 2. Организация безопасной среды анализа	Изолированные среды и песочницы. Виртуализация. Инструменты с открытым исходным кодом. Правовые и этические аспекты анализа.
Раздел 3. Статический анализ вредоносного ПО	Структура исполняемых файлов. Дизассемблирование. Анализ строк, импорта и сигнатур. Обнаружение обфускации и упаковки.
Раздел 4. Динамический анализ и поведение вредоносного ПО	Запуск в контролируемой среде. Мониторинг процессов, файловой системы и сети. Анализ поведения и индикаторов компрометации.
Раздел 5. Обнаружение, реагирование и расследование инцидентов	Индикаторы компрометации (IoC). Обнаружение и нейтрализация угроз. Реагирование на инциденты. Проведение расследований и подготовка отчета.

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
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-7. Способен разрабатывать и применять решения на основе математических моделей для обеспечения информационной безопасности	ИПК-7.1. Знает принципы построения математических моделей для обеспечения информационной безопасности
	ИПК-7.2. Умеет разрабатывать и внедрять математические модели для обеспечения информационной безопасности
	ИПК-7.3. Владеет методами сбора, анализа и использования данных для математического моделирования в составе решений, обеспечивающих информационную безопасность в информационных системах и объектах критической информационной инфраструктуры