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)

«Технологии искусственного интеллекта для задач информационной безопасности»

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 у обучающихся представления о применении методов искусственного интеллекта и машинного обучения для решения задач информационной безопасности — обнаружения вторжений, выявления аномалий, классификации угроз и автоматизации реагирования.

4. Задачи дисциплины (модуля):
– сформировать представление о задачах информационной безопасности, решаемых методами искусственного интеллекта и машинного обучения;
– обеспечить владение методами подготовки данных и построения моделей для выявления угроз и аномалий;
– научить применять модели машинного обучения для обнаружения вторжений, классификации угроз и автоматизации реагирования.

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

Наименование раздела (темы) дисциплины (модуля)	**Краткое содержание**
Раздел 1. Задачи информационной безопасности и методы ИИ	Обзор задач ИБ, решаемых средствами ИИ. Типы данных безопасности. Постановка задач классификации, кластеризации и обнаружения аномалий.
Раздел 2. Подготовка и анализ данных безопасности	Источники данных (сетевой трафик, журналы событий, телеметрия). Извлечение признаков. Очистка и разметка данных. Несбалансированные выборки.
Раздел 3. Обнаружение вторжений и аномалий	Сигнатурные и поведенческие методы. Модели обнаружения аномалий. Системы обнаружения вторжений на основе машинного обучения. Оценка качества.
Раздел 4. Классификация угроз и вредоносной активности	Классификация вредоносного ПО и сетевых атак. Признаки и модели. Снижение числа ложных срабатываний. Интерпретация результатов.
Раздел 5. Автоматизация реагирования на инциденты	Применение ИИ в SOC и SIEM. Приоритизация и триаж инцидентов. Автоматизация реагирования (SOAR). Ограничения и риски применения ИИ в ИБ.

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