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)

«Работа с системами мониторинга и анализа событий»

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): знакомство с основами систем мониторинга и анализа событий; формирование представления о методах сбора, анализа и визуализации данных; формирование навыков работы с различными системами мониторинга и анализа событий (SIEM).

4. Задачи дисциплины (модуля):
– сформировать представление о принципах работы систем мониторинга и анализа событий безопасности;
– обеспечить владение методами сбора, нормализации, корреляции и визуализации событий;
– научить настраивать системы мониторинга и анализа событий и выявлять инциденты информационной безопасности.

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

Наименование раздела (темы) дисциплины (модуля)	**Краткое содержание**
Раздел 1. Основы систем мониторинга и анализа событий	Назначение и архитектура систем мониторинга. Понятие события и инцидента безопасности. Источники событий. Класс систем SIEM.
Раздел 2. Сбор и нормализация данных	Сбор журналов и телеметрии. Агенты и коллекторы. Нормализация и обогащение событий. Хранение и индексация данных.
Раздел 3. Корреляция событий и обнаружение инцидентов	Правила корреляции. Выявление аномалий и подозрительной активности. Управление ложными срабатываниями. Приоритизация инцидентов.
Раздел 4. Визуализация и анализ данных	Дашборды и отчеты. Анализ временных рядов событий. Поиск и расследование инцидентов. Метрики и показатели мониторинга.
Раздел 5. Эксплуатация систем мониторинга в SOC	Организация центра мониторинга безопасности (SOC). Процессы реагирования. Интеграция с другими средствами защиты. Сопровождение и настройка системы.

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-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 различных операционных системах и облачных платформах