Приложение № 4
к образовательной программе среднего профессионального образования –
программе подготовки специалистов среднего звена по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(на базе основного общего образования)

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

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«Технологии искусственного интеллекта в кибербезопасности»

1. Трудоемкость профессионального модуля: 306 ак.ч.

2. Место профессионального модуля в учебном плане:

Профессиональный модуль «Технологии искусственного интеллекта в кибербезопасности» входит в образовательный компонент программы П.00 «Профессиональный цикл» (ПМ.07) и является вариативным. Профессиональный модуль реализуется в 7 семестре.

3. Цель профессионального модуля: сформировать у обучающихся профессиональные компетенции для применения технологий искусственного интеллекта (ИИ) и машинного обучения (МО) в целях обнаружения, анализа и предотвращения киберугроз, а также для повышения эффективности систем защиты информационных систем.

4. Задачи профессионального модуля:

– изучить теоретические основы ИИ и МО в контексте кибербезопасности: освоить базовые концепции машинного обучения (обучение с учителем/без учителя, глубокое обучение), разобраться в типах алгоритмов, подходящих для задач кибербезопасности (классификация, кластеризация, обнаружение аномалий), понять специфику их применения для выявления киберугроз;

– освоить методы сбора, предобработки и анализа данных для обучения моделей ИИ: научиться работать с сетевыми логами, данными SIEM-систем, телеметрией конечных точек; освоить техники очистки, нормализации и разметки данных; сформировать навыки создания репрезентативных обучающих выборок для обнаружения атак;

– овладеть практическими навыками построения и настройки моделей ИИ для обнаружения киберугроз: научиться применять алгоритмы МО (случайный лес, SVM, нейронные сети) для выявления вредоносной активности; освоить работу с фреймворками и библиотеками (TensorFlow, PyTorch, Scikit-learn); отработать настройку гиперпараметров и валидацию моделей на примерах реальных и синтетических данных об атаках;

– изучить применение ИИ-решений для автоматизации реагирования на инциденты и прогнозирования угроз: освоить использование ИИ для классификации событий безопасности, приоритизации алёртов, автоматического блокирования подозрительной активности; научиться применять методы прогнозной аналитики для выявления потенциальных векторов атак и оценки рисков; рассмотреть сценарии интеграции ИИ-инструментов с SOC и системами оркестрации (SOAR);

– развить навыки оценки эффективности и безопасности ИИ-систем в киберзащите: научиться измерять ключевые метрики качества моделей (точность, полнота, F1-мера, AUC-ROC), анализировать ложные срабатывания и пропуски атак; освоить методы защиты самих ИИ-систем от adversarial-атак (состязательных атак); изучить этические и нормативные аспекты применения ИИ в кибербезопасности, включая вопросы приватности и соответствия требованиям регуляторов.

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

Наименования разделов (тем) профессионального модуля	Содержание разделов (тем) профессионального модуля
МДК.07.01 Основы искусственного интеллекта и машинного обучения для кибербезопасности	

Тема 1. Введение в ИИ и его роль в кибербезопасности	Понятие искусственного интеллекта. Эволюция ИИ. Основные направления: ML, DL, NLP, компьютерное зрение. Место ИИ в современных системах защиты информации. Преимущества и ограничения.
Тема 2. Основы машинного обучения	Типы машинного обучения: с учителем, без учителя, с подкреплением. Понятие признакового пространства. Этапы построения ML-модели. Основные библиотеки Python для ML.
Тема 3. Методы предобработки данных для задач ИБ	Сбор и разметка данных. Работа с пропусками и выбросами. Нормализация и стандартизация. Балансировка классов (SMOTE, undersampling). Особенности работы с сетевыми логами.
Тема 4. Классические ML-алгоритмы для обнаружения угроз	Логистическая регрессия, дерево решений, случайный лес, метод опорных векторов (SVM), k-ближайших соседей (kNN). Критерии оценки моделей: Accuracy, Precision, Recall, F1-score, ROC-AUC.
Тема 5. Нейронные сети и глубокое обучение	Перцептрон. Архитектура многослойного перцептрона. Функции активации. Метод обратного распространения ошибки. Регуляризация. Понятие переобучения.
Тема 6. Обнаружение аномалий методами ML	Задача обнаружения аномалий. Алгоритмы: Isolation Forest, One-Class SVM, методы кластеризации (K-means, DBSCAN). Применение в обнаружении вторжений и инсайдерских угроз.
МДК.07.02 Применение искусственного интеллекта для обнаружения угроз и реагирования на инциденты	
Тема 1. ИИ в системах обнаружения вторжений (IDS/IPS)	Различия сигнатурных и поведенческих методов. Современные IDS на основе ML. Примеры: Snort с ML-расширениями, Zeek с анализом аномалий.
Тема 2. Анализ вредоносного ПО с использованием ИИ	Статический и динамический анализ. Извлечение признаков из PE-файлов. Классификация вредоносного ПО с использованием случайного леса и нейронных сетей. Обнаружение полиморфных и метаморфных вирусов.
Тема 3. ИИ для анализа сетевого трафика	Глубокий анализ пакетов (Deep Packet Inspection) с использованием ML. Выявление атак DDoS, ботнет-активности. Анализ DNS-запросов для обнаружения доменов C2.
МДК.07.03 Большие языковые модели (LLM) и защита от социальной инженерии	
Тема 1. Применение NLP в кибербезопасности	Обработка естественного языка для анализа логов, отчетов об уязвимостях, фишинговых писем. Извлечение сущностей (NER). Анализ тональности.
Тема 2. ИИ в системах SIEM и SOAR	Автоматизация корреляции событий. Применение ML для снижения ложных срабатываний. Оркестрация реагирования с элементами ИИ.
Тема 3. Прогнозирование кибератак	Методы прогнозирования временных рядов (ARIMA, LSTM, Prophet). Прогнозирование интенсивности атак. Обнаружение подготовки к атаке по ранним признакам.

УП.07.01 Учебная практика (Технологии искусственного интеллекта в кибербезопасности)
Выполнение практических заданий по темам, изученным в МДК профессионального модуля. Закрепление освоенных навыков на учебных примерах

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Результаты освоения дисциплины
ЛК-02. Использует современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	ИЛК-02.1. Применяет номенклатуру информационных источников в профессиональной деятельности
	ИЛК-02.2. Формулирует поисковый запрос, выделяет и оценивает практическую значимость полученных результатов, структурирует и оформляет результаты поиска
ПК-01. Выполняет монтаж, настройку и администрирование сетевого оборудования и систем обеспечения информационной безопасности	ИПК-01.4. Реализует сетевую безопасность (межсетевые экраны, VPN, ACL, IDS/IPS)
ПК-02. Обеспечивает бесперебойное функционирование, мониторинг и защиту сетевой инфраструктуры	ИПК-02.5. Анализирует сетевой трафик и выявляет инциденты информационной безопасности
ПК-03. Применяет программно-аппаратные средства и методы обеспечения информационной безопасности, включая тестирование на проникновение и анализ защищённости	ИПК-03.1. Применяет криптографические средства и методы защиты информации
ПК-04. Применяет средства автоматизации для администрирования, управления инцидентами и настройки систем информационной безопасности	ИПК-04.2. Осуществляет мониторинг и управление инцидентами в ИТ-системах
	ИПК-04.4. Применяет инструменты автоматизации для настройки средств защиты
ПК-07. Применяет методы математического анализа, дискретной математики и математической логики для построения моделей, разработки алгоритмов и анализа информационных систем в профессиональной деятельности	ИПК-07.5. Использует методы теории вероятностей и математической статистики для оценки надежности программных средств, обработки результатов экспериментов и анализа рисков в информационных системах
	ИПК-07.6. Применяет элементы теории алгоритмов и формальных языков (конечные автоматы, рекурсия, оценка сложности) для выбора оптимальных структур данных и разработки эффективных алгоритмов обработки информации