Бауманский учебный центр «Специалист»

Программа курса Искусственный интеллект и машинное обучение в информационной безопасности

Код курса: **ИИБЕЗОП**

Тема	Ак. часов

Модуль 1. Введение в ИИ и ML для ИБ — основы, задачи и инструменты
 	
• Что такое AI, Machine Learning и Deep Learning?
• Отличие ML от классических правил (rule-based systems).
• Где ML применяется в кибербезопасности.
• Типы машинного обучения.
• Основные задачи ML в безопасности:
  ◦ обнаружение аномалий;
  ◦ классификация угроз;
  ◦ обнаружение вредоносного ПО;
  ◦ анализ сетевого трафика;
  ◦ антифрод системы.
• Экосистема инструментов:
  ◦ Python для ML;
  ◦ Jupyter Notebook;
  ◦ библиотеки: (numpy, pandas, scikit-learn, matplotlib, seaborn).
• Основы работы с данными безопасности:
  ◦ сетевые логи;
  ◦ NetFlow;
  ◦ системные события;
  ◦ IDS/IPS логи;
  ◦ SIEM данные.
 	
Практика
 	
• Установка Python среды
	4

Модуль 2. Сбор и подготовка данных — очистка, нормализация, feature engineering Этот модуль посвящён **самой важной части ML — данным**. Источники данных безопасности • сетевые логи • firewall logs • IDS/IPS • endpoint telemetry • threat intelligence feeds Очистка данных (Data Cleaning) • удаление пропусков • обработка NaN • удаление дубликатов • исправление некорректных значений Нормализация данных Методы: Min-Max Scaling, Standardization, Robust Scaling Feature Engineering Создание новых признаков: пример: из сетевого трафика • packets/sec • bytes/sec • connection duration • failed login rate Типы признаков: • числовые, категориальные, бинарные, временные Кодирование категориальных данных • One-Hot Encoding • Label Encoding • Target Encoding Разделение данных • train • validation • test **Практика** • Подготовка датасета сетевого трафика	**4**

Модуль 3. Классификация и обнаружение аномалий — алгоритмы и метрики Здесь изучаются **ключевые алгоритмы ML для SOC**. **Алгоритмы классификации** Основные модели: • Logistic Regression • Decision Trees • Random Forest • Gradient Boosting • Support Vector Machine (SVM) • k-Nearest Neighbors Примеры задач: • классификация фишинга **Обнаружение аномалий** Очень важная задача в SOC. Методы: • Isolation Forest • Local Outlier Factor • One-Class SVM • Autoencoders Примеры аномалий: • необычный сетевой трафик **Метрики оценки моделей** Что изучается: • Accuracy • Precision • Recall • F1-score • ROC-AUC Почему важно: например в SOC Recall часто важнее Accuracy. **Практика** • Детекция аномалий в сетевом трафике	**4**

Модуль 4. Нейронные сети для кибербезопасности- построение и обучение моделей, LSTM для временных рядов **Основы нейросетей** • нейрон • слои • функции активации Основные функции: • ReLU • Sigmoid • Tanh • Softmax **Архитектуры нейронных сетей** 1. Feedforward Networks классические нейросети 2. CNN используются для: ◦ анализа malware ◦ бинарных файлов 3. RNN используются для: ◦ анализа последовательностей событий **LSTM для временных рядов** Используется для анализа: • сетевых потоков • последовательности логов • поведения пользователей Пример: *login -> file access -> privilege escalation* Модель учится находить подозрительные последовательности. **Практика** • Построение нейросети на TensorFlow / PyTorch	**4**

Модуль 5. Практические кейсы SOC - DDoS, фишинг, внутренняя угроза, вредоносное ПО **Обнаружение DDoS** Используются признаки: packets/sec, source IP entropy, number of connections. Алгоритмы: Random Forest, XGBoost, LSTM. **Обнаружение фишинга** Анализируются: URL, домены, email заголовки. Признаки: длина URL, количество поддоменов, наличие IP вместо домена. **Insider Threat** Анализ: поведение пользователя, время входа, доступ к файлам. Методы: anomaly detection, clustering. **Malware Detection** Методы: статический анализ, динамический анализ. Используются: Random Forest, CNN.	**4**
Модуль 6. Автоматизация и интеграция - — REST API, мониторинг и обновление моделей **REST API** Создание сервисов: *POST /predict* пример: отправка логов > получение результата ML Используемые технологии: FastAPI **Интеграция с системами безопасности** Интеграция с: SIEM, IDS, SOAR пример: ML -> обнаружил атаку -> отправил alert в SIEM	**4**

Модуль 7. Продвинутая статистика и вероятностные модели. Защита моделей, атаки на ML, устойчивость моделей Статистика • распределения • доверительные интервалы • гипотезы • Bayesian inference Вероятностные модели • Naive Bayes • Hidden Markov Models • Bayesian Networks Атаки на ML модели • Adversarial Attacks- модификация входных данных. • Data Poisoning - отравление датасета. • Model Inversion -извлечение данных из модели. Защита моделей Методы: adversarial training, data validation, monitoring inputs, differential privacy	**4**

Модуль 8. Итоговый проект - полный цикл от анализа до отчета Финальный проект — **полный ML pipeline для безопасности**. **Этапы проекта** 1. Выбор задачи например: ◦ обнаружение DDoS ◦ обнаружение фишинга ◦ анализ сетевого трафика 2. Сбор данных источники: CICIDS, KDD Cup, собственные логи 3. Подготовка данных: очистка, feature engineering, нормализация 4. Обучение моделей сравнение алгоритмов: ◦ Random Forest ◦ XGBoost ◦ Neural Network 5. Оценка ◦ метрики ◦ ROC curve ◦ confusion matrix 6. Развёртывание ◦ REST API ◦ интеграция с SIEM 7. Финальный отчёт содержит: ◦ описание задачи ◦ методы ◦ результаты ◦ анализ ошибок ◦ рекомендации	**4**
Аудиторная нагрузка в классе с преподавателем	**32 ак.ч. + 32 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru