# ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ В ИНФОРМАЦИОННОЙ И КИБЕРБЕЗОПАСНОСТИ

**Цель программы** — обучение специалистов в области информационной безопасности основам и современным подходам использования искусственного интеллекта и машинного обучения для повышения уровня защиты информации и предотвращения киберугроз.

**Выпускники курса получают свидетельство о повышении квалификации в области информационной безопасности государственного образца.**

**Целевая аудитория:**

- специалисты по информационной и кибербезопасности, желающие расширить свои знания в области ИИ;
- аналитики данных, заинтересованные в применении ИИ для повышения уровня безопасности;
- разработчики ПО, работающие в области ИБ и стремящиеся интегрировать технологии ИИ в свои решения.

**Требуемая предварительная подготовка слушателей:**

- Опыт работы с языками программирования для реализации алгоритмов машинного обучения.

**Форма обучения –** очная (дневная).

**Стоимость обучения одного слушателя** – 1700 рублей**.**

Обучение проводится по адресу: г. Минск, ул. К. Цеткин, 24, в соответствии с графиком учебного процесса.

Продолжительность программы – 56 академических часов (2 недели).

**Учебный план курса:**

| Наименования разделов, модулей, тем |
|---|
| **ВВОДНАЯ ЧАСТЬ** |
| **РАЗДЕЛ: Основы искусственного интеллекта и машинного обучения** |
| **Тема: Введение в искусственный интеллект и машинное обучение** |
| *Основные понятия* |
| *Типы задач машинного обучения* |
| *Жизненный цикл ML-системы* |
| *Области применения AI* |
| **Тема: Обзор правового регулирования и стандартов в сфере искусственного интеллекта** |
| *Существующие стандарты* |
| *Проекты стандартов* |
| *Правовое регулирование использования технологий искусственного интеллекта* |
| **Тема: Генеративный ИИ и безопасность** |
| *Основы генеративного ИИ* |
| *Архитектуры и подходы* |
| *Угрозы генеративного ИИ* |
| *Защита LLM-систем* |

| |
|---|
| **Тема: Данные и подготовка данных** |
| **Типы данных** |
| **Качество данных** |
| **Предобработка данных** |
| **Feature Engineering** |
| **РАЗДЕЛ: Алгоритмы, оценка и объяснимость** |
| **Тема: Основные алгоритмы машинного обучения** |
| *Обучение с учителем* |
| *Деревья решений и ансамбли* |
| *Другие алгоритмы* |
| *Обучение без учителя* |
| *Введение в нейронные сети* |
| **Тема: Метрики и оценка моделей** |
| *Базовые метрики* |
| *Матрица ошибок* |
| *ROC и PR-кривые* |
| *Валидация моделей* |
| *Метрики в задачах ИБ* |
| **Тема: Объяснимый искусственный интеллект** |
| *Основы explainability* |
| *Типы объяснимости* |
| *Методы объяснения* |
| *Ограничения explainability* |
| **РАЗДЕЛ: Применение ИИ в информационной безопасности** |
| **Тема: Применение ML в информационной безопасности** |
| *Анализ сетевого трафика* |
| *Обнаружение вредоносного ПО* |
| *Анализ поведения пользователей (UEBA)* |
| *Обнаружение атак и инцидентов* |
| **Тема: Безопасность машинного обучения** |
| *Угрозы ML-системам* |
| *Утечки и атаки на модели* |
| *Защита ML-систем* |
| *Мониторинг моделей* |
| **РАЗДЕЛ: Практические кейсы применения искусственного интеллекта в информационной безопасности** |
| **Тема: Анализ сетевого трафика** |
| **Тема: Обнаружение вредоносных файлов** |