Международный центр образования НЦОТ

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Применение технологий искусственного интеллекта и машинного обучения в информационной и кибербезопасности

Продолжительность	Форма получения образования	Стоимость
60 академ. часов	Очная (дневная)	1 700 руб.

Цель программы

Формирование знаний и практических навыков применения готовых моделей искусственного интеллекта и машинного обучения, оценки их результатов и рисков, определения условий безопасного использования ИИ-автоматизаций в организации.

Целевая аудитория

✓Специалисты по информационной безопасности, применяющие или оценивающие готовые решения на основе искусственного интеллекта.

✓Аналитики данных и разработчики программного обеспечения, участвующие в решении задач информационной безопасности.

Преимущества программы

- 32 часа практики с готовыми ИИ-моделями и автоматизациями.
- LLM, RAG и агенты: применение, оценка результатов и безопасность.

Чему вы научитесь

- Применять готовые ИИ-средства для анализа угроз.
- Проверять ответы моделей и оценивать риски ИИ-систем.

ДОКУМЕНТ ПО ИТОГАМ ОБУЧЕНИЯ

Свидетельство о повышении квалификации

государственного образца

Рассрочка для физических лиц

Условия и подробности уточняйте у специалистов центра.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ В ИНФОРМАЦИОННОЙ И КИБЕРБЕЗОПАСНОСТИ

Учебный план

№	Наименование раздела и темы
1.	**ОСНОВЫ ИИ И ВЫБОР ПОДХОДА К РЕШЕНИЮ ЗАДАЧ ИБ**
1.1.	Введение в ИИ и машинное обучение: задачи и возможности в ИБ
1.2.	Генеративный ИИ и LLM: понимание и работа с моделью
1.3.	Основные алгоритмы и готовые модели машинного обучения в ИБ
2.	**ДАННЫЕ И УПРАВЛЯЕМАЯ АВТОМАТИЗАЦИЯ**
2.1.	Данные и подготовка данных для машинного обучения и LLM
2.2.	RAG: поиск и ответы по документам организации
2.3.	Автоматизации на базе LLM: конвейеры, агенты и MCP
3.	**ПРИМЕНЕНИЕ ИИ И ОЦЕНКА РЕЗУЛЬТАТОВ**
3.1.	Метрики и оценка моделей и автоматизаций
3.2.	Объяснимый ИИ и проверка обоснованности выводов
3.3.	Анализ сетевого трафика и журналов с помощью ИИ
3.4.	Обнаружение вредоносных файлов
3.5.	Обнаружение базовых DGA
4.	**БЕЗОПАСНОСТЬ И УСЛОВИЯ ВНЕДРЕНИЯ ИИ**
4.1.	Безопасность систем машинного обучения и LLM
4.2.	Атаки на LLM, RAG и агентов: границы и защита
4.3.	Правовое регулирование и условия применения ИИ в Республике Беларусь
4.4.	Применение ИИ в ИБ: оценка инициатив и внедрение