

Искусственный интеллект и автоматизация в киберзащите

Академия бизнеса EY
Кавказ и Центральная Азия

1 день | 8 академических часа
6 CPD-единиц | 7 CPE-часов

Программа тренинга

Блок 1. Говорим на одном языке

- Что такое информационная безопасность сегодня: сервис, а не продукт
- Многослойная защита и матричный подход (NIST CSF 2.0, ISO 27001)
- Знакомство с SOC: структура, области работы и роль в защите бизнеса

Блок 2. Масштаб киберугроз

- Три вектора атак: человек, процесс, технология
- Разбор реальных кейсов: Salt Typhoon, Supply-chain атаки, SEO-poisoning
- Киберпреступность как третья экономика мира: статистика и цифры

Блок 3. ИИ на стороне злоумышленников

- 5 уровней применения ИИ в кибератаках
- Возможности LLM и Dark LLM уже сегодня
- Дипфейки: подготовленные и в реальном времени

Блок 4. Автоматизация - ключ к противоборству

- Философия автоматизации: от понимания проблемы к решению
- Декомпозиция, workflow и алгоритмы на понятных примерах
- Поколения автоматизации SOC: вчера, сегодня и завтра

Блок 5. Начинаем автоматизировать вместе

- Выявление проблемных зон для автоматизации
- Запуск ресерча в своей области + подарок: промпт для брейншторма
- Use cases: почтовая защита, PM Agent, работа ИБ-аналитика, Claude Cowork

Блок 6. Применяем ИИ уже сегодня

- Промптинг, типы ИИ (генеративный, агентный), RAG и MCP
- Workflow-мышление: проектируем сценарий автоматизации в группах
- Практика: создаём GPTs / Claude Skill / Copilot Agent и проект на n8n

Блок 7. Почему ИИ - не замена, а ассистент

- Human-in-the-loop: финальное решение за человеком
- Один шаг, который можно сделать уже завтра

Цели обучения

- Сформировать единое понимание информационной безопасности, её структуры и ключевых компонентов
- Оценить масштаб и тренды современных киберугроз и их влияние на бизнес
- Получить фундаментальное понимание автоматизации – от философии до конкретных инструментов
- Познакомиться с лучшими мировыми практиками (NIST CSF, MITRE ATT&CK, ISO 27001) на доступных примерах
- Научиться выявлять зоны для автоматизации в своей области и запускать ресерч
- Получить практический опыт работы с ИИ, промптингом и workflow-инструментами



Подробнее



Что вы получите в результате обучения

- Фундаментальное понимание информационной безопасности: структура, ландшафт, угрозы и тренды
- Чёткое понимание феномена автоматизации и умение применять современные подходы для развития процессов
- Детализированное знакомство с ИИ – генеративным, агентным и мультиагентным
- Практические навыки: промптинг, создание GPTs / Claude Skill / Copilot Agent, работа с n8n
- Готовый ИИ-проект, созданный на тренинге
- Промпт-запрос или ИИ-skill для брейншторма автоматизации (подарок от спикера)
- Документ с полезными ссылками на лучшие AI- и workflow-сервисы

Как проходит обучение

- Интерактивно, с фокусом на практическое применение полученных знаний
- Включает групповые дискуссии, командные и индивидуальные задания, самопрезентации, ролевые игры

Тренеры

Тренинг проводит команда бизнес-тренеров Академии бизнеса EY. Тренеры обладают богатым практическим опытом, а также международными квалификациями ACCA, ACCA DiplFR(Rus), CFA®, CIA®, CIMA®, DiplPSAS, IPMA®, MBA, MBTI®, PMP® и др.

Запросить CV тренера и задать вопросы о тренинге: academy@kz.ey.com

Для кого этот тренинг

- IT-специалисты, которые хотят понять, как ИИ меняют ландшафт кибербезопасности
- Технические и нетехнические сотрудники, взаимодействующие с системами информационной безопасности
- Все, кто хочет научиться применять ИИ для автоматизации рабочих процессов уже сегодня

Форматы участия

Для участия необходим ноутбук с Power BI и Python последней версии с библиотеками pandas, numpy, requests, доступ в интернет, аккаунт в ChatGPT

Открытый формат

Тренинг проводится по расписанию Академии бизнеса EY с 10:00 до 17:00 с перерывом на обед и двумя кофе-брейками.

Корпоративный формат

Программа может быть адаптирована и проведена специально для Вашей компании.

- предварительный анализ потребностей в обучении, определение целей и задач
- гибкий подход к выбору места, сроков и времени проведения тренинга
- адаптация тренинга с учетом отраслевой специфики
- отчет о результатах тренинга по запросу клиента

