UNIVERSITY OF CENTRAL ASIA

Курс «Специалист Кибербезопасности»
UCA Executive Education

Курс «Специалист кибербезопасности» от UCA Executive Education - это уникальная образовательная программа, разработанная экспертами-практиками, чтобы быстро и эффективно ввести вас в мир кибербезопасности.

Вы изучите современные угрозы, научитесь защищать системы, проводить анализ уязвимостей и реагировать на инциденты. Программа охватывает и защитные (Blue Team), и атакующие (Red Team) подходы, а также отдельные модули по Linux, Windows, сетям и пентесту.

Практическая направленность, реальные сценарии, работа с профессиональными инструментами (SIEM, EDR, Metasploit, Wireshark, PowerShell, BurpSuite, Cisco Packet Tracer и др.) - всё это поможет вам не просто понять, а научиться делать.

Подходит как новичкам, так и специалистам, стремящимся усилить свою позицию в кибербезопасности.

01. Введение в кибербезопасность

Модуль о методах и инструментах тестирования на проникновение. Включает весь цикл: от разведки до написания отчётов. Вы прикоснётесь к миру кибербезопасности перед тем как погрузиться в обучение.

- Основы информационной безопасности
- Разведка и сканирование, OSINT
- Техники эксплуатации уязвимостей
- Повышение привилегий в ОС Windows
- Повышение привилегий в ОС Linux
- Методы защиты информации
- Законодательно правовые аспекты кибербезопасности

02. Linux для безопасности

Изучение Kali и Ubuntu. Управление пользователями, настройка сервисов, защита, скрипты, атаки и защита Linux-среды.

- Введение в администрирование ОС Linux
- Основы управления ОС с помощью командной строки
- Управление пользователями и группами
- Файловая система Linux
- Настройка сети
- Установка и настройка почтового и веб-сервера
- Введение в контейнеризацию (Docker)
- Основные типы атак на ОС Linux
- Укрепление и защита сервера

03. Компьютерные сети на базе Cisco

Базовые принципы сетей, IP-адресация, маршрутизация, протоколы, Wireshark, безопасность и архитектура сетей, Cisco Packet Tracer.

- Введение в сетевое администрирование
- Конфигурация сетевых устройств Cisco
- Протоколы и модели
- Полный обзор модели OSI
- Маршрутизация и сегментация сети
- Основы безопасности сети
- Обнаружение и блокировка вредоносного трафика

04. Windows для безопасности

Основы администрирования и защиты Windows. Active Directory, PowerShell, уязвимости, атаки и защита.

- Введение в администрирование ОС Windows
- Настройка сети
- Установка и настройка веб-сервера
- CMD и PowerShell I
- CMD и PowerShell II
- CMD и PowerShell III
- Active Directory I
- Active Directory II
- Основные типы атак на ОС Windows
- Укрепление и защита сервера
- Форензика Windows и реагирование на инциденты

05. Blue Team/Defensive

Оборонительные меры: мониторинг, SIEM, инциденты, форензика, защита AD, EDR, анализ вредоносного ПО.

- Введение в Blue Team
- Управление логами и SIEM I
- Управление логами и SIEM II
- Анализ угроз и противодействие разведке злоумышленников
- Защита сети – продвинутый уровень
- Защита конечных точек (EDR)
- Реагирование на инциденты – продвинутый уровень
- Основы анализа вредоносных программ
- Active Directory Security – продвинутый уровень
- Выпускной проект – Расследование инцидента и написание подробного отчета

06. Red Team/Offensive

Атакующие техники: разведка, эксплуатация уязвимостей, постэксплуатация, эскалация привилегий, атаки на Windows/Linux/AD, социальная инженерия, мобильный пентест.

- Введение в пентест
- Разведка и сканирование, OSINT
- Техники эксплуатации уязвимостей – продвинутый уровень
- Повышение привилегий в ОС Windows

- Повышение привилегий в ОС Linux
- Техники закрепления в системе
- Тестирование на проникновение Android приложений
- Основы Python для пентестера I
- Основы Python для пентестера II
- Выпускной проект – Пентест веб-приложения