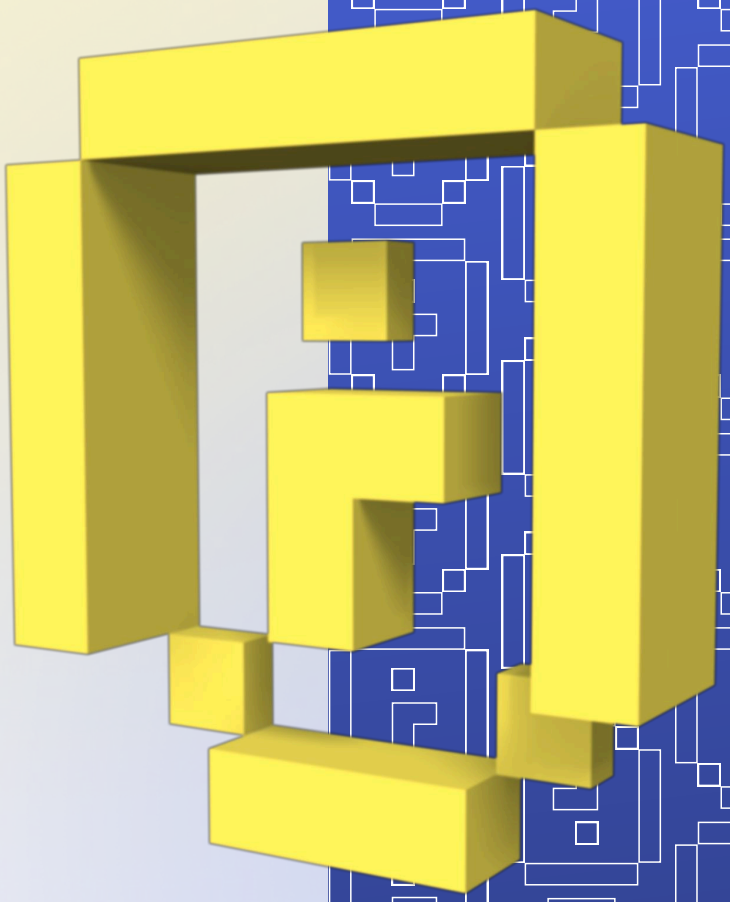
interactive range

Силлабус

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ



+7 700 792 38 44
г. Астана, ул. Дінмухаммед Қонаев 2,
БЦ “ССС”, 3 этаж
sales@cyberlabs.kz
cyberlabs.kz
@interactiverange

2025

1. Общая информация о платформе

Interactive Range — это симуляционная платформа практического обучения по кибербезопасности от новичка до эксперта.

- Выделенная и изолированная среда для каждого участника.
- Симуляция корпоративной инфраструктуры, использование реальных систем и приложений.
- Масштабируемость и доступ через веб-браузер.
- Библиотека готовых сценариев.
- Поддержка современных технологий (актуальные CVE, MITRE ATT&CK, NIST).

2. Методология обучения

Обучение на платформе Interactive Range основано прежде всего на практике, а теория и видеоматериалы используются для поддержки и закрепления знаний. Такой подход позволяет максимально приблизить процесс обучения к условиям реальной работы специалиста по кибербезопасности.

Компоненты методологии:

- Практические лабораторные работы — ключевой элемент курса. Студенты выполняют задания в виртуальной среде, отрабатывая реальные сценарии атак и защиты.
- Red Team / Blue Team тренировки — моделирование кибератак и реагирования в командном формате.
- Capture the Flag (CTF) — задачи для закрепления навыков поиска и эксплуатации уязвимостей.
- Теоретические материалы — структурированные модули, которые дают необходимую базу.
- Видеоматериалы — лекции и демонстрации для пояснения ключевых тем и примеров из практики.

Подход обучения:

- Основной упор: 70% практика.
- Теория и видео (30%) помогают подготовиться к практическим заданиям и лучше понять применяемые техники.
- Цикл обучения: ознакомление с материалом → выполнение лабораторной работы → разбор сложных вопросов с ментором → закрепление знаний.
- Все ресурсы и практики доступны студенту онлайн 24/7.

3. Целевая аудитория

Курс разработан для:

- Новичков — для тех, кто только начинает свой путь в ИТ и кибербезопасности. Программа поможет освоить базовые знания, получить практический опыт и сформировать необходимые навыки для старта карьеры в сфере информационной безопасности.
- IT-специалистов — для тех, кто уже работает в смежных областях (системное администрирование, сетевые технологии, разработка и др.) и хочет переквалифицироваться, чтобы перейти в кибербезопасность или расширить свои компетенции для карьерного роста.
- Профессионалов в ИБ — для специалистов, которые уже работают в сфере безопасности и стремятся повысить уровень квалификации, изучить современные подходы и инструменты, а также отработать навыки противодействия реальным киберугрозам в практических лабораториях.

4. Авторы программы платформы

Данияр Касенов, CEO CyberLabs — выпускник Rochester Institute of Technology (RIT), New York, USA, имеет более 10 лет опыта в сфере информационной безопасности. Обладатель международной сертификации OSCP. Участвовал в создании первого в Казахстане Security Operation Center (SOC) для EXPO 2017. Спикер профильных конференций: DEFCON, KazHackStan, SOCFORUM. Руководит разработкой и внедрением SaaS-платформы Interactive Range, которая используется для практического обучения, моделирования атак и отработки инцидентов. В рамках курса отвечает за стратегическое развитие, методологию и практическую направленность программы.

Диас Жумашев — эксперт по информационной безопасности и контент-менеджер курса. Более 6 лет опыта в сфере ИБ. Обладатель сертификатов OSCP, CWAPT, PT1. Победитель и призёр международных соревнований: Standoff (SPIEF, BRICS), GISEC WorldRecordCTF, Cyberkumbez Kazhackstan, AITU Military CTF, а также Bug Bounty-программ. В курсе отвечает за подготовку учебных материалов и практических лабораторных заданий, основанных на современных методиках и актуальных сценариях кибератак.

КУРС “ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ”

5. Подробнее о курсе

Курс создан для тех, кто хочет освоить базовые знания и практические навыки в сфере информационной безопасности. Программа сочетает теорию и практику через лабораторные работы и реальные сценарии, что позволяет студентам шаг за шагом познакомиться с ключевыми направлениями киберзащиты: от Linux и OSINT до веб-безопасности и цифровой криминалистики.

6. Цель и задачи курса

Цель курса – сформировать у студентов прочную базу знаний и навыков, необходимых для старта карьеры в кибербезопасности.

Задачи курса:

- Изучить основы работы с Linux и сетевыми инструментами.
- Получить практические навыки разведки (OSINT) и анализа логов.
- Освоить базовые методы криптографии и взламывания паролей.
- Познакомиться с процессами сканирования, анализа трафика и цифровой криминалистики.
- Понять основы защиты веб-приложений и эксплуатации уязвимостей.

7. Навыки по завершению обучения

По завершении курса студенты смогут:

- Работать с Linux и базовыми инструментами системного администрирования.
- Применять OSINT для поиска и анализа информации.
- Использовать криптографические методы для защиты данных.
- Проводить аудит безопасности паролей и анализировать логи.
- Настраивать сканирование и анализировать сетевой трафик.
- Понимать принципы цифровой криминалистики.
- Оценивать безопасность веб-приложений и выявлять уязвимости.
- Работать с инструментами для эксплуатации и тестирования систем.

8. Карьерные возможности студентов

После прохождения курса выпускники смогут претендовать на стартовые должности в сфере информационной безопасности, среди которых:

- Специалист по информационной безопасности (Junior Level)
  Выпускник сможет выполнять базовые задачи по защите информационных систем: настройка политик безопасности, работа с антивирусами и системами мониторинга, участие в расследовании инцидентов, ведение отчетности. Такие специалисты часто входят в команду SOC (Security Operations Center) или ИТ-отдел компании.
- Помощник пентестера (Junior Penetration Tester Assistant)
  Выпускник получит навыки поиска уязвимостей и проведения простых тестов на проникновение под руководством более опытного специалиста. Он сможет работать с инструментами для сканирования сетей и веб-приложений, составлять отчеты о найденных проблемах и помогать в подготовке к аудитам безопасности.
- Системный администратор с уклоном в безопасность
  Такой специалист будет отвечать не только за настройку и поддержку серверов и сетевой инфраструктуры, но и за их базовую защиту: управление учетными записями, настройка прав доступа, обновления и патчи, резервное копирование, контроль логов и базовые меры по защите инфраструктуры от атак.

9. Программа курса

Тема 1. Linux 101
- Linux 101
- Лабораторная работа 1: Введение в Linux

Тема 2. Разведка / OSINT
- Разведка / OSINT
- Лабораторная работа 2: OSINT

Тема 3. Криптография
- Криптография
- Лабораторная работа 3: Криптография

Тема 4. Взламывание паролей
- Взламывание паролей
- Лабораторная работа 4: Взламывание паролей

КУРС “ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ”

Тема 5. Анализ логов
- Анализ логов
- Лабораторная работа 5: Анализ логов

Тема 6. Сканирование
- Сканирование
- Лабораторная работа 6: Intro to NMAP

Тема 7. Анализ сетевого трафика
- Анализирование сети
- Лабораторная работа 7: Анализ сетевого трафика

Тема 8. Форензика
- Форензика
- Лабораторная работа 8: Форензика

Тема 9. Промежуточный тест
- KK — Промежуточный тест

Тема 10. Безопасность веб-приложений
- Безопасность веб-приложений
- Лабораторная работа 9: Безопасность веб-приложений

Тема 11. Перечисление и эксплуатация
- Перечисление и применение эксплоитов
- Лабораторная работа 10: Initial Access — Meterpreter