Силлабус по курсу
«Red Team»

1. Наименование школы*[1]

📋 **Инструкция:** Укажите полное официальное название школы.
📐 **Формат:** *Текст*
💡 *Например: ТОО «Coding»*

✏️ **Заполните ниже:**
ТОО “CyberLabs”

2. Наименование курса*

📋 **Инструкция:** Укажите полное официальное название курса. Название должно быть чётким, кратким и отражать основное содержание программы.
📐 **Формат:** *Текст*
💡 *Например: «Основы Python для начинающих», «Full-Stack веб-разработка на JavaScript»*

✏️ **Заполните ниже:**
Red Team

3. Цели и задачи Курса*

📋 **Инструкция:** Опишите основные цели и задачи курса.
Рекомендуется разделить цели и задачи на два подраздела.
📐 **Формат:** *Текст, 2–4 абзаца или маркированный список*

✏️ **Заполните ниже:**
Цели:

Подготовка специалистов в области наступательной кибербезопасности, способных выявлять уязвимости, моделировать действия злоумышленников и оценивать уровень защищённости информационных систем. Курс направлен на формирование практических навыков этичного хакинга, тестирования на проникновение и анализа безопасности корпоративной инфраструктуры.

Задачи:

- Изучение методов разведки, сканирования и сбора информации.
- Освоение техник эксплуатации уязвимостей и пост-эксплуатации.
- Изучение атак на веб-приложения и инфраструктуру Active Directory.
- Получение навыков работы с инструментами Red Team и Bug Bounty.
- Формирование понимания методов обхода защитных механизмов и моделирования атак.
- Ознакомление с современными уязвимостями и практиками повышения защищённости систем.

[1*] Поля, обязательные для заполнения

4. Уровень курса*

📋 **Инструкция:** Укажите уровень курса (выберите один из вариантов)

✔ **начинающий** ☐ профессиональный/продвинутый

☐ продолжающий ☐ для всех

5. Язык обучения*

📋 **Инструкция:** Укажите язык обучения (выберите один из вариантов)

☐ казахский ✔ **русский** ☐ английский

6. Формат проведения занятий*

📋 **Инструкция:** Укажите формат: онлайн / оффлайн / гибрид). Уточните детали: запись лекций, живые вебинары, очные практикумы и т.д.

📐 **Формат:** *Текст, 2–4 предложения*

✔ онлайн ☐ оффлайн ☐ гибрид

Уточните детали:

Обучение проводится в онлайн-формате с использованием образовательной платформы и практических лабораторий. Студентам предоставляется доступ к видеолекциям, учебным материалам и практическим заданиям для самостоятельного изучения.

7. Продолжительность курса в неделях и академических часах*

📋 **Инструкция:** Укажите общую продолжительность курса в неделях и общее количество академических часов (1 ак. час = 45 минут).

📐 **Формат:** *Число, 2 строки*

💡 *Например: 12 недель*
96 академических часов

✏️ **Заполните ниже:**

27 недель

270 академических часов

8. Старт обучения*

📋 **Инструкция:** Укажите планируемый месяц или период начала обучения.

📐 **Формат:** *текст, 1 строка*

💡 *Например: сентябрь, 2026г. или первая декада октября 2026г.*

✏️ **Заполните ниже:**
октябрь, 2026 г.

9. Стоимость курса*

📋 **Инструкция:** Укажите полную стоимость курса.
📐 **Формат: Текст и число**
Например: Стоимость курса “Cyber security” – 500.000 тенге

✏️ **Заполните ниже:**
Стоимость курса “Red Team” – 400.000 тенге

10. Особые условия*

📋 **Инструкция:** Укажите критерии отбора студентов (при наличии).
Опишите особые условия: скидки, рассрочка, депозитная система, предоплата, гарантийный взнос.
Отдельно распишите условия для студентов из Листа Ожидания.
📐 **Формат:** *Текст (3–6 предложений) или таблица*

✏️ **Заполните ниже:**
Особые условия:

Критерии отбора студентов (при наличии): Для поступления на курс Red Team кандидаты проходят предварительный отбор, направленный на выявление базовых технических знаний, аналитического мышления и высокой мотивации к развитию в сфере кибербезопасности.

Отбор осуществляется на основе анализа резюме кандидатов, где учитываются уровень подготовки, предыдущий опыт, участие в профильных проектах, соревнованиях и наличие технических навыков. Дополнительно оцениваются результаты выполнения CTF-заданий (Capture The Flag) — практических задач, позволяющих определить уровень владения инструментами информационной безопасности, навыки поиска уязвимостей, анализа систем и решения нестандартных технических задач.

Такой подход позволяет формировать группы из наиболее мотивированных и перспективных участников, готовых к интенсивному практическому обучению в направлениях наступательной и оборонительной кибербезопасности.

11. Описание Курса*

📋 **Инструкция:** представьте информацию по курсу в 5–7 предложениях. Раскройте чему посвящён курс, для кого предназначен, какие ключевые темы охватываются, какой результат получит студент после завершения. Описание курса будет размещено на витрине.
📐 **Формат:** *Текст, 5–7 предложений*

✏️ **Заполните ниже:**
Курс «Red Team — Основы этичного хакинга» направлен на формирование практических навыков поиска и эксплуатации уязвимостей в реальных ИТ-системах. В рамках обучения участники изучают основы сетевой безопасности: методы сбора информации, сканирования, проведения разведки, MITM-атаки, а также подходы к оценке уязвимостей и пост-эксплуатации. Отдельный блок посвящен безопасности веб-приложений, включая разбор

ключевых уязвимостей из OWASP Top 10, таких как XSS, SQL-инъекции, ошибки аутентификации и SSRF.

Также курс охватывает атаки на инфраструктуру Active Directory: от этапов разведки и получения доступа до закрепления в системе и проведения полноценного Red Teaming. Участники познакомятся с методами социальной инженерии и их применением в атаках. В завершение рассматриваются основы Bug Bounty, включая техники обхода защитных механизмов (WAF) и анализ реальных кейсов уязвимостей на основе известных CVE. Курс ориентирован на практику и помогает сформировать мышление атакующего для повышения уровня защиты систем.

12. Преимущества Курса*

📋 **Инструкция:** Опишите ключевые преимущества и уникальные особенности курса по сравнению с аналогами.

📐 **Формат:** *Маркированный список, 3–10 пунктов*

✏️ **Заполните ниже:**

- Практико-ориентированное обучение: курс состоит на 70% из практики и моделирует реальные сценарии кибератак и защиты инфраструктуры.
- Обучение проходит на собственной платформе киберполигона Interactive Range с персональной виртуальной средой для каждого участника.
- Использование сценариев, основанных на реальных техниках атак и матрице MITRE ATT&CK, а также актуальных CVE и современных методов эксплуатации уязвимостей.
- Доступ к учебным материалам, видеолекциям и лабораторным работам 24/7 с возможностью ежедневной онлайн-практики.
- Реалистичная симуляция корпоративной инфраструктуры, включая сети, Active Directory, веб-приложения и средства защиты.
- Сопровождение ментора на протяжении всего обучения с отслеживанием прогресса и поддержкой студентов.
- Оценка навыков через практические задания, лабораторные работы и CTF-задачи, приближенные к реальным кейсам из сферы кибербезопасности.

13. Содержание Курса. Разбивка по темам и модулям*

📋 **Инструкция:** Распишите содержание курса по модулям и темам, с указанием длительности, количества часов. Для каждого модуля укажите: номер, название, перечень тем. Используйте таблицу из Приложения 1 или свободный формат. Этот раздел может занимать несколько страниц.

📐 **Формат:** *Таблица или структурированный список, 1–5 страниц*

✏️ **Заполните ниже:**

КУРС RED TEAM – ОСНОВЫ ЭТИЧНОГО ХАКИНГА

Раздел: Сетевая безопасность

• Сбор информации

• Сканирование
• Разведка
• MITM атаки
• Оценка уязвимости и эксплуатация
• Пост эксплуатация
• Социальная инженерия

Раздел: Безопасность веб-приложений
• Введение в OWASP TOP10
• Нарушение контроля доступа (Broken access control)
• Недочеты криптографии (Cryptographic Failure)
• Инъекции (Injections)
• Небезопасный дизайн (Insecure Design)
• Небезопасная конфигурация (Security Misconfiguration)
• Использование уязвимых или устаревших компонентов (Vulnerable and outdated components)
• Ошибки идентификации и аутентификации (Identification and Authentication Failures)
• Нарушения целостности программного обеспечения и данных (Software and Data integrity Failures)
• Ошибки логирования и мониторинга безопасности (Security logging and Monitoring Failures)
• Подделка запросов на стороне сервера (Server-Side Request Forgery)

Раздел: Атаки на AD инфраструктуру
• Атака через социальную инженерию
• Расширенная разведка AD
• Атаки MITM
• Получение доступа
• Red Teaming Active Directory
• Закрепление в среде

Раздел: Основы Bug Bounty
• Введение в BugBounty
• Практические примеры
_ CVE-2019-15107 - WebMin
_ CVE-2023-23752 - Joomla
_ CVE-2021-43008 - AdminerRead SSRF
_ CVE-2018-8715 - AppWeb
_ CVE-2024-23897 - Jenkins

14. Методы обучения*

📋 **Инструкция:** опишите методы обучения: лекции, практические занятия, менторство, проектная работа, кейс-стади, групповая работа и т.п.. Укажите соотношение теории и практики.

📐 **Формат:** *Текст*

✏️ **Заполните ниже:**

Обучение на курсе построено по практико-ориентированному подходу: 70% программы составляют практические занятия и 30% — теоретическая подготовка. Теоретическая часть включает видеолекции, разбор ключевых тем по кибербезопасности, изучение современных техник атак и методов защиты, а также анализ реальных кейсов и актуальных CVE.

Практическая подготовка проходит на платформе Interactive Range в формате лабораторных работ, симуляции атак, CTF-задач и выполнения сценариев, приближенных к реальным инцидентам информационной безопасности. Студенты работают в собственной виртуальной среде, где отрабатывают навыки тестирования на проникновение, эксплуатации уязвимостей, анализа инфраструктуры и реагирования на угрозы.

В процессе обучения предусмотрено сопровождение менторов, проведение живых онлайн-разборов, консультаций и практических сессий. Особое внимание уделяется обучению через практику, самостоятельное решение задач и моделирование действий в условиях, максимально приближенных к реальной корпоративной среде.

15. Информация о преподавательском составе*

📋 **Инструкция:** По каждому преподавателю укажите: ФИО, специализацию, опыт в отрасли, опыт преподавания, краткую биографию (3–5 предложений). Используйте таблицу из Приложения Б или свободный формат. При большом количестве преподавателей раздел может занимать несколько страниц.

📐 **Формат:** *Таблица или текст по каждому преподавателю, 1–3 страницы*

✏️ **Заполните ниже:**

Данияр Касенов — CEO компании CyberLabs, выпускник Rochester Institute of Technology (RIT, Нью-Йорк, США) с более чем 10-летним опытом в области информационной безопасности. Является спикером на международных и локальных конференциях по кибербезопасности, включая DEFCON 2016, DEFCON Almaty 2016 (Buffer Overflow vulnerability), участие в проекте EXPO 2017 в качестве SOC-эксперта, а также выступления на SOCFORUM 2019 и KazHackStan 2019.

16. Приобретаемые навыки и квалификация по окончании учёбы*

📋 **Инструкция:** перечислите все конкретные навыки (hard skills и soft skills), которые студент приобретёт в результате обучения. Группируйте по категориям, если это необходимо.

📐 **Формат:** *Маркированный список, 5–20 пунктов*

✔ Junior ☐ Middle ☐ Senior

✏️ **Заполните ниже:**

Навыки, которые будут приобретены после завершения обучения на курсе (перечислить):

Hard Skills

- Проведение разведки, сбора информации и сканирования инфраструктуры.
- Выполнение тестирования на проникновение (Penetration Testing) в контролируемой среде.
- Выявление и эксплуатация уязвимостей в сетях, веб-приложениях и Active Directory.
- Работа с уязвимостями из OWASP Top 10, включая XSS, SQL Injection, SSRF и ошибки аутентификации.
- Проведение MITM-атак и анализ сетевого трафика.
- Использование инструментов Red Team и фреймворков для моделирования атак.
- Навыки пост-эксплуатации и закрепления в инфраструктуре.
- Анализ и эксплуатация реальных CVE и уязвимых сервисов.
- Понимание принципов Bug Bounty и методов обхода защитных механизмов (WAF).
- Проведение атак и разведки в инфраструктуре Active Directory.
- Настройка и использование виртуальных лабораторий и киберполигонов.
- Работа со сценариями на основе MITRE ATT&CK и моделирование действий злоумышленников.
- Базовые навыки обнаружения и противодействия AI-усиленным атакам.
- Практический опыт решения задач Capture The Flag (CTF).

Soft Skills

- Аналитическое и критическое мышление при исследовании уязвимостей и инцидентов.
- Навыки решения нестандартных задач в условиях, приближенных к реальным кибератакам.
- Развитие мышления атакующего для оценки защищённости систем.
- Работа в команде и взаимодействие в рамках сценариев Red Team / Blue Team.
- Навыки самостоятельного исследования и поиска информации.
- Способность быстро адаптироваться к новым угрозам и технологиям.
- Навыки коммуникации и взаимодействия с менторами и участниками команды.
- Умение работать в условиях ограниченного времени и повышенной нагрузки при выполнении практических задач и киберучений.

17. Платформа для проведения обучения*

📋 **Инструкция:** Укажите основную платформу, на которой будет проходить обучение (Zoom, Google Meet, LMS и т.д.),а также все дополнительные инструменты, которые будут использоваться в учебном процессе. Укажите наличие лицензий на используемые платформы, инструменты, возможность обеспечения доступа для студентов.

📐 **Формат: Ссылки, текст.**

✏️ **Заполните ниже:**

Наличие специальной LMS платформы для обучения по Курсу: ✔ Да ☐ Нет

Наименование платформы: Interactive Range

Необходимость получения лицензии для использования платформы: нет

Доступность платформы для студентов: Платформа предоставляет студентам круглосуточный доступ (24/7) к видеолекциям, лабораторным работам, виртуальным машинам, сценариям атак и учебным материалам через веб-браузер без необходимости развертывания собственной инфраструктуры.

18. Самостоятельная работа студента*

📋 **Инструкция:** Опишите кратко каким образом будет проводиться контроль за прогрессом и процессом обучения студента - частоту и объём домашних заданий, работа по проекту(проектам), тестирование и т.п. Опишите формат итоговой работы (проект, экзамен, тест, защита). Если итоговая работа — проект, опишите требования к нему.

📐 **Формат:** *Текст*

✏️ **Заполните ниже:**

Контроль прогресса студентов осуществляется на протяжении всего обучения через выполнение практических лабораторных работ, домашних заданий, мини-тестов и CTF-зач. Менторы курса отслеживают активность студентов, качество выполнения заданий и уровень освоения практических навыков в виртуальной среде.

Итоговая аттестация проводится в формате онлайн-тестирования и практического задания, направленного на проверку навыков поиска и эксплуатации уязвимостей, анализа инфраструктуры и выполнения сценариев Red Team. Оценка включает как технические знания, так и способность применять их в условиях, приближенных к реальным киберинцидентам.

19. Система оценки успеваемости студентов*

📋 **Инструкция:** Опишите систему оценивания, способ проверки (автоматически / преподавателем / код-ревью / peer review), шкалу оценок, критерии успешного завершения, минимальные проходные баллы, условия получения сертификата. Можно оформить в виде таблицы.

📐 **Формат:** *Текст или таблица.*

✏️ **Заполните ниже:**

Система оценивания студентов включает проверку теоретических знаний и практических навыков на протяжении всего периода обучения. Контроль осуществляется через выполнение лабораторных работ, домашних заданий, мини-тестов и практических CTF-задач в виртуальной среде киберполигона. Проверка заданий проводится как автоматически средствами платформы, так и преподавателями и менторами курса.

Особое внимание уделяется практической подготовке студентов: оценивается способность выявлять уязвимости, выполнять тестирование на проникновение, анализировать инфраструктуру и применять инструменты Red Team в условиях, приближенных к реальным киберинцидентам. Менторы курса также отслеживают активность, прогресс и качество выполнения практических заданий.

Сертификат выдается студентам, успешно завершившим программу обучения и выполнившим все обязательные требования курса.

20. Партнеры Курса (при наличии)

📋 **Инструкция:** Укажите компании-партнёры. Опишите характер партнёрства и преимущества от этого партнерства для студентов.

📐 **Формат:** *Текст или список*

✏️ **Заполните ниже:**

Партнёрство платформы Interactive Range выстроено в формате устойчивой экосистемы взаимодействия с государственными организациями, образовательными учреждениями, технологическими компаниями и международными

сертификационными центрами. Среди ключевых партнёров — CompTIA, Classera, ORLEU, Государственная техническая служба, а также Inova Tech и другие индустриальные и академические организации. Дополнительно взаимодействие с государственными структурами, включая профильные органы в сфере информационной безопасности, усиливает практическую направленность обучения.

Такой формат партнёрства позволяет интегрировать в обучение актуальные отраслевые стандарты, реальные кейсы и требования рынка к специалистам по кибербезопасности. Студенты получают доступ к сертификационным возможностям международного уровня (например, CompTIA), а также к программам поддержки. Благодаря сотрудничеству с индустриальными партнёрами расширяются возможности прохождения практики, стажировок и дальнейшего трудоустройства в IT и SOC-командах.

Кроме того, партнёрская сеть обеспечивает актуализацию учебных сценариев и лабораторий в соответствии с реальными угрозами и технологиями, используемыми в отрасли. Это позволяет студентам работать с приближёнными к реальности кейсами, повышая их конкурентоспособность на рынке труда и ускоряя профессиональную адаптацию после завершения обучения.

21. Иная информация

📋 **Инструкция:** Укажите дополнительную информацию для демонстрации качества курса: отзывы выпускников, рейтинги, статистика трудоустройства, награды, публикации и т.д.
📐 **Формат: текст**

✏️ **Заполните ниже:**
Программа обучения разработана компанией CyberLabs, имеющей более 10 лет опыта в области информационной безопасности и практической подготовки специалистов по кибербезопасности. Обучение проводится на собственной платформе-криполигоне Interactive Range, которая используется для моделирования реальных сценариев атак и защиты инфраструктуры.

22. Контактные данные*

📋 **Инструкция:** Укажите: телефон, e-mail, адрес, сайт, ссылки на социальные сети.
📐 **Формат:** *Текст, 3–5 строк*

✏️ **Заполните ниже:**
sales@cyberlabs.kz
cyberlabs.kz

87007923844

https://www.instagram.com/interactiverange/

Юр.адрес: 01000, Казахстан, г. Астана, район Есиль, улица Дінмұхамед Конаев, здание 2, БЦ "CCC"