Силлабус по курсу
«Blue 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:**
Blue 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:

Курс «Blue Team» направлен на подготовку специалистов в области кибербезопасности, способных эффективно защищать корпоративную ИТ-инфраструктуру от современных киберугроз. Основная цель программы — сформировать у студентов практические навыки обнаружения, анализа и реагирования на инциденты информационной безопасности в условиях, максимально приближенных к реальной инфраструктуре организаций.

Обучение построено на практико-ориентированном подходе с использованием киберполигона Interactive Range, где участники работают с реальными сценариями атак, инструментами мониторинга и системами защиты. Курс позволяет развить системное мышление специалиста Blue Team, понимание жизненного цикла кибератак и методов противодействия злоумышленникам.

Задачи:

[1*] Поля, обязательные для заполнения

- обучить студентов выявлению и анализу киберугроз с использованием современных средств мониторинга и защиты;
- сформировать практические навыки работы с SIEM, IDS/IPS, Threat Intelligence, YARA, Active Directory и другими инструментами защиты;
- научить обнаруживать действия злоумышленников на различных этапах Kill Chain и MITRE ATT&CK;
- освоить методы расследования инцидентов, Threat Hunting и реагирования на атаки;
- развить навыки укрепления инфраструктуры, управления уязвимостями и предотвращения эксплуатации систем;
- подготовить участников к работе в SOC и Blue Team-командах через выполнение практических лабораторных работ и CTF-задач;
- повысить уровень киберосведомленности, аналитического мышления и способности принимать решения в условиях реальных киберинцидентов.

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 “Blue 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 Blue 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 «Blue Team» направлен на развитие практических навыков защиты ИТ-инфраструктуры и эффективного противодействия киберугрозам. Участники изучают процессы обнаружения и реагирования на атаки с использованием современных инструментов, таких как SIEM, IDS/IPS и honeypot, работая в приближенной к реальности лабораторной среде. В рамках курса рассматриваются этапы атаки через призму MITRE ATT&CK, включая доставку и выполнение вредоносного кода, а также методы его предотвращения с применением YARA и политик whitelisting.

Особое внимание уделяется моделированию угроз, управлению уязвимостями (Patch Management), выявлению каналов управления (C2) и защите от перемещения злоумышленников внутри сети, включая атаки на Kerberos. Участники также освоят использование Threat Intelligence для выявления и предотвращения атак, а также методы обмана противника. В завершение курса рассматриваются подходы к Threat Hunting и выстраиванию эффективного процесса реагирования на инциденты. Курс ориентирован на практику и формирует системное мышление защитника.

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 на 70% состоит из лабораторных работ, киберучений и практических заданий в виртуальной среде.
- Обучение на собственном киберполигоне Interactive Range с симуляцией реальной корпоративной инфраструктуры и актуальных сценариев атак.
- Использование современных методологий и фреймворков, включая MITRE ATT&CK, Kill Chain, Threat Intelligence и Threat Hunting.

- Каждый студент получает доступ к индивидуальной изолированной виртуальной среде для безопасной и полноценной практики.
- Программа охватывает реальные инструменты и технологии Blue Team: SIEM, IDS/IPS, YARA, Active Directory, Patch Management и анализ сетевого трафика.
- Курс разработан экспертами-практиками с опытом работы в SOC, международных проектах и выступлений на конференциях DEFCON, SOCFORUM и KazHackStan.
- Обучение построено на реальных сценариях кибератак и расследовании инцидентов, что позволяет студентам получить опыт, приближенный к работе в SOC.
- Сопровождение ментора на протяжении всего обучения, регулярная проверка прогресса и помощь в освоении практических задач.
- Подготовка к востребованным позициям в сфере кибербезопасности: SOC Analyst, Blue Team Specialist, Incident Response Analyst и Threat Hunting Specialist.

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 BLUE TEAM - ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ НА КИБЕР-УГРОЗЫ

Раздел: Введение и разведка

• План курса и ознакомление с лабораторной средой
• Нашумевшие кейсы кибератак
• Эмуляция злоумышленника
• Знакомство с Kill Chain
• Фреймворк MITRE ATT&CK
• Ключевые средства предотвращения и обнаружения
• Построение систем обнаружения
• Разведка - Знакомство с целью

Раздел: Доставка и выполнение зловредного кода/программы.

• Общие механизмы доставки зловредного кода.
• Как препятствовать доставке зловредного кода?
• Съемные носители и сетевое управление.
• Управление почтой, веб-прокси и песочница для вредоносных программ.
• YARA
• Предотвращение выполнения зловредного кода/программы.
• Список разрешенных приложений (whitelisting)
• Выполнение скриптов HTA, PowerShell и др.

• Как обнаружить выполнение зловредного кода?
• Знакомство с ProcFilter

Раздел: Эксплуатация, укрепление в среде и C2
• Защита приложений от эксплуатации
• Жизненный цикл разработки программного обеспечения (SDL) и моделирование угроз
• Patch Management
• Методы защиты от эксплойтов
• Как избежать установки зловредного кода
• Типичные методы укрепления в сети
• Как злоумышленники укрепляются в инфраструктуре
• C2 (command&control)
• Обнаружение каналов управления и контроля – C2

Раздел: Перемещение атакующих в сети
• Защита административного доступа
• Концепции безопасности Active Directory
• Принцип наименьших привилегий и UAC
• Методы повышения привилегий в Windows
• Основные методы атак на AD
• Использование прав локального администратора для угона дополнительных учетных данных
• Bloodhound - Определение векторов атаки AD
• Атаки Kerberos: Kerberoasting, Silver tickets, Over-PtH
• Как обнаружить перемещение в сети?
• Ключевые логи для обнаружения передвижения в AD
• Обман противника

Раздел: Поиск угроз и реагирование на инциденты
• Доминирование в AD - Основные стратегии
• Golden ticket, DCSync и другие
• Обнаружение доминирования в AD
• Общие стратегии угона данных
• Использование Threat Intelligence (TI)
• Поиск угроз и реагирование на инциденты
• Стратегия поиска угроз (Threat Hunting)
• Процесс реагирования на инциденты

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

- Анализ и обнаружение киберугроз в корпоративной инфраструктуре
- Мониторинг событий информационной безопасности с использованием SIEM-систем
- Выявление и анализ подозрительного сетевого трафика
- Реагирование на инциденты информационной безопасности
- Проведение Threat Hunting и поиск скрытых угроз
- Работа с фреймворком MITRE ATT&CK и Kill Chain
- Использование IDS/IPS для обнаружения и предотвращения атак
- Анализ логов Windows, Active Directory и сетевых устройств
- Выявление и расследование атак на Active Directory и Kerberos
- Применение YARA для обнаружения вредоносного кода
- Настройка политик whitelisting и контроля приложений
- Управление уязвимостями и Patch Management
- Обнаружение каналов Command & Control (C2)
- Анализ методов закрепления злоумышленников в инфраструктуре
- Использование Threat Intelligence для выявления угроз
- Проведение расследований инцидентов и подготовка технической отчетности
- Работа в виртуальной лабораторной среде и выполнение CTF-задач

Soft Skills

- Аналитическое и критическое мышление
- Навыки решения сложных технических задач
- Принятие решений в условиях ограниченного времени
- Работа в команде и взаимодействие в SOC/Blue Team
- Навыки коммуникации и технического обсуждения инцидентов
- Внимательность к деталям при анализе угроз и логов
- Самостоятельная работа и исследовательский подход
- Стрессоустойчивость при реагировании на киберинциденты
- Системное мышление и понимание процессов информационной безопасности
- Навыки постоянного самообучения и адаптации к новым угрозам

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 обнаружения и анализа киберугроз, расследования инцидентов и реагирования на атаки в корпоративной инфраструктуре. Практическая часть включает работу в условиях, максимально приближенных к реальным сценариям Blue Team: анализ логов, выявление подозрительной активности, использование SIEM-систем, IDS/IPS и инструментов Threat Intelligence.

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 и анализировать киберугрозы, расследовать инциденты информационной безопасности, анализировать инфраструктуру и применять инструменты Blue Team в условиях, приближенных к реальным киберинцидентам. В рамках практических заданий студенты работают с SIEM-системами, логами, сетевым трафиком и механизмами обнаружения атак, а также отрабатывают сценарии реагирования и локализации угроз.

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"