Курс профессиональной подготовки

Кибербезопасность

Red Team

tech технологический университет

tech технологический университет

Курс профессиональной подготовки

Кибербезопасность

Red Team

- Формат: **онлайн**
- Продолжительность: **6 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

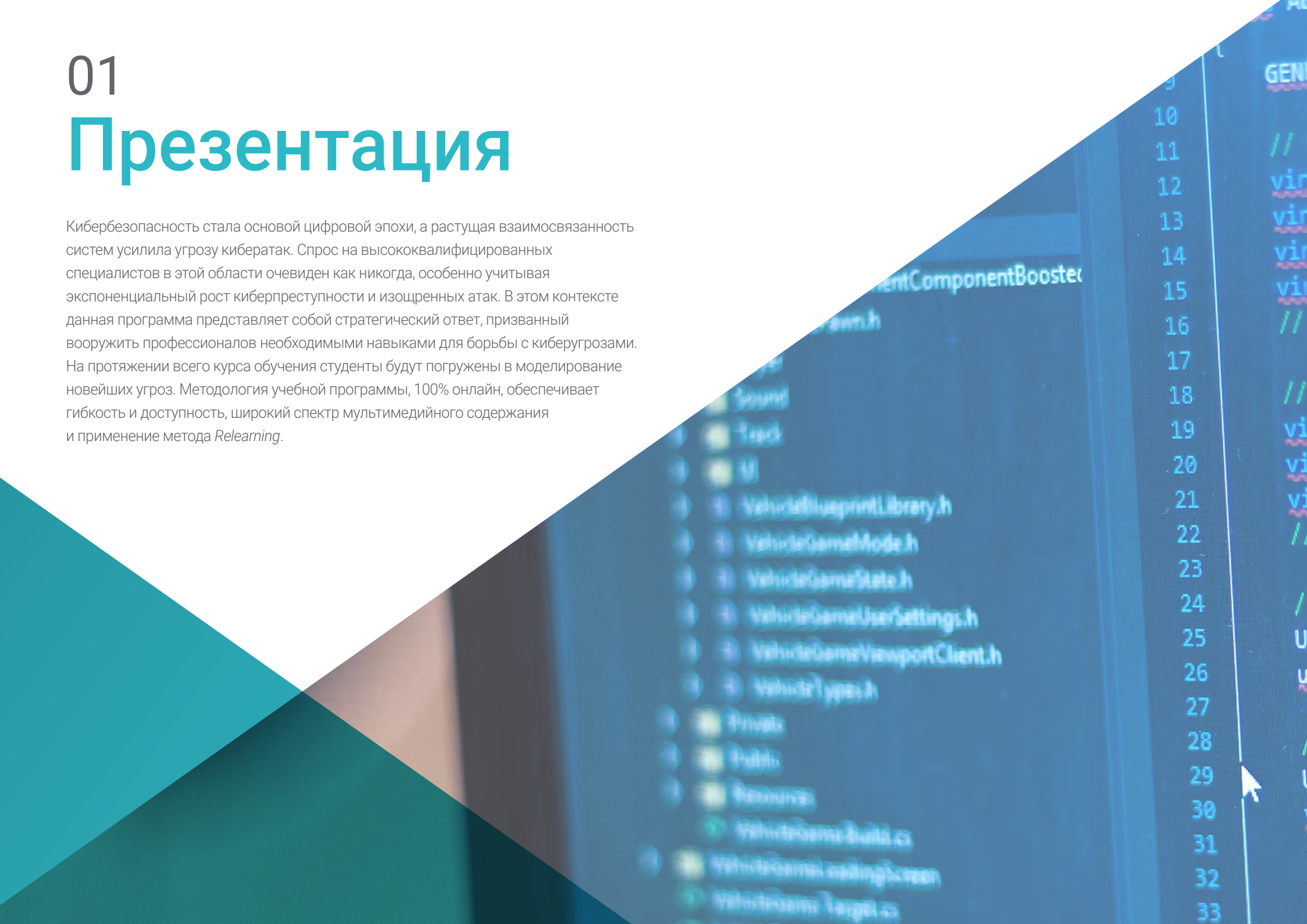
Веб-доступ: www.techtitute.com/ru/infromation-technology/postgraduate-diploma/postgraduate-diploma-red-team-cybersecurity

Оглавление

01

Презентация

Кибербезопасность стала основой цифровой эпохи, а растущая взаимосвязанность систем усилила угрозу кибератак. Спрос на высококвалифицированных специалистов в этой области очевиден как никогда, особенно учитывая экспоненциальный рост киберпреступности и изощренных атак. В этом контексте данная программа представляет собой стратегический ответ, призванный вооружить профессионалов необходимыми навыками для борьбы с киберугрозами. На протяжении всего курса обучения студенты будут погружены в моделирование новейших угроз. Методология учебной программы, 100% онлайн, обеспечивает гибкость и доступность, широкий спектр мультимедийного содержания и применение метода *Relearning*.



Вы внесете свой вклад в повышение уровня кибербезопасности и предотвратите крупные цифровые преступления. Не упустите эту возможность и зарегистрируйтесь прямо сейчас!”

В условиях сложной системы кибербезопасности наличие эксперта в этой области является насущной необходимостью для организаций, стремящихся укрепить свою защиту от постоянно развивающихся угроз. Такой проактивный подход, основанный на постоянном совершенствовании системы безопасности, подчеркивает острую необходимость в экспертах.

Внедрение проактивных мер крайне важно, и специализированное обучение в области Red Team дает профессионалам возможность активно предвидеть, выявлять и устранять уязвимости в системах и сетях. В рамках Курса профессиональной подготовки студент приобретет навыки тестирования на проникновение и симуляции, направленные на выявление и эксплуатацию уязвимостей. В этом смысле они будут не только развивать передовые технические компетенции, но и способствовать эффективному сотрудничеству с командами безопасности, интегрируя стратегии против *вредоносных программных* угроз.

Кроме того, студенты приобретут твердое понимание фундаментальных принципов цифровой криминалистики (DFIR), применимых при разрешении кибер-инцидентов. Кроме того, такой целостный подход к учебной программе гарантирует, что специалисты будут обладать самыми современными навыками в области кибербезопасности.

Эта академическая программа отличается не только содержанием, но и передовой методологией. Она будет доступна студентам полностью в режиме онлайн, что обеспечит им гибкость, необходимую для продвижения по карьерной лестнице без ущерба для их рабочих обязанностей.

Кроме того, для закрепления знаний и эффективного обучения будет применяться методология *Relearning*, основанная на повторении ключевых понятий. Такое сочетание доступности и надежного педагогического подхода делает Курс профессиональной подготовки не только передовым вариантом образования, но и важным стимулом для тех, кто стремится достичь успехов в области кибербезопасности.

Данный **Курс профессиональной подготовки в области кибербезопасности Red Team** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных экспертами в области кибербезопасности Red Team
- Наглядное, схематичное и исключительно практическое содержание программы предоставляет актуальную и практическую информацию по тем дисциплинам, которые необходимы для осуществления профессиональной деятельности
- Практические упражнения для самопроверки, контроля и повышения успеваемости
- Особое внимание уделяется инновационным методологиям
- Теоретические занятия, вопросы экспертам, дискуссионные форумы по спорным темам и самостоятельная работа
- Учебные материалы курса доступны с любого стационарного или мобильного устройства с выходом в интернет

Благодаря этой эксклюзивной университетской программе TECH вы сможете выделиться в перспективном секторе"

Вы погрузитесь в детальную криминалистическую отчетность в университете с самым высоким рейтингом студентов в мире, согласно платформе Trustpilot (4,9/5)"

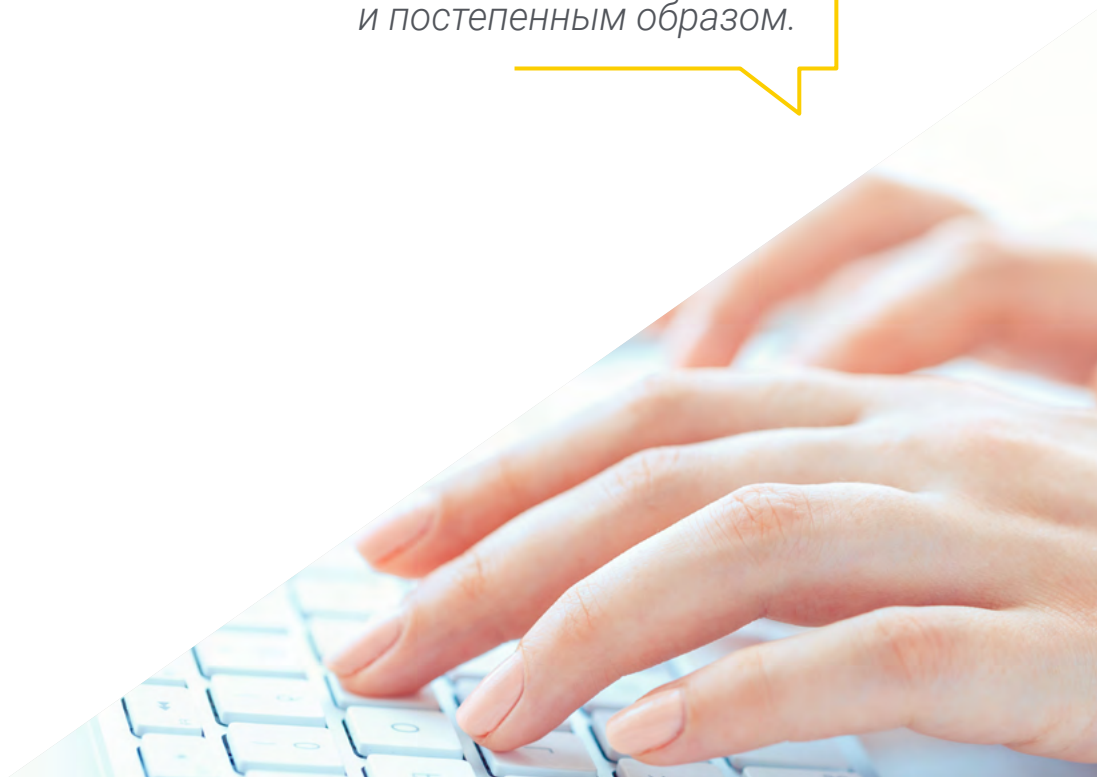
Вы приобретете навыки оценки и выбора средств защиты от вредоносных программ.

Забудьте о заучивании! С системой Relearning вы будете осваивать знания естественным и постепенным образом.

В преподавательский состав программы входят профессионалы из данного сектора, которые привносят в обучение опыт своей работы, а также признанные специалисты из ведущих сообществ и престижных университетов.

Мультимедийное содержание программы, разработанное с использованием новейших образовательных технологий, позволит студенту проходить обучение с учетом контекста и ситуации, т.е. в симулированной среде, обеспечивающей иммерсивный учебный процесс, запрограммированный на обучение в реальных ситуациях.

Структура этой программы основана на проблемно-ориентированном обучении, с помощью которого студент должен попытаться разрешить различные ситуации из профессиональной практики, возникающие в течение учебного курса. В этом студентам поможет инновационная интерактивная видеосистема, созданная признанными специалистами.



02

Цели

Основная цель Курса профессиональной подготовки в области кибербезопасности *Red Team* - обучение студентов навыкам моделирования современных угроз. На протяжении всей программы студенты будут погружены в воспроизведение тактик, техник и процедур (TTP), используемых злоумышленниками. В этом контексте специализированный подход не только укрепит технические навыки студентов, но и позволит им решать реальные задачи в этой области. Кроме того, использование методологии *Relearning* облегчит обучение, закрепляя ключевые понятия без особых усилий.

Вы будете выявлять слабые места и уязвимости в киберинфраструктурах компаний. Достигайте своей цели с помощью TECH!”

Общие цели

- Приобрести передовые навыки в области тестирования на проникновение и моделирования работы *Red team*, направленные на выявление и эксплуатацию уязвимостей в системах и сетях
- Развить лидерские навыки для координации команд, специализирующихся на наступательной кибербезопасности, оптимизируя выполнение проектов *пентестов* и *Red team*
- Сформировать навыки анализа и изучения *вредоносных программ*, понять их функциональность и применить защитные и образовательные стратегии
- Отточить коммуникативные навыки, составляя подробные технические и исполнительные отчеты, эффективно представляя полученные результаты технической и исполнительной аудитории
- Продвигать этическую и ответственную практику в области кибербезопасности, учитывая этические и правовые принципы во всех видах деятельности
- Ознакомить студентов с новыми тенденциями и технологиями в области кибербезопасности

Вы достигнете поставленных целей благодаря дидактическим инструментам TECH, включая пояснительные видеоролики и интерактивные конспекты”

Конкретные цели

Модуль 1. Анализ и исследование вредоносных программ

- Приобрести расширенные знания о природе, функциональности и поведении *вредоносных программ*, понять их различные формы и цели
- Развить навыки криминалистического анализа применительно к *вредоносных программ*, позволяющие выявлять индикаторы компрометации (IoC) и модели атак
- Изучить стратегии эффективного обнаружения *вредоносных программ*, включая развертывание передовых решений безопасности
- Ознакомиться с разработкой *вредоносных программ* для образовательных и защитных целей, позволяя глубоко понять тактику, используемую злоумышленниками
- Пропагандировать этические и правовые нормы при анализе и исследовании *вредоносных программ*, обеспечивая честность и подотчетность во всех видах деятельности
- Применять теоретические знания в смоделированных средах, участвовать в практических занятиях для понимания и противодействия вредоносным атакам
- Развить навыки оценки и выбора средств защиты от *вредоносных программ* с учетом их эффективности и адаптируемость к конкретным средам
- Научиться реализовывать эффективные средства защиты от вредоносных угроз, снижая воздействие и распространение вредоносных программ на системы и сети
- Наладить эффективное сотрудничество с командами безопасности, интегрировать стратегии и усилия по защите от угроз *вредоносных программ*
- Информировать студента о последних тенденциях и методах, используемых в области анализа *вредоносных программ*, обеспечивая постоянную актуальность и эффективность приобретенных навыков

Модуль 2. Основы криминалистики и DFIR

- Приобрести твердое понимание фундаментальных принципов цифровой криминалистики (DFIR) и их применения для разрешения кибер-инцидентов
- Развить навыки безопасного и криминалистического сбора цифровых доказательств, обеспечив сохранение цепочки хранения
- Научиться проводить криминалистический анализ файловых наборов
- Ознакомить студентов с передовыми методами анализа записей и журналов, позволяющими реконструировать события в цифровой среде
- Научиться применять методологии цифровой криминалистической экспертизы при разрешении дел, от идентификации до документирования выводов
- Ознакомить студентов с анализом цифровых доказательств и применением методов криминалистики в условиях *пентеста*
- Развить навыки составления подробных и четких отчетов по судебной экспертизе, представляя результаты и выводы в понятной форме
- Способствовать эффективному сотрудничеству с группами реагирования на инциденты (IR), оптимизируя координацию в расследовании и устранении угроз
- Продвигать этические и правовые практики в области цифровой судебной экспертизы, обеспечивая соблюдение правил и стандартов поведения в сфере кибербезопасности

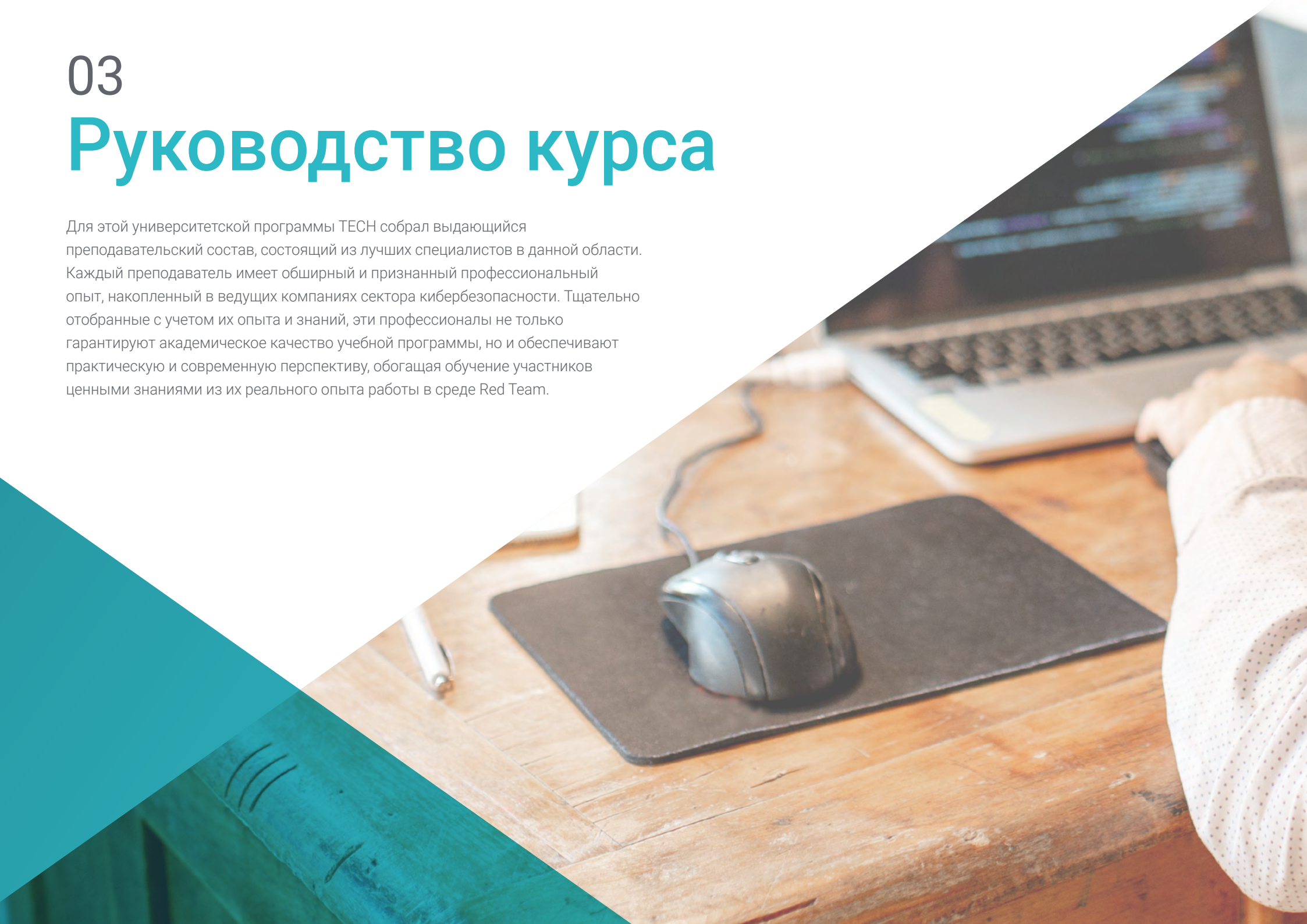
Модуль 3. Продвинутые учения Red Team

- Развить навыки моделирования современных угроз, воспроизводя тактику, технику и процедуры (TTP), используемые потенциальными злоумышленниками
- Научиться выявлять слабые места и уязвимости в инфраструктуре с помощью реалистичных учений с участием *Red Team*, что позволит укрепить систему безопасности
- Ознакомить студентов с передовыми методами обхода защиты, позволяющими оценить устойчивость инфраструктуры к потенциальным атакам
- Развить навыки эффективной координации и сотрудничества между членами *Red Team*, оптимизируя выполнение тактики и стратегии для всесторонней оценки безопасности организации
- Научиться моделировать текущие сценарии угроз, такие как атаки *ransomware* и продвинутые *фишинговые акции,* чтобы оценить способность организации к реагированию
- Ознакомить студентов с методами анализа после проведения учений, оценки работы *Red Team* и извлечение уроков для постоянного совершенствования
- Развить навыки оценки устойчивости организации к смоделированным атакам, выявляя области для улучшения политик и процедур
- Научиться составлять подробные отчеты, документирующие результаты, использованные методики и рекомендации, полученные в ходе учений *Red Team*
- Продвигать этические и правовые практики при проведении учений *Red Team*, обеспечивая соблюдение правил кибербезопасности и этических стандартов

03

Руководство курса

Для этой университетской программы TECH собрал выдающийся преподавательский состав, состоящий из лучших специалистов в данной области. Каждый преподаватель имеет обширный и признанный профессиональный опыт, накопленный в ведущих компаниях сектора кибербезопасности. Тщательно отобранные с учетом их опыта и знаний, эти профессионалы не только гарантируют академическое качество учебной программы, но и обеспечивают практическую и современную перспективу, обогащая обучение участников ценными знаниями из их реального опыта работы в среде Red Team.



Получите новые знания о новейших методах шифрования шелл-кода (XQR) от лучших экспертов в области кибербезопасности. Начните свою карьеру с TECH!"

Руководство

Г-н Гомес Пинтадо, Карлос

- Руководитель группы кибербезопасности и красных команд в Grupo Oesía
- Руководитель, советник и инвестор в компании Wesson App
- Степень бакалавра в области программирования и технологий информационного общества в Политехническом университете Мадрида
- Сотрудничает с учебными заведениями для подготовки циклов обучения высшего уровня в области кибербезопасности

Преподаватели

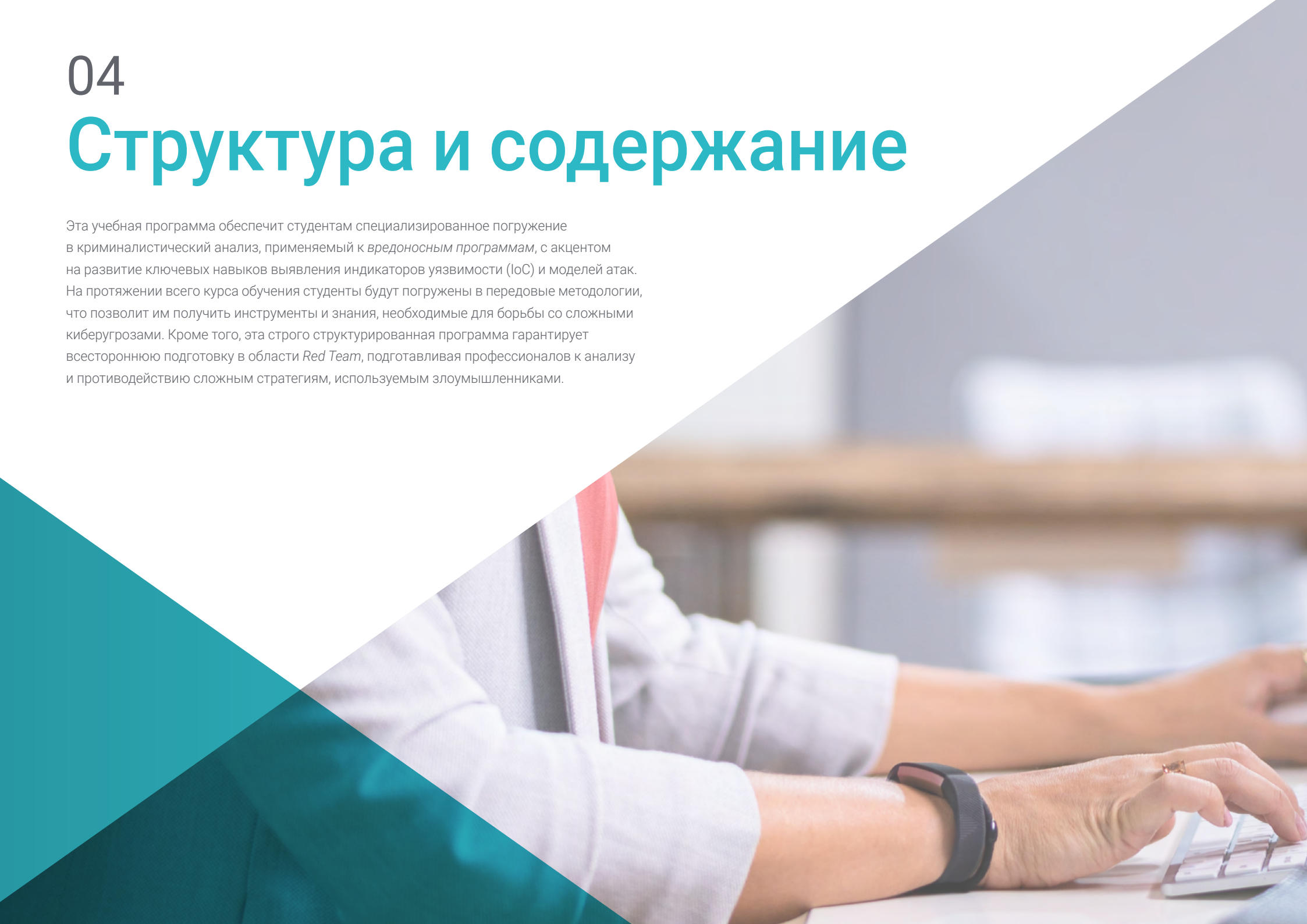
Г-н Гонсалес Санс, Маркос

- Консультант по кибербезопасности в компании Cipherbit
- Сертифицированный разработчик eLearnSecurity eXploit
- Сертифицированный профессионал Offensive Security
- Сертифицированный профессионал Offensive Security Wireless
- Virtual Hacking Labs Plus
- Степень бакалавра в области программирования в Политехническом университете Мадрида

04

Структура и содержание

Эта учебная программа обеспечит студентам специализированное погружение в криминалистический анализ, применяемый к *вредоносным программам*, с акцентом на развитие ключевых навыков выявления индикаторов уязвимости (IoC) и моделей атак. На протяжении всего курса обучения студенты будут погружены в передовые методологии, что позволит им получить инструменты и знания, необходимые для борьбы со сложными киберугрозами. Кроме того, эта строго структурированная программа гарантирует всестороннюю подготовку в области *Red Team*, подготавливая профессионалов к анализу и противодействию сложным стратегиям, используемым злоумышленниками.



Вы изучите передовые методы постэксплуатации и сможете зарекомендовать себя как выдающийся специалист Red Team"

Модуль 1. Анализ и исследование *вредоносных программ*

1.1. Анализ и исследование *вредоносных программ*
- 1.1.1. История и эволюция *вредоносных программ*
- 1.1.2. Классификация и типы *вредоносных программ*
- 1.1.3. Анализ *вредоносных программ*
- 1.1.4. Исследование *вредоносных программ*

1.2. Подготовка среды
- 1.2.1. Настройка виртуальных машин и *Snapshots*
- 1.2.2. Средства анализа *вредоносных программ*
- 1.2.3. Средства разработки *вредоносных программ*

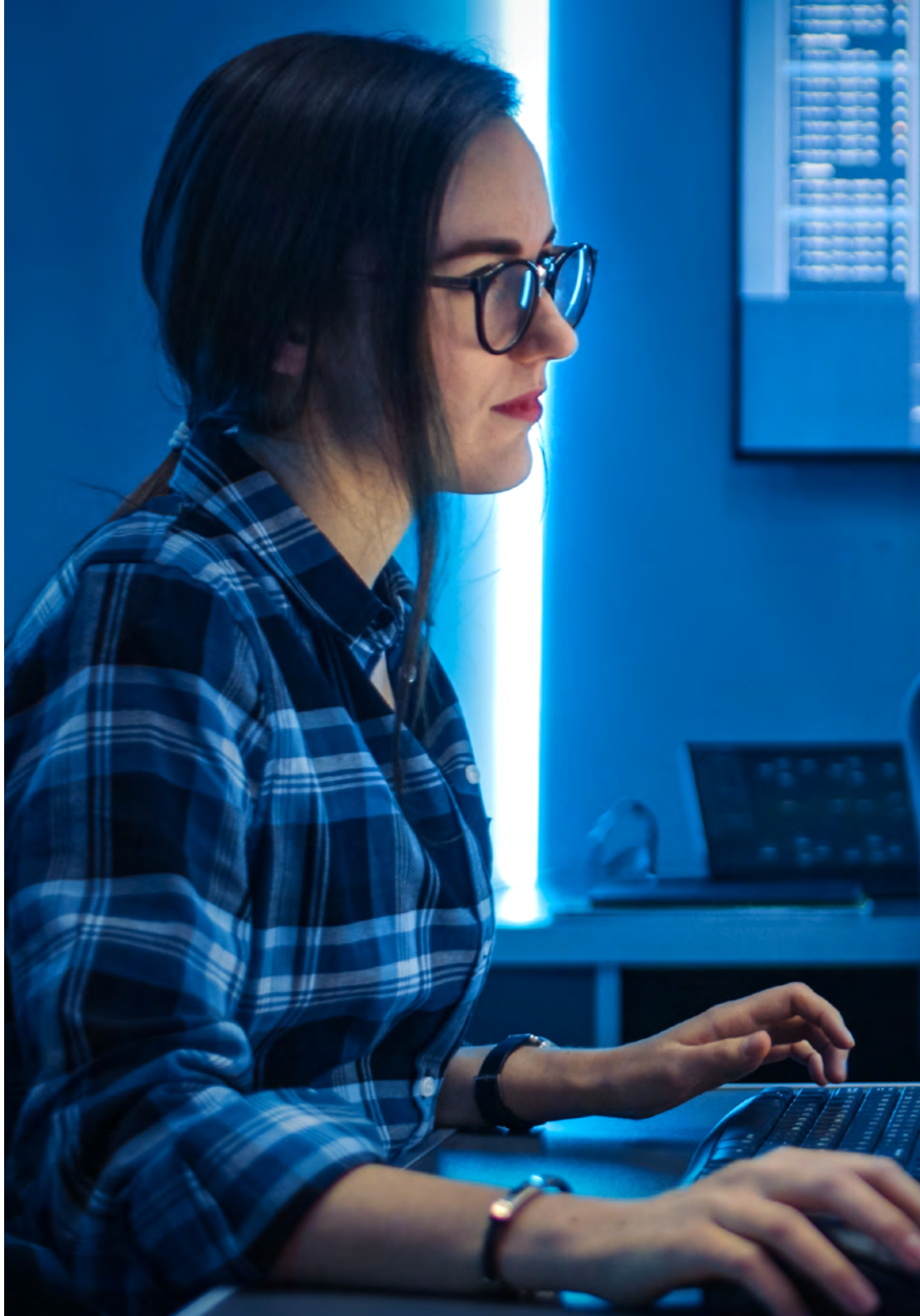
1.3. Основы Windows
- 1.3.1. Формат файлов PE (*Portable Executable*)
- 1.3.2. Процессы и *потоки*
- 1.3.3. Файловая система и реестр
- 1.3.4. *Защитник Windows*

1.4. Основные методы борьбы с *вредоносными программами*
- 1.4.1. Генерация *шелл-кода*
- 1.4.2. Выполнение *шелл-кода* на диске
- 1.4.3. Диск против оперативной памяти
- 1.4.4. Выполнение *шелл-кода* в памяти

1.5. Промежуточные техники *вредоносных программ*
- 1.5.1. Устойчивость Windows
- 1.5.2. Стартовая папка
- 1.5.3. Ключи реестра
- 1.5.4. Скринсейверы

1.6. Передовые методы работы с *вредоносными программами*
- 1.6.1. Шифрование *шелл-кода* (XOR)
- 1.6.2. Шифрование *шелл-кода* (RSA)
- 1.6.3. Обфускация *строк*
- 1.6.4. Инъекция в процессы

1.7. Статический анализ *вредоносных программ*
- 1.7.1. Анализ *упаковщиков* с помощью DIE (*Detect It Easy*)
- 1.7.2. Анализ секций с помощью PE-Bear
- 1.7.3. Декомпиляция с помощью Ghidra



1.8. Динамический анализ *вредоносных программ*
- 1.8.1. Наблюдение за поведением с помощью Process Hacker
- 1.8.2. Анализ вызовов с помощью API Monitor
- 1.8.3. Анализ изменений в реестре с помощью Regshot
- 1.8.4. Наблюдение за сетевыми запросами с помощью TCPView

1.9. Анализ в .NET
- 1.9.1. Введение в .NET
- 1.9.2. Декомпиляция с помощью dnSpy
- 1.9.3. Отладка с помощью dnSpy

1.10. Анализ реальных *вредоносных* программ
- 1.10.1. Подготовка среды
- 1.10.2. Статический анализ *вредоносных программ*
- 1.10.3. Динамический анализ *вредоносных программ*
- 1.10.4. Создание правил YARA

Модуль 2. Основы криминалистики и DFIR

2.1. Цифровая криминалистика
- 2.1.1. История и развитие компьютерной криминалистики
- 2.1.2. Важность компьютерной криминалистики в кибербезопасности
- 2.1.3. История и развитие компьютерной криминалистики

2.2. Основы компьютерной криминалистики
- 2.2.1. Цепочка хранения и ее применение
- 2.2.2. Виды цифровых улик
- 2.2.3. Процессы получения улик

2.3. Системы хранения и структура данных
- 2.3.1. Основные системы хранения
- 2.3.2. Методы сокрытия данных
- 2.3.3. Анализ метаданных и атрибутов файлов

2.4. Анализ операционных систем
- 2.4.1. Криминалистический анализ систем Windows
- 2.4.2. Криминалистический анализ систем Linux
- 2.4.3. Криминалистический анализ систем macOS

2.5. Восстановление данных и анализ дисков
- 2.5.1. Восстановление данных с поврежденных носителей
- 2.5.2. Инструменты для анализа дисков
- 2.5.3. Интерпретация файловых систем

2.6. Анализ сети и трафика
- 2.6.1. Захват и анализ сетевых пакетов
- 2.6.2. Анализ журналов *брандмауэра*
- 2.6.3. Обнаружение сетевых вторжений

2.7. Анализ *вредоносных программ* и вредоносного кода
- 2.7.1. Классификация *вредоносных программ* и их характеристики
- 2.7.2. Статический и динамический анализ *вредоносных программ*
- 2.7.3. Методы деассемблирования и отладки

2.8. Анализ журналов и событий
- 2.8.1. Типы журналов в системах и приложениях
- 2.8.2. Интерпретация соответствующих событий
- 2.8.3. Инструменты анализа журналов

2.9. Реагирование на инциденты безопасности
- 2.9.1. Процесс реагирования на инциденты
- 2.9.2. Создание плана реагирования на инциденты
- 2.9.3. Координация действий с командами безопасности

2.10. Представление улик и доказательств
- 2.10.1. Правила представления цифровых доказательств в правовой среде
- 2.10.2. Подготовка отчетов о судебной экспертизе
- 2.10.3. Выступление в суде в качестве свидетеля-эксперта

Модуль 3. Продвинутые учения *Red Team*

3.1. Продвинутые методы исследования
- 3.1.1. Продвинутое перечисление субдоменов
- 3.1.2. Продвинутый *Google Dorking*
- 3.1.3. Социальные сети и theHarvester

3.2. Продвинутые *фишинговые* операции
- 3.2.1. Что такое *фишинг с обратным прокси*
- 3.2.2. *Обход 2FA* с помощью Evilginx
- 3.2.3. Эксфильтрация данных

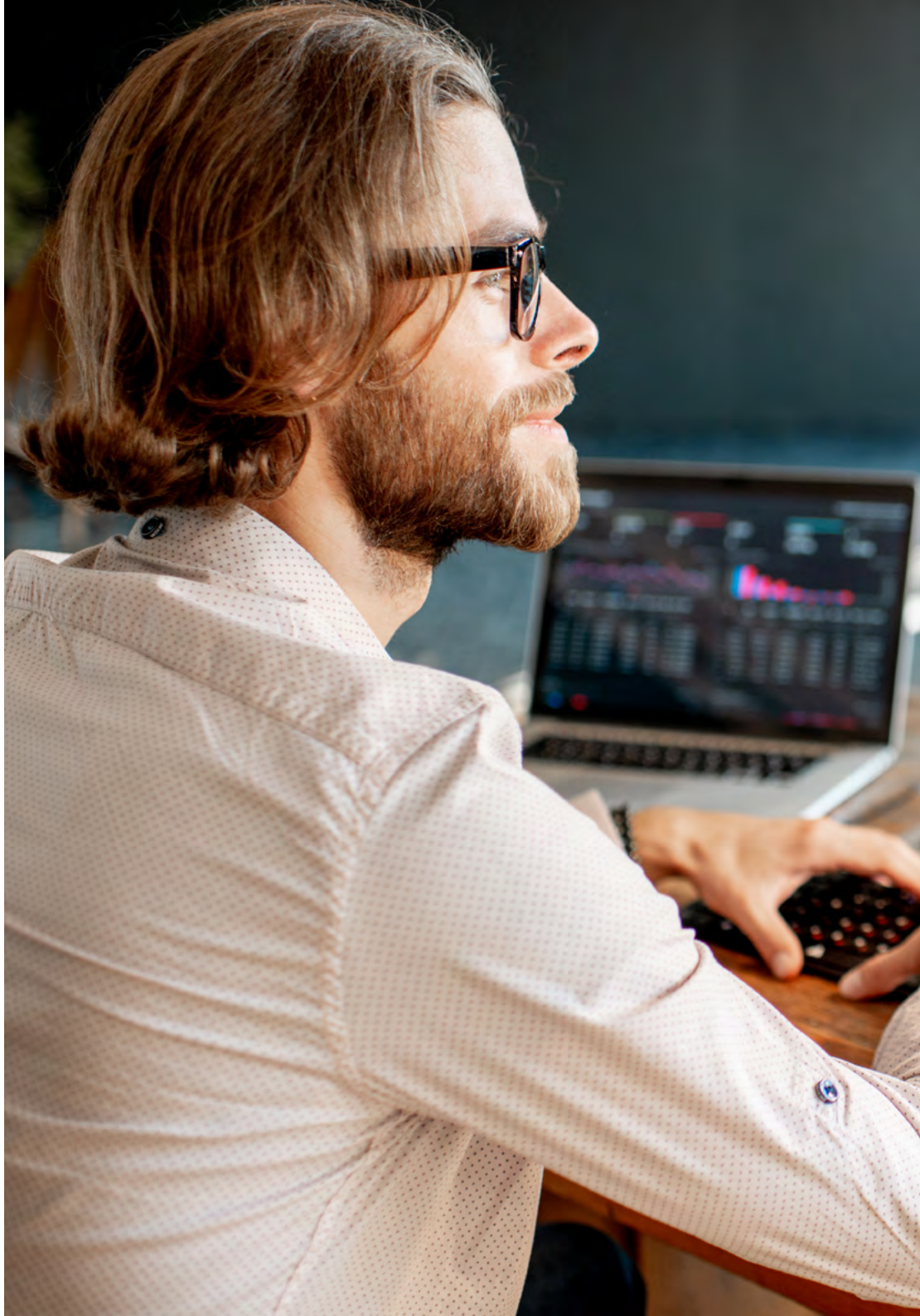
3.3. Продвинутые техники устойчивости
- 3.3.1. *Золотые билеты*
- 3.3.2. *Серебряные билеты*
- 3.3.3. Техника *DCShadow*

3.4. Продвинутые техники предотвращения
- 3.4.1. *Обход* AMSI
- 3.4.2. Модификация существующих инструментов
- 3.4.3. Обфускация *Powershell*

3.5. Продвинутые техники латерального перемещения
- 3.5.1. *Pass-the-Ticket* (PtT)
- 3.5.2. *Overpass-the-Hash (Pass-the-Key)*
- 3.5.3. Ретрансляция NTLM

3.6. Продвинутые техники пост-эксплойтов
- 3.6.1. *Дамп* LSASS
- 3.6.2. *Дамп* SAM
- 3.6.3. Атака *DCSync*

3.7. Продвинутые техники *пивотирования*
- 3.7.1. Что такое *пивотирование*
- 3.7.2. Туннелирование SSH
- 3.7.3. *Пивотирование* с помощью Chisel



3.8. Физические вторжения
- 3.8.1. Наблюдение и разведка
- 3.8.2. *Tailgating и Piggybacking*
- 3.8.3. *Lock-Picking*

3.9. Атаки Wi-Fi
- 3.9.1. Атаки WPA/WPA2 PSK
- 3.9.2. Атаки на неавторизованные точки доступа
- 3.9.3. Атаки на WPA2 *Enterprise*

3.10. Атаки RFID
- 3.10.1. Считывание RFID-карт
- 3.10.2. Манипуляции с RFID-картами
- 3.10.3. Создание клонированных карт

Не упустите возможность поднять свою карьеру на новый уровень с помощью этой инновационной программы" Станьте экспертом в области кибербезопасности!"

05

Методика обучения

TECH — первый в мире университет, объединивший метод ***кейс-стади*** с ***Relearning***, системой 100% онлайн-обучения, основанной на направленном повторении.

Эта инновационная педагогическая стратегия была разработана для того, чтобы предложить профессионалам возможность обновлять свои знания и развивать навыки интенсивным и эффективным способом. Модель обучения, которая ставит студента в центр учебного процесса и отводит ему ведущую роль, адаптируясь к его потребностям и оставляя в стороне более традиционные методологии.

TECH подготовит вас к решению новых задач в условиях неопределенности и достижению успеха в карьере”

Студент — приоритет всех программ TECH

В методике обучения TECH студент является абсолютным действующим лицом. Педагогические инструменты каждой программы были подобраны с учетом требований к времени, доступности и академической строгости, которые предъявляют современные студенты и наиболее конкурентоспособные рабочие места на рынке.

В асинхронной образовательной модели TECH студенты сами выбирают время, которое они выделяют на обучение, как они решат выстроить свой распорядок дня, и все это — с удобством на любом электронном устройстве, которое они предпочитают. Студентам не нужно посещать очные занятия, на которых они зачастую не могут присутствовать. Учебные занятия будут проходить в удобное для них время. Вы всегда можете решить, когда и где учиться.

“В TECH у вас НЕ будет занятий в реальном времени, на которых вы зачастую не можете присутствовать”

Самые обширные учебные планы на международном уровне

TECH характеризуется тем, что предлагает наиболее обширные академические планы в университетской среде. Эта комплексность достигается за счет создания учебных планов, которые охватывают не только основные знания, но и самые последние инновации в каждой области.

Благодаря постоянному обновлению эти программы позволяют студентам быть в курсе изменений на рынке и приобретать навыки, наиболее востребованные работодателями. Таким образом, те, кто проходит обучение в TECH, получают комплексную подготовку, которая дает им значительное конкурентное преимущество для продвижения по карьерной лестнице.

Более того, студенты могут учиться с любого устройства: компьютера, планшета или смартфона.

> *Модель TECH является асинхронной, поэтому вы можете изучать материал на своем компьютере, планшете или смартфоне в любом месте, в любое время и в удобном для вас темпе”*

Case studies или метод кейсов

Метод кейсов является наиболее распространенной системой обучения в лучших бизнес-школах мира. Разработанный в 1912 году для того, чтобы студенты юридических факультетов не просто изучали законы на основе теоретических материалов, он также имел цель представить им реальные сложные ситуации. Таким образом, они могли принимать взвешенные решения и выносить обоснованные суждения о том, как их разрешить. В 1924 году он был установлен в качестве стандартного метода обучения в Гарвардском университете.

При такой модели обучения студент сам формирует свою профессиональную компетенцию с помощью таких стратегий, как *обучение действием* (learning by doing) или *дизайн-мышление* (*design thinking*), используемых такими известными учебными заведениями, как Йель или Стэнфорд.

Этот метод, ориентированный на действия, будет применяться на протяжении всего академического курса, который студент проходит в TECH. Таким образом, они будут сталкиваться с множеством реальных ситуаций и должны будут интегрировать знания, проводить исследования, аргументировать и защищать свои идеи и решения. Все это делается для того, чтобы ответить на вопрос, как бы они поступили, столкнувшись с конкретными сложными событиями в своей повседневной работе.

Метод *Relearning*

В TECH *метод кейсов* дополняется лучшим методом онлайн-обучения — *Relearning*.

Этот метод отличается от традиционных методик обучения, ставя студента в центр обучения и предоставляя ему лучшее содержание в различных форматах. Таким образом, студент может пересматривать и повторять ключевые концепции каждого предмета и учиться применять их в реальной среде.

Кроме того, согласно многочисленным научным исследованиям, повторение является лучшим способом усвоения знаний. Поэтому в TECH каждое ключевое понятие повторяется от 8 до 16 раз в рамках одного занятия, представленного в разных форматах, чтобы гарантировать полное закрепление знаний в процессе обучения.

Метод Relearning позволит тебе учиться с меньшими усилиями и большей эффективностью, глубже вовлекаясь в свою специализацию, развивая критическое мышление, умение аргументировать и сопоставлять мнения — прямой путь к успеху.

Виртуальный кампус на 100% в онлайн-формате с лучшими учебными ресурсами

Для эффективного применения своей методики TECH предоставляет студентам учебные материалы в различных форматах: тексты, интерактивные видео, иллюстрации, карты знаний и др. Все они разработаны квалифицированными преподавателями, которые в своей работе уделяют особое внимание сочетанию реальных случаев с решением сложных ситуаций с помощью симуляции, изучению контекстов, применимых к каждой профессиональной сфере, и обучению на основе повторения, с помощью аудио, презентаций, анимации, изображений и т.д.

Последние научные данные в области нейронаук указывают на важность учета места и контекста, в котором происходит доступ к материалам, перед началом нового процесса обучения. Возможность индивидуальной настройки этих параметров помогает людям лучше запоминать и сохранять знания в гиппокампе для долгосрочного хранения. Речь идет о модели, называемой *нейрокогнитивным контекстно-зависимым электронным обучением*, которая сознательно применяется в данной университетской программе.

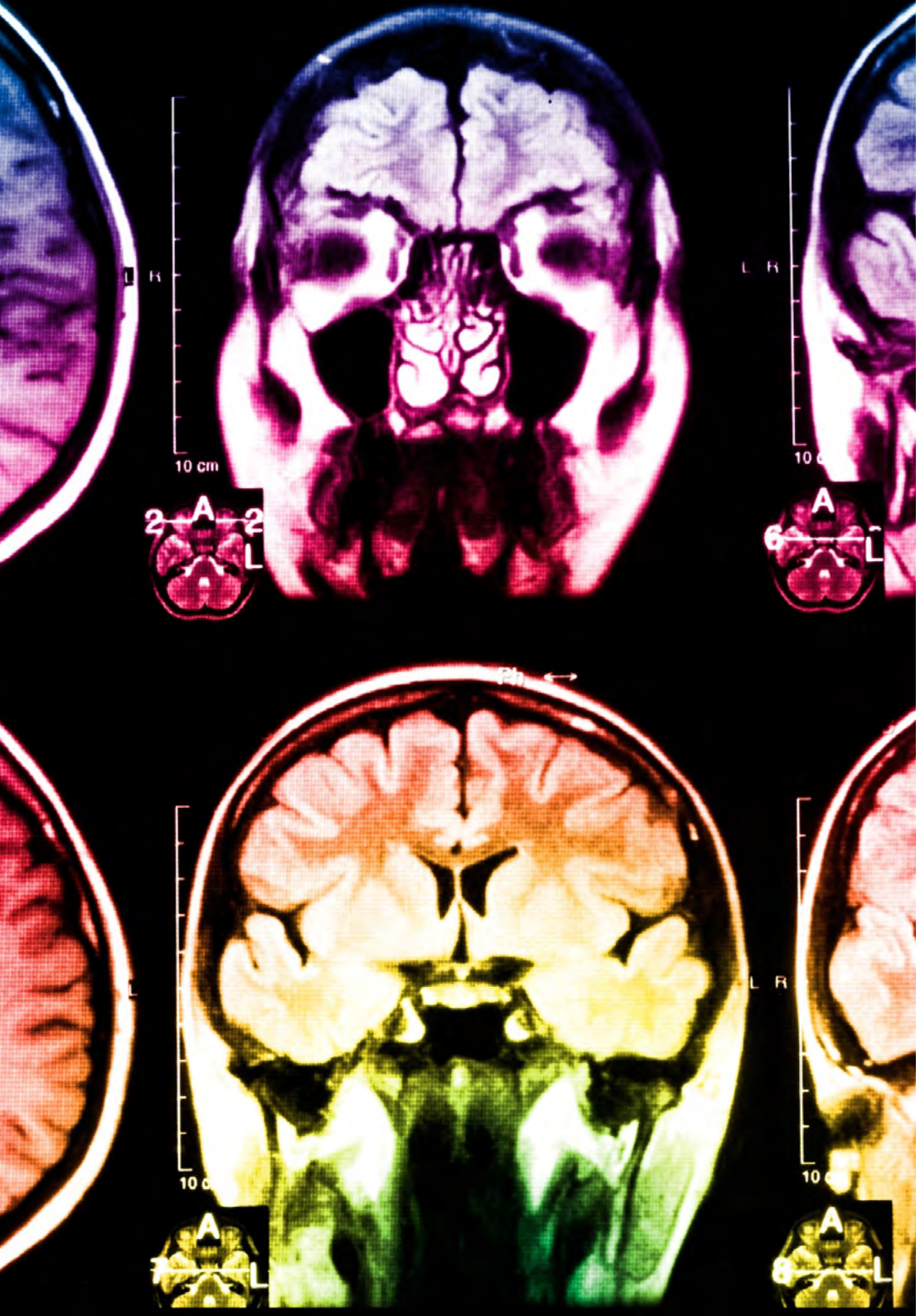
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи с техническим отделом, чат и видеоконференции).

Этот полноценный Виртуальный кампус также позволит студентам TECH организовывать свое учебное расписание в соответствии с личной доступностью или рабочими обязательствами. Таким образом, студенты смогут полностью контролировать академические материалы и учебные инструменты, необходимые для быстрого профессионального развития.

> *Онлайн-режим обучения на этой программе позволит вам организовать свое время и темп обучения, адаптировав его к своему расписанию”*

Эффективность метода обосновывается четырьмя ключевыми достижениями:

1. Студенты, которые следуют этому методу, не только добиваются усвоения знаний, но и развивают свои умственные способности с помощью упражнений по оценке реальных ситуаций и применению своих знаний.
2. Обучение прочно опирается на практические навыки, что позволяет студенту лучше интегрироваться в реальный мир.
3. Усвоение идей и концепций становится проще и эффективнее благодаря использованию ситуаций, возникших в реальности.
4. Ощущение эффективности затраченных усилий становится очень важным стимулом для студентов, что приводит к повышению интереса к учебе и увеличению времени, посвященному на работу над курсом.



Методика университета, получившая самую высокую оценку среди своих студентов

Результаты этой инновационной академической модели подтверждаются высокими уровнями общей удовлетворенности выпускников TECH.

Студенты оценивают качество преподавания, качество материалов, структуру и цели курса на отлично. Неудивительно, что учебное заведение стало лучшим университетом по оценке студентов на платформе отзывов Trustpilot, получив 4,9 балла из 5.

Благодаря тому, что TECH идет в ногу с передовыми технологиями и педагогикой, вы можете получить доступ к учебным материалам с любого устройства с подключением к Интернету (компьютера, планшета или смартфона).

Вы сможете учиться, пользуясь преимуществами доступа к симулированным образовательным средам и модели обучения через наблюдение, то есть учиться у эксперта (learning from an expert).

Таким образом, в этой программе будут доступны лучшие учебные материалы, подготовленные с большой тщательностью:

Учебные материалы

Все дидактические материалы создаются преподавателями специально для студентов этого курса, чтобы они были действительно четко сформулированными и полезными.

Затем эти материалы переносятся в аудиовизуальный формат, на основе которого строится наш способ работы в интернете, с использованием новейших технологий, позволяющих нам предложить вам отличное качество каждого из источников, предоставленных к вашим услугам.

Практика навыков и компетенций

Студенты будут осуществлять деятельность по развитию конкретных компетенций и навыков в каждой предметной области. Практика и динамика приобретения и развития навыков и способностей, необходимых специалисту в рамках глобализации, в которой мы живем.

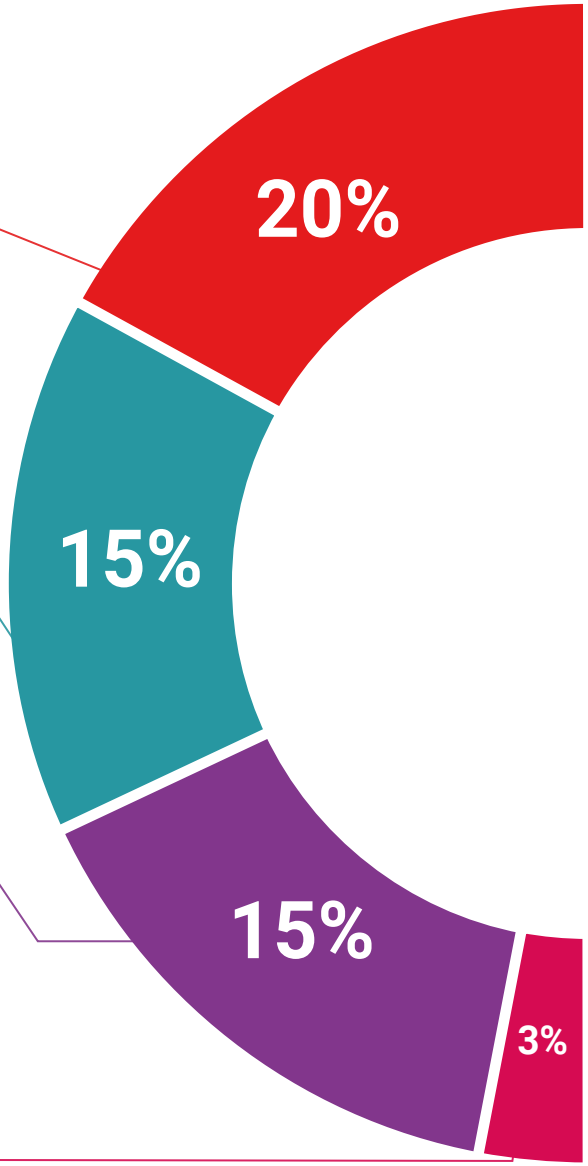
Интерактивные конспекты

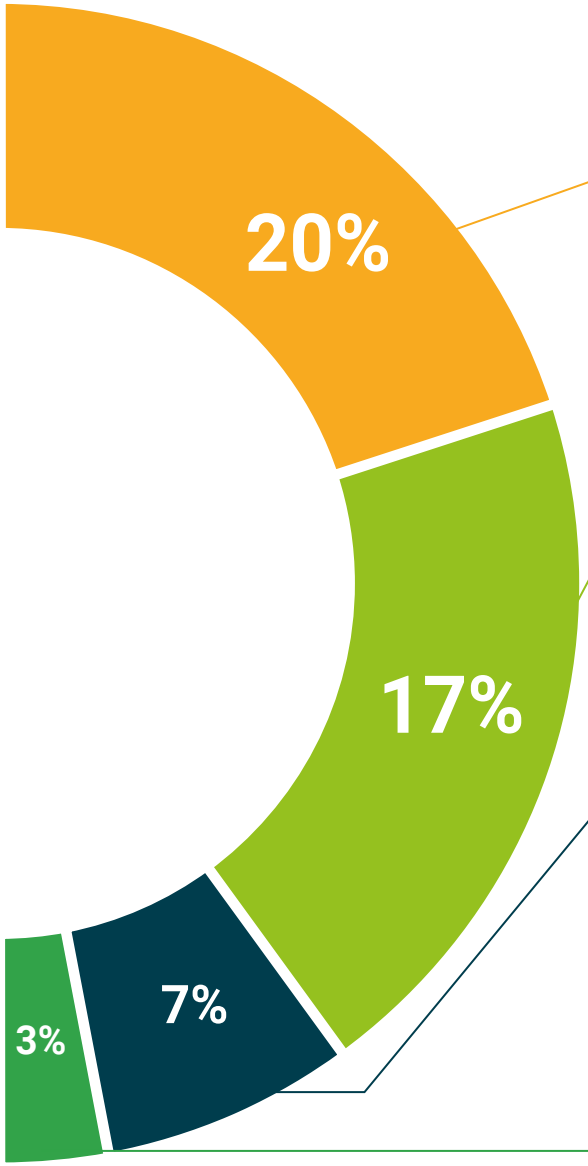
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

Эта эксклюзивная образовательная система для презентации мультимедийного содержания была награждена Microsoft как "Кейс успеха в Европе".

Дополнительная литература

Последние статьи, консенсусные документы, международные рекомендации... В нашей виртуальной библиотеке вы получите доступ ко всему, что необходимо для прохождения обучения.





Кейс-стади

Студенты завершат выборку лучших *кейс-стади* по предмету. Кейсы представлены, проанализированы и преподаются ведущими специалистами на международной арене.

Тестирование и повторное тестирование

Мы периодически оцениваем и переоцениваем ваши знания на протяжении всей программы. Мы делаем это на 3 из 4 уровней пирамиды Миллера.

Мастер-классы

Существуют научные данные о пользе экспертного наблюдения третьей стороны.

Так называемый метод *обучения у эксперта* (learning from an expert) укрепляет знания и память, а также формирует уверенность в ваших будущих сложных решениях.

Краткие справочные руководства

TECH предлагает наиболее актуальные материалы курса в виде карточек или кратких справочных руководств. Это сжатый, практичный и эффективный способ помочь студенту продвигаться в обучении.

06

Квалификация

Курс профессиональной подготовки в области кибербезопасности Red Team гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Курса профессиональной подготовки, выдаваемого TECH Технологическим университетом.

Успешно завершите эту программу и получите университетский диплом без хлопот, связанных с поездками и бумажной волокитой”

Данный **Курс профессиональной подготовки в области кибербезопасности Red Team** содержит самую полную и современную программу на рынке.

После прохождения аттестации студент получит по почте* с подтверждением получения соответствующий диплом о прохождении **Курса профессиональной подготовки**, выданный **TECH Технологическим университетом.**

Диплом, выданный **TECH Технологическим университетом**, подтверждает квалификацию, полученную на Курсе профессиональной подготовки, и соответствует требованиям, обычно предъявляемым биржами труда, конкурсными экзаменами и комитетами по оценке карьеры.

Диплом: **Курс профессиональной подготовки в области кибербезопасности Red Team**

Формат: **онлайн**

Продолжительность: **6 месяцев**


tech технологический университет

Настоящий

ДИПЛОМ

свидетельствует о том, что

Г-н/Г-жа _____, с документом, удостоверяющий личность_____

Освоил(а) и успешно прошел(ла) аккредитацию программы

КУРС ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

в области

кибербезопасности Red Team

Данный диплом специализированной программы, присуждаемый Университетом, соответствует 450 учебным часам, с датой начала дд/мм/гггг и датой окончания дд/мм/гггг.

TECH является частным высшим учебным заведением, признанным Министерством народного образования Мексики с 28 июня 2018 года.

17 июня 2020 г.

Д-р Tere Guevara Navarro
Ректор

unique TECH code: AFWOR23S techtitute.com/certificates

*Гаагский апостиль. В случае, если студент потребует, чтобы на его диплом в бумажном формате был проставлен Гаагский апостиль, TECH EDUCATION предпримет необходимые шаги для его получения за дополнительную плату.

tech технологический университет

Курс профессиональной подготовки

Кибербезопасность

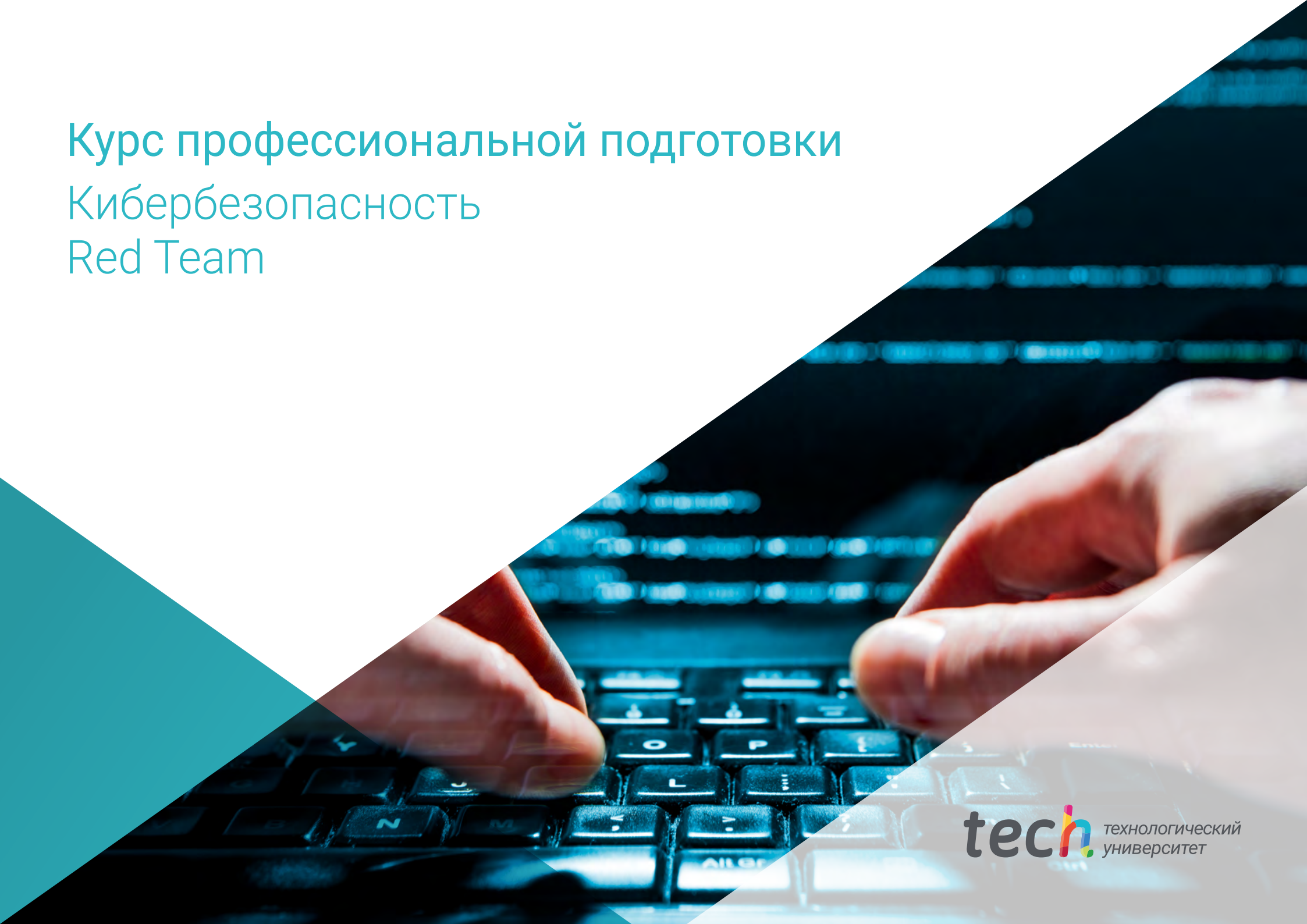
Red Team

- Формат: **онлайн**
- Продолжительность: **6 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

Курс профессиональной подготовки

Кибербезопасность

Red Team



tech технологический университет