Специализированная магистратура

Пентест и Red Team

tech технологический университет

технологический университет

Специализированная магистратура
Пентест и Red Team

- Формат: **онлайн**
- Продолжительность: **12 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

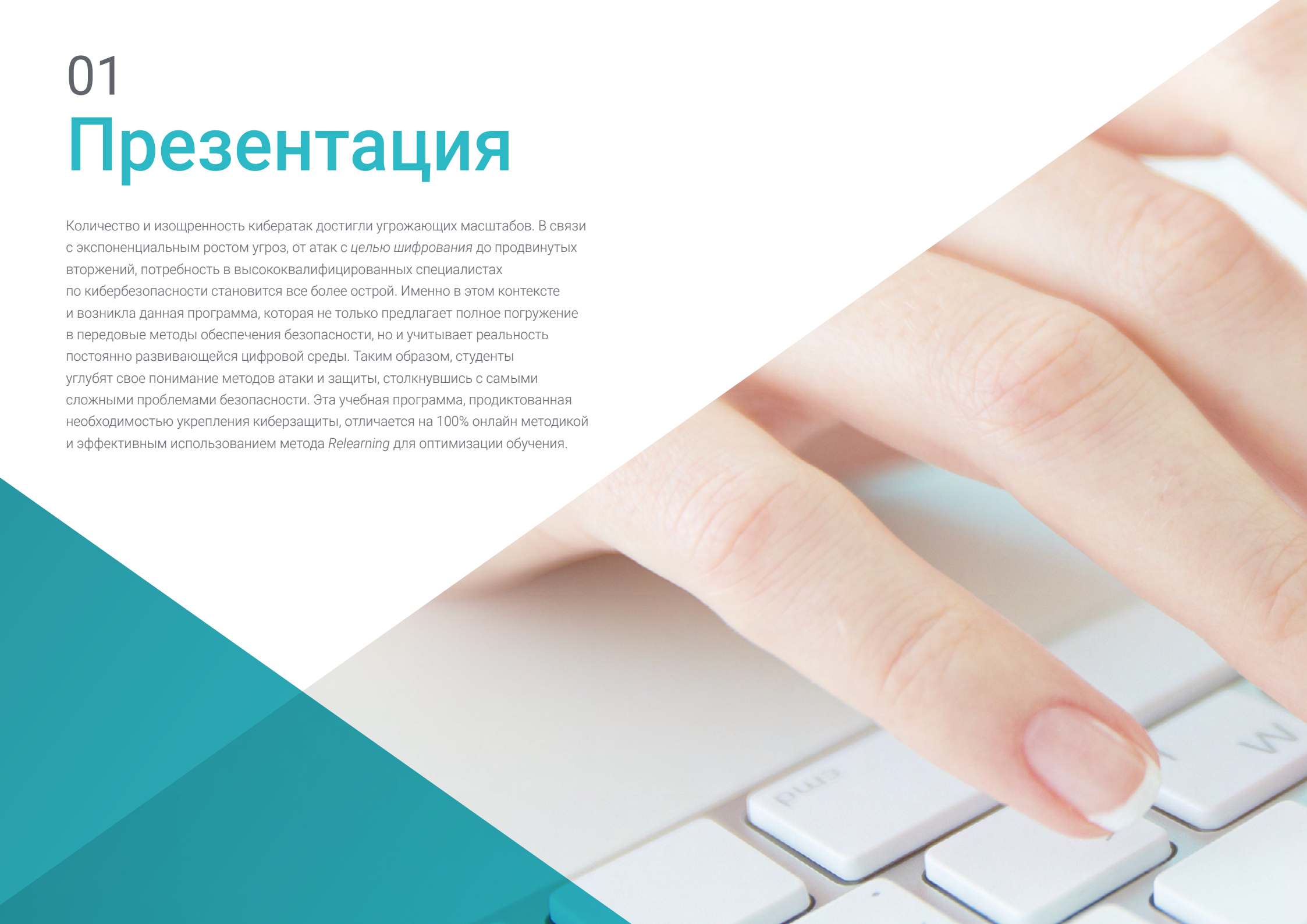
Веб-доступ: www.techtitute.com/ru/information-technology/professional-master-degree/master-pentesting-red-team

Оглавление

01

Презентация

Количество и изощренность кибератак достигли угрожающих масштабов. В связи с экспоненциальным ростом угроз, от атак с *целью шифрования* до продвинутых вторжений, потребность в высококвалифицированных специалистах по кибербезопасности становится все более острой. Именно в этом контексте и возникла данная программа, которая не только предлагает полное погружение в передовые методы обеспечения безопасности, но и учитывает реальность постоянно развивающейся цифровой среды. Таким образом, студенты углубят свое понимание методов атаки и защиты, столкнувшись с самыми сложными проблемами безопасности. Эта учебная программа, продиктованная необходимостью укрепления киберзащиты, отличается на 100% онлайн методикой и эффективным использованием метода *Relearning* для оптимизации обучения.



Благодаря этой новаторской программе вы будете разрабатывать неприступные протоколы безопасности с гарантией TECH"

Постоянное совершенствование жизненно важно для сохранения эффективности защиты от текущих и возникающих угроз. В связи с этим быстрая эволюция технологий и кибернетических тактик сделала постоянное обновление знаний обязательным. Распространение угроз подчеркивает настоятельную необходимость в высококвалифицированных специалистах.

В этом контексте данная программа оказывается крайне важной, поскольку она не только обеспечит глубокое понимание самых передовых методов в области кибербезопасности, но и позволит специалистам быть в авангарде новейших тенденций и технологий.

В рамках программы Специализированной магистратуры по пентесту и Red Team студент будет всесторонне рассматривать требования в области кибербезопасности. Так, студенты будут внедрять эффективные меры безопасности в сетях, включая брандмауэры, системы обнаружения вторжений (IDS) и сегментацию сети. Для этого специалисты будут применять методики цифровых криминалистических исследований для раскрытия дел, начиная с идентификации и заканчивая документированием результатов.

Кроме того, студенты будут развивать навыки моделирования современных угроз, воспроизводя тактику, технику и процедуры, наиболее часто используемые злоумышленниками. Новаторский подход TECH обеспечит приобретение навыков, применимых в рабочей среде кибербезопасности.

Методология академической программы усиливает ее инновационный характер, так как она предлагает 100% онлайн образовательную среду. Эта программа соответствует потребностям действующих специалистов, желающих продвинуться по карьерной лестнице. Кроме того, в ней будет использоваться методология *Relearning*, основанная на повторении ключевых понятий для закрепления знаний и облегчения обучения. Таким образом, сочетание гибкости и надежного педагогического подхода сделает программу не только доступной, но и высокоэффективной в подготовке ИТ-специалистов к решению динамичных задач в области кибербезопасности.

Данная **Специализированная магистратура в области пентеста и Red Team** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных экспертами в области пентеста и Red Team
- Наглядное, схематичное и исключительно практическое содержание программы предоставляет актуальную и практическую информацию по тем дисциплинам, которые необходимы для профессиональной практики
- Практические упражнения для самооценки, 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

Всего за 12 месяцев вы придадите своей карьере необходимый импульс. Поступайте прямо сейчас и ощутите немедленный прогресс!"

Хотите ощутить качественный скачок в своей карьере? В TECH вас обучат реализации стратегий для эффективного выполнения проектов по кибербезопасности"

Вы получите глубокие знания по выявлению и оценке уязвимостей в веб-приложениях благодаря лучшему цифровому университету в мире по версии Forbes.

Вы освоите методы криминалистики в условиях пентеста. Позиционируйте себя как эксперта по кибербезопасности, которого ждут все компании!

В преподавательский состав программы входят профессионалы в данной области, которые привносят в обучение свой обширный опыт, 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 этой академической программы – обучить студентов тестированию на проникновение и симуляции работы *Red Team*. На протяжении всей программы ИТ-специалисты будут погружены в практический и специализированный процесс, развивая навыки по выявлению и эксплуатации уязвимостей в системах и сетях. Кроме того, учебная программа призвана обеспечить глубокое понимание тактики и стратегии кибербезопасности, подготовив студентов к решению реальных задач и руководству эффективной реализацией мер кибербезопасности.

Вы углубитесь в анализ и изучение вредоносных программ, чтобы стать ведущим специалистом. Достигайте своих целей вместе с 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. Наступательная безопасность

- Ознакомить студента с методологией тестирования на проникновение, включая такие ключевые этапы, как сбор информации, анализ уязвимостей, эксплуатация и документирование
- Развить практические навыки использования специализированных инструментов *пентеста* для выявления и оценки уязвимостей в системах и сетях
- Изучить и понять тактику, технику и процедуры, используемые злоумышленниками, что позволит выявлять и моделировать угрозы
- Применять теоретические знания в практических сценариях и симуляциях, сталкиваясь с реальными проблемами, чтобы укрепить навыки *пентеста*
- Развить навыки эффективного документирования, создавая подробные отчеты, отражающие результаты, использованные методики и рекомендации по улучшению безопасности
- Практиковать эффективное взаимодействие в командах наступательной безопасности, оптимизируя координацию и выполнение мероприятий по *пентесту*

Модуль 2. Управление командами кибербезопасности

- Развить лидерские навыки, характерные для команд кибербезопасности, включая умение мотивировать, вдохновлять и координировать усилия для достижения общих целей
- Научиться эффективно распределять ресурсы в команде кибербезопасности, учитывая индивидуальные навыки и добиваясь максимальной производительности в проектах
- Совершенствовать навыки общения, характерные для технической среды, облегчая понимание и координацию между членами команды
- Изучить стратегии выявления и разрешения конфликтов в команде специалистов по кибербезопасности, содействовать атмосфере сотрудничества и эффективности
- Научиться устанавливать метрики и системы оценки для определения эффективности работы команды кибербезопасности и вносить корректировки по мере необходимости
- Содействовать внедрению этических норм в управление командами кибербезопасности, обеспечивая этичность и законность всех действий
- Развить компетенции для обеспечения готовности и эффективного управления инцидентами кибербезопасности, обеспечивая быстрое и эффективное реагирование на угрозы

Модуль 3. Управление проектами безопасности

- Развить навыки планирования проектов по кибербезопасности, определяя цели, масштабы, ресурсы и сроки реализации
- Изучить стратегии эффективного выполнения проектов по безопасности, обеспечивающие успешную реализацию запланированных мер
- Развить навыки эффективного управления бюджетами и распределения ресурсов в проектах по безопасности, максимизируя эффективность и минимизируя затраты
- Повысить эффективность общения с *заинтересованными сторонами*, представляя отчеты и обновления в ясной и понятной форме
- Освоить методы мониторинга и контроля проектов, выявлять отклонения и принимать необходимые корректирующие меры
- Ознакомить студентов с agile методологией *пентеста*
- Развить навыки составления подробной документации и отчетов, обеспечивающих четкое представление о ходе проекта и достигнутых результатах
- Поощрять эффективное сотрудничество между различными командами и подразделениями в рамках проектов по безопасности, обеспечивая эффективное выполнение работ, обеспечивая целостный и скоординированный подход
- Освоить стратегии оценки и измерения эффективности реализованных мер, обеспечивая постоянное совершенствование системы безопасности организации

Модуль 4. Атаки на сети и системы Windows

- Развить навыки выявления и оценки специфических уязвимостей в операционных системах Windows
- Изучить передовые тактики, используемые злоумышленниками для проникновения и пребывания в сетях на базе Windows
- Приобрести навыки работы со стратегиями и инструментами для снижения специфических угроз, направленных на операционные системы Windows
- Ознакомить студента с методами криминалистического анализа, применяемыми к системам Windows, облегчающими идентификацию и реагирование на инциденты

- Применять теоретические знания в смоделированных средах, участвуя в практических занятиях по пониманию и противодействию конкретным атакам на системы Windows
- Изучить конкретные стратегии защиты корпоративных сред, использующих операционные системы Windows, с учетом сложности корпоративных инфраструктур
- Развить компетенции по оценке и улучшению конфигураций безопасности в системах Windows, обеспечивая реализацию эффективных мер
- Продвигать этические и правовые практики при выполнении атак и тестов на системы Windows, учитывая этические принципы кибербезопасности
- Держивать студентов в курсе последних тенденций и угроз в области атак на системы Windows, обеспечивая постоянную актуальность и эффективность полученных навыков

Модуль 5. Продвинутый веб-*хакинг*

- Развить навыки выявления и оценки уязвимостей в веб-приложениях, включая SQL-инъекции, *межсайтовый скриптинг* (XSS) и другие распространенные векторы атак
- Узнать, как проводить тестирование безопасности современных веб-приложений
- Приобрести компетенции в области передовых методов веб-хакинга, изучить стратегии обхода мер безопасности и использования сложных уязвимостей
- Ознакомить студента с оценкой безопасности API и веб-сервисов, выявлением потенциальных уязвимостей и укреплением безопасности интерфейсов программирования
- Развить навыки реализации эффективных мер по снижению уязвимостей в веб-приложениях, уменьшению подверженности атакам и укреплению безопасности
- Участвовать в практических симуляциях по оценке безопасности в сложных веб-средах, применяя знания к реальным сценариям
- Развить компетенции в разработке эффективных стратегий защиты веб-приложений от киберугроз
- Научиться согласовывать передовые методы веб-***хакинга*** с соответствующими правилами и стандартами безопасности, обеспечивая соблюдение правовых и этических рамок
- Содействовать эффективному сотрудничеству между командами разработки и безопасности

Модуль 6. Сетевая архитектура и безопасность

- Приобрести расширенные знания об архитектуре сетей, включая топологии, протоколы и ключевые компоненты
- Развить навыки выявления и оценки конкретных уязвимостей в сетевых инфраструктурах с учетом потенциальных угроз
- Научиться применять эффективные меры сетевой безопасности, включая *брандмауэры*, системы обнаружения вторжений (IDS) и сегментацию сети
- Ознакомить студентов с новыми сетевыми технологиями, такими как программно-определяемые сети (SDN), и понять их влияние на безопасность
- Развить навыки обеспечения безопасности сетевых коммуникаций, включая защиту от таких угроз, как *сниффинг* и атаки типа "человек посередине"
- Научиться оценивать и улучшать конфигурации безопасности в корпоративных сетевых средах, обеспечивая адекватную защиту
- Развить навыки реализации эффективных мер по борьбе с угрозами в корпоративных сетях, от внутренних атак до внешних угроз

- Способствовать эффективному сотрудничеству с командами безопасности, объединяя стратегии и усилия по защите сетевой инфраструктуры
- Продвигать этические и правовые практики при реализации мер сетевой безопасности, обеспечивая соблюдение этических принципов во всех видах деятельности

Модуль 7. 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 *вредоносным программам*, позволяющим выявлять индикаторы компрометации (IoC) и модели атак
- Изучить стратегии эффективного обнаружения вредоносного ПО, 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 8. 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 9. 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* или 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

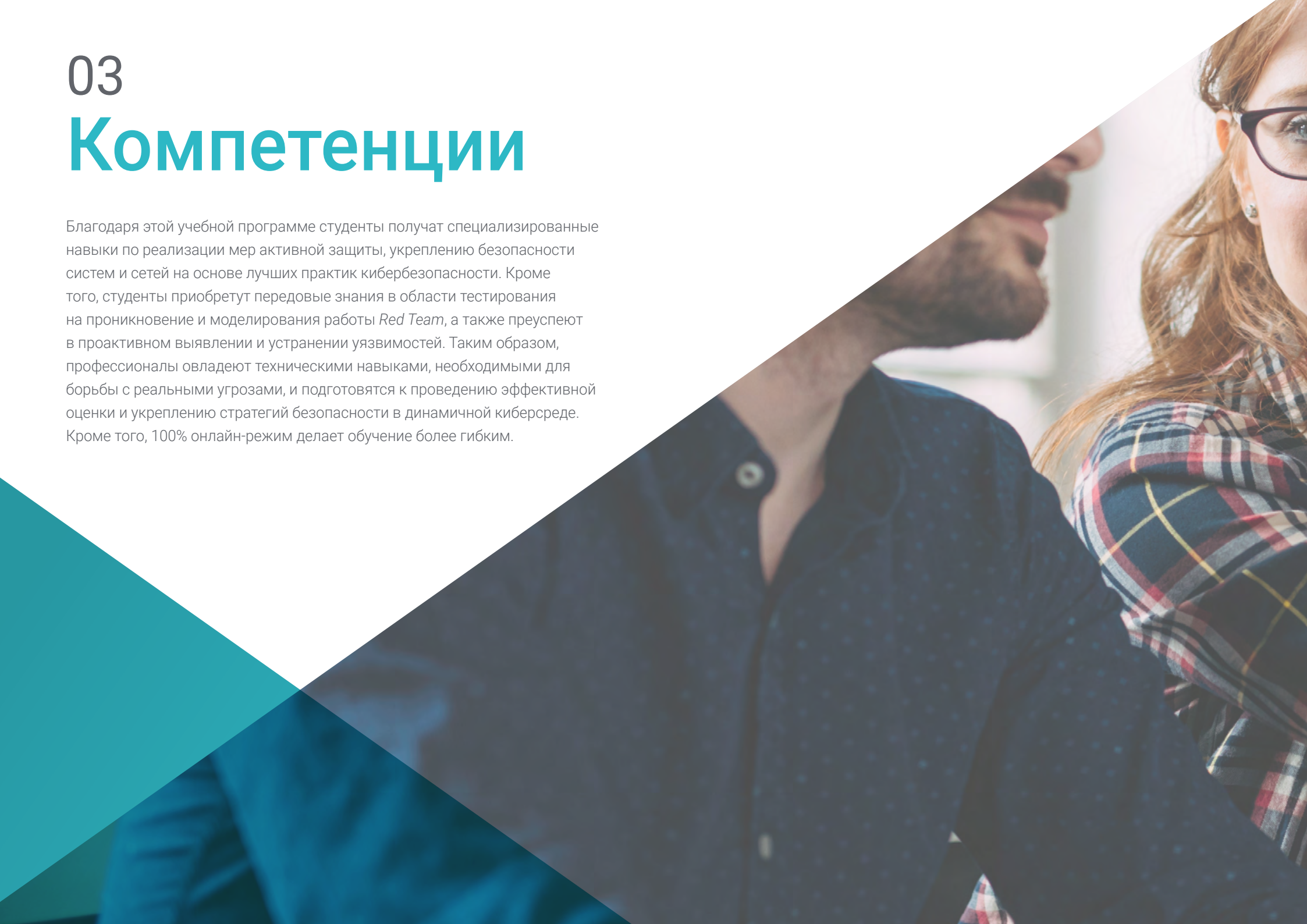
Модуль 10. Техническая и исполнительная отчетность

- Развить навыки подготовки подробных технических отчетов, четко и всесторонне представляющих результаты, использованные методики и рекомендации
- Научиться эффективно общаться с технической группой, используя точные и подходящие формулировки для передачи сложной технической информации
- Развить навыки формулирования практических рекомендаций, направленных на устранение уязвимостей и повышение уровня безопасности
- Научиться оценивать потенциальное воздействие выявленных уязвимостей, учитывая технические, операционные и стратегические вопросы
- Ознакомить студента с лучшими практиками составления отчетов для руководителей, адаптации технических отчетов для нетехнической аудитории
- Развить навыки согласования выводов и рекомендаций со стратегическими и оперативными целями организации
- Научиться использовать инструменты визуализации данных для графического представления информации, содержащейся в отчетах, для облегчения ее понимания
- Способствовать включению в отчеты соответствующей информации о соответствии нормативным требованиям и стандартам, обеспечивая соблюдение правовых требований
- Поощрять эффективное сотрудничество между техническими и руководящими сотрудниками, обеспечивая понимание и поддержку мер по улучшению, предлагаемых в отчете

03

Компетенции

Благодаря этой учебной программе студенты получат специализированные навыки по реализации мер активной защиты, укреплению безопасности систем и сетей на основе лучших практик кибербезопасности. Кроме того, студенты приобретут передовые знания в области тестирования на проникновение и моделирования работы *Red Team*, а также преуспеют в проактивном выявлении и устранении уязвимостей. Таким образом, профессионалы овладеют техническими навыками, необходимыми для борьбы с реальными угрозами, и подготовятся к проведению эффективной оценки и укреплению стратегий безопасности в динамичной киберсреде. Кроме того, 100% онлайн-режим делает обучение более гибким.



Станьте экспертом в области кибербезопасности благодаря 1 800 часам лучшего мультимедийного материала со знаком качества TECH"

Общие профессиональные навыки

- Приобрести навыки планирования, выполнения и управления проектами в области кибербезопасности, обеспечивая эффективные результаты и соответствие поставленным целям
- Овладеть передовыми знаниями в области сетевой архитектуры и ее аспектов безопасности, оценки уязвимостей и применение стратегий по укреплению инфраструктуры
- Развить навыки в области цифровой криминалистики и реагирования на инциденты – от сбора доказательств до устранения угроз и восстановления работоспособности
- Применять передовые тактики при планировании и проведении учений *Red Team*, моделируя реальные сценарии для оценки устойчивости инфраструктуры, выявления слабых мест и повышения готовности к киберугрозам

Получите новые знания в процессе выявления, оценки и снижения рисков, характерных для проектов по кибербезопасности. Выбирайте TECH!"

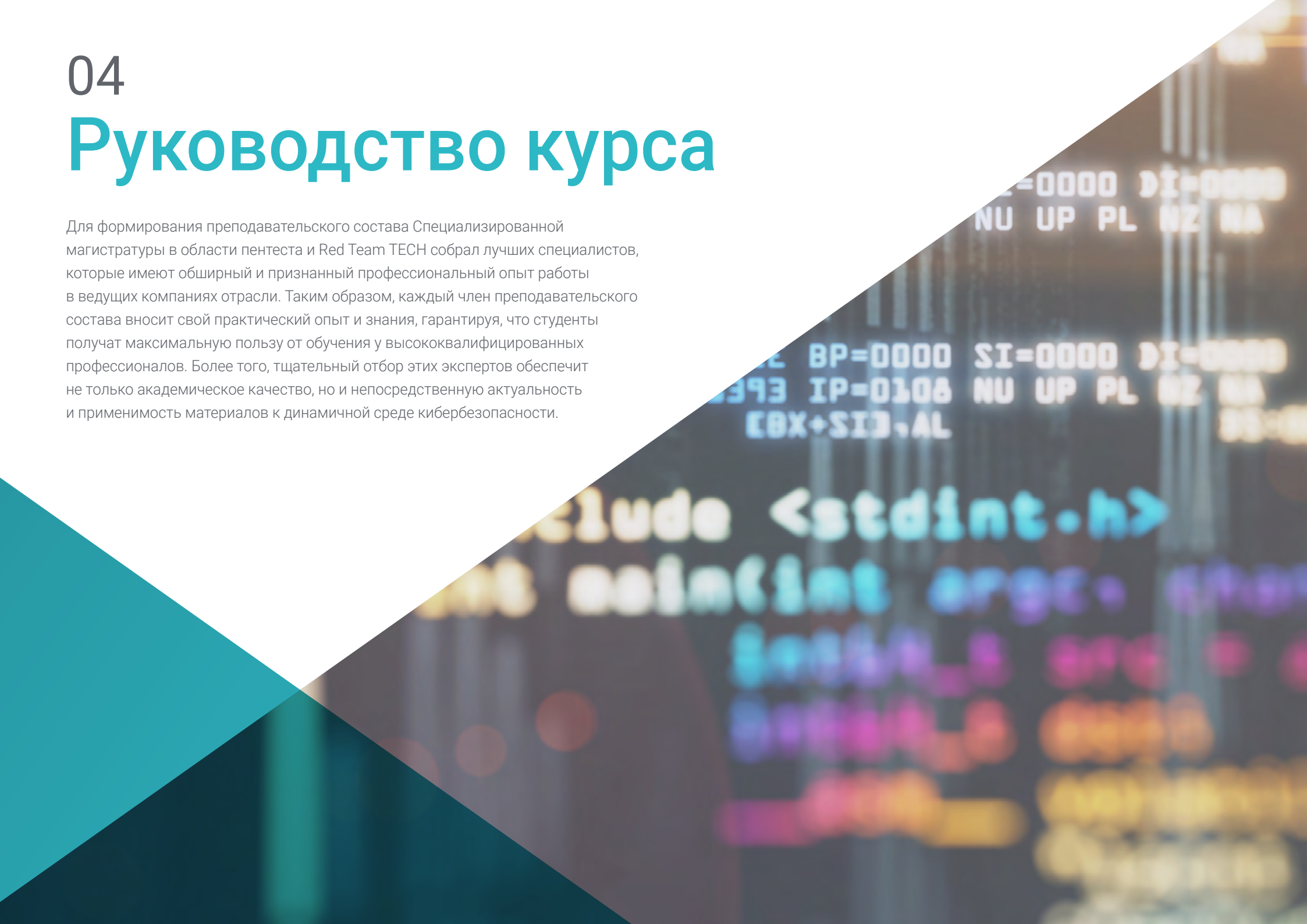
Профессиональные навыки

- Приобрести навыки коучинга для профессионального развития членов команды, стимулирования роста и совершенствования
- Развить навыки принятия стратегических решений в ситуациях кибербезопасности, учитывая краткосрочное и долгосрочное влияние на организационную безопасность
- Приобрести навыки выявления, оценки и снижения рисков, характерных для проектов по кибербезопасности
- Развить навыки реализации мер активной защиты, усиления системной и сетевой безопасности
- Освоить методы анализа веб-трафика для выявления закономерностей и аномального поведения, облегчающие обнаружение возможных угроз
- Приобрести навыки криминалистического анализа применительно к сетевым средам, что позволит выявления и эффективного реагирования на кибер-инциденты
- Изучить стратегии эффективного обнаружения вредоносных программ, включая развертывание передовых решений в области безопасности
- Развить навыки выявления индикаторов компрометации (IoC) в ходе криминалистического исследования, облегчить судебно-экспертного расследования, облегчения обнаружения и реагирования на инциденты
- Приобрести навыки стратегического планирования учений *Red Team* с учетом целей, масштаба, ресурсов и реалистичных сценариев
- Овладеть навыками идентификации и приоритизации уязвимостей, выделяя те из них, которые представляют наибольший риск для безопасности

04

Руководство курса

Для формирования преподавательского состава Специализированной магистратуры в области пентеста и Red Team TECH собрал лучших специалистов, которые имеют обширный и признанный профессиональный опыт работы в ведущих компаниях отрасли. Таким образом, каждый член преподавательского состава вносит свой практический опыт и знания, гарантируя, что студенты получат максимальную пользу от обучения у высококвалифицированных профессионалов. Более того, тщательный отбор этих экспертов обеспечит не только академическое качество, но и непосредственную актуальность и применимость материалов к динамичной среде кибербезопасности.



Гиганты индустрии кибербезопасности приведут вас к успеху всего за 12 месяцев обучения по этой уникальной программе 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 Силес Рубиа, Марселино

- Инженер по кибербезопасности
- Степень бакалавра в области инженерии кибербезопасности в Университете короля Хуана Карлоса
- Навыки: Конкурентное программирование, *веб-хакинг, Active Directory и защита от вредоносных программ*
- Победитель конкурса AdaByron

Г-н Редондо Кастро, Пабло

- Пентестер в Grupo Oesía
- Степень бакалавра в области инженерии кибербезопасности в Университете короля Хуана Карлоса
- Большой опыт работы в качестве *эксперта по кибербезопасности в компании* Traineev
- Обладает преподавательским опытом, проводит тренинги, связанные с турнирами по Capture The Flag

Г-н Гонсалес Паррилья, Юба

- Координатор проектов по наступательной линии безопасности и Red Team
- Специалист по *предиктивному* управлению проектами в Project Management Institute
- Специалист по *SmartDefense*
- Эксперт по *тестированию веб-приложений на предмет проникновения* в eLearnSecurity
- *Младший тестировщик на проникновение* в eLearnSecurity
- Степень бакалавра в области компьютерной инженерии в Политехническом университете Мадрида

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

Г-н Вильяверде, Давид

- Консультант по кибербезопасности в компании Cipherbit
- Эксперт сложных хакерских платформ и HackTheBox
- Специалист по пентесту
- Эксперт по вредоносным программам
- Степень бакалавра в области программирования, специализирующийся на кибербезопасности в Университетском центре технологий и цифрового искусства Лас-Розас

Г-н Кастильо, Карлос

- Консультант по кибербезопасности и специалист по работе с красными командами в Cipherbit
- Сертифицированный профессионал Offensive Security Wireless
- Тестер на проникновение в веб-приложения eLearnSecurity
- Сертифицированный профессиональный тестировщик на проникновение v2 eLearnSecurity
- Младший тестировщик на проникновение eLearnSecurity
- Консультант по кибербезопасности
- Степень бакалавра в области программирования в Политехническом университете Мадрида

Г-н Вебер Санчес, Алехандро

- Пентестер в Grupo Oesía
- Консультант по кибербезопасности в Integración Tecnológica Empresarial, S.L
- Аудиовизуальный техник в компании Ingeniería Audiovisual S.A
- Степень бакалавра в области кибербезопасности в Университете короля Хуана Карлоса, Мадрид

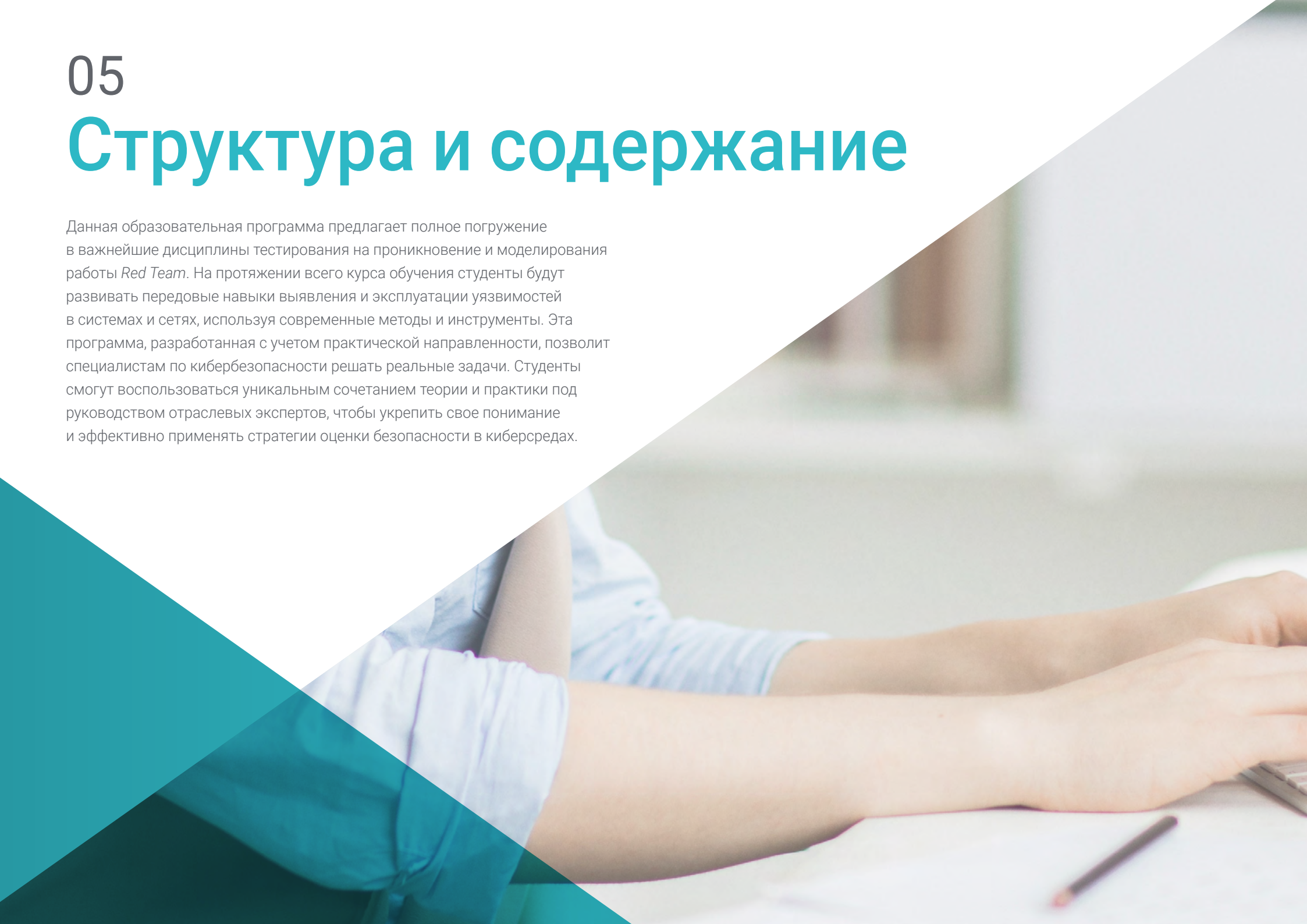
Г-н Мора Навас, Серхио

- Консультант по кибербезопасности в Oesía Group
- Степень бакалавра в области кибербезопасности, Университет короля Хуана Карлоса
- Степень бакалавра в области компьютерных технологий Университета Бургоса

05

Структура и содержание

Данная образовательная программа предлагает полное погружение в важнейшие дисциплины тестирования на проникновение и моделирования работы *Red Team*. На протяжении всего курса обучения студенты будут развивать передовые навыки выявления и эксплуатации уязвимостей в системах и сетях, используя современные методы и инструменты. Эта программа, разработанная с учетом практической направленности, позволит специалистам по кибербезопасности решать реальные задачи. Студенты смогут воспользоваться уникальным сочетанием теории и практики под руководством отраслевых экспертов, чтобы укрепить свое понимание и эффективно применять стратегии оценки безопасности в киберсредах.



Вы познакомитесь с различными ролями и обязанностями команды специалистов по кибербезопасности. Поступайте сейчас!"

Модуль 1. Наступательная безопасность

1.1. Определение и контекст
- 1.1.1. Фундаментальные концепции наступательной безопасности
- 1.1.2. Важность кибербезопасности сегодня
- 1.1.3. Вызовы и возможности в области наступательной безопасности

1.2. Основы кибербезопасности
- 1.2.1. Первые вызовы и эволюционирующие угрозы
- 1.2.2. Технологические этапы и их влияние на кибербезопасность
- 1.2.3. Кибербезопасность в современную эпоху

1.3. Основы наступательной безопасности
- 1.3.1. Ключевые понятия и терминология
- 1.3.2. *Думайте нестандартно*
- 1.3.3. Различия между наступательным и оборонительным хакингом

1.4. Методики наступательной безопасности
- 1.4.1. PTES (*Penetration Testing Execution Standard*)
- 1.4.2. OWASP (*Open Web Application Security Project*)
- 1.4.3. *Cyber Security Kill Chain*

1.5. Роли и обязанности в наступательной безопасности
- 1.5.1. Основные профили
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Исследования:* Искусство исследования

1.6. Арсенал наступающего аудитора
- 1.6.1. Операционные системы для *хакерства*
- 1.6.2. Введение в C2
- 1.6.3. *Metasploit*: Основы и применение
- 1.6.4. Полезные технологические ресурсы

1.7. OSINT: Информация в открытых источников
- 1.7.1. Основы OSINT
- 1.7.2. Техники и инструменты OSINT
- 1.7.3. Применение OSINT в наступательной безопасности

1.8. *Написание скриптов*: Введение в автоматизацию
- 1.8.1. Основы написания скриптов
- 1.8.2. Создание *скриптов* на Bash
- 1.8.3. Создание *скриптов* на Python

1.9. Классификация уязвимостей
- 1.9.1. CVE (*Common Vulnerabilities and Exposure*)
- 1.9.2. CWE (*Common Weakness Enumeration*)
- 1.9.3. CAPEC (*Common Attack Pattern Enumeration and Classification*)
- 1.9.4. CVSS (*Common Vulnerability Scoring System*)
- 1.9.5. MITRE ATT & CK

1.10. Этика и *хакинг*
- 1.10.1. Принципы *хакерской* этики
- 1.10.2. Граница между *этичным* хакингом и злонамеренным *взломом*
- 1.10.3. Правовые последствия и ответственность
- 1.10.4. Кейс-стади: Этические ситуации в кибербезопасности

Модуль 2. Управление командами кибербезопасности

2.1. Руководство командой
- 2.1.1. Кто есть кто
- 2.1.2. Руководитель
- 2.1.3. Выводы

2.2. Роли и обязанности
- 2.2.1. Определение ролей
- 2.2.2. Эффективное делегирование
- 2.2.3. Управление ожиданиями

2.3. Формирование и развитие команды
- 2.3.1. Этапы формирования команды
- 2.3.2. Групповая динамика
- 2.3.3. Оценка и обратная связь

2.4. Управление талантами
- 2.4.1. Идентификация талантов
- 2.4.2. Развитие способностей
- 2.4.3. Удержание талантов

2.5. Лидерство и мотивация команды
- 2.5.1. Стили лидерства
- 2.5.2. Теории мотивации
- 2.5.3. Признание достижений

2.6. Коммуникация и координация
- 2.6.1. Средства коммуникации
- 2.6.2. Барьеры для коммуникации
- 2.6.3. Стратегии координации

2.7. Стратегическое планирование развития персонала
- 2.7.1. Определение потребностей в обучении
- 2.7.2. Индивидуальные планы развития
- 2.7.3. Мониторинг и оценка

2.8. Разрешение конфликтов
- 2.8.1. Выявление конфликтов
- 2.8.2. Методы измерения
- 2.8.3. Предотвращение конфликтов

2.9. Управление качеством и постоянное улучшение
- 2.9.1. Принципы качества
- 2.9.2. Методы непрерывного улучшения
- 2.9.3. *Обратная связь* и отзывы

2.10. Инструменты и технологии
- 2.10.1. Платформы для совместной работы
- 2.10.2. Управление проектами
- 2.10.3. Выводы

Модуль 3. Управление проектами безопасности

3.1. Управление проектами безопасности
- 3.1.1. Определение и цель управления проектами в кибербезопасности
- 3.1.2. Основные проблемы
- 3.1.3. Соображения

3.2. Соображения
- 3.2.1. Жизненный цикл проекта по безопасности
- 3.2.2. Реализация и выполнение
- 3.2.3. Оценка и анализ

3.3. Планирование и оценка ресурсов
- 3.3.1. Основные концепции управления бюджетом
- 3.3.2. Определение человеческих и технических ресурсов
- 3.3.3. Составление бюджета и сопутствующие расходы

3.4. Реализация и контроль проекта
- 3.4.1. Мониторинг и последующие действия
- 3.4.2. Адаптация и изменения в проекте
- 3.4.3. Среднесрочная оценка и обзоры

3.5. Коммуникация и отчетность по проекту
- 3.5.1. Стратегии эффективной коммуникации
- 3.5.2. Отчетность и презентации
- 3.5.3. Коммуникация с клиентами и руководством

3.6. Инструменты и технологии
- 3.6.1. Инструменты для планирования и организации
- 3.6.2. Инструменты для совместной работы и коммуникации
- 3.6.3. Инструменты для работы с документацией и хранения данных

3.7. Документация и протоколы
- 3.7.1. Структурирование и создание документации
- 3.7.2. Протоколы действий
- 3.7.3. Руководства

3.8. Регулирование и соблюдение требований в проектах по кибербезопасности
- 3.8.1. Международные законы и нормы
- 3.8.2. Соответствие требованиям
- 3.8.3. Аудиты

3.9. Управление рисками в проектах по безопасности
- 3.9.1. Идентификация и анализ рисков
- 3.9.2. Стратегии снижения рисков
- 3.9.3. Мониторинг и обзор рисков

3.10. Закрытие проекта
- 3.10.1. Обзор и оценка
- 3.10.2. Итоговая документация
- 3.10.3. Обратная связь

Модуль 4. Атаки на сети и системы Windows

4.1. Windows и Active Directory
- 4.1.1. История и эволюция Windows
- 4.1.2. Основы Active Directory
- 4.1.3. Функции и службы Active Directory
- 4.1.4. Общая архитектура Active Directory

4.2. Сетевая структура в средах Active Directory
- 4.2.1. Сетевые протоколы в Windows
- 4.2.2. DNS и его работа в Active Directory
- 4.2.3. Средства диагностики сети
- 4.2.4. Реализация сети в Active Directory

4.3. Аутентификация и авторизация в Active Directory
- 4.3.1. Процесс и поток аутентификации
- 4.3.2. Типы учетных данных
- 4.3.3. Хранение и управление учетными данными
- 4.3.4. Безопасность аутентификации

4.4. Разрешения и политики в Active Directory
- 4.4.1. GPO
- 4.4.2. Применение и управление GPO
- 4.4.3. Управление разрешениями в Active Directory
- 4.4.4. Уязвимости разрешений и их устранение

4.5. Основы Kerberos
- 4.5.1. Что такое Kerberos?
- 4.5.2. Компоненты и работа
- 4.5.3. Тикеты в Kerberos
- 4.5.4. Kerberos в контексте Active Directory

4.6. Передовые методы в Kerberos
- 4.6.1. Распространенные атаки на Kerberos
- 4.6.2. Профилактика и защита
- 4.6.3. Мониторинг трафика Kerberos
- 4.6.4. Расширенные атаки на Kerberos

4.7. *Службы сертификатов Active Directory* (ADCS)
- 4.7.1. Основные концепции PKI
- 4.7.2. Роли и компоненты ADCS
- 4.7.3. Конфигурация и развертывание ADCS
- 4.7.4. Безопасность ADCS

4.8. Атаки и защита *служб сертификатов Active Directory* (ADCS)
- 4.8.1. Распространенные уязвимости в ADCS
- 4.8.2. Атаки и методы эксплуатации
- 4.8.3. Защита и смягчение последствий
- 4.8.4. Мониторинг и аудит ADCS

4.9. Аудит Active Directory
- 4.9.1. Важность аудита Active Directory
- 4.9.2. Инструменты аудита
- 4.9.3. Обнаружение аномалий и подозрительного поведения
- 4.9.4. Реагирование на инциденты и восстановление

4.10. Azure AD
- 4.10.1. Основы Azure AD
- 4.10.2. Синхронизация с локальной Active Directory
- 4.10.3. Управление идентификацией в Azure AD
- 4.10.4. Интеграция с приложениями и службами

Модуль 5. Продвинутый веб-*хакинг*

5.1. Функции DAO
- 5.1.1. URL и его части
- 5.1.2. Методы HTTP
- 5.1.3. Заголовки
- 5.1.4. Как просматривать веб-запросы с помощью Burp Suite

5.2. Сессии
- 5.2.1. *Cookies*
- 5.2.2. JWT-*Tokens*
- 5.2.3. Атаки с перехватом сеанса
- 5.2.4. Атаки на JWT

5.3. *Межсайтовый скриптинг* (XSS)
- 5.3.1. Что такое XSS
- 5.3.2. Типы XSS
- 5.3.3. Эксплуатация XSS
- 5.3.4. Введение в *XSLeaks*

5.4. Инъекции в базу данных
- 5.4.1. Что такое *SQL-инъекция*
- 5.4.2. Перехват информации с помощью *SQLi*
- 5.4.3. *Слепая, основанная на времени и основанная на ошибках SQLi*
- 5.4.4. NoSQLi инъекции

5.5. *Path Traversal* и *Local File Inclusion*
- 5.5.1. Что это такое и в чем их отличие
- 5.5.2. Общие фильтры и способы их обхода
- 5.5.3. *Log Poisoning*
- 5.5.4. LFI в PHP

5.6. *Нарушенная аутентификация*
- 5.6.1. *Перечисление пользователей*
- 5.6.2. *Брутфорс*
- 5.6.3. *Обход 2FA*
- 5.6.4. Файлы *cookies* с уязвимой и модифицируемой информацией

5.7. *Удаленное выполнение команд*
- 5.7.1. *Command Injection*
- 5.7.2. *Blind Command Injection*
- 5.7.3. *Небезопасная десериализация PHP*
- 5.7.4. *Небезопасная десериализация Java*

5.8. *Загрузка файлов*
- 5.8.1. RCE через *веб-оболочки*
- 5.8.2. XSS при загрузке файлов
- 5.8.3. *Инъекция* XML *External Entity* (XXE)
- 5.8.4. *Обходные пути* при загрузке файлов

5.9. *Нарушенный контроль доступа*
- 5.9.1. Неограниченный доступ к панелям
- 5.9.2. *Небезопасные прямые ссылки на объекты* (IDOR)
- 5.9.3. Обход фильтров
- 5.9.4. Недостаточные методы авторизации

5.10. Уязвимости DOM и более сложные атаки
- 5.10.1. *Regex Denial of Service*
- 5.10.2. DOM *Clobbering*
- 5.10.3. *Prototype Pollution*
- 5.10.4. Контрабанда *HTTP-запросов*

Модуль 6. Сетевая архитектура и безопасность

6.1. Информационные сети
- 6.1.1. Основные понятия: Протоколы LAN, WAN, CP, CC
- 6.1.2. Модель OSI и TCP/IP
- 6.1.3. *Коммутация:* Основные понятия
- 6.1.4. *Маршрутизация:* Основные понятия

6.2. *Коммутация*
- 6.2.1. Введение в виртуальные локальные сети VLAN
- 6.2.2. STP
- 6.2.3. *EtherChannel*
- 6.2.4. Атаки второго уровня OSI

6.3. VLAN
- 6.3.1. Важность виртуальных локальных сетей
- 6.3.2. Уязвимости в виртуальных локальных сетях
- 6.3.3. Распространенные атаки на виртуальные локальные сети
- 6.3.4. Средства защиты

6.4. *Маршрутизация*
- 6.4.1. IP-адресация - IPv4 и IPv6
- 6.4.2. Маршрутизация: Ключевые понятия
- 6.4.3. Статическая маршрутизация
- 6.4.4. Динамическая маршрутизация: Введение

6.5. Протоколы IGP
- 6.5.1. RIP
- 6.5.2. OSPF
- 6.5.3. RIP vs OSPF
- 6.5.4. Анализ требований к топологии

6.6. Защита периметра
- 6.6.1. DMZ
- 6.6.2. *Брандмауэры*
- 6.6.3. Общие архитектуры
- 6.6.4. *Доступ к сети Zero Trust*

6.7. IDS и IPS
- 6.7.1. Характеристики
- 6.7.2. Внедрение
- 6.7.3. SIEM и SIEM CLOUDS
- 6.7.4. Детекция на основе *HoneyPots*

6.8. TLS и VPN
- 6.8.1. SSL/TLS
- 6.8.2. TLS: Основные типы атак
- 6.8.3. VPN с TLS
- 6.8.4. VPN с IPSEC

6.9. Безопасность в беспроводных сетях
- 6.9.1. Введение в беспроводные сети
- 6.9.2. Протоколы
- 6.9.3. Ключевые элементы
- 6.9.4. Основные типы атак

6.10. Корпоративные сети и способы их защиты
- 6.10.1. Логическая сегментация
- 6.10.2. Физическая сегментация
- 6.10.3. Контроль доступа
- 6.10.4. Другие меры, которые необходимо принять во внимание

Модуль 7. Анализ и исследование *вредоносных программ*

7.1. Анализ и исследование *вредоносных программ*
- 7.1.1. История и эволюция *вредоносных программ*
- 7.1.2. Классификация и типы *вредоносных программ*
- 7.1.3. Анализ *вредоносных программ*
- 7.1.4. Исследование *вредоносных программ*

7.2. Подготовка среды
- 7.2.1. Настройка виртуальных машин и *Snapshots*
- 7.2.2. Средства анализа *вредоносных программ*
- 7.2.3. Средства разработки *вредоносных программ*

7.3. Основы Windows
- 7.3.1. Формат файлов PE (*Portable Executable*)
- 7.3.2. Процессы и *потоки*
- 7.3.3. Файловая система и реестр
- 7.3.4. *Защитник Windows*

7.4. Основные методы борьбы с вредоносными программами
- 7.4.1. Генерация *шелл-кода*
- 7.4.2. Выполнение *шелл-кода* на диске
- 7.4.3. Диск против оперативной памяти
- 7.4.4. Выполнение шелл-кода в памяти

7.5. Промежуточные техники вредоносных программ
- 7.5.1. Устойчивость Windows
- 7.5.2. Стартовая папка
- 7.5.3. Ключи реестра
- 7.5.4. Скринсейверы

7.6. Передовые методы работы с *вредоносными программами*
- 7.6.1. Шифрование *шелл-кода* (XOR)
- 7.6.2. Шифрование *шелл-кода* (RSA)
- 7.6.3. Обфускация *строк*
- 7.6.4. Инъекция в процессы

7.7. Статический анализ *вредоносных программ*
- 7.7.1. Анализ *упаковщиков* с помощью DIE (Detect It Easy)
- 7.7.2. Анализ секций с помощью PE-Bear
- 7.7.3. Декомпиляция с помощью Ghidra

7.8. Динамический анализ *вредоносных программ*
- 7.8.1. Наблюдение за поведением с помощью Process Hacker
- 7.8.2. Анализ вызовов с помощью API Monitor
- 7.8.3. Анализ изменений в реестре с помощью Regshot
- 7.8.4. Наблюдение за сетевыми запросами с помощью TCPView

7.9. Анализ в .NET
- 7.9.1. Введение в .NET
- 7.9.2. Декомпиляция с помощью dnSpy
- 7.9.3. Отладка с помощью dnSpy

7.10. Анализ реальных *вредоносных программ*
- 7.10.1. Подготовка среды
- 7.10.2. Статический анализ *вредоносных программ*
- 7.10.3. Динамический анализ *вредоносных программ*
- 7.10.4. Создание правил YARA

Модуль 8. Основы криминалистики и DFIR

8.1. Цифровая криминалистика
- 8.1.1. История и развитие компьютерной криминалистики
- 8.1.2. Важность компьютерной криминалистики в кибербезопасности
- 8.1.3. История и развитие компьютерной криминалистики

8.2. Основы компьютерной криминалистики
- 8.2.1. Цепочка хранения и ее применение
- 8.2.2. Виды цифровых улик
- 8.2.3. Процессы получения улик

8.3. Системы хранения и структура данных
- 8.3.1. Основные системы хранения
- 8.3.2. Методы сокрытия данных
- 8.3.3. Анализ метаданных и атрибутов файлов

8.4. Анализ операционных систем
- 8.4.1. Криминалистический анализ систем Windows
- 8.4.2. Криминалистический анализ систем Linux
- 8.4.3. Криминалистический анализ систем macOS

8.5. Восстановление данных и анализ дисков
- 8.5.1. Восстановление данных с поврежденных носителей
- 8.5.2. Инструменты для анализа дисков
- 8.5.3. Интерпретация файловых систем

8.6. Анализ сети и трафика
- 8.6.1. Захват и анализ сетевых пакетов
- 8.6.2. Анализ журналов *брандмауэра*
- 8.6.3. Обнаружение сетевых вторжений

8.7. Анализ вредоносных программ и вредоносного кода
- 8.7.1. Классификация *вредоносных программ* и их характеристики
- 8.7.2. Статический и динамический анализ *вредоносных программ*
- 8.7.3. Методы деассемблирования и отладки

8.8. Анализ журналов и событий
- 8.8.1. Типы журналов в системах и приложениях
- 8.8.2. Интерпретация соответствующих событий
- 8.8.3. Инструменты анализа журналов

8.9. Реагирование на инциденты безопасности
- 8.9.1. Процесс реагирования на инциденты
- 8.9.2. Создание плана реагирования на инциденты
- 8.9.3. Координация действий с командами безопасности

8.10. Представление улик и доказательств
- 8.10.1. Правила представления цифровых доказательств в правовой среде
- 8.10.2. Подготовка отчетов о судебной экспертизе
- 8.10.3. Выступление в суде в качестве свидетеля-эксперта

Модуль 9. Продвинутые учения *Red Team*

9.1. Продвинутые методы исследования
- 9.1.1. Продвинутое перечисление субдоменов
- 9.1.2. Продвинутый *Google Dorking*
- 9.1.3. Социальные сети и theHarvester

9.2. Продвинутые *фишинговые* операции
- 9.2.1. Что такое *фишинг с обратным прокси*
- 9.2.2. *Обход 2FA* с помощью Evilginx
- 9.2.3. Эксфильтрация данных

9.3. Продвинутые техники устойчивости
- 9.3.1. *Золотые билеты*
- 9.3.2. *Серебряные билеты*
- 9.3.3. Техника *DCShadow*

9.4. Продвинутые техники предотвращения
- 9.4.1. Обход AMSI
- 9.4.2. Модификация существующих инструментов
- 9.4.3. Обфускация *Powershell*

9.5. Продвинутые техники латерального перемещения
- 9.5.1. *Pass-the-Ticket* (PtT)
- 9.5.2. *Overpass-the-Hash* (Pass-the-Key)
- 9.5.3. Ретрансляция NTLM

9.6. Продвинутые техники пост-эксплойтов
- 9.6.1. *Дамп* LSASS
- 9.6.2. *Дамп* SAM
- 9.6.3. Атака *DCSync*

9.7. Продвинутые техники *пивотирования*
- 9.7.1. Что такое *пивотирование*
- 9.7.2. Туннелирование SSH
- 9.7.3. Пивотирование с помощью Chisel

9.8. Физические вторжения
- 9.8.1. Наблюдение и разведка
- 9.8.2. *Tailgating* и *Piggybacking*
- 9.8.3. *Lock-Picking*

9.9. Атаки Wi-Fi
- 9.9.1. Атаки WPA/WPA2 PSK
- 9.9.2. Атаки на неавторизованные точки доступа
- 9.9.3. Атаки на WPA2 *Enterprise*

9.10. Атаки RFID
- 9.10.1. Считывание RFID-карт
- 9.10.2. Манипуляции с RFID-картами
- 9.10.3. Создание клонированных карт

Модуль 10. Техническая и исполнительная отчетность

10.1. Процесс отчетности
- 10.1.1. Структура отчета
- 10.1.2. Процесс отчетности
- 10.1.3. Ключевые понятия
- 10.1.4. Исполнительный vs технический

10.2. Руководства
- 10.2.1. Введение
- 10.2.2. Типы руководств
- 10.2.3. Национальные руководства
- 10.2.4. Примеры использования

10.3. Методики
- 10.3.1. Оценка
- 10.3.2. *Пентест*
- 10.3.3. Обзор общих методологий
- 10.3.4. Знакомство с национальными методологиями

10.4. Технический подход к этапу подготовки отчетности
- 10.4.1. Понимание пределов возможностей *пентестера*
- 10.4.2. Использование и приемы языка
- 10.4.3. Представление информации
- 10.4.4. Распространенные ошибки

10.5. Подход руководителя к этапу подготовки отчета
- 10.5.1. Приведение отчета в соответствие с контекстом
- 10.5.2. Использование и приемы языка
- 10.5.3. Стандартизация
- 10.5.4. Распространенные ошибки

10.6. OSSTMM
- 10.6.1. Понимание методологии
- 10.6.2. Распознавание
- 10.6.3. Документация
- 10.6.4. Подготовка отчета

10.7. LINCE
- 10.7.1. Понимание методологии
- 10.7.2. Распознавание
- 10.7.3. Документация
- 10.7.4. Подготовка отчета

10.8. Отчет об уязвимостях
- 10.8.1. Ключевые понятия
- 10.8.2. Количественная оценка масштаба
- 10.8.3. Уязвимости и доказательства
- 10.8.4. Распространенные ошибки

10.9. Составление отчета для клиента
- 10.9.1. Важность рабочих тестов
- 10.9.2. Решения и снижения рисков
- 10.9.3. Деликатные и важные данные
- 10.9.4. Практические примеры и кейсы

10.10. Отчетность *о пересдачах*
- 10.10.1. Ключевые понятия
- 10.10.2. Понимание унаследованной информации
- 10.10.3. Проверка ошибок
- 10.10.4. Добавление информации

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.

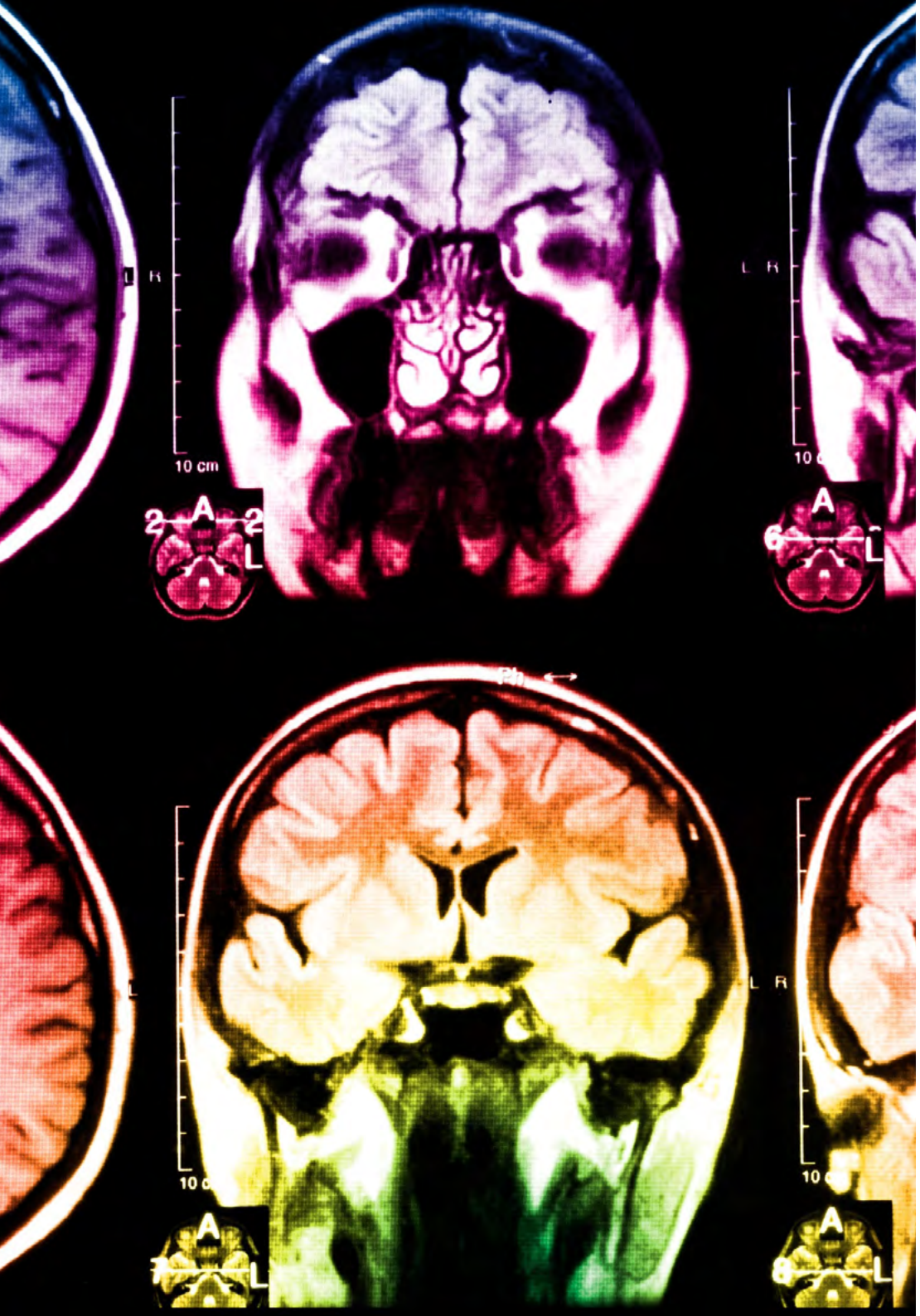
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи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

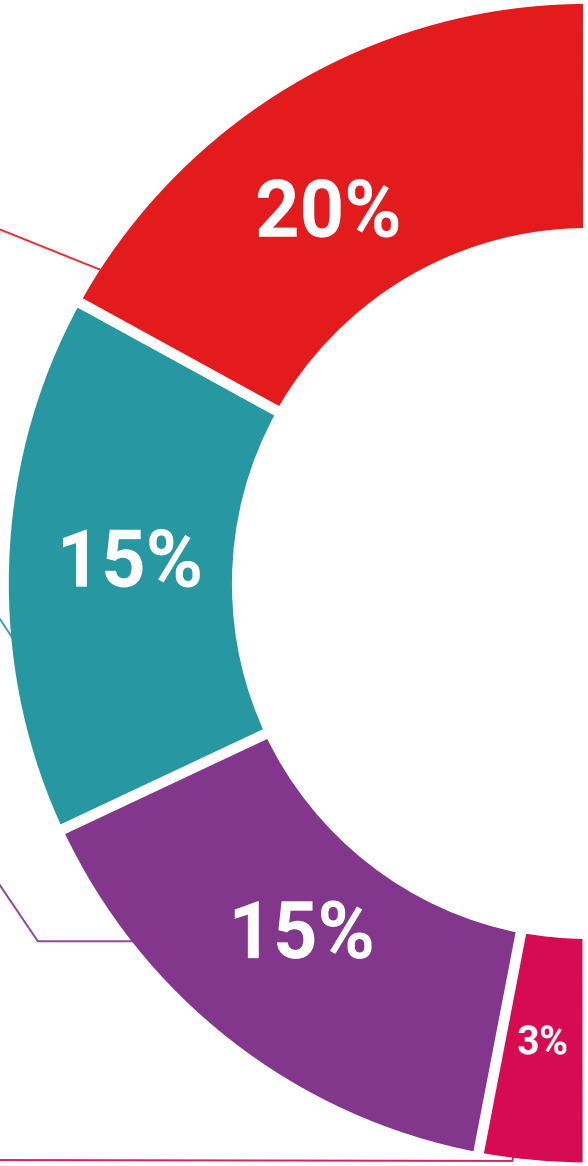
Интерактивные конспекты

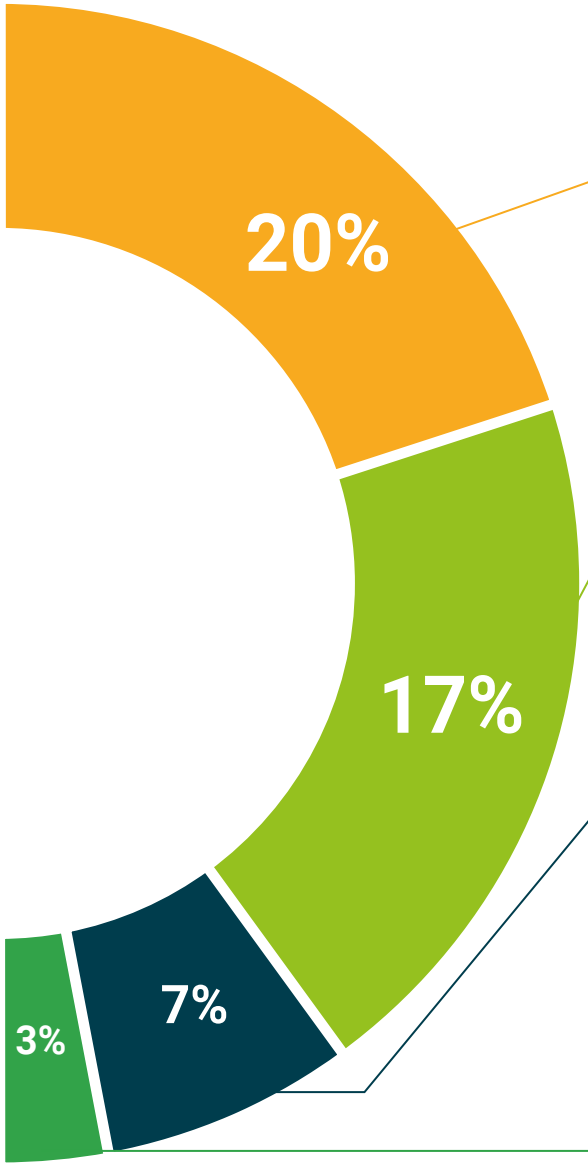
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

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.

07

Квалификация

Специализированная магистратура в области пентеста и Red Team гарантирует, помимо самого строгого и современного обучения, получение диплома об окончании Специализированной магистратуры, выдаваемого TECH Технологическим университетом.

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

Данная **Специализированная магистратура в области пентеста и Red Team** содержит самую полную и современную программу на рынке.

После прохождения аттестации студент получит по почте* с подтверждением получения соответствующий диплом **Специализированной магистратуры,** выданный **TECH Технологическим университетом.**

Диплом, выданный **TECH Технологическим университетом**, подтверждает квалификацию, полученную в Специализированной магистратуре, и соответствует требованиям, обычно предъявляемым биржами труда, конкурсными экзаменами и комитетами по оценке карьеры.

Диплом: **Специализированная магистратура в области пентеста и Red Team**

Формат: **онлайн**

Продолжительность: **12 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

СПЕЦИАЛИЗИРОВАННАЯ МАГИСТРАТУРА

в области

пентеста и Red Team

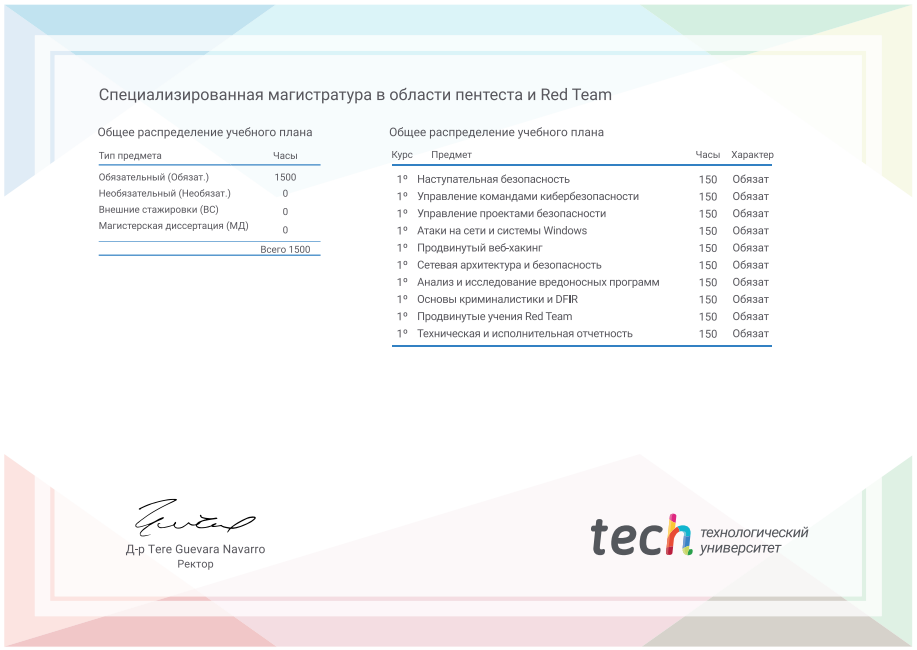
Данный диплом специализированной программы, присуждаемый Университетом, соответствует 1500 учебным часам, с датой начала дд/мм/гггг и датой окончания дд/мм/гггг.

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


Специализированная магистратура в области пентеста и Red Team

Общее распределение учебного плана

Тип предмета	Часы
Обязательный (Обязат.)	1500
Необязательный (Необязат.)	0
Внешние стажировки (ВС)	0
Магистерская диссертация (МД)	0
Всего 1500	

Общее распределение учебного плана

Курс	Предмет	Часы	Характер
1º	Наступательная безопасность	150	Обязат
1º	Управление командами кибербезопасности	150	Обязат
1º	Управление проектами безопасности	150	Обязат
1º	Атаки на сети и системы Windows	150	Обязат
1º	Продвинутый веб-хакинг	150	Обязат
1º	Сетевая архитектура и безопасность	150	Обязат
1º	Анализ и исследование вредоносных программ	150	Обязат
1º	Основы криминалистики и DFIR	150	Обязат
1º	Продвинутые учения Red Team	150	Обязат
1º	Техническая и исполнительная отчетность	150	Обязат

Д-р Tere Guevara Navarro
Ректор

tech технологический университет

*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

Специализированная магистратура

Пентест и Red Team

- Формат: **онлайн**
- Продолжительность: **12 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

Специализированная магистратура

Пентест и Red Team

tech технологический университет