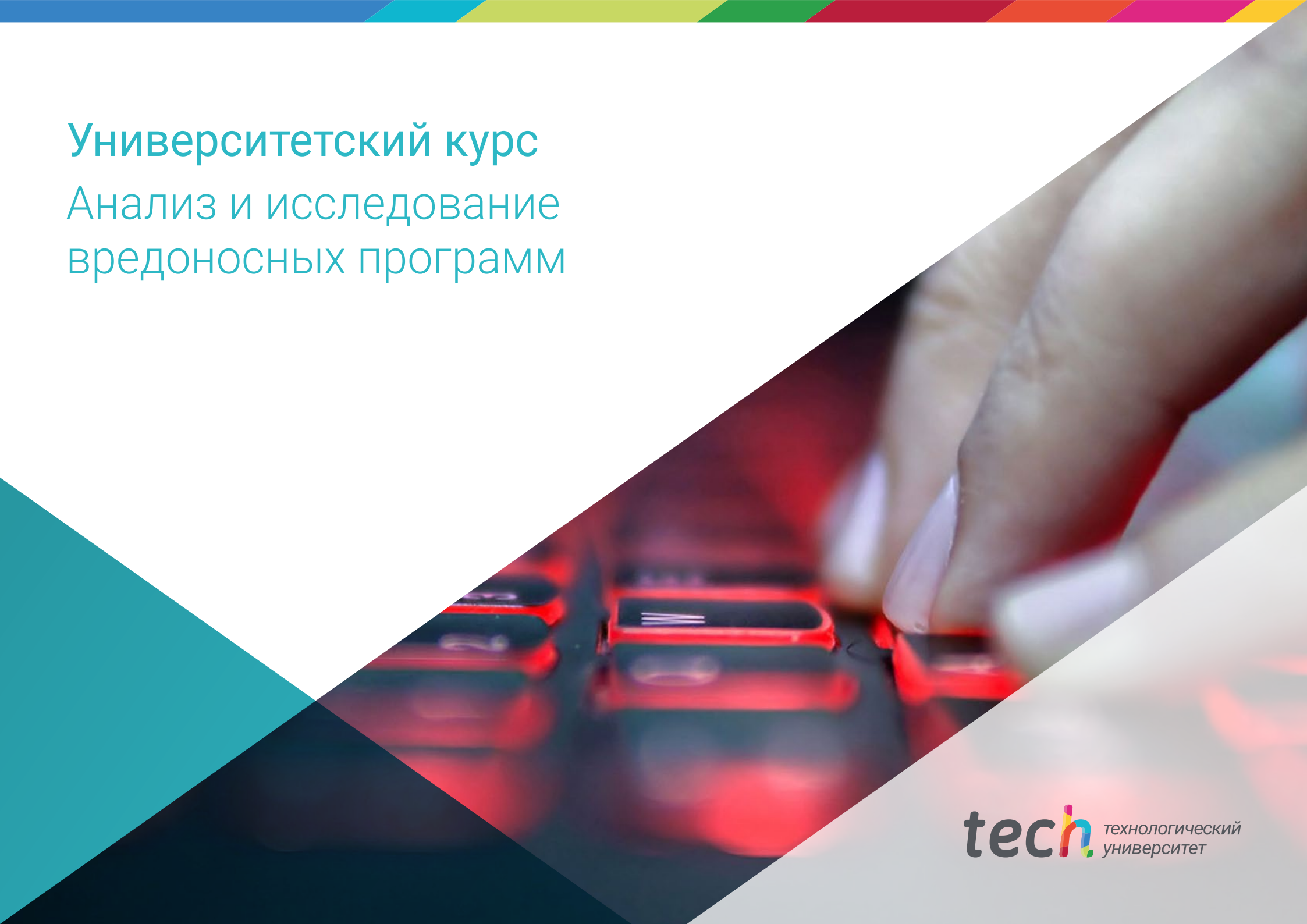
Университетский курс

Анализ и исследование вредоносных программ



tech технологический университет

tech технологический университет

Университетский курс
Анализ и исследование вредоносных программ

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

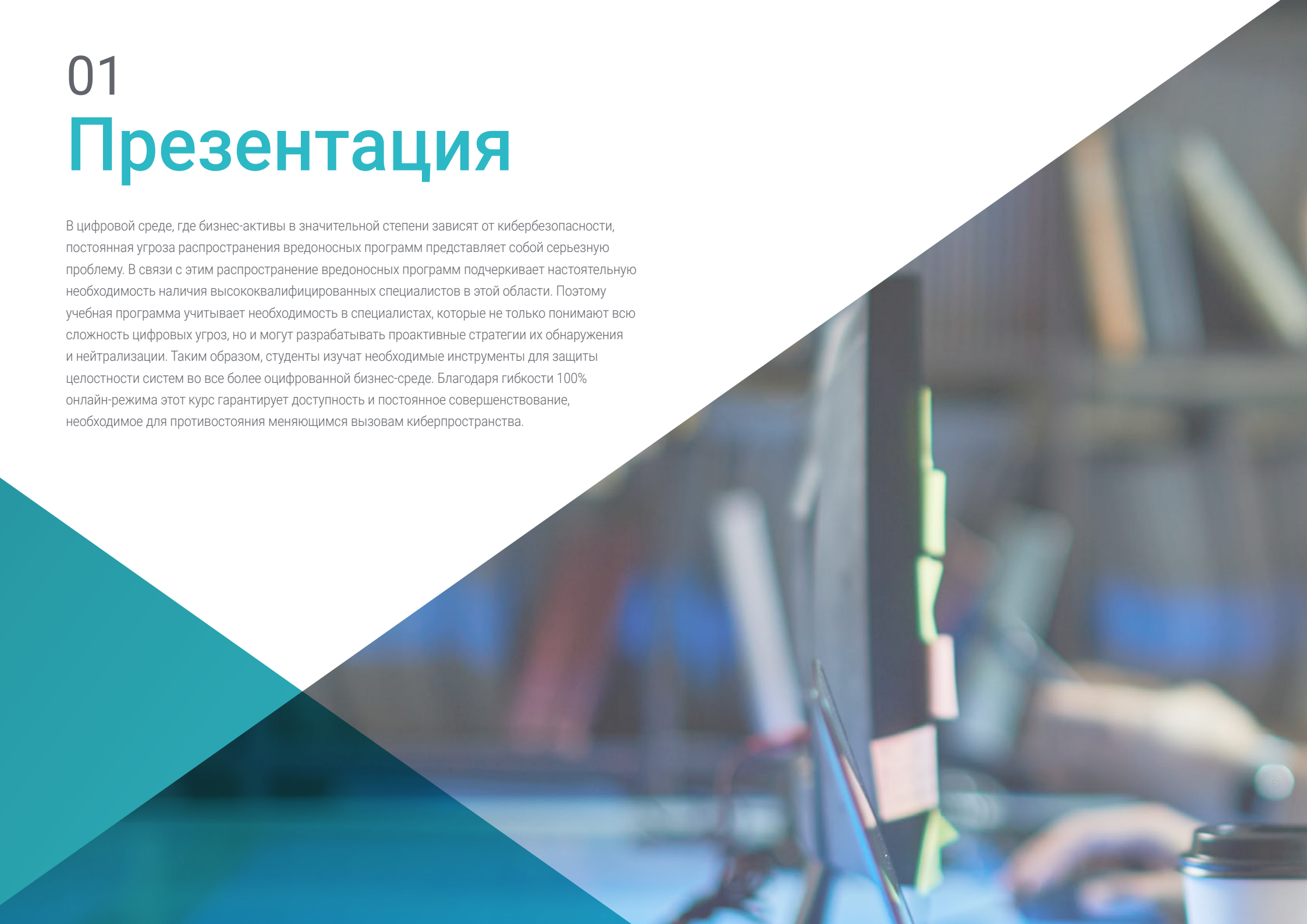
Веб-доступ: www.techtitute.com/ru/information-technology/postgraduate-certificate/malware-analysis-development

Оглавление

01

Презентация

В цифровой среде, где бизнес-активы в значительной степени зависят от кибербезопасности, постоянная угроза распространения вредоносных программ представляет собой серьезную проблему. В связи с этим распространение вредоносных программ подчеркивает настоятельную необходимость наличия высококвалифицированных специалистов в этой области. Поэтому учебная программа учитывает необходимость в специалистах, которые не только понимают всю сложность цифровых угроз, но и могут разрабатывать проактивные стратегии их обнаружения и нейтрализации. Таким образом, студенты изучат необходимые инструменты для защиты целостности систем во все более оцифрованной бизнес-среде. Благодаря гибкости 100% онлайн-режима этот курс гарантирует доступность и постоянное совершенствование, необходимое для противостояния меняющимся вызовам киберпространства.



Станьте экспертом по вредоносным программам, владеющим инновационными методами динамического анализа, с помощью этой уникальной 100% онлайн-программы"

В современном мире кибербезопасности изощренность киберугроз достигла беспрецедентного уровня, что порождает растущий спрос на профессионалов, специализирующихся на анализе и исследовании вредоносных программ. Постоянная эволюция вредоносных тактик требует столь же динамичного ответа от экспертов по кибербезопасности. В этом контексте данная университетская программа TECH является комплексным решением для удовлетворения этих потребностей. Программа охватывает широкий спектр вопросов, начиная от глубокого понимания природы вредоносных программ и заканчивая оценки средств защиты от злоумышленников. Этот комплексный подход готовит специалистов к борьбе с текущими и будущими угрозами.

Учебный план программы TECH по анализу и исследованию вредоносных программ представляет собой надежный источник знаний, охватывающий различные аспекты мира вредоносных программ. Студенты углубленно изучат различные формы и цели вредоносных программ, получат передовые знания об их природе, функциональности и поведении. Программа посвящена криминалистическому анализу вредоносного ПО, что позволяет студентам получить навыки, необходимые для выявления индикаторов компрометации (IoC) и моделей атак, что крайне важно для раннего обнаружения и эффективного реагирования на инциденты безопасности. Кроме того, курс направлен на развитие специальных навыков по оценке и выбору средств защиты от вредоносных программ. Студенты научатся определять эффективность этих инструментов и их адаптируемость к конкретным средам, что очень важно для реализации стратегий защиты от вредоносных программ.

Благодаря инновационному и адаптируемому подходу эта университетская программа представляет собой уникальное учебное предложение. 100% онлайн-форма и методология *Relearning* гарантируют гибкий и эффективный образовательный опыт, позволяя профессионалам продвигаться по карьерной лестнице без перерывов и постоянно адаптироваться к меняющимся требованиям сферы кибербезопасности.

Данный **Университетский курс в области анализа и исследования вредоносных программ** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных экспертами в области анализа и исследования вредоносных программ
- 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 улучшения успеваемости
- Особое внимание уделяется инновационным методологиям
- Теоретические занятия, вопросы эксперту, дискуссионные форумы по спорным темам и самостоятельная работа
- Учебные материалы курса доступны с любого стационарного или мобильного устройства с выходом в интернет

Вы освоите анализ вызовов с помощью API monitor всего за 6 недель лучшего онлайн-обучения"

Вы научитесь генерировать шелл-код в лучшем университете мира по оценкам его студентов согласно платформе Trustpilot (4,9/5)"

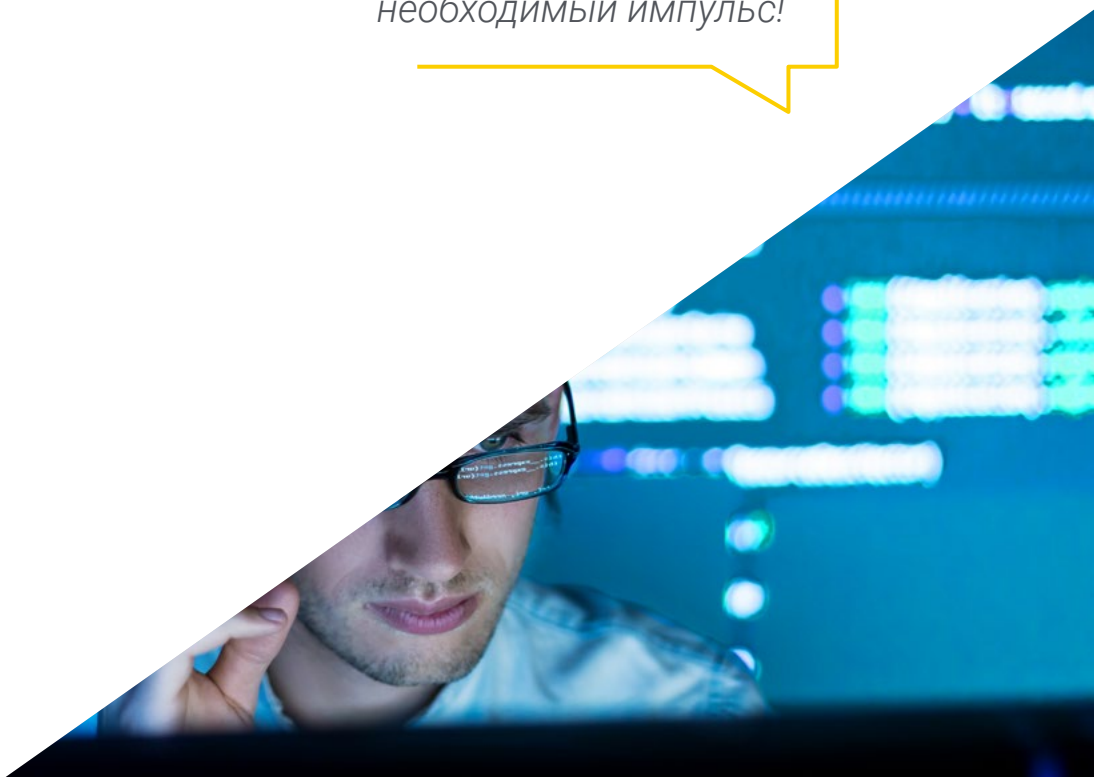
Вы получите доступ к системе обучения, основанной на повторении, с естественным и прогрессивным процессом обучения.

Вы углубитесь в обфускацию строк и придадите своей карьере необходимый импульс!

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

Мультимедийное содержание программы, разработанное с использованием новейших образовательных технологий, позволит специалисту 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 специалист должен попытаться разрешать различные ситуации из профессиональной практики, возникающие в течение учебного курса. В этом студенту поможет инновационная интерактивная видеосистема, созданная признанными экспертами.



02

Цели

Основная цель данной учебной программы - дать студентам возможность овладеть передовыми знаниями о природе, функциональности и поведении вредоносных программ. На протяжении всей программы студенты будут изучать различные формы и цели вредоносных программ, что позволит им анализировать и разрабатывать эффективные защитные стратегии в области кибербезопасности. Этот комплексный подход направлен на подготовку специалистов, способных решать возникающие проблемы в области обнаружения, анализа и смягчения угроз вредоносных программ в сложных цифровых средах. Кроме того, использование 100% онлайн-методики делает обучение более гибким, предоставляя возможность доступа в любое время и в любом месте.

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

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

Хотите ощутить качественный скачок в своей карьере? В TECH вы приобретете навыки криминалистического анализа, применяемого к вредоносным программам"

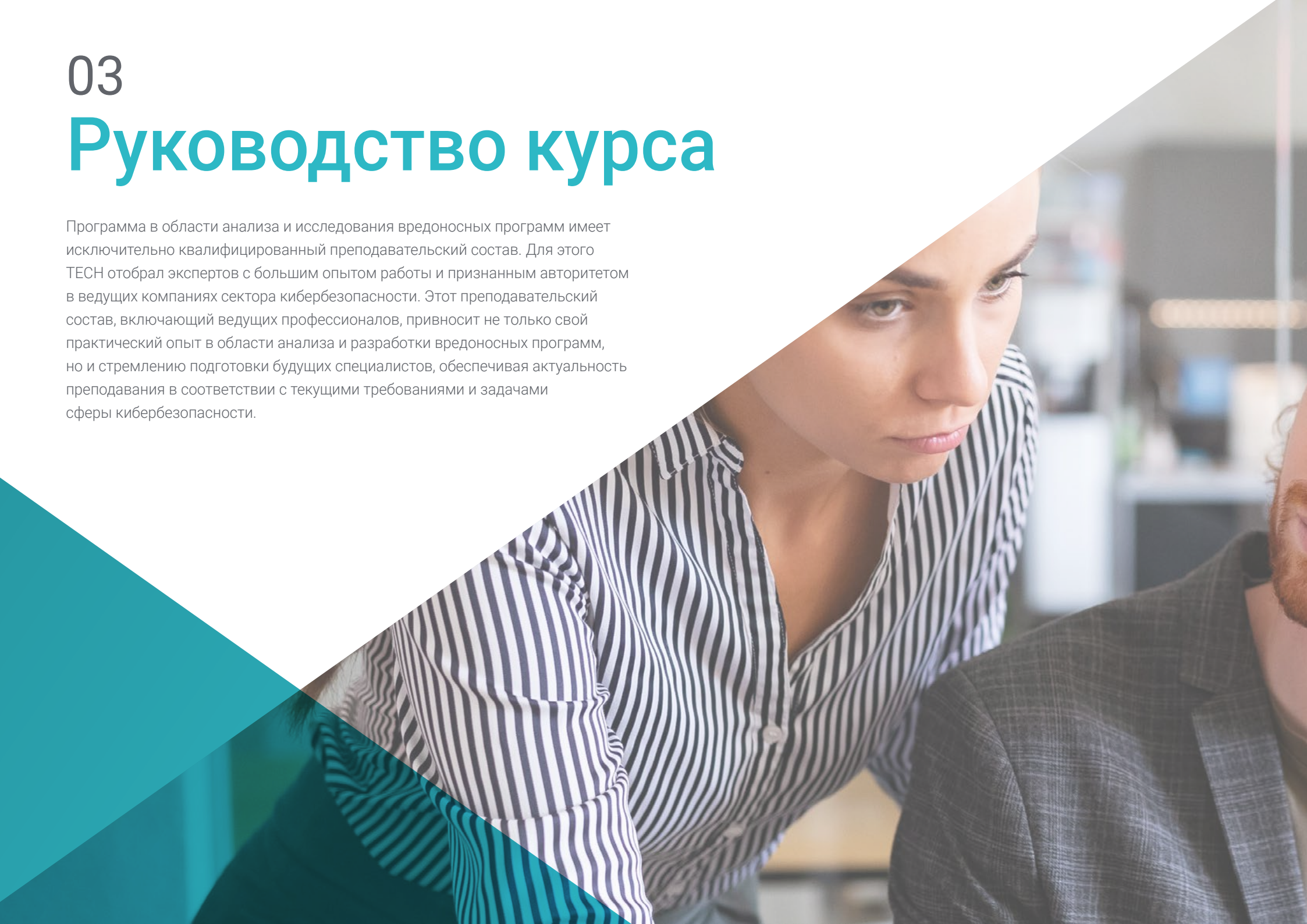
Конкретные цели

- Приобрести расширенные знания о природе, функциональности и поведении вредоносных программ, понять их различные формы и цели
- Развить навыки криминалистического анализа применительно к вредоносным программам, позволяющие 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

03

Руководство курса

Программа в области анализа и исследования вредоносных программ имеет исключительно квалифицированный преподавательский состав. Для этого TECH отобрал экспертов с большим опытом работы и признанным авторитетом в ведущих компаниях сектора кибербезопасности. Этот преподавательский состав, включающий ведущих профессионалов, привносит не только свой практический опыт в области анализа и разработки вредоносных программ, но и стремлению подготовки будущих специалистов, обеспечивая актуальность преподавания в соответствии с текущими требованиями и задачами сферы кибербезопасности.



Получите новые знания по настройке виртуальных машин и snapshot от лучших экспертов в этой области. 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

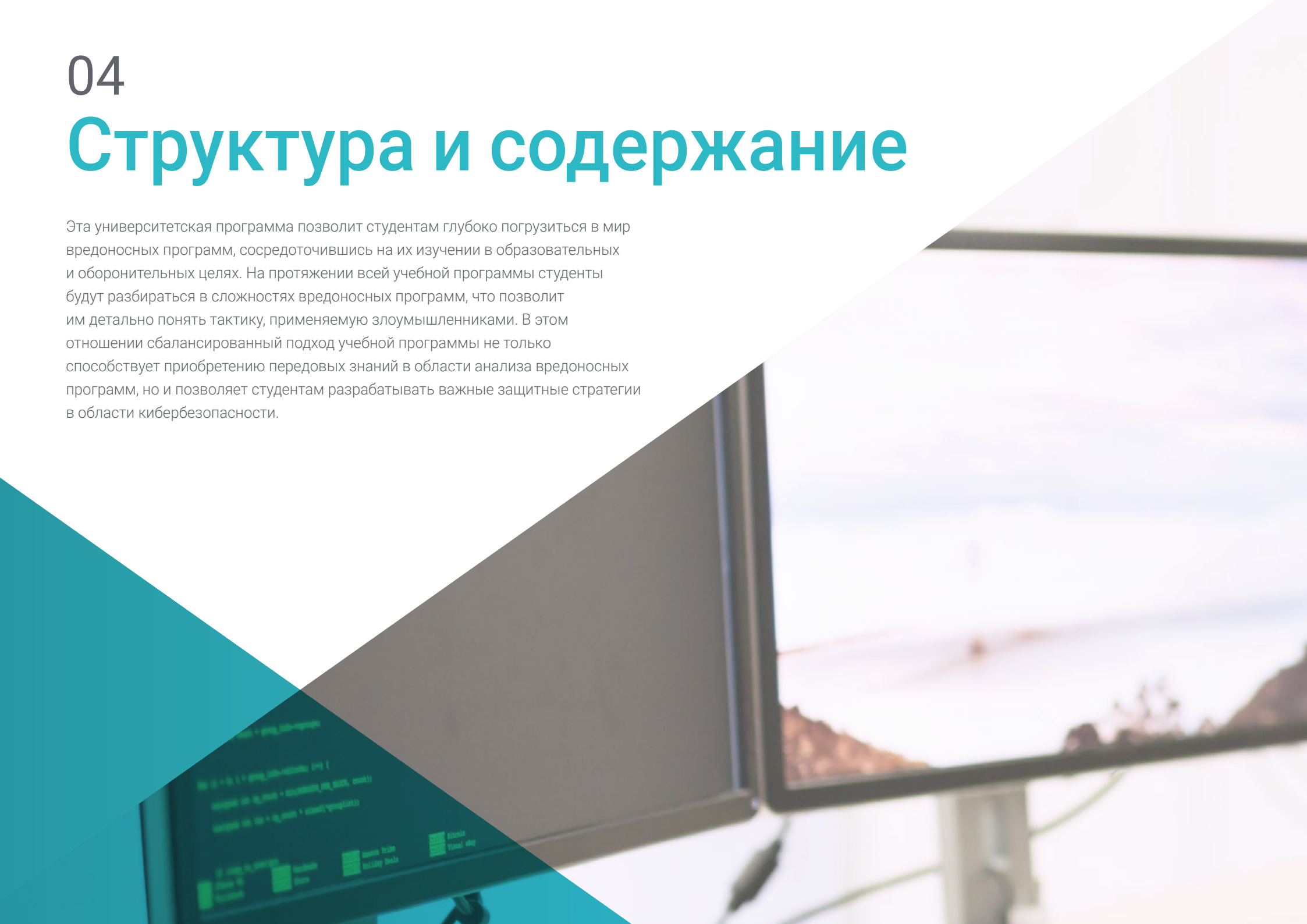
Г-н Гонсалес Санс, Марко

- 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 университетская программа позволит студентам глубоко погрузиться в мир вредоносных программ, сосредоточившись на их изучении в образовательных и оборонительных целях. На протяжении всей учебной программы студенты будут разбираться в сложностях вредоносных программ, что позволит им детально понять тактику, применяемую злоумышленниками. В этом отношении сбалансированный подход учебной программы не только способствует приобретению передовых знаний в области анализа вредоносных программ, но и позволяет студентам разрабатывать важные защитные стратегии в области кибербезопасности.



У вас будет доступ к учебной программе, разработанной авторитетным преподавательским составом, что гарантирует вам успешное обучение"

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

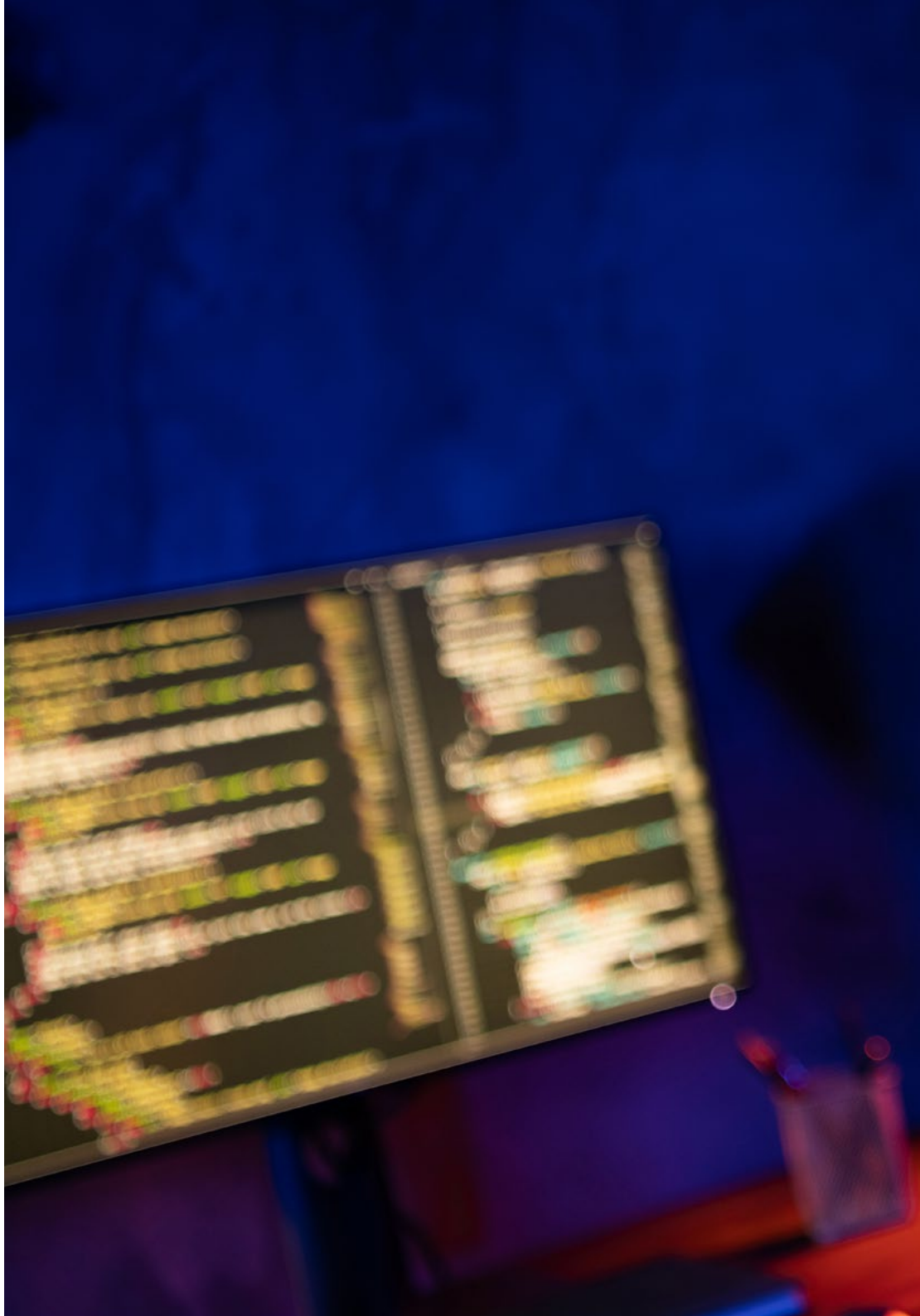
1.2. Подготовка среды
- 1.2.1. Настройка виртуальных машин и Snapshots
- 1.2.2. Средства анализа вредоносных программ
- 1.2.3. Средства разработки вредоносных программ

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

Не упустите возможность поднять свою карьеру на новый уровень с помощью этой инновационной программы"

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.

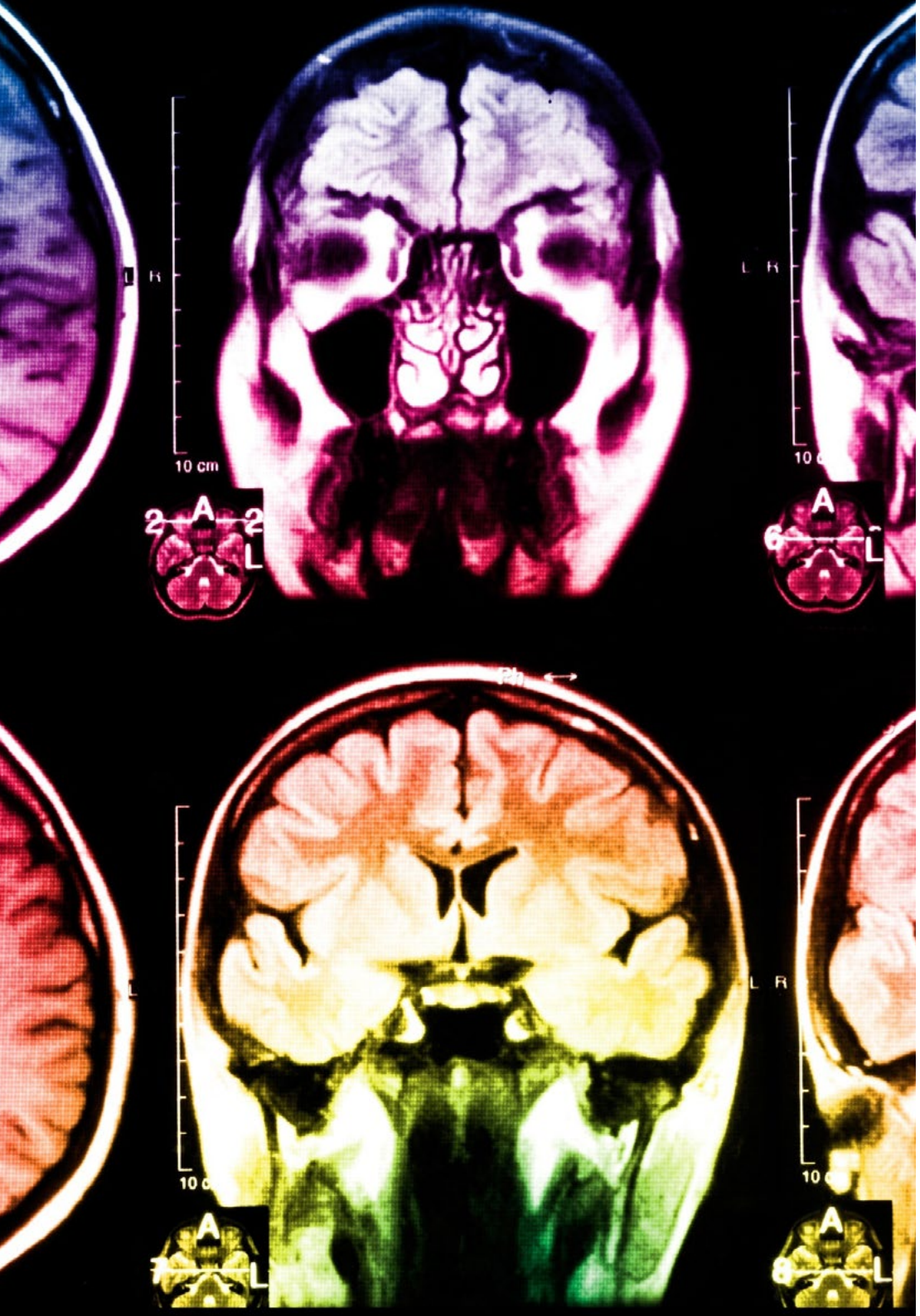
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи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

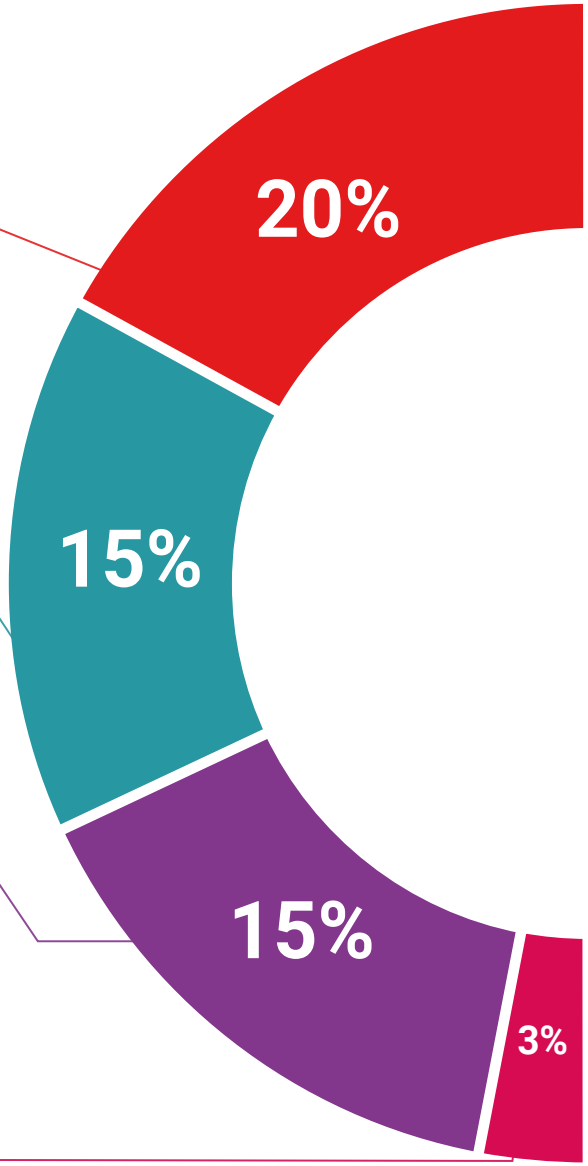
Интерактивные конспекты

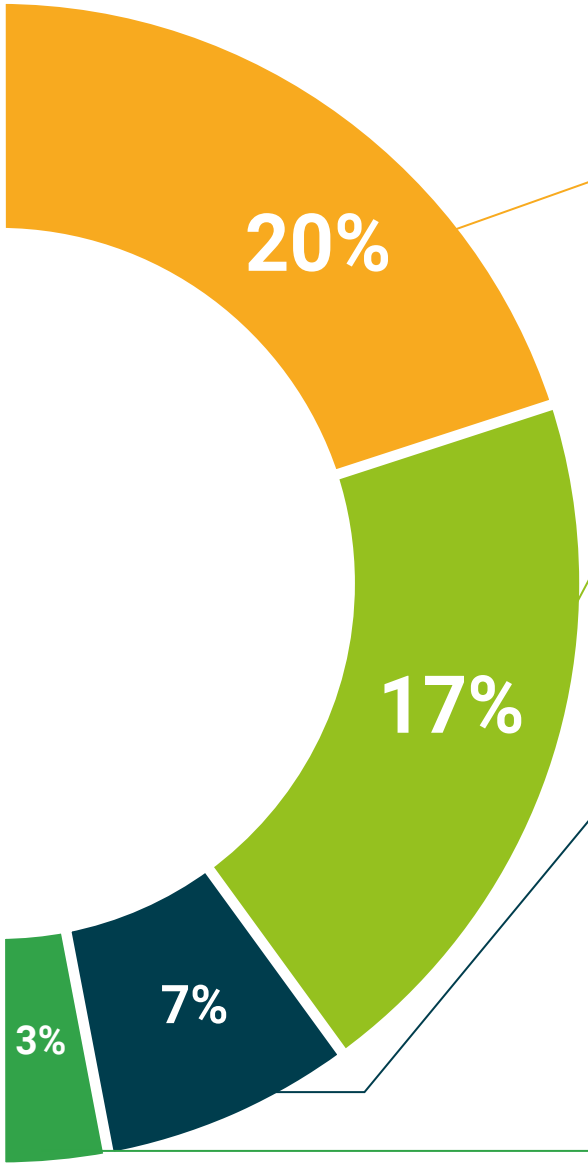
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

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

Университетский курс в области анализа и исследования вредоносных программ гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Университетского курса, выдаваемого TECH Технологическим университетом.

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

Данный **Университетский курс в области анализа и исследования вредоносных программ** содержит самую полную и современную программу на рынке.

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

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

Диплом: **Университетский курс в области анализа и исследования вредоносных программ**

Формат: **онлайн**

Продолжительность: **6 недель**


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

УНИВЕРСИТЕТСКИЙ КУРС

в области

анализа и исследования вредоносных программ

Данный диплом специализированной программы, присуждаемый Университетом, соответствует 150 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: AFWOR235 techitute.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.

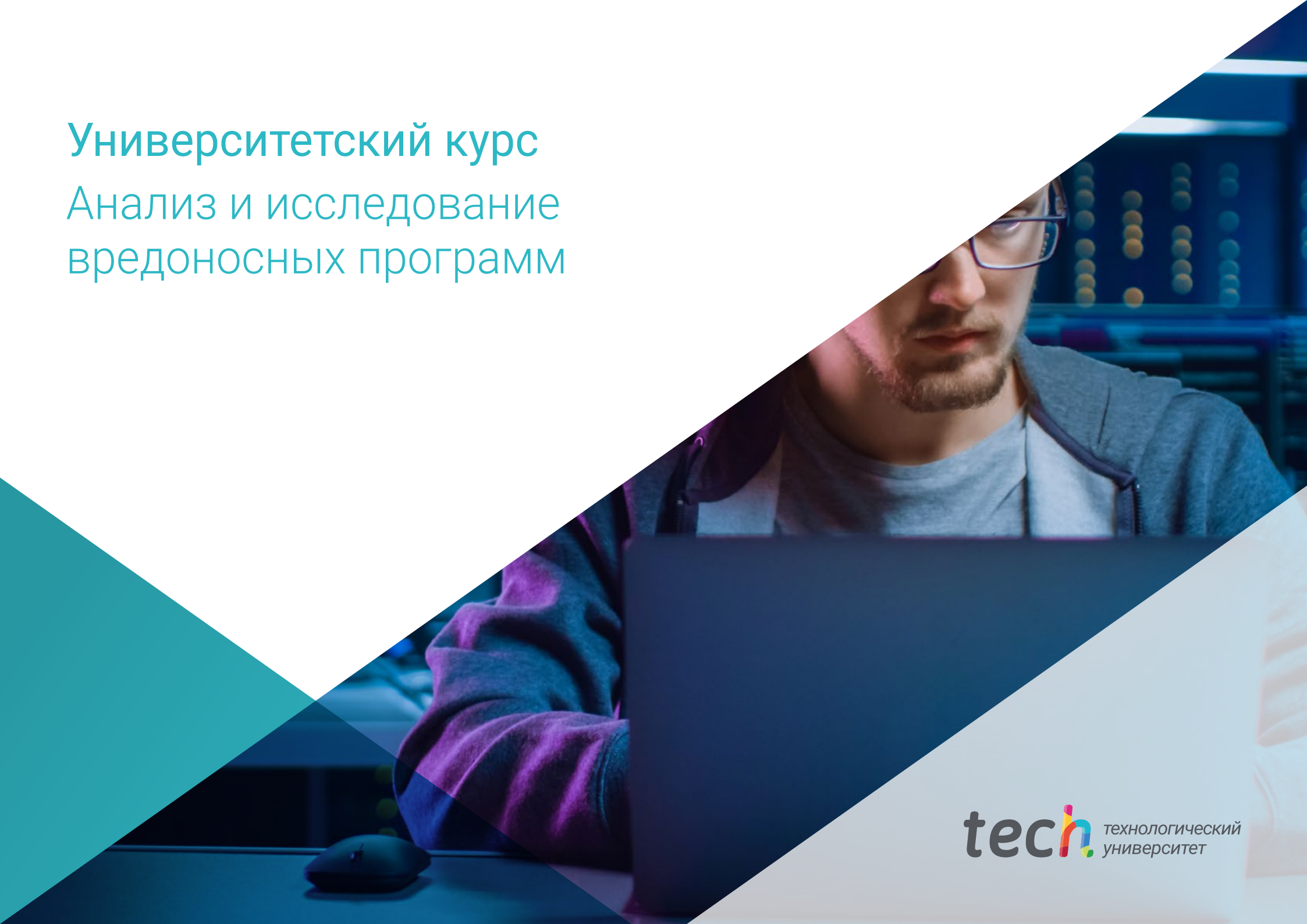
tech технологический университет

Университетский курс
Анализ и исследование вредоносных программ

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

Университетский курс

Анализ и исследование вредоносных программ



tech технологический университет