Университетский курс

Основы криминалистики и DFIR

tech технологический университет

tech технологический университет

Университетский курс
Основы криминалистики и DFIR

- 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/forensic-fundamentals-dfir

Оглавление

01

Презентация

С развитием новых технологий, таких как IT-системы, учреждения все чаще присутствуют в интернете. Однако с ростом числа кибератак компании подвергаются различным угрозам. Так, если хакеры получают доступ к их сетям, они могут удалить конфиденциальные данные и даже потребовать денежный выкуп за разблокировку заблокированных систем. По этой причине компаниям важно иметь специалистов по основам криминалистики, чтобы обнаружить недостатки в системе безопасности и максимально снизить их влияние. В ответ на эту потребность TECH запускает инновационную программу по внедрению передовых методов анализа цифровых доказательств. Кроме того, обучение ведется в 100% онлайн-режиме, что гарантирует удобство для студентов.

Хотите анализировать журналы брандмауэра и обнаруживать сетевые вторжения? Добейтесь этого за 150 часов благодаря этому курсу"

Компании все больше осознают важность наличия в своей организации специалистов по кибербезопасности. Их преимущества заключаются в защите цифровых активов и проведении криминалистических исследований для определения причин и масштабов потенциальных инцидентов. В свою очередь, эти специалисты также собирают информацию, которая может быть использована в качестве доказательств в суде и для преследования киберпреступников. В этом смысле они даже помогают организациям соблюдать правила безопасности данных и отвечать требованиям по уведомлению о нарушениях безопасности.

Столкнувшись с этой ситуацией, TECH разрабатывает передовые методы обучения, чтобы студенты могли предотвращать хакерские атаки, применяя наиболее подходящие стратегии. Академический план обучения будет посвящен процессу получения доказательств, основанному на цепочке их передачи. Таким образом, студенты будут работать в качестве компьютерных криминалистических экспертов и разрешать инциденты, затрагивающие организации. Кроме того, в программе рассматривается анализ сетевых пакетов, поэтому студенты будут изучать журналы *брандмауэра*. Также будет анализировано вредоносное программное обеспечение с целью выполнения методов дизассемблирования.

Студенты будут применять методологии DFIR и раскроют свой творческий потенциал для создания самых инновационных бизнес-решений.

С другой стороны, для закрепления усвоенного материала в данной университетской программе применяется революционная система *Relearning*. TECH является пионером в использовании этой модели обучения, которая способствует усвоению сложных понятий путем их естественного и постепенного повторения. В этом направлении программа также использует материалы в различных форматах, таких как инфографика, интерактивные конспекты и пояснительные видео. И все это в удобном 100% онлайн-режиме, который позволяет студентам корректировать свое расписание в соответствии с их обязанностями и личными обстоятельствами.

Данный **Университетский курс в области основ криминалистики и DFIR** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных экспертами в области основ криминалистики и DFIR
- 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 будете создавать планы реагирования на инциденты в лучшем в мире цифровом университете по версии Forbes"*

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

Нужно восстановить данные с поврежденного носителя? TECH предоставит вам лучшие инструменты для этого.

Вы подготовите отчеты по судебной экспертизе, с которыми сможете выступать в качестве свидетеля-эксперта на важных судебных процессах.

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 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

В рамках этой программы студенты изучат передовые методы сбора и анализа цифровых доказательств и рассмотрят случаи нарушения безопасности. Студенты углубятся в архивный анализ, а также в сохранность цепочки хранения. Кроме того, студенты изучат наиболее эффективные тактики минимизации последствий потенциальных кибер-инцидентов.

Забудьте о заучивании! С системой Relearning вы будете осваивать концепции естественным и прогрессивным способом"

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

Вас будет поддерживать преподавательский состав, включающий выдающихся профессионалов в области кибербезопасности"

Конкретные цели

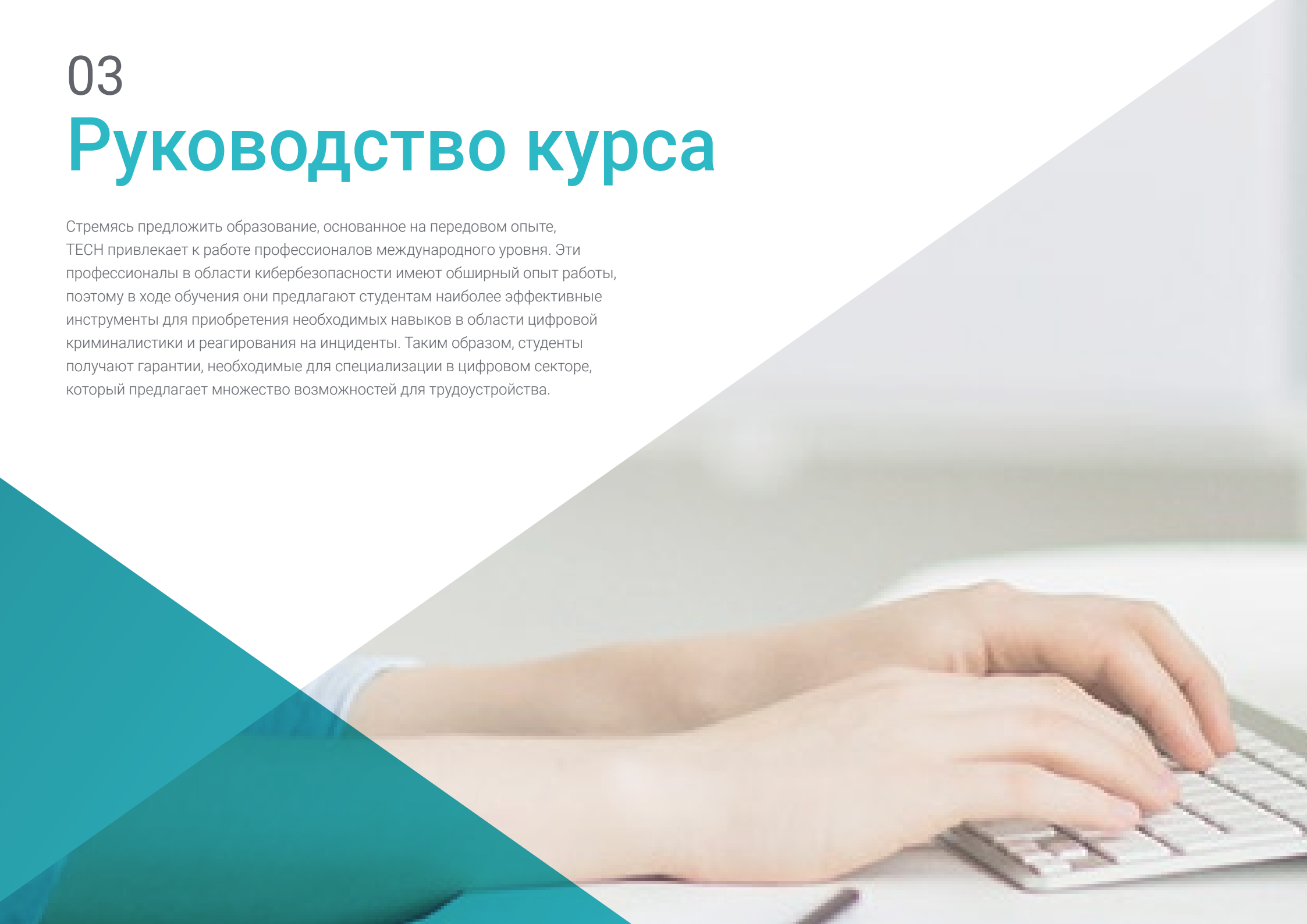
Модуль 1. Основы криминалистики и DFIR

- 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

03

Руководство курса

Стремясь предложить образование, основанное на передовом опыте, TECH привлекает к работе профессионалов международного уровня. Эти профессионалы в области кибербезопасности имеют обширный опыт работы, поэтому в ходе обучения они предлагают студентам наиболее эффективные инструменты для приобретения необходимых навыков в области цифровой криминалистики и реагирования на инциденты. Таким образом, студенты получают гарантии, необходимые для специализации в цифровом секторе, который предлагает множество возможностей для трудоустройства.

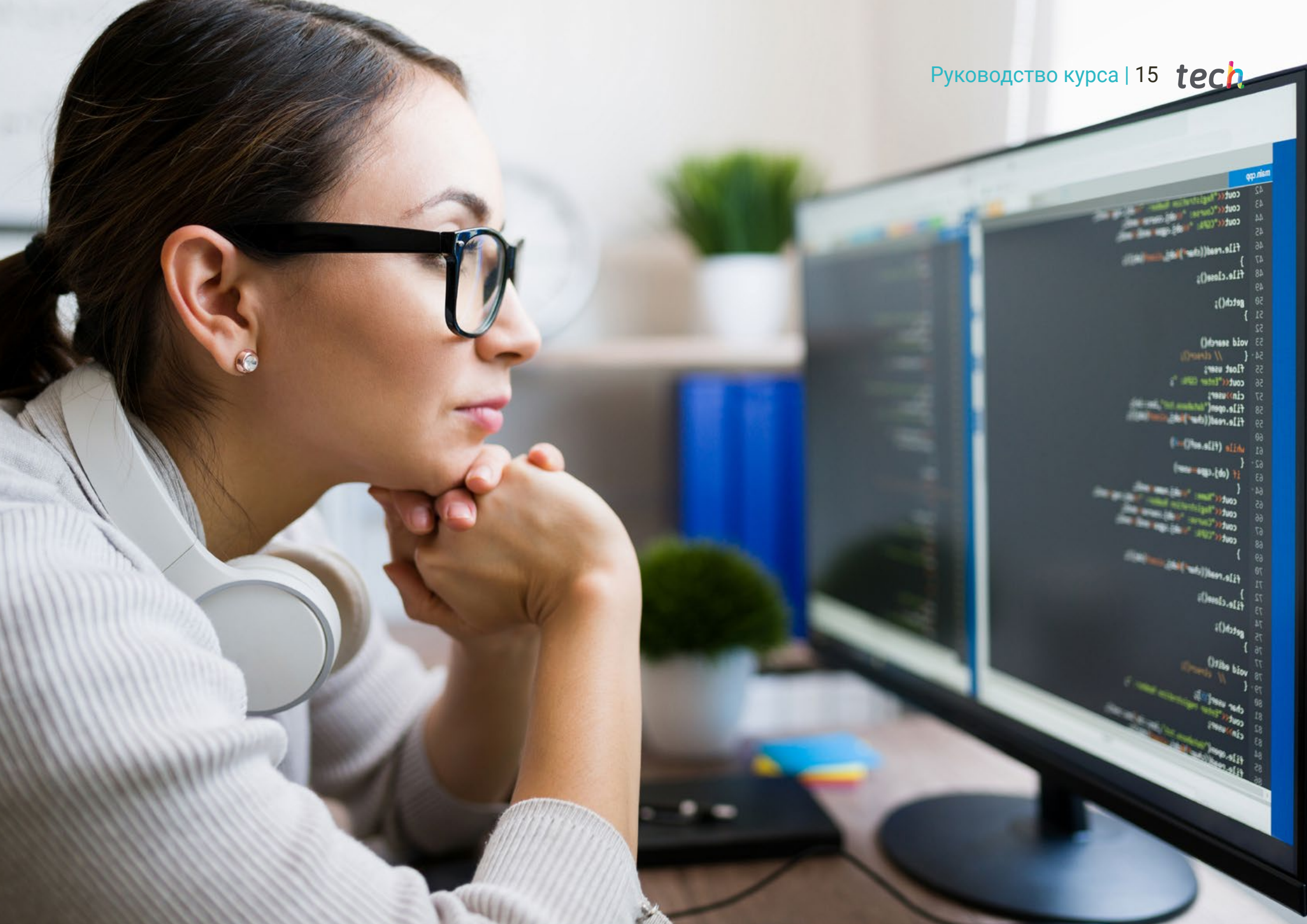


Библиотека наполнена мультимедийными ресурсами в различных аудиовизуальных форматах"

Руководство

Г-н Гомес Пинтадо, Карлос

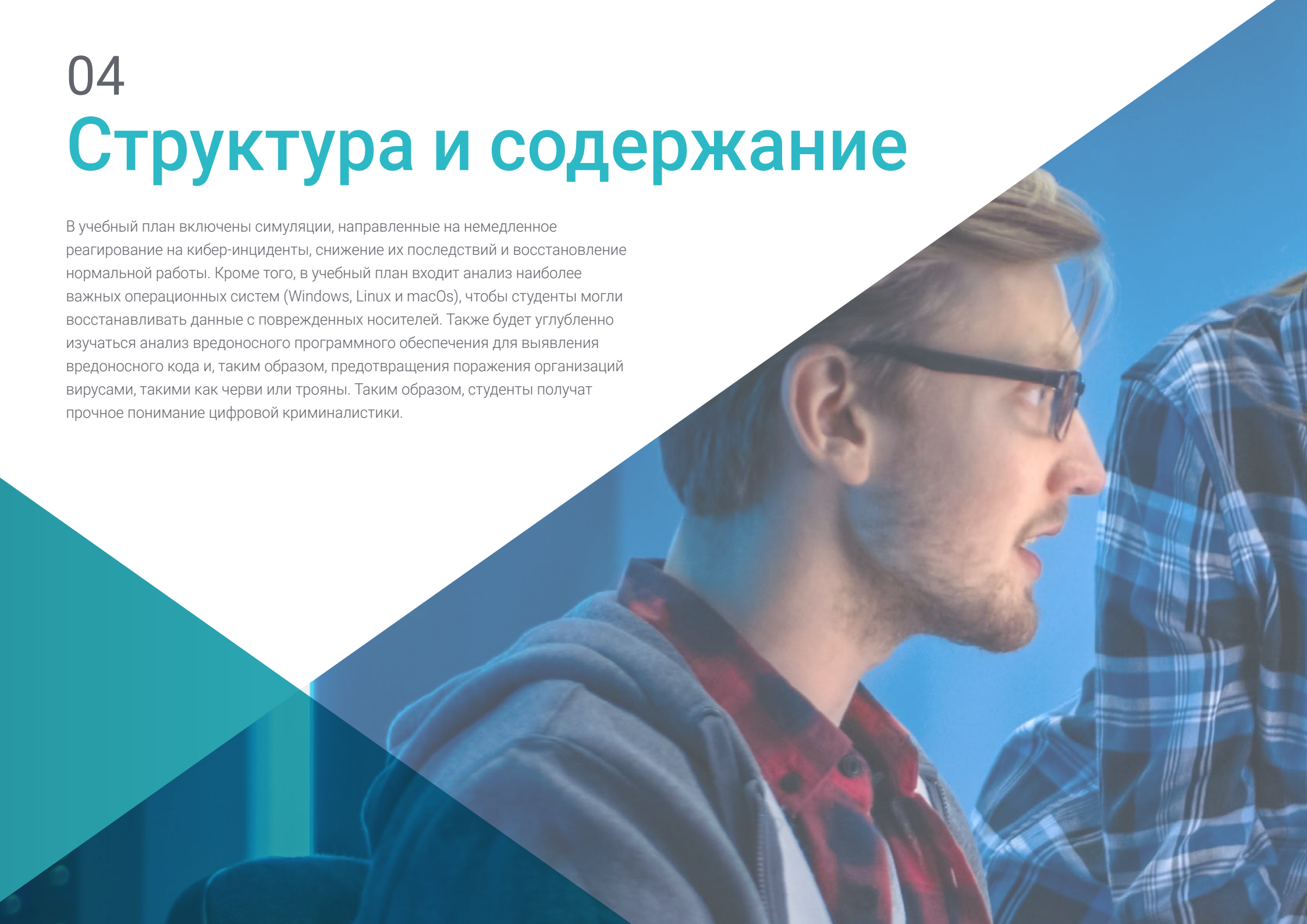
- Руководитель группы кибербезопасности и красных команд в Grupo Oesía
- Руководитель, *советник и инвестор* в компании Wesson App
- Степень бакалавра в области программирования и технологий информационного общества в Политехническом университете Мадрида
- Сотрудничает с учебными заведениями для подготовки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

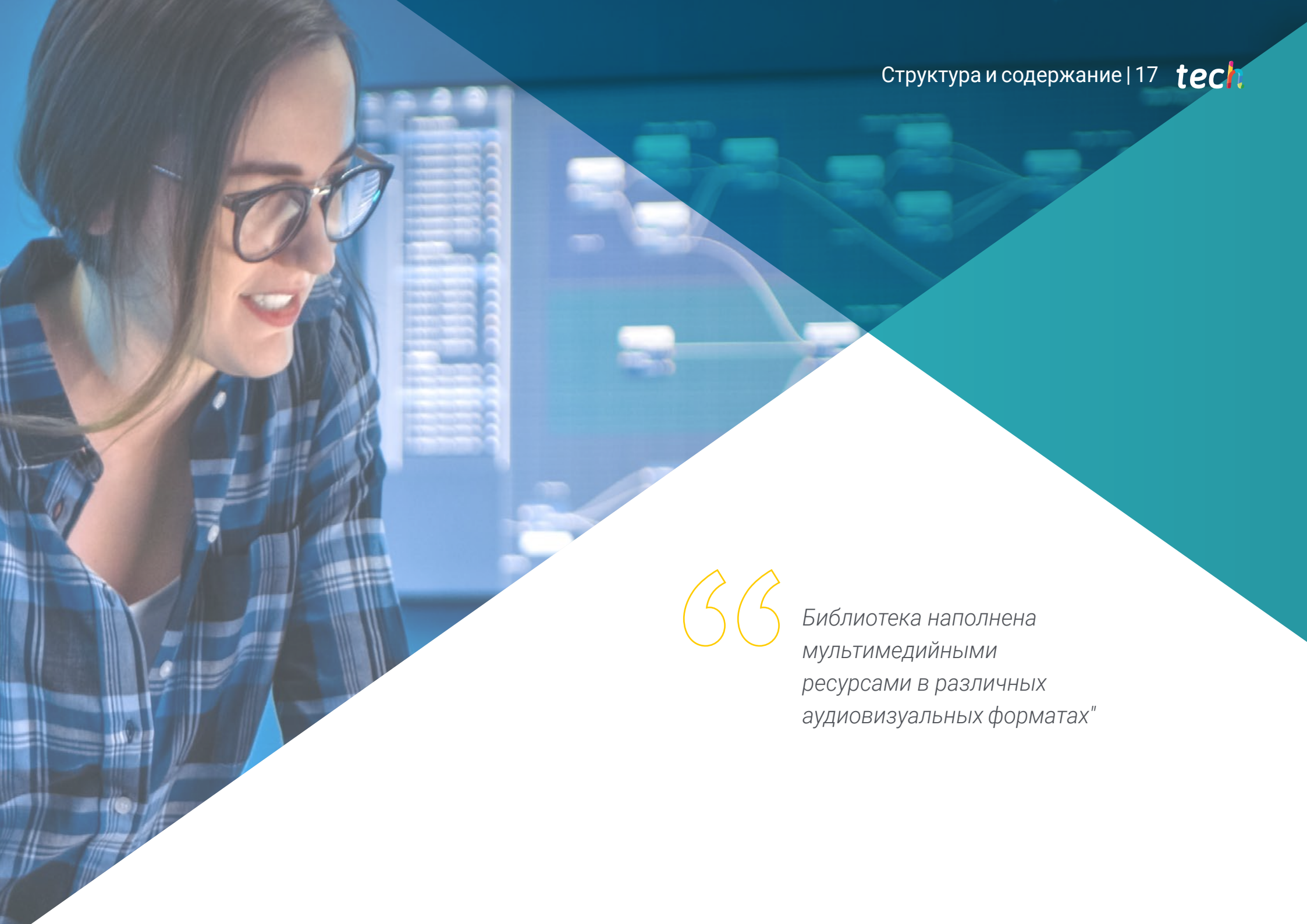


04

Структура и содержание

В учебный план включены симуляции, направленные на немедленное реагирование на кибер-инциденты, снижение их последствий и восстановление нормальной работы. Кроме того, в учебный план входит анализ наиболее важных операционных систем (Windows, Linux и macOs), чтобы студенты могли восстанавливать данные с поврежденных носителей. Также будет углубленно изучаться анализ вредоносного программного обеспечения для выявления вредоносного кода и, таким образом, предотвращения поражения организаций вирусами, такими как черви или трояны. Таким образом, студенты получат прочное понимание цифровой криминалистики.





Библиотека наполнена мультимедийными ресурсами в различных аудиовизуальных форматах"

Модуль 1. Основы криминалистики и DFIR

1.1. Цифровая криминалистика
- 1.1.1. История и развитие компьютерной криминалистики
- 1.1.2. Важность компьютерной криминалистики в кибербезопасности
- 1.1.3. История и развитие компьютерной криминалистики

1.2. Основы компьютерной криминалистики
- 1.2.1. Цепочка хранения и ее применение
- 1.2.2. Виды цифровых улик
- 1.2.3. Процессы получения улик

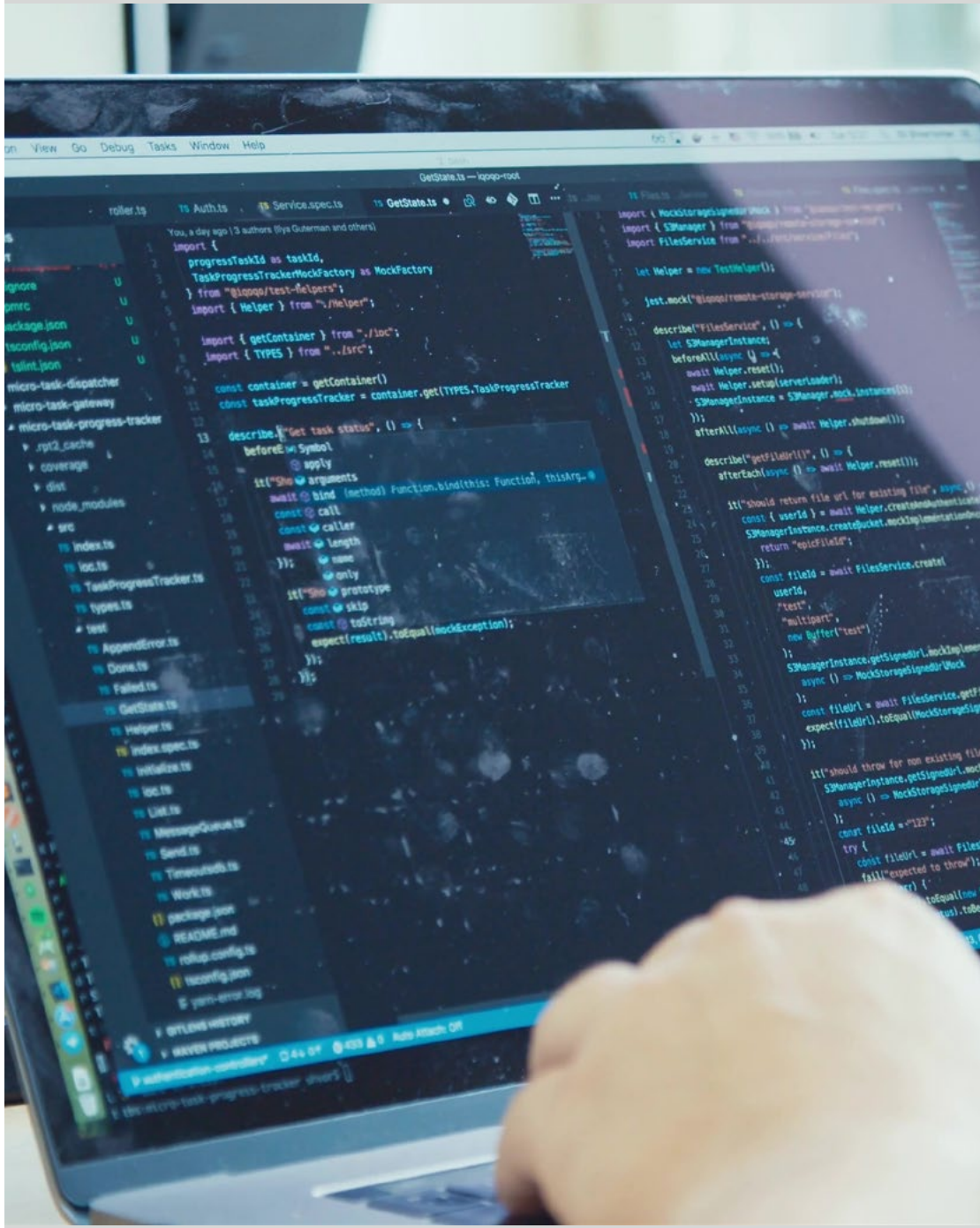
1.3. Системы хранения и структура данных
- 1.3.1. Основные системы хранения
- 1.3.2. Методы сокрытия данных
- 1.3.3. Анализ метаданных и атрибутов файлов

1.4. Анализ операционных систем
- 1.4.1. Криминалистический анализ систем Windows
- 1.4.2. Криминалистический анализ систем Linux
- 1.4.3. Криминалистический анализ систем macOS

1.5. Восстановление данных и анализ дисков
- 1.5.1. Восстановление данных с поврежденных носителей
- 1.5.2. Инструменты для анализа дисков
- 1.5.3. Интерпретация файловых систем

1.6. Анализ сети и трафика
- 1.6.1. Захват и анализ сетевых пакетов
- 1.6.2. Анализ журналов брандмауэра
- 1.6.3. Обнаружение сетевых вторжений

1.7. Анализ вредоносных программ и вредоносного кода
- 1.7.1. Классификация вредоносных программ и их характеристики
- 1.7.2. Статический и динамический анализ вредоносных программ
- 1.7.3. Методы деассемблирования и отладки



1.8. Анализ журналов и событий
  1.8.1. Типы журналов в системах и приложениях
  1.8.2. Интерпретация соответствующих событий
  1.8.3. Инструменты анализа журналов
1.9. Реагирование на инциденты безопасности
  1.9.1. Процесс реагирования на инциденты
  1.9.2. Создание плана реагирования на инциденты
  1.9.3. Координация действий с командами безопасности
1.10. Представление улик и доказательств
  1.10.1. Правила представления цифровых доказательств в правовой среде
  1.10.2. Подготовка отчетов о судебной экспертизе
  1.10.3. Выступление в суде в качестве свидетеля-эксперта

Библиотека наполнена мультимедийными ресурсами в различных аудиовизуальных форматах"

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.

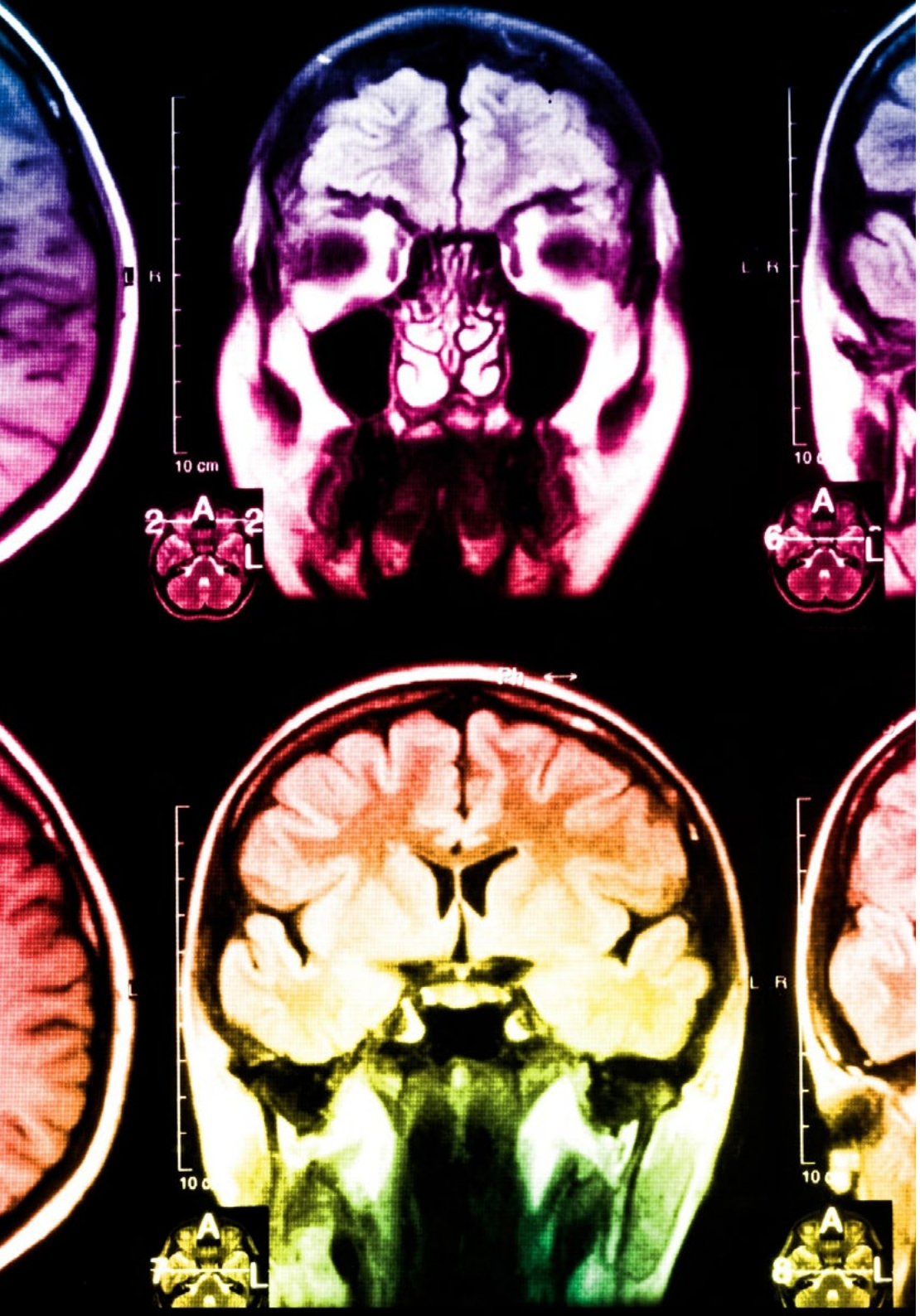
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи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

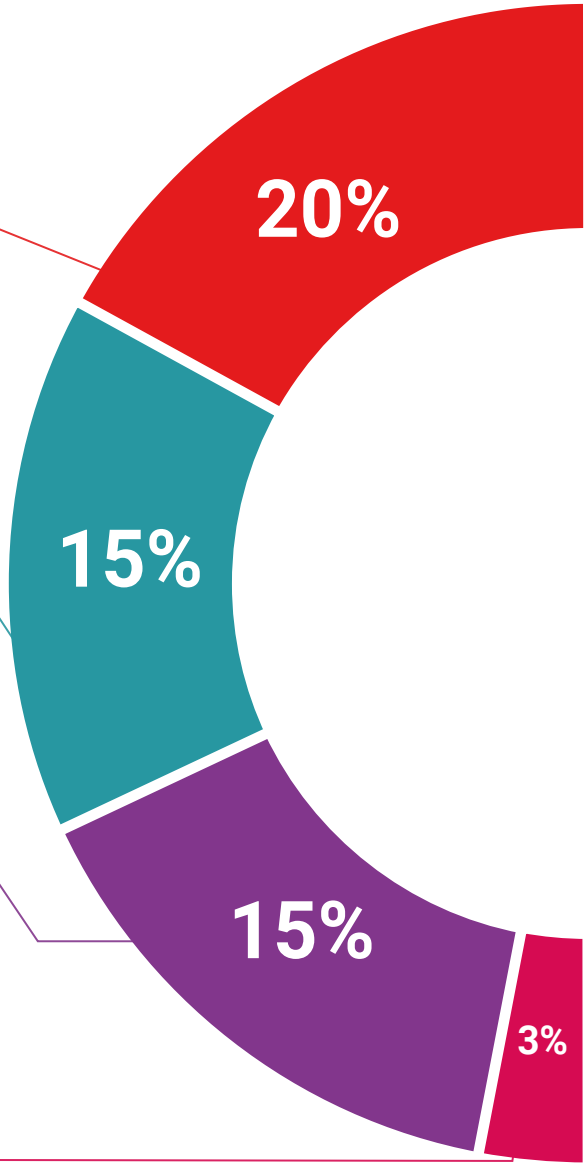
Интерактивные конспекты

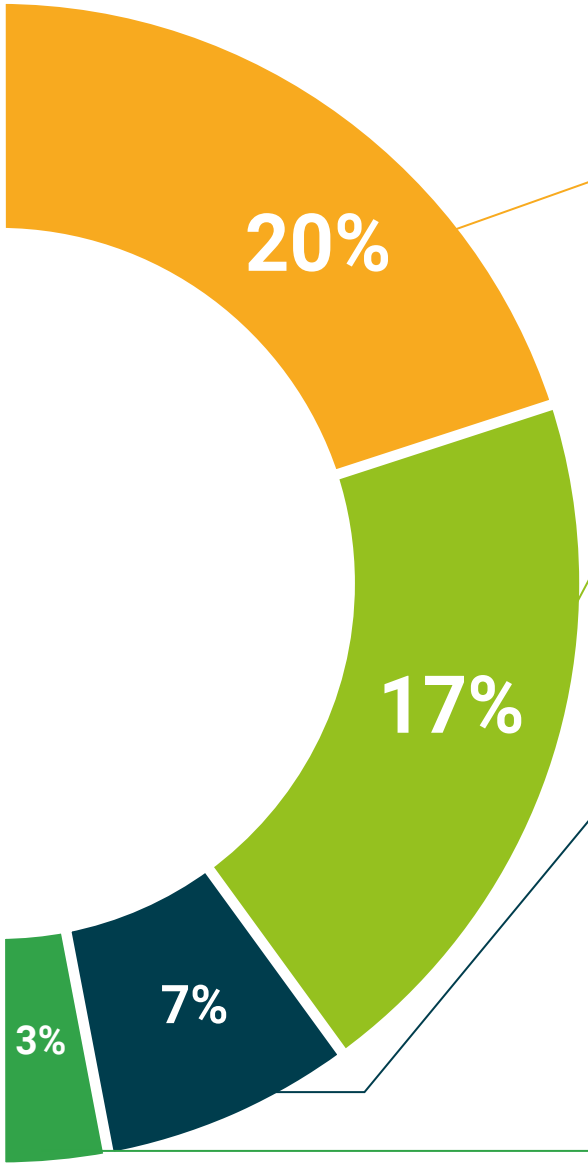
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

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 основ криминалистики и DFIR 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 основ криминалистики и DFIR** 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 основ криминалистики и DFIR**

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

основ криминалистики и DFIR

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.

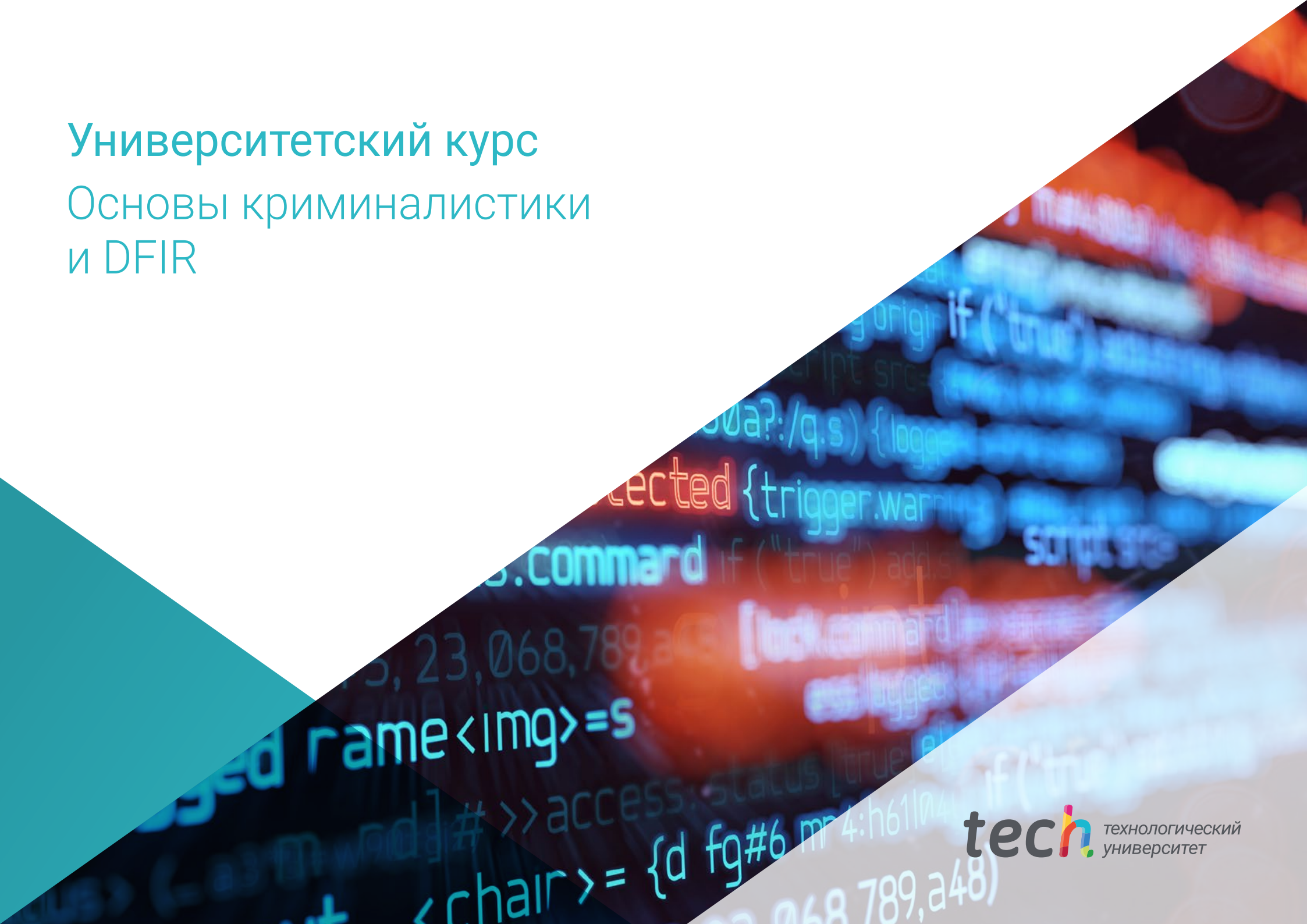
tech технологический университет

Университетский курс
Основы криминалистики и DFIR

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

Университетский курс

Основы криминалистики и DFIR



tech технологический университет