Курс профессиональной подготовки

Наступательная кибербезопасность

tech технологический университет

tech технологический университет

Курс профессиональной подготовки

Наступательная кибербезопасность

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

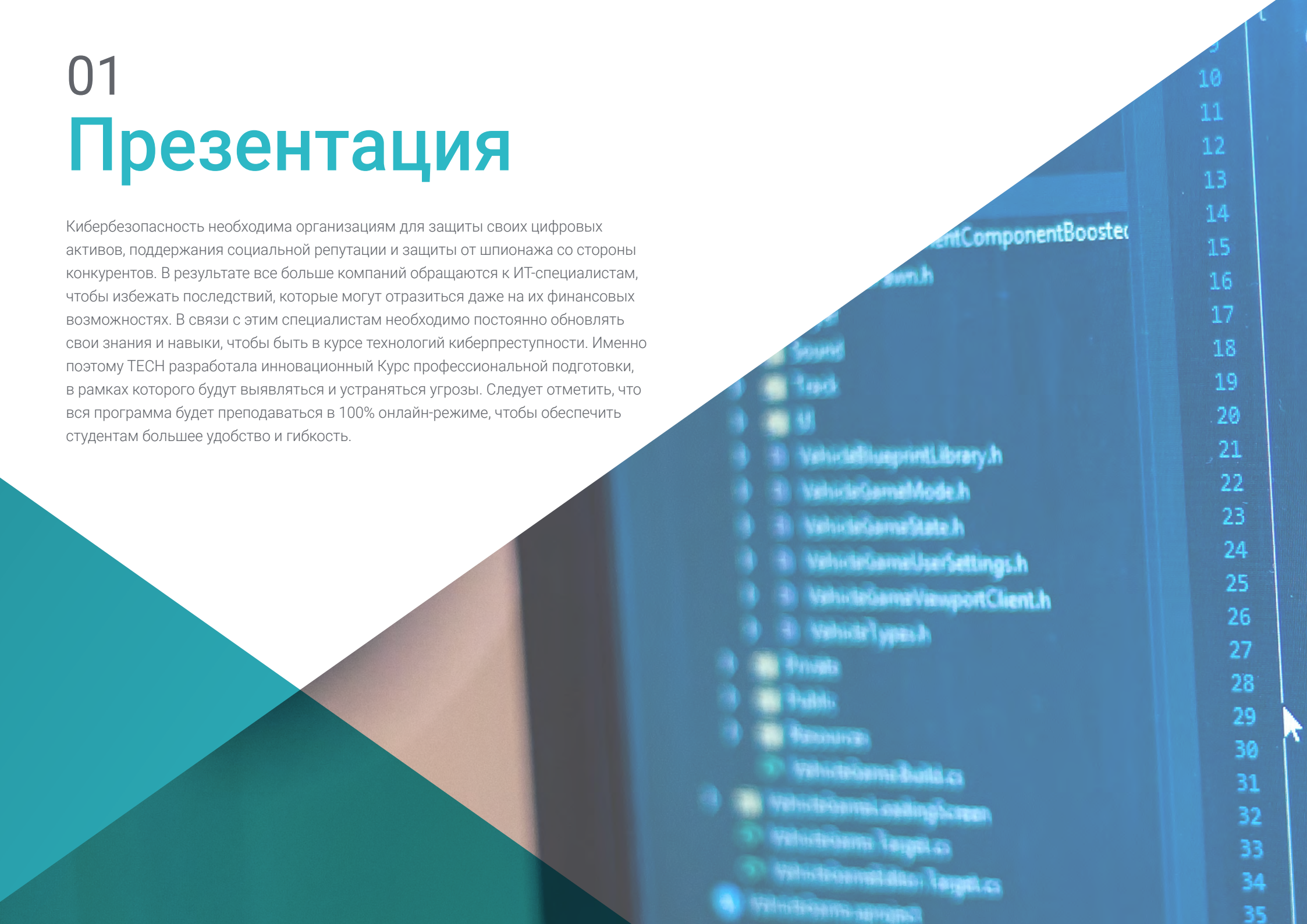
Веб-доступ: www.techtitute.com/ru/information-technology/postgraduate-diploma/postgraduate-diploma-offensive-cybersecurity

Оглавление

01

Презентация

Кибербезопасность необходима организациям для защиты своих цифровых активов, поддержания социальной репутации и защиты от шпионажа со стороны конкурентов. В результате все больше компаний обращаются к ИТ-специалистам, чтобы избежать последствий, которые могут отразиться даже на их финансовых возможностях. В связи с этим специалистам необходимо постоянно обновлять свои знания и навыки, чтобы быть в курсе технологий киберпреступности. Именно поэтому TECH разработала инновационный Курс профессиональной подготовки, в рамках которого будут выявляться и устраняться угрозы. Следует отметить, что вся программа будет преподаваться в 100% онлайн-режиме, чтобы обеспечить студентам большее удобство и гибкость.



Вы углубите свои знания о протоколе Kerberos и защите информации в сетевых средах"

Каждый день в СМИ появляются сообщения о случаях, когда хакеры наносят ущерб учреждениям, получая доступ к их базам данных. Последствия этих атак очень серьезны, поскольку они нарушают работу и мешают компаниям эффективно функционировать. Более того, это может напрямую повлиять на их бюджет, приведя к штрафам за несоблюдение нормативных требований и ограничению доходов.

В связи с этим TECH создал передовой курс, позволяющий выявить наиболее часто используемые методы вторжения, а также наиболее оптимальные стратегии борьбы с ними. Под руководством преподавателей, обладающих большим опытом работы в данной области, учебная программа заложит основы для понимания того, как мыслят хакеры. Кроме того, будет предложен ряд решений, направленных на создание безопасных инфраструктур для управления цифровыми сертификатами в корпоративной сети.

Специалисты также узнают, как оптимально подготовить виртуальные среды благодаря настройке виртуальных машин и *Snapshots*. Кроме того, будет проведен анализ вредоносного ПО, исследование вызовов с помощью API Monitor и наблюдение за сетевыми запросами с помощью TCPView. Студенты изучат теоретические концепции в смоделированных средах, что подготовит их к решению реальных задач в области наступательной кибербезопасности. Наконец, особое внимание будет уделено этике и социальной ответственности, которые должны характеризовать специалистов в этой области.

Чтобы закрепить усвоение всех этих знаний, Курс профессиональной подготовки применяет инновационную систему *Relearning*. TECH является пионером в использовании этой модели обучения, которая способствует усвоению сложных понятий путем их естественного и постепенного повторения. В программе также используются ресурсы различных форматов, такие как объясняющие видео, интерактивные конспекты и инфографика. И все это в удобном 100% онлайн-режиме, который позволяет каждому подстроить свое расписание под свои обязанности.

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

- Разбор практических кейсов, представленных экспертами в области кибербезопасности
- Наглядное, схематичное и исключительно практичное содержание курса предоставляет полную 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

Развивайте свои навыки в качестве наступательного аудитора и приступайте к новому профессиональному вызову в самых престижных цифровых компаниях"

Вы достигнете поставленных целей с помощью дидактических средств TECH, включая пояснительные видеоролики и интерактивные конспекты”

Хотите стать большим Bug Bounty Hunter? Благодаря этой программе вы сможете обнаружить любую уязвимость в Интернете.

Всего за 6 месяцев вы освоите управление идентификацией в Azure AD. Поступайте сейчас!

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

Структура этой программы предлагает уникальный образовательный опыт, который отличается практическим и инновационным подходом к кибербезопасности. Таким образом, студенты рассмотрят все аспекты - от анализа уязвимостей до передовых методов вторжения. В рамках этого направления будут предложены оптимальные меры по оценке и укреплению различных кибернетических систем. Кроме того, особое внимание будет уделено юридической и этической ответственности, которую должны нести специалисты в этой области.

Уменьшите угрозы вредоносных программ с помощью лучшего в мире цифрового университета по версии Forbes"

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

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 по наступательной безопасности, оптимизируя координацию и выполнение мероприятий по *пентесту*

Модуль 2. 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
- Поддерживать студентов в курсе последних тенденций и угроз в области атак на системы Windows, обеспечивая постоянную актуальность и эффективность полученных навыков

Модуль 3. Анализ и исследование *вредоносных программ*

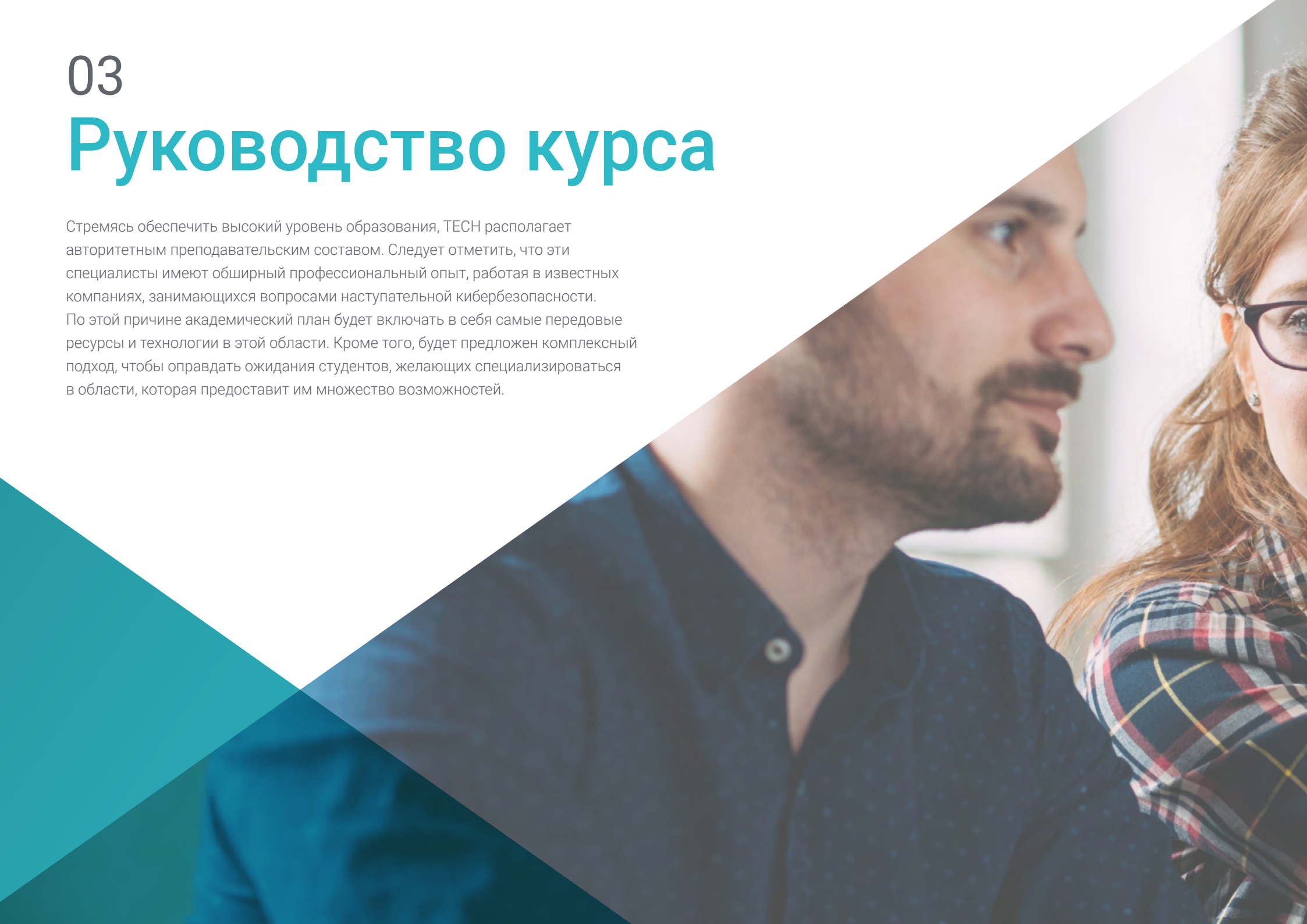
- Приобрести расширенные знания о природе, функциональности и поведении *вредоносных программ*, понять их различные формы и цели
- Развить навыки криминалистического анализа применительно к *вредоносным программам*, позволяющие выявлять индикаторы компрометации (IoC) и модели атак
- Изучить стратегии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

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

03

Руководство курса

Стремясь обеспечить высокий уровень образования, TECH располагает авторитетным преподавательским составом. Следует отметить, что эти специалисты имеют обширный профессиональный опыт, работая в известных компаниях, занимающихся вопросами наступательной кибербезопасности.
По этой причине академический план будет включать в себя самые передовые ресурсы и технологии в этой области. Кроме того, будет предложен комплексный подход, чтобы оправдать ожидания студентов, желающих специализироваться в области, которая предоставит им множество возможностей.



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

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 Паррилья, Юба

- Координатор проектов по наступательной линии безопасности и красной команды
- 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 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

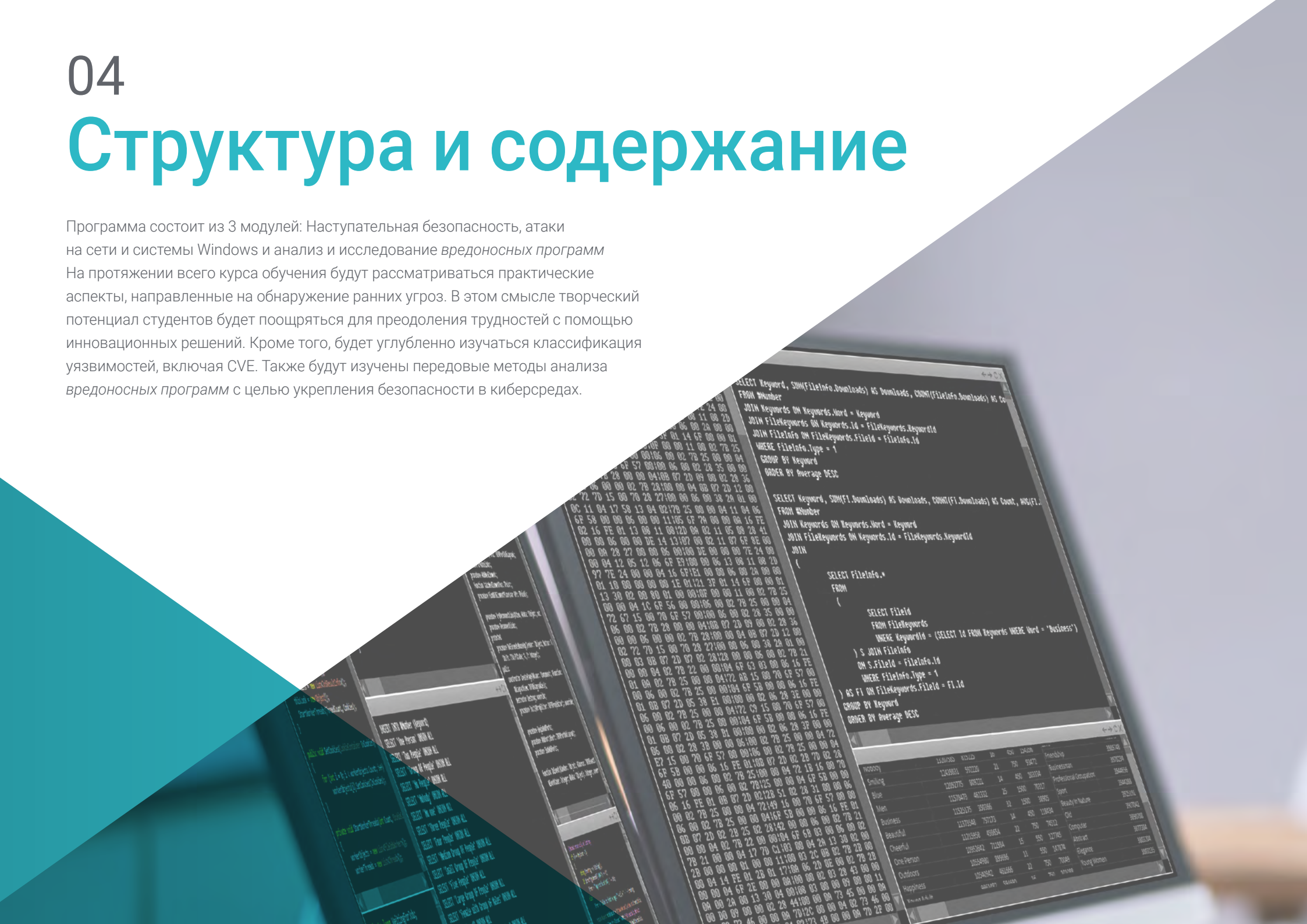
Г-н Гонсалес Санс, Маркос

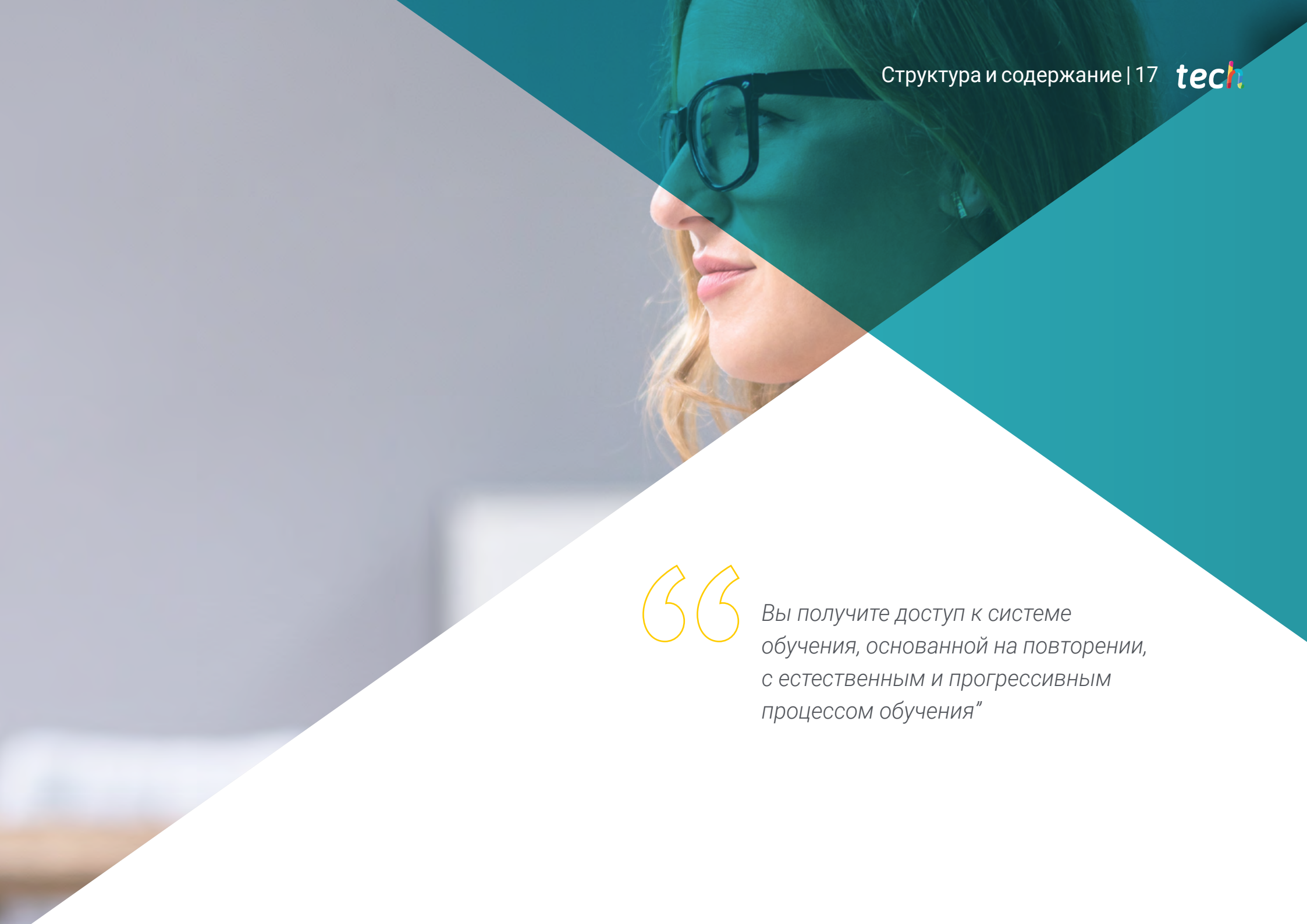
- Консультант по кибербезопасности в компании Cipherbit
- Сертифицированный разработчик eLearnSecurity eXploit
- Сертифицированный профессионал Offensive Security
- Сертифицированный профессионал Offensive Security Wireless
- Virtual Hacking Labs Plus
- Степень бакалавра в области программирования в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

04

Структура и содержание

Программа состоит из 3 модулей: Наступательная безопасность, атаки на сети и системы Windows и анализ и исследование *вредоносных программ* На протяжении всего курса обучения будут рассматриваться практические аспекты, направленные на обнаружение ранних угроз. В этом смысле творческий потенциал студентов будет поощряться для преодоления трудностей с помощью инновационных решений. Кроме того, будет углубленно изучаться классификация уязвимостей, включая CVE. Также будут изучены передовые методы анализа *вредоносных программ* с целью укрепления безопасности в киберсредах.





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

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. Ранние 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

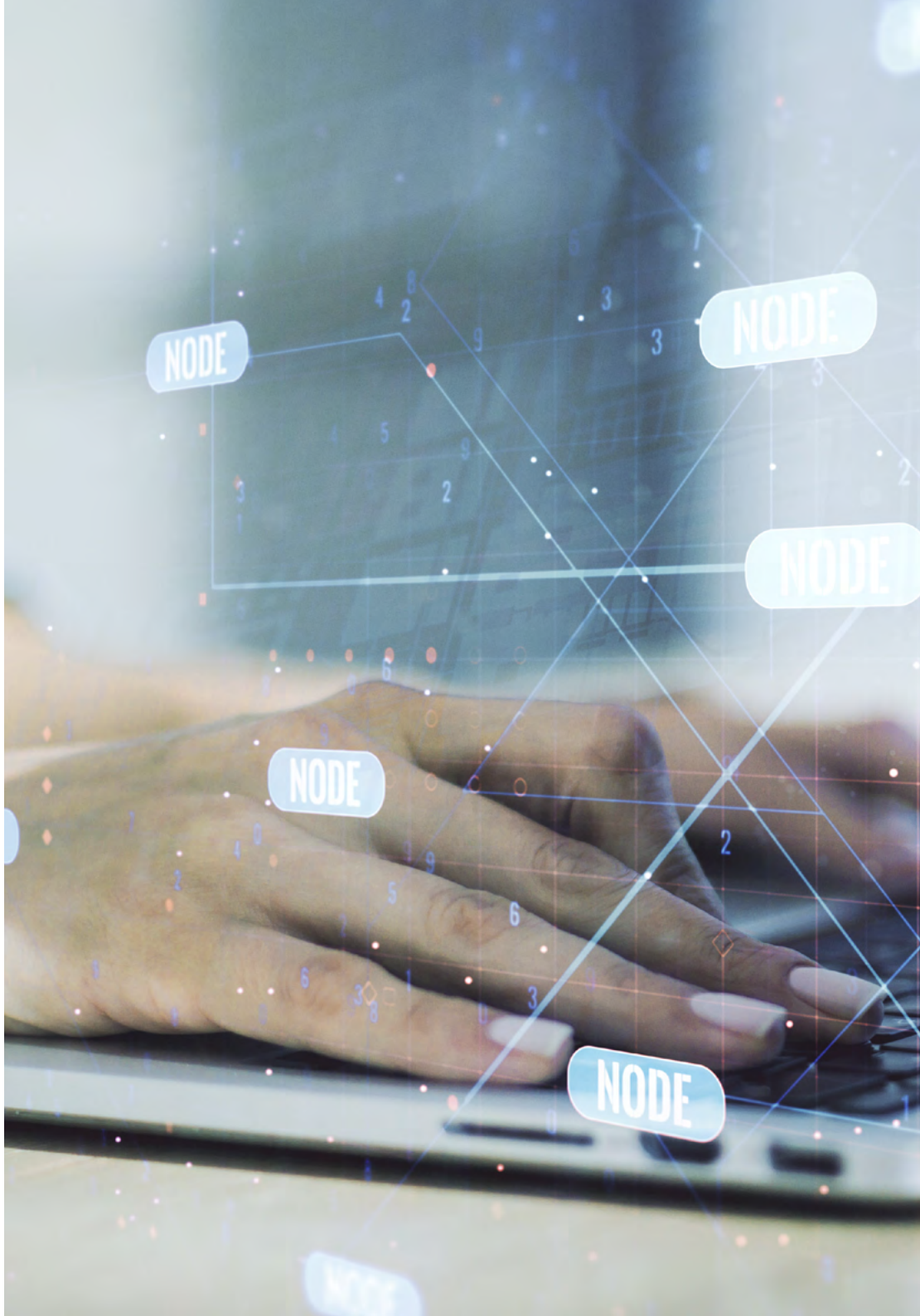
1.4. Методики наступательной безопасности
- 1.4.1. PTES (*Penetration Testing Execution Standard*)
- 1.4.2. OWASP (*Open Web Application Security Project*)
- 1.4.3. *Cyber Security Kill Chain*

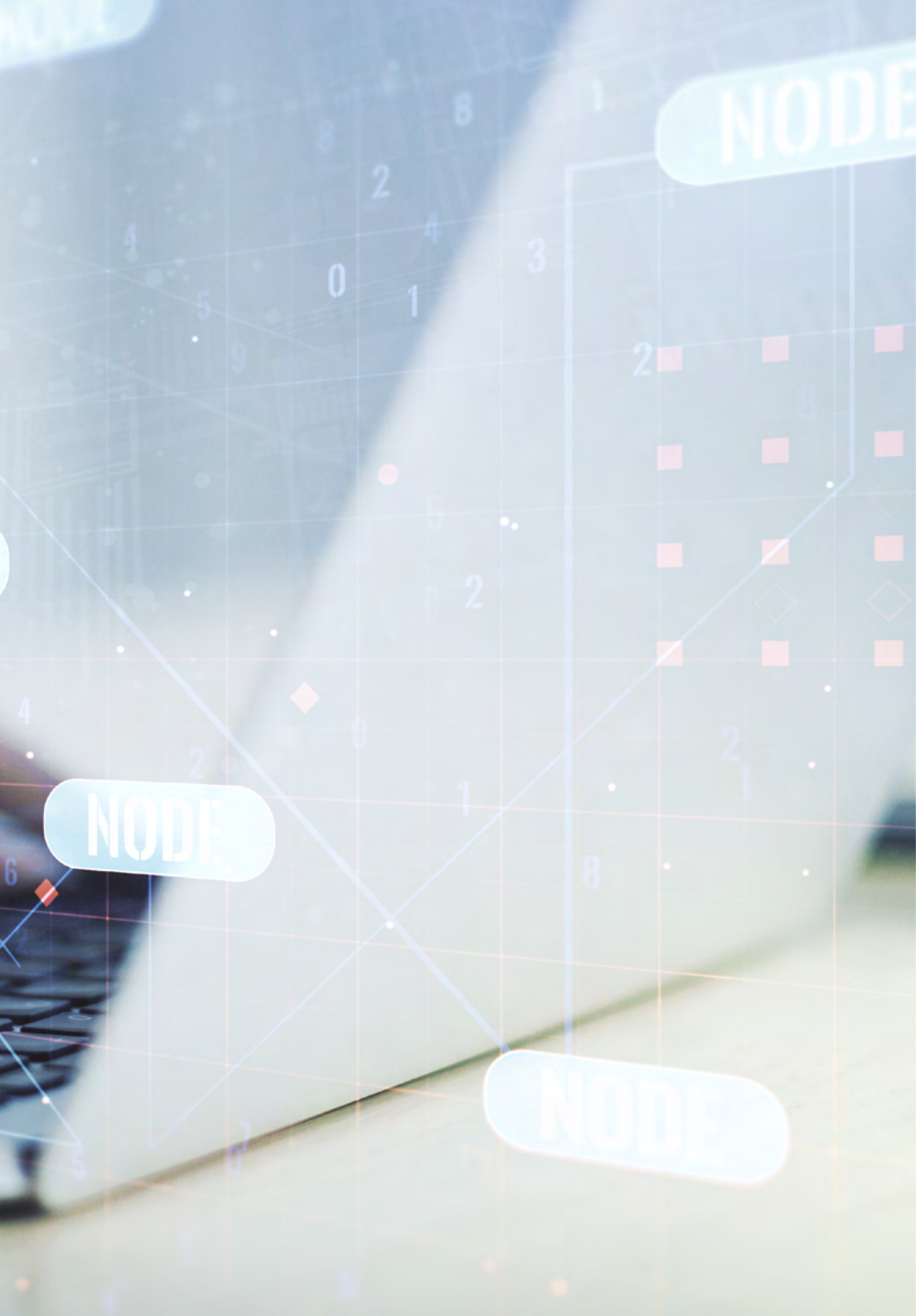
1.5. Роли и обязанности в наступательной безопасности
- 1.5.1. Основные профили
- 1.5.2. *Bug Bounty Hunters*
- 1.5.3. *Исследования:* Искусство исследования

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 источниках
- 1.7.1. Основы OSINT
- 1.7.2. Техники и инструменты OSINT
- 1.7.3. Применение OSINT в наступательной безопасности

1.8. Скриптинг: 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. Тематические кейсы: Этические ситуации в кибербезопасности

Модуль 2. Атаки на сети и системы Windows

2.1. Windows и Active Directory
- 2.1.1. История и эволюция Windows
- 2.1.2. Основы Active Directory
- 2.1.3. Функции и службы Active Directory
- 2.1.4. Общая архитектура Active Directory

2.2. Сетевая структура в средах Active Directory
- 2.2.1. Сетевые протоколы в Windows
- 2.2.2. DNS и его работа в Active Directory
- 2.2.3. Средства диагностики сети
- 2.2.4. Реализация сети в Active Directory

2.3. Аутентификация и авторизация в Active Directory
- 2.3.1. Процесс и поток аутентификации
- 2.3.2. Типы учетных данных
- 2.3.3. Хранение и управление учетными данными
- 2.3.4. Безопасность аутентификации

2.4. Разрешения и политики в Active Directory
- 2.4.1. GPO
- 2.4.2. Применение и управление GPO
- 2.4.3. Управление разрешениями в Active Directory
- 2.4.4. Уязвимости разрешений и их устранение

2.5. Основы Kerberos
- 2.5.1. Что такое Kerberos?
- 2.5.2. Компоненты и работа
- 2.5.3. Тикеты в Kerberos
- 2.5.4. Kerberos в контексте Active Directory

2.6. Передовые методы в Kerberos
- 2.6.1. Распространенные атаки на Kerberos
- 2.6.2. Профилактика и защита
- 2.6.3. Мониторинг трафика Kerberos
- 2.6.4. Расширенные атаки на Kerberos

2.7. *Службы сертификатов Active Directory* (ADCS)
- 2.7.1. Основные концепции PKI
- 2.7.2. Роли и компоненты ADCS
- 2.7.3. Конфигурация и развертывание ADCS
- 2.7.4. Безопасность ADCS

2.8. Атаки и защита *Active Directory Certificate Services* (ADCS)
- 2.8.1. Распространенные уязвимости в ADCS
- 2.8.2. Атаки и методы эксплуатации
- 2.8.3. Защита и смягчение последствий
- 2.8.4. Мониторинг и аудит ADCS

2.9. Аудит Active Directory
- 2.9.1. Важность аудита Active Directory
- 2.9.2. Инструменты аудита
- 2.9.3. Обнаружение аномалий и подозрительного поведения
- 2.9.4. Реагирование на инциденты и восстановление

2.10. Azure AD
- 2.10.1. Основы Azure AD
- 2.10.2. Синхронизация с локальной Active Directory
- 2.10.3. Управление идентификацией в Azure AD
- 2.10.4. Интеграция с приложениями и службами

Модуль 3. Анализ и исследование *вредоносных программ*

3.1. Анализ и исследование *вредоносных программ*
- 3.1.1. История и эволюция *вредоносных программ*
- 3.1.2. Классификация и типы *вредоносных программ*
- 3.1.3. Анализ *вредоносных программ*
- 3.1.4. Исследование *вредоносных программ*

3.2. Подготовка среды
- 3.2.1. Настройка виртуальных машин и *Snapshots*
- 3.2.2. Средства анализа вредоносных программ
- 3.2.3. Средства разработки вредоносных программ

3.3. Основы Windows
- 3.3.1. Формат файлов PE (*Portable Executable*)
- 3.3.2. Процессы и *потоки*
- 3.3.3. Файловая система и реестр
- 3.3.4. *Защитник Windows*

3.4. Основные методы борьбы с *вредоносными программами*
- 3.4.1. Генерация *шелл-кода*
- 3.4.2. Выполнение *шелл-кода* на диске
- 3.4.3. Диск против оперативной памяти
- 3.4.4. Выполнение *шелл-кода* в памяти

3.5. Промежуточные техники *вредоносных программ*
- 3.5.1. Устойчивость Windows
- 3.5.2. Стартовая папка
- 3.5.3. Ключи реестра
- 3.5.4. Скринсейверы

3.6. Передовые методы работы с *вредоносными программами*
- 3.6.1. Шифрование *шелл-кода* (XOR)
- 3.6.2. Шифрование *шелл-кода* (RSA)
- 3.6.3. Обфускация *строк*
- 3.6.4. Инъекция в процессы

3.7. Статический анализ *вредоносных программ*
- 3.7.1. Анализ *packers* с помощью DIE (*Detect It Easy*)
- 3.7.2. Анализ секций с помощью PE-Bear
- 3.7.3. Декомпиляция с помощью Ghidra

3.8. Динамический анализ *вредоносных программ*
- 3.8.1. Наблюдение за поведением с помощью Process Hacker
- 3.8.2. Анализ вызовов с помощью API Monitor
- 3.8.3. Анализ изменений в реестре с помощью Regshot
- 3.8.4. Наблюдение за сетевыми запросами с помощью TCPView

3.9. Анализ в .NET
- 3.9.1. Введение в .NET
- 3.9.2. Декомпиляция с помощью dnSpy
- 3.9.3. Отладка с помощью dnSpy

3.10. Анализ реальных вредоносных программ
- 3.10.1. Подготовка среды
- 3.10.2. Статический анализ *вредоносных программ*
- 3.10.3. Динамический анализ *вредоносных программ*
- 3.10.4. Создание правил YARA

Никаких строгих расписаний или графиков. Вот что такое обучение в TECH!

05

Методика обучения

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

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

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

Студент — приоритет всех программ TECH

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

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

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

Самые обширные учебные планы на международном уровне

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

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

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

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

Case studies или метод кейсов

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

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

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

Метод *Relearning*

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

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

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

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

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

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

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

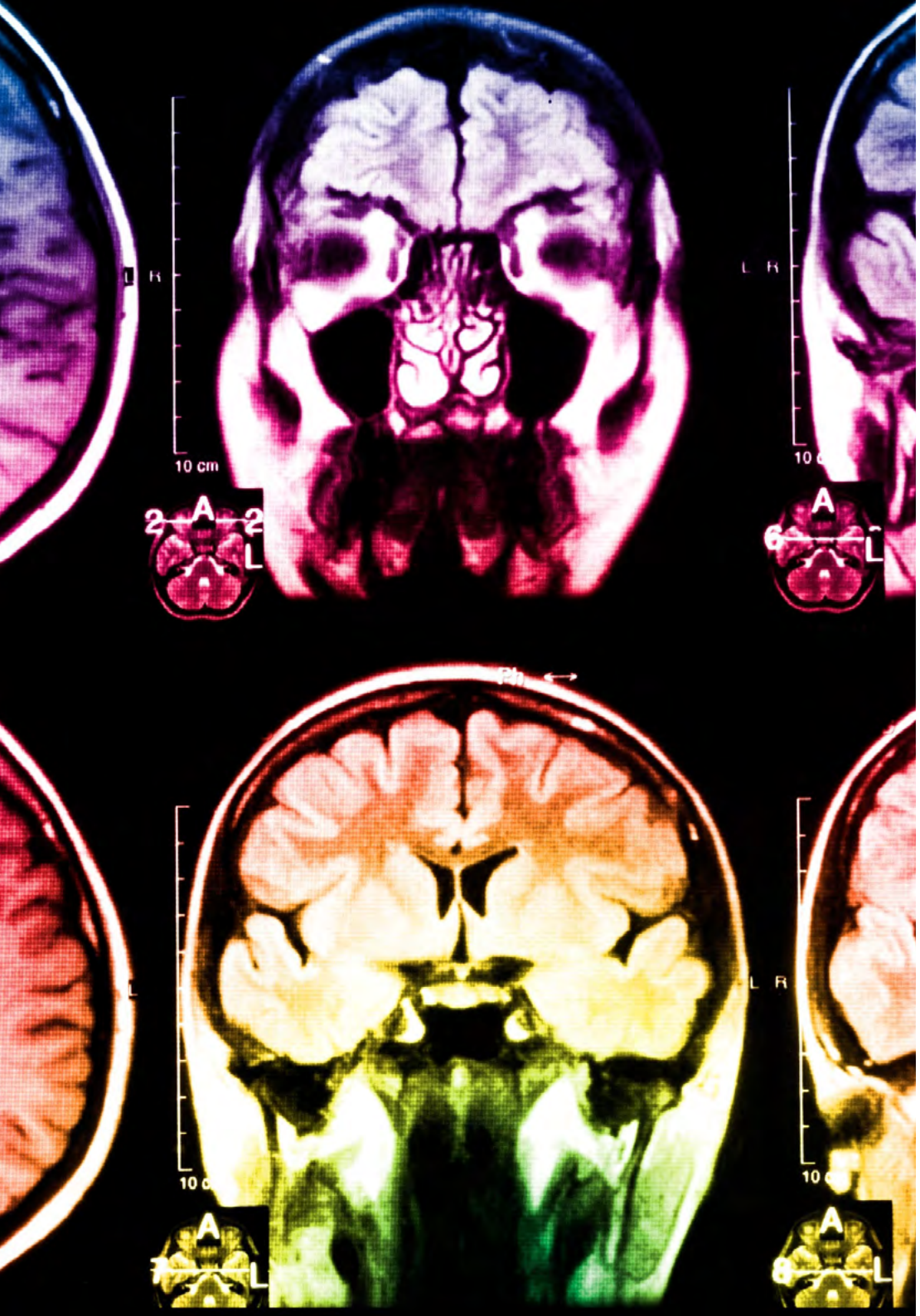
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи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

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

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

Эффективность метода обосновывается четырьмя ключевыми достижениями:

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



Методика университета, получившая самую высокую оценку среди своих студентов

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

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

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

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

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

Учебные материалы

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

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

Практика навыков и компетенций

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

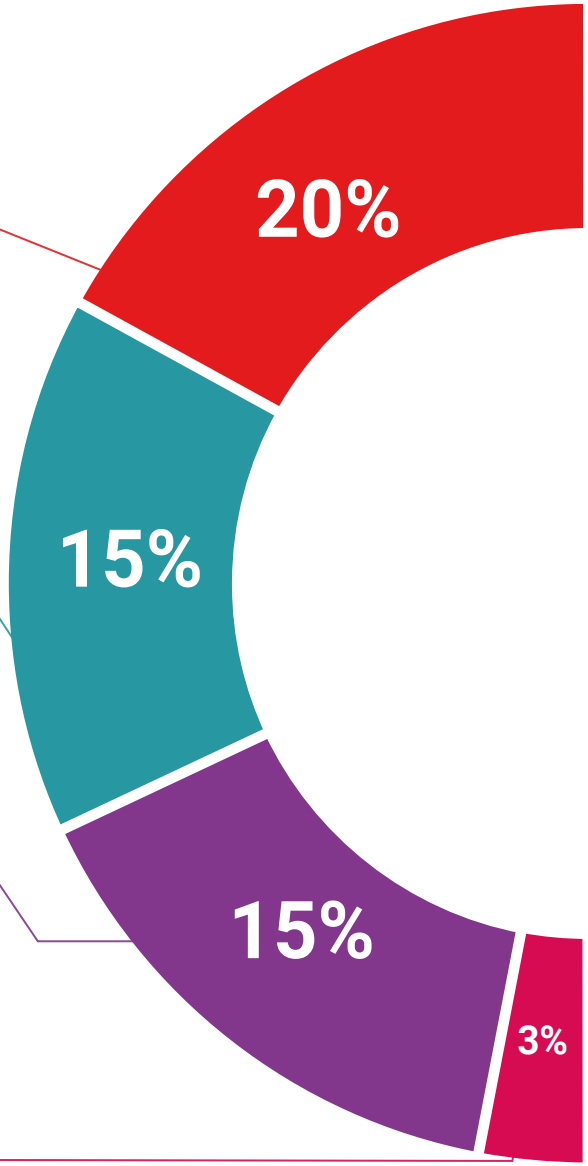
Интерактивные конспекты

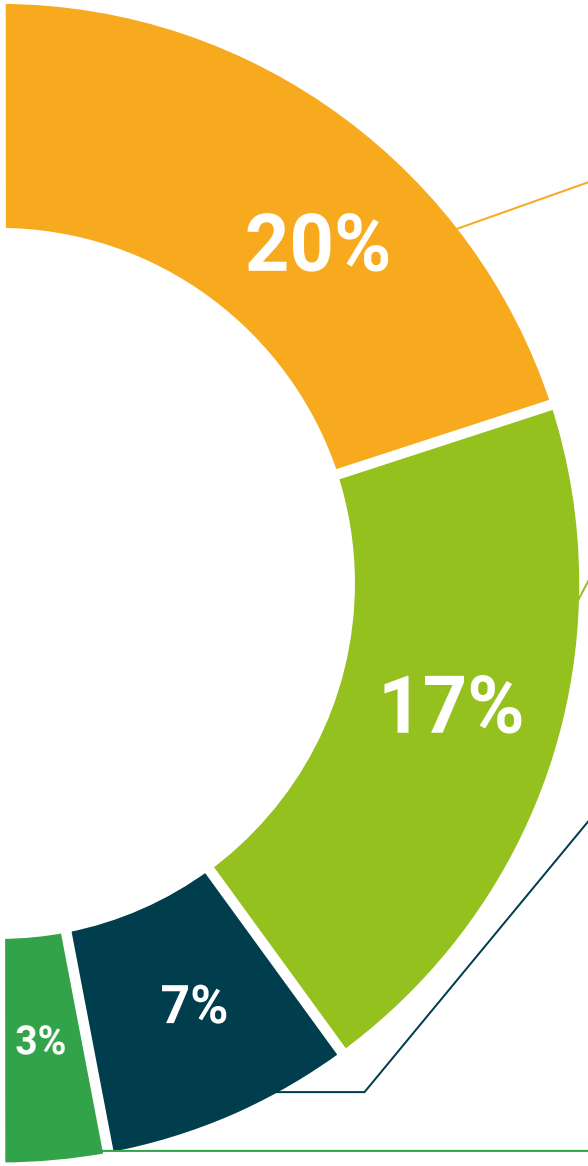
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

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

Дополнительная литература

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





Кейс-стади

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

Тестирование и повторное тестирование

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

Мастер-классы

Существуют научные данные о пользе экспертного наблюдения третьей стороны.

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

Краткие справочные руководства

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

06

Квалификация

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

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

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

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

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

Диплом: **Курс профессиональной подготовки в области наступательной кибербезопасности**

Формат: **онлайн**

Продолжительность: **6 месяцев**


tech технологический университет

Настоящий

ДИПЛОМ

свидетельствует о том, что

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

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

КУРС ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

в области

наступательной кибербезопасности

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

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

17 июня 2020 г.

Д-р Tere Guevara Navarro
Ректор

unique TECH code: AFWOR23S techtitute.com/certificates

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

tech технологический университет

Курс профессиональной подготовки

Наступательная кибербезопасность

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

Курс профессиональной подготовки

Наступательная кибербезопасность

tech технологический университет