Бизнес-магистратура

Пентест и Red Team

tech технологический университет

tech технологический университет

Бизнес-магистратура
Пентест и Red Team

- Формат: **онлайн**
- Продолжительность: **12 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**
- Программа предназначена для: **выпускников университетов и дипломированных специалистов, ранее окончивших любую из специальностей в области социальных, юридических, административных и деловых наук**

Веб-доступ: **www.techtitute.com/ru/school-of-business/executive-master-degree/master-pentesting-red-team**

Оглавление

01

Добро пожаловать

В настоящее время кибератаки приобрели значительный размах и силу, беспокоя население и сами компании. В результате компании испытывают огромный ущерб от этих угроз, вынужденные обеспечивать максимальную защиту баз данных и конфиденциальной информации своих клиентов. Таким образом, этот сектор находится в постоянном поиске высококвалифицированных специалистов по кибербезопасности, поэтому TECH разработал эту академическую программу, включающую технологические ресурсы и другие наработки по тактике, технике и процедурам, используемым злоумышленниками. И все это с помощью методологии *Relearning* и комплексной 100% онлайн-платформы, которая обеспечивает гибкость и удобное расписание.

Бизнес-магистратура в области пентеста и Red Team
TECH Технологический университет

Благодаря этой 100% онлайн-программе вы сможете специализироваться на продвижении этических и правовых практик при проведении атак и тестов на системы Windows"

02

Почему стоит учиться в TECH?

TECH — это крупнейшая бизнес-школа 100% онлайн-формата в мире. Мы являемся элитной бизнес-школой с образовательной моделью с самыми высокими академическими стандартами. Международный высокопроизводительный центр интенсивного обучения управленческим навыкам.

TECH — это передовой технологический университет, который предоставляет все свои ресурсы в распоряжение студентов, чтобы помочь им достичь успеха в бизнесе"

В TECH Технологический университет

Инновации

Мы предлагаем вам модель онлайн-обучения, сочетающую в себе новейшие образовательные технологии и максимальную педагогическую строгость. Уникальный метод с высочайшим международным признанием, который даст вам возможность развиваться в мире постоянных перемен, где инновации играют ключевую роль в деятельности каждого предпринимателя.

"История успеха Microsoft Europe" за включение в программы инновационной интерактивной мультивидеосистемы.

Высокие требования

Чтобы поступить в TECH, не потребуется большие затраты. Чтобы учиться у нас, вам не нужно делать большие инвестиции. Однако для того, чтобы получить диплом в TECH, необходимо проверить уровень знаний и возможностей студента. Наши академические стандарты очень высоки...

95% | **студентов TECH успешно завершают обучение**

Нетворкинг

Профессионалы со всего мира принимают участие в TECH, чтобы вы смогли создать большую сеть контактов, полезных для вашего будущего.

100 000+

менеджеров, прошедших ежегодную подготовку

200+

разных национальностей

Расширение прав и возможностей

Развивайтесь наряду с лучшими компаниями и профессионалами, обладающими большим авторитетом и влиянием. Мы создали стратегические альянсы и ценную сеть контактов с основными экономическими субъектами на 7 континентах.

+500+ | **соглашений о сотрудничестве с лучшими компаниями**

Талант

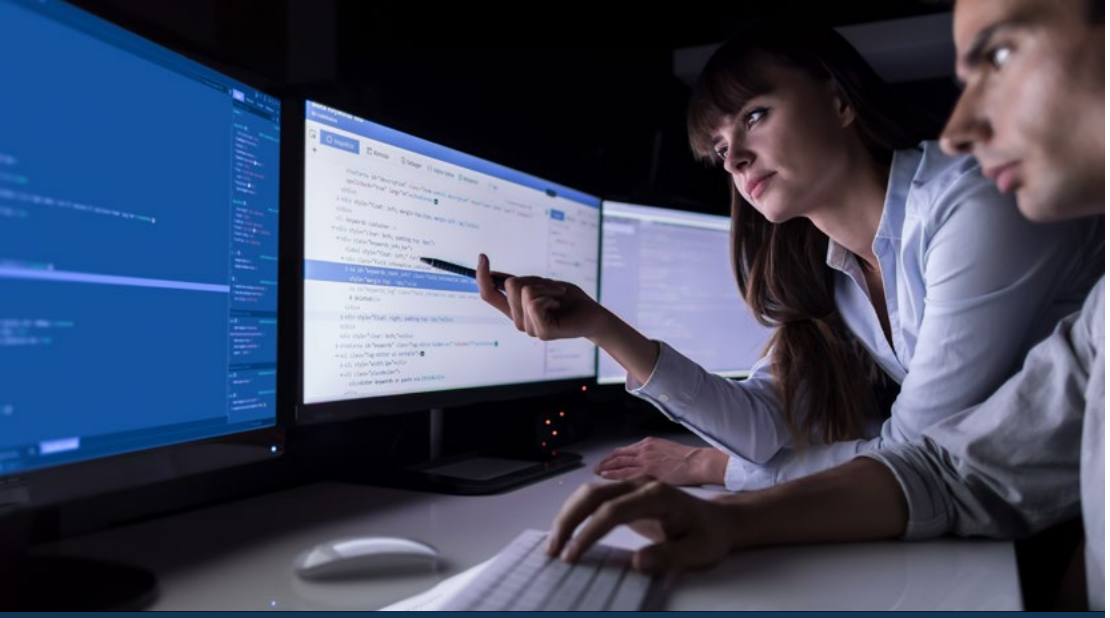
Наша программа - это уникальное предложение для раскрытия вашего таланта в мире бизнеса. Возможность, с помощью которой вы сможете заявить о своих интересах и видении своего бизнеса.

TECH помогает студентам показать миру свой талант при прохождении этой программы.

Мультикультурный контекст

Обучаясь в TECH, студенты могут получить уникальный опыт. Вы будете учиться в многокультурном контексте. В данной программе мы применяем глобальный подход, благодаря которому вы сможете узнать о том, как работают в разных частях света, собрать самую свежую информацию, которая наилучшим образом соответствует вашей бизнес-идее.

Наши студенты представляют более 200 национальностей.



Учитесь у лучших

Наши преподаватели объясняют в аудиториях, что привело их к успеху в их компаниях, работая в реальном, живом и динамичном контексте. Преподаватели, которые полностью посвящают себя тому, чтобы предложить вам качественную специализацию, которая позволит вам продвинуться по карьерной лестнице и выделиться в мире бизнеса.

Преподаватели представляют 20 различных национальностей.

В TECH у вас будет доступ к самому строгому и современному методу кейсов в академической среде"

TECH стремится к совершенству и для этого обладает рядом характеристик, которые делают его уникальным университетом:

Анализ

TECH исследует критическую сторону студента, его способность задавать вопросы, навыки решения проблем и навыки межличностного общения.

Академическое превосходство

TECH предлагает студентам лучшую методику онлайн-обучения. Университет сочетает метод *Relearning* (наиболее признанная во всем мире методология последипломного обучения) с «методом кейсов» Гарвардской школы бизнеса. Традиции и современность в сложном балансе и в контексте самого требовательного академического маршрута.

Экономия за счет масштаба

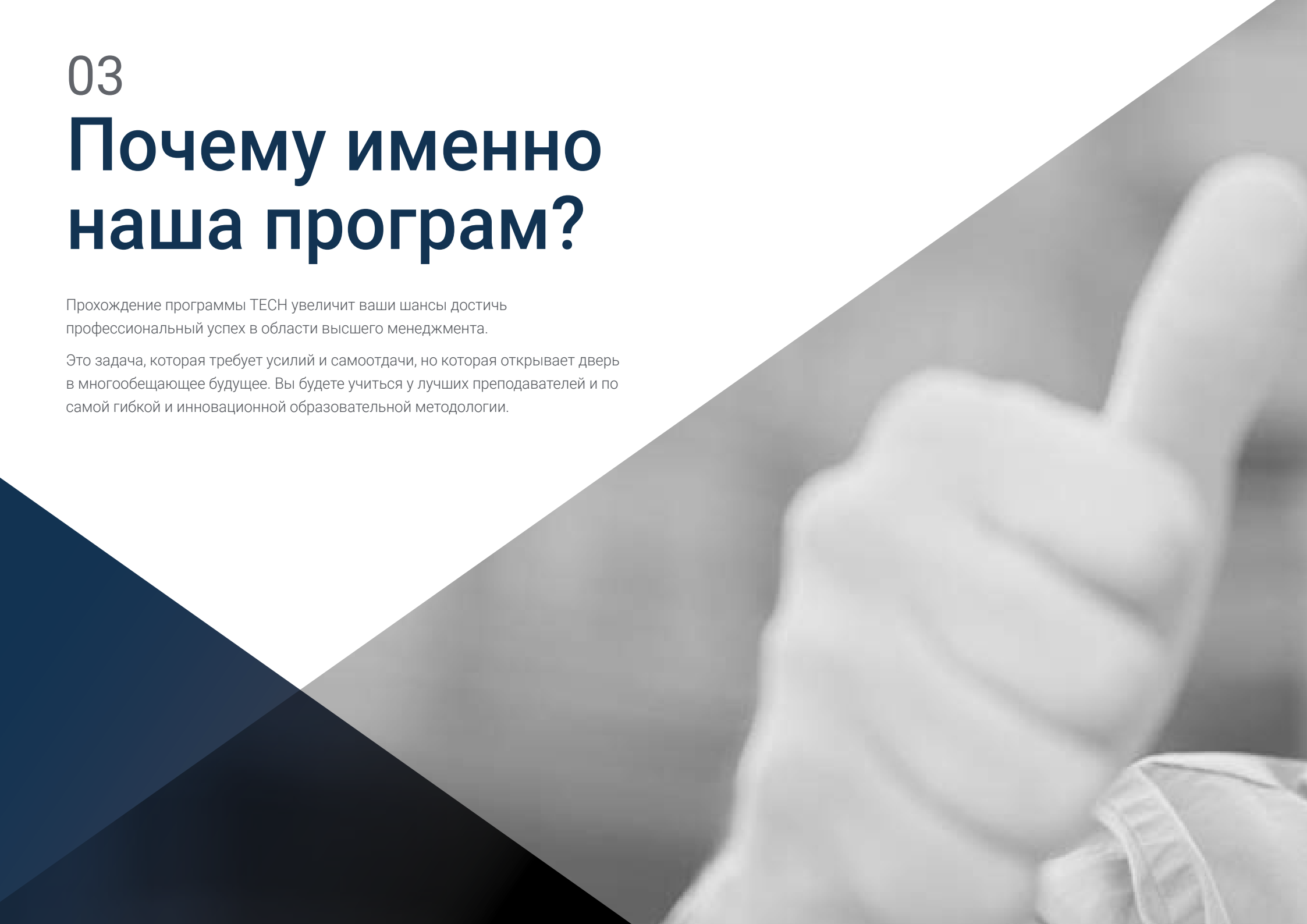
TECH — крупнейший в мире онлайн-университет. В его портфолио насчитывается более 10 000 университетских последипломных программ. А в новой экономике **объем + технология = разорительная цена**. Таким образом, мы заботимся о том, чтобы учеба для вас была не такой дорогой, как в другом университете.

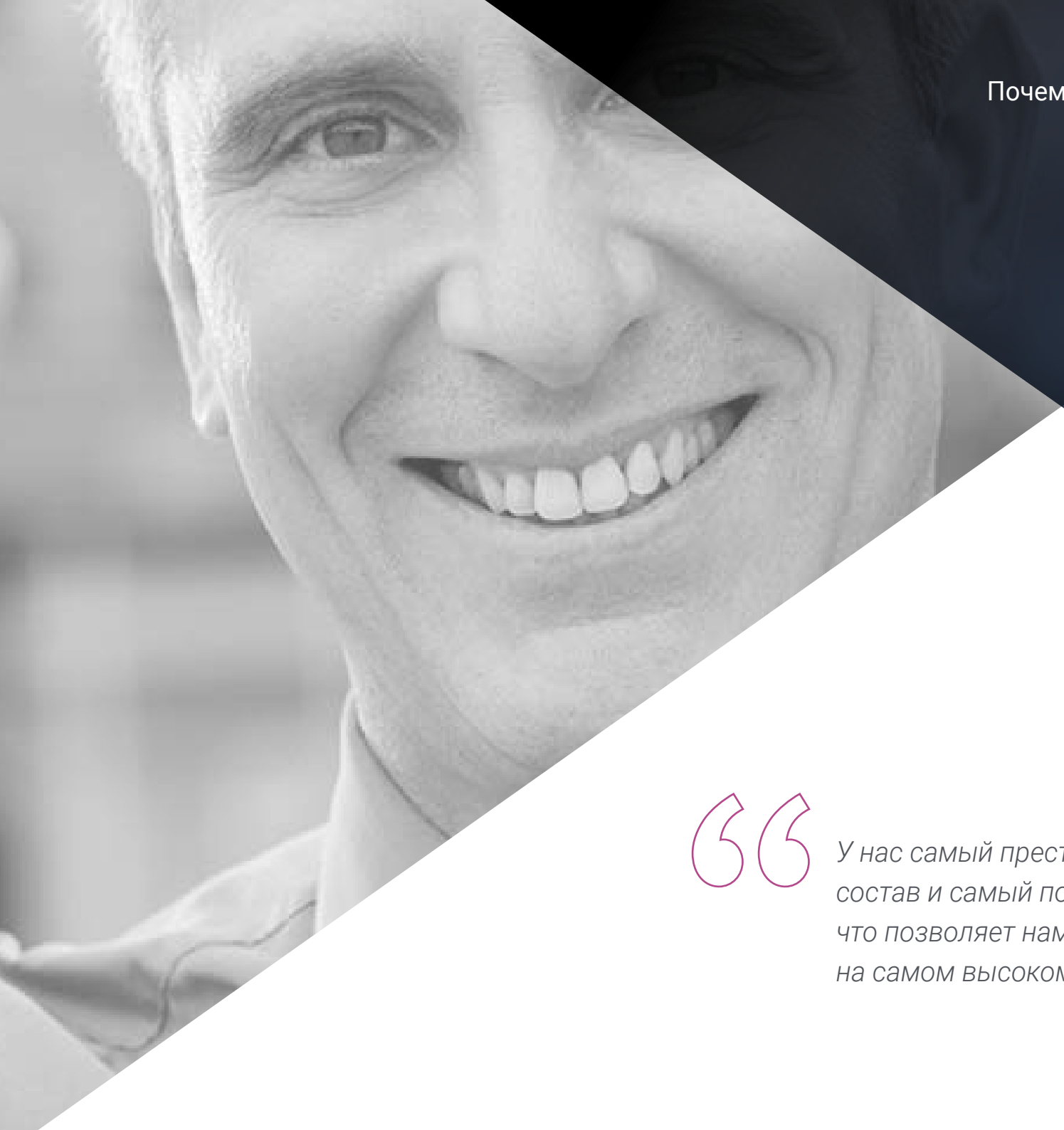
03

Почему именно наша програм?

Прохождение программы TECH увеличит ваши шансы достичь профессиональный успех в области высшего менеджмента.

Это задача, которая требует усилий и самоотдачи, но которая открывает дверь в многообещающее будущее. Вы будете учиться у лучших преподавателей и по самой гибкой и инновационной образовательной методологии.





У нас самый престижный преподавательский состав и самый полный учебный план на рынке, что позволяет нам предложить вам обучение на самом высоком академическом уровне"

Эта программа обеспечит вам множество преимуществ в трудоустройстве и вопросах личностного развития, включая следующие:

01

Дать решающий толчок карьере студента

Мы даем вам возможность взять под контроль свое будущее и полностью раскрыть свой потенциал. Пройдя нашу программу, вы приобретете необходимые навыки, чтобы за короткий срок добиться положительных изменений в своей карьере.

70% студентов этой специализации добиваются успешных изменений в своей карьере менее чем за 2 года.

02

Разрабатывать стратегическое и глобальное видение компании

Мы предлагаем вам глубокое понимание общего менеджмента, чтобы вы узнали, как каждое решение влияет на различные функциональные области компании.

Наше глобальное видение компании улучшит ваше стратегическое мышление.

03

Закрепиться в высшем руководстве предприятия

Обучение в TECH открывает двери в профессиональную среду, в которой студенты смогут позиционировать себя в качестве руководителей высокого уровня, обладающих широким видением международной среды.

Вы будете работать над более чем 100 реальными кейсами из области высшего менеджмента.

04

Брать на себя новые обязанности

Мы покажем вам последние тенденции, разработки и стратегии для осуществления вашей профессиональной деятельности в меняющихся условиях.

45% наших студентов получают повышение внутри компании.

05

Получить доступ к мощной сети контактов

TECH формирует своих студентов, чтобы максимально расширить их возможности. Студенты с теми же интересами и желанием развиваться. Таким образом, можно будет обмениваться контактами партнеров, клиентов или поставщиков.

Вы найдете сеть контактов, необходимых для вашего профессионального развития.

06

Разрабатывать свой бизнес-проект в строгой последовательности

Вы получите глубокое стратегическое видение, которое поможет вам разработать собственный проект, принимая во внимание различные направления деятельности компании.

20% наших студентов разрабатывают собственную бизнес-идею.

07

Совершенствовать свои *софт-скиллы* и управленческие умения

Мы помогаем вам применять и развивать полученные знания и совершенствовать навыки межличностного общения, чтобы стать лидером, который меняет мир к лучшему.

Улучшите свои коммуникативные и лидерские навыки и продвигайтесь по карьерной лестнице.

08

Стать частью эксклюзивного сообщества

Мы предлагаем вам возможность стать частью сообщества элитных менеджеров, крупных компаний, известных институтов и квалифицированных преподавателей из самых престижных университетов мира: сообщества TECH Технологический университет.

Мы даем вам возможность специализироваться с командой признанных преподавателей на международной сцене.

04

Цели

Данная университетская программа предоставит студентам инновационные технологии, касающиеся регулирования и соблюдения требований в проектах по кибербезопасности в области *пентеста*, что повысит ценность их профессиональной карьеры. В этом смысле TECH будет предоставлять дидактические ресурсы на протяжении всей разработки программы, развивая навыки, связанные с обнаружением аномалий и подозрительного поведения. Таким образом, по окончании этой программы студент расширит свои знания в области *пентеста и Red Team*. И все это — за 12 месяцев онлайн-обучения.

После окончания Специализированной магистратуры вы будете знать все о применении цифровых криминалистических исследований (DFIR) для раскрытия киберпреступлений"

TECH делает цели своих студентов своими собственными
Мы работаем вместе для достижения этих целей

Бизнес-магистратура в области пентеста и Red Team научит вас:

01 Изучить и понять тактику, технику и процедуры, используемые злоумышленниками, что позволит выявлять и моделировать угрозы

02 Применять теоретические знания в практических сценариях и симуляциях, сталкиваясь с реальными проблемами, чтобы укрепить навыки *пентеста*

03 Научиться эффективно распределять ресурсы в команде кибербезопасности, учитывая индивидуальные навыки и добиваясь максимальной производительности в проектах

04 Совершенствовать навыки общения, характерные для технической среды, облегчая понимание и координацию между членами команды

05 Освоить методы мониторинга и контроля проектов, выявлять отклонения и принимать необходимые корректирующие меры

06 Развить компетенции по оценке и улучшению конфигураций безопасности в системах Windows, обеспечивая реализацию эффективных мер

07 Продвигать этические и правовые практики при выполнении атак и тестов на системы Windows, учитывая этические принципы кибербезопасности

08 Ознакомить студента с оценкой безопасности API и веб-сервисов, выявлением потенциальных уязвимостей и укреплением безопасности интерфейсов программирования

09 Способствовать эффективному сотрудничеству с командами безопасности, объединяя стратегии и усилия по защите сетевой инфраструктуры

10 Пропагандировать этические и правовые нормы при анализе и исследовании вредоносных программ, обеспечивая честность и подотчетность во всех видах деятельности

11 Применять теоретические знания в смоделированных средах, участвовать в практических занятиях для понимания и противодействия вредоносным атакам

12 Приобрести твердое понимание фундаментальных принципов цифровой криминалистики (DFIR) и их применения для разрешения кибер-инцидентов

13 Научиться составлять подробные отчеты, документирующие результаты, использованные методики и рекомендации, полученные в ходе учений *Red Team*

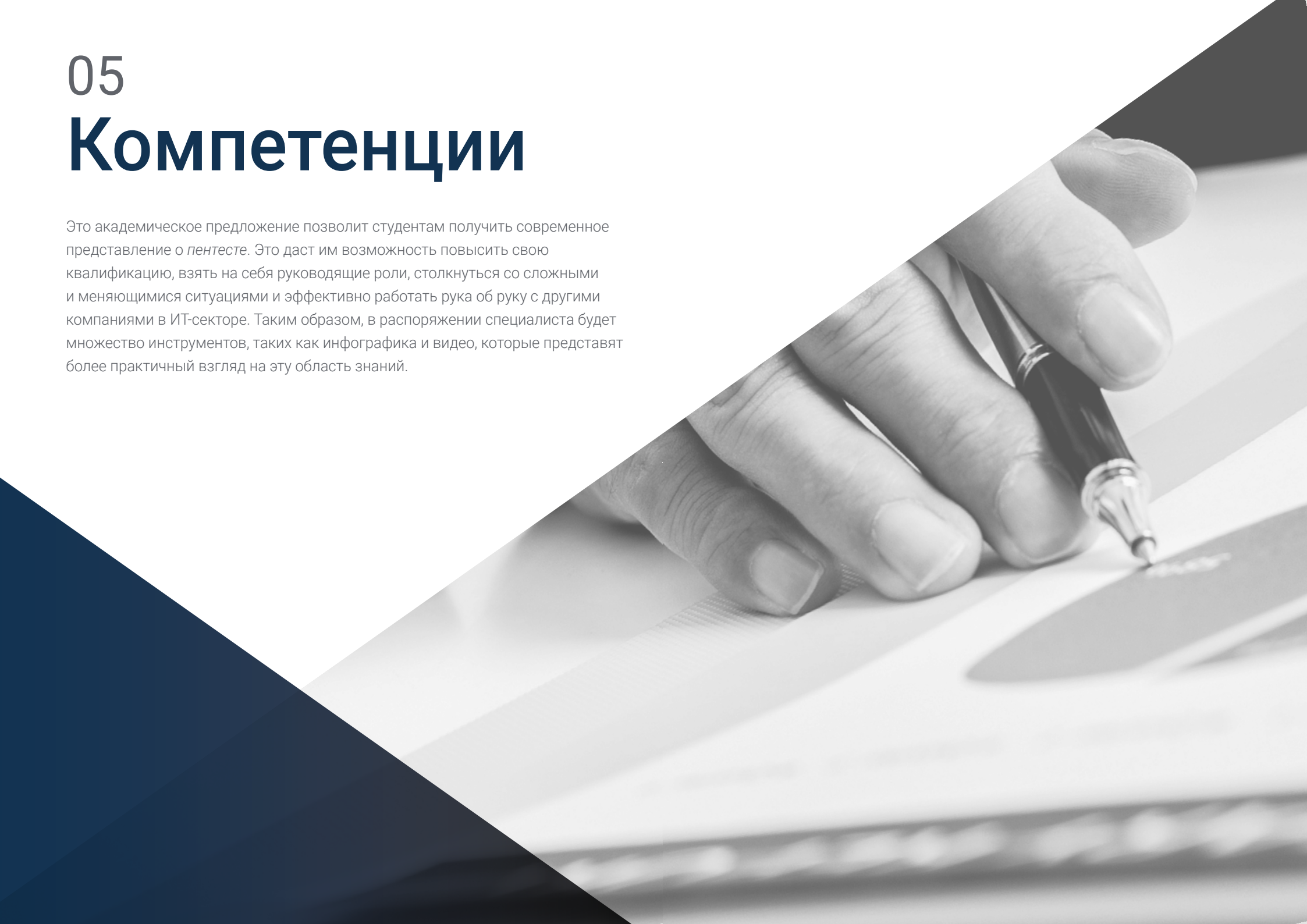
14 Развить навыки формулирования практических рекомендаций, направленных на устранение уязвимостей и повышение уровня безопасности

15 Ознакомить студента с лучшими практиками составления отчетов для руководителей, адаптации технических отчетов для нетехнической аудитории

05

Компетенции

Это академическое предложение позволит студентам получить современное представление о *пентесте*. Это даст им возможность повысить свою квалификацию, взять на себя руководящие роли, столкнуться со сложными и меняющимися ситуациями и эффективно работать рука об руку с другими компаниями в ИТ-секторе. Таким образом, в распоряжении специалиста будет множество инструментов, таких как инфографика и видео, которые представят более практичный взгляд на эту область знаний.



Усовершенствуйте свои навыки эффективного обнаружения и защиты от вредоносных программ, решая самые сложные ситуации в ИТ-секторе"

01 Приобретите навыки *коучинга* для профессионального развития членов команды, способствуя их росту и совершенствованию.

02 Развить навыки принятия стратегических решений в ситуациях кибербезопасности, учитывая краткосрочное и долгосрочное влияние на организационную безопасность

03 Приобрести навыки выявления, оценки и снижения рисков, характерных для проектов по кибербезопасности

04 Развить навыки реализации мер активной защиты, усиления системной и сетевой безопасности

05 Освоить методы анализа веб-трафика для выявления закономерностей и аномального поведения, облегчающие обнаружение возможных угроз

06 Приобрести навыки криминалистического анализа применительно к сетевым средам, что позволит выявления и эффективного реагирования на кибер-инциденты

07 Изучить стратегии эффективного обнаружения вредоносного ПО, включая развертывание передовых решений безопасности

08 Развить навыки выявления индикаторов компрометации (IoC) в ходе криминалистического исследования, облегчить судебно-экспертного расследования, облегчения обнаружения и реагирования на инциденты

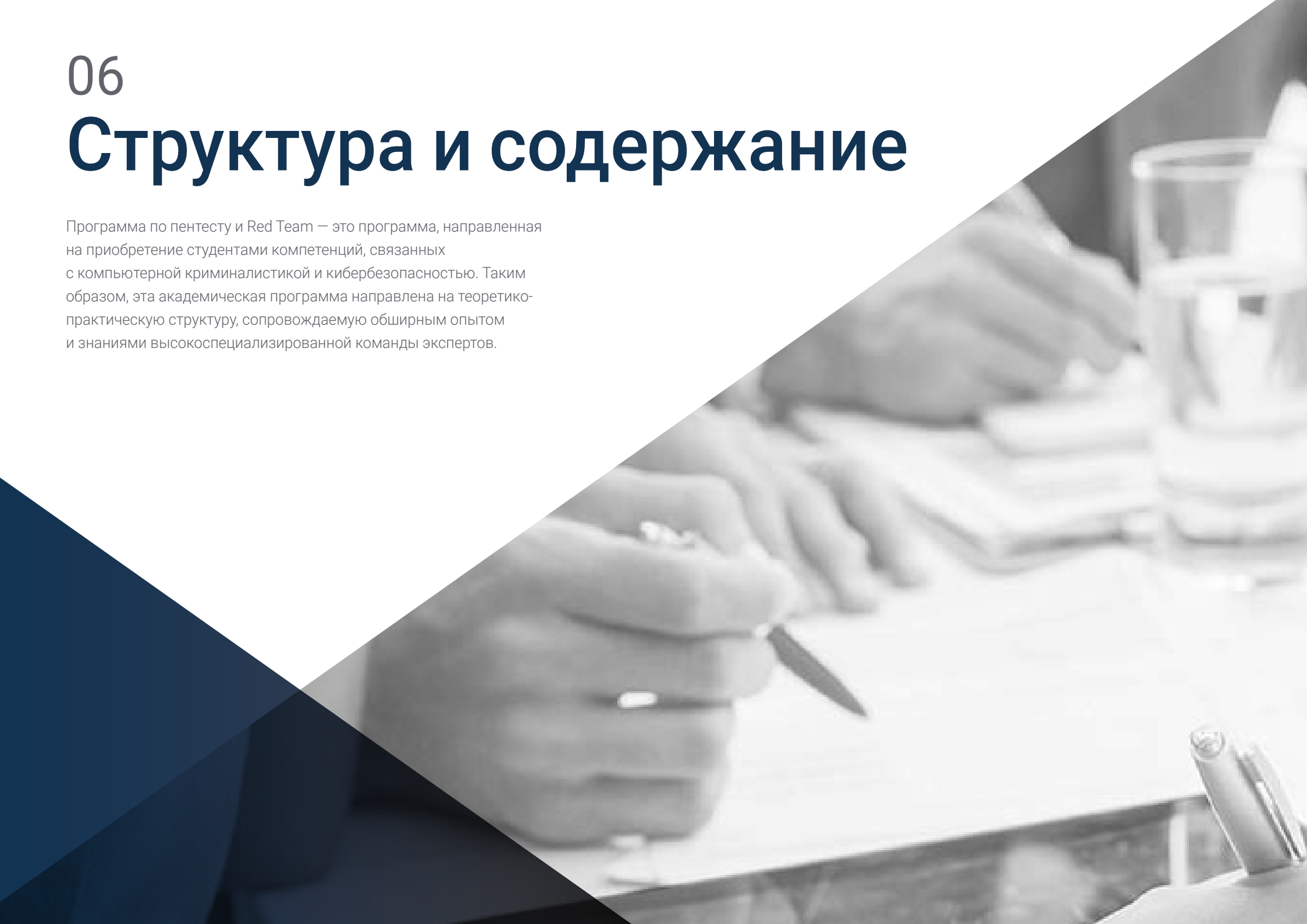
09 Приобрести навыки стратегического планирования учений *красной команды* с учетом целей, масштаба, ресурсов и реалистичных сценариев

10 Овладеть навыками идентификации и приоритизации уязвимостей, выделяя те из них, которые представляют наибольший риск для безопасности

06

Структура и содержание

Программа по пентесту и Red Team — это программа, направленная на приобретение студентами компетенций, связанных с компьютерной криминалистикой и кибербезопасностью. Таким образом, эта академическая программа направлена на теоретико-практическую структуру, сопровождаемую обширным опытом и знаниями высокоспециализированной команды экспертов.



Никаких расписаний и постоянных аттестаций: TECH гарантирует вам самый быстрый и гибкий доступ к академическому содержанию"

Учебный план

Данная университетская программа предполагает непрерывное обучение в течение всего курса, преподавание по самым высоким стандартам, благодаря чему студент сможет занять лучшие позиции в сфере информационных технологий и бизнеса. Таким образом, студенты смогут преодолеть различные препятствия, возникающие в рабочей сфере. Эта специализация позволит получить многочисленные навыки, которые касаются передовых технологий Kerberos, смягчения последствий и защиты.

Команда преподавателей разработала эксклюзивный учебный план, включающий 10 модулей, целью которых является приобретение студентами фундаментальных навыков, связанных с оценкой безопасности API и веб-сервисов, выявлением возможных точек уязвимости.

Кроме того, специалист изучит практические рекомендации, направленные на устранение уязвимостей и повышение уровня безопасности. В этом смысле они станут важными экспертами в области методов определения и предотвращения конфликтов.

В рамках этой академической программы студентам будет помогать уникальная методология *Relearning*, с помощью которой они смогут изучить сложные концепции и усвоить их повседневное применение без особых усилий. В то же время, обучение будет проходить на инновационной платформе 100% онлайн-обучения, которая не зависит от фиксированного расписания и графиков аттестации.

Данная Бизнес-магистратура рассчитана на 12 месяцев и состоит из 10 модулей:

Модуль 1	Наступательная безопасность
Модуль 2	Управление командами кибербезопасности
Модуль 3	Управление проектами безопасности
Модуль 4	Атаки на сети и системы Windows
Модуль 5	Продвинутый ***веб-хакинг***
Модуль 6	Сетевая архитектура и безопасность
Модуль 7	Анализ и исследование ***вредоносных программ***
Модуль 8	Основы криминалистики и DFIR
Модуль 9	Продвинутые учения ***Red Team***
Модуль 10	Техническая и исполнительная отчетность

Где, когда и как учиться?

TECH предлагает возможность пройти Специализированную магистратуру в области в области пентеста и Red Team в онлайн-формате. В течение 12 месяцев обучения вы сможете в любое время получить доступ ко всему содержанию данной программы, что позволит вам самостоятельно управлять учебным временем.

Уникальный, ключевой и решающий опыт обучения для повышения вашего профессионального роста"

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 проблемы и развивающиеся 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. *Researching*: 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. *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. Управление командами кибербезопасности

2.1. Руководство командой
2.1.1. Кто есть кто
2.2.1. Руководитель
2.3.1. 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 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. Последующие действия 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 непрерывное совершенствование
2.9.1. Принципы качества
2.9.2. Методы непрерывного совершенствования
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. Начальные этапы и определение целей
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. Справочники

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
4.1.2. 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. Как работает веб-сайт
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. Файлы *cookies*
5.2.2. JWT-*токены*
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 *Injection*
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. XML *External Entity* (XXE) *Injection*
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 Отказ в обслуживании*
5.10.2. DOM *Clobbering*
5.10.3. *Prototype Pollution*
5.10.4. HTTP *Request Smuggling*

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 *вредоносного ПО*
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. *Windows Defender*

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 *packers* 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 *Reverse-Proxy Phishing*
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. *Dump* LSASS
9.6.2. *Dump* 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. Исполнительная vs техническая

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. Благодарность
10.6.3. Документация
10.6.4. Подготовка отчета

10.7. LINCE
10.7.1. Понимание методологии
10.7.2. Благодарность
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

07

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.

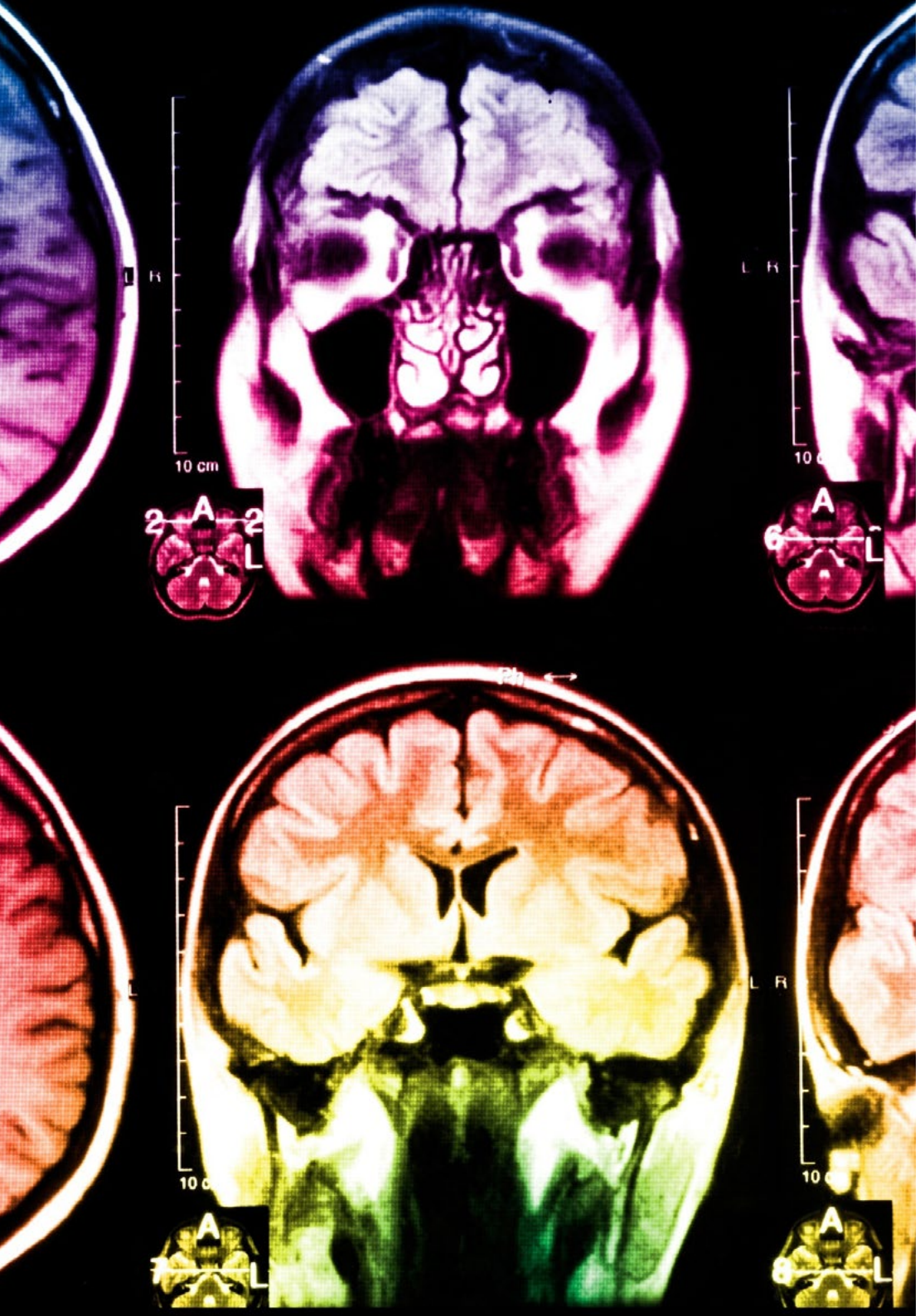
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи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

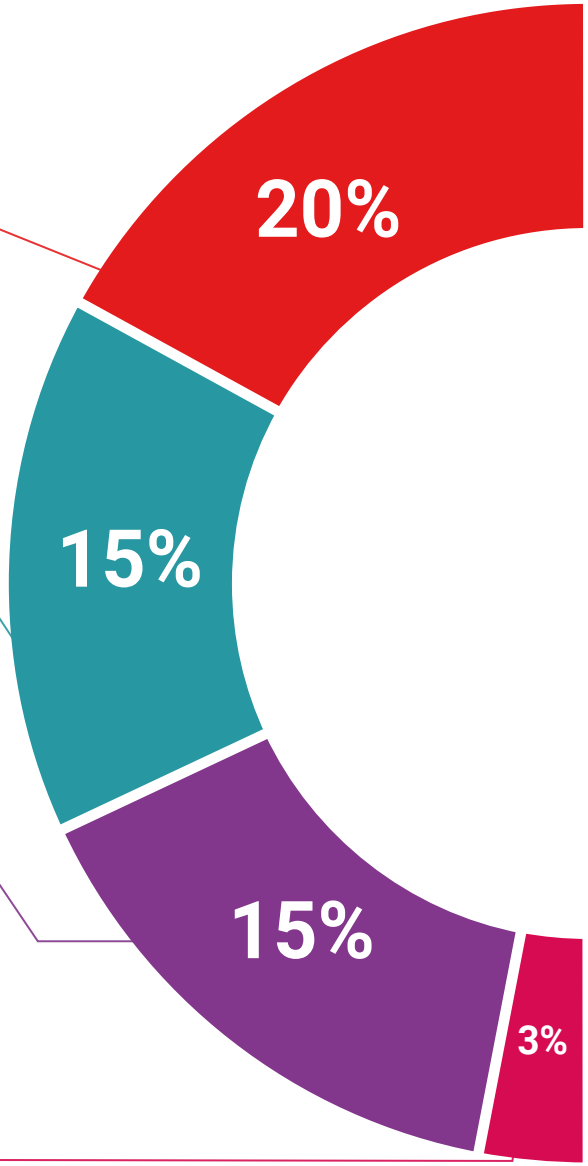
Интерактивные конспекты

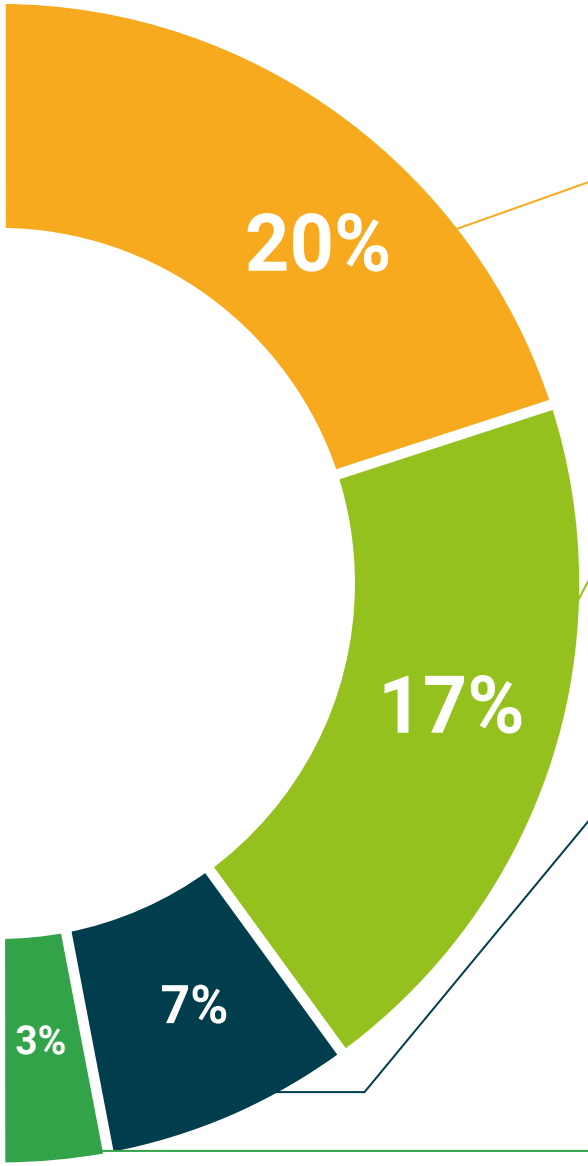
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

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.

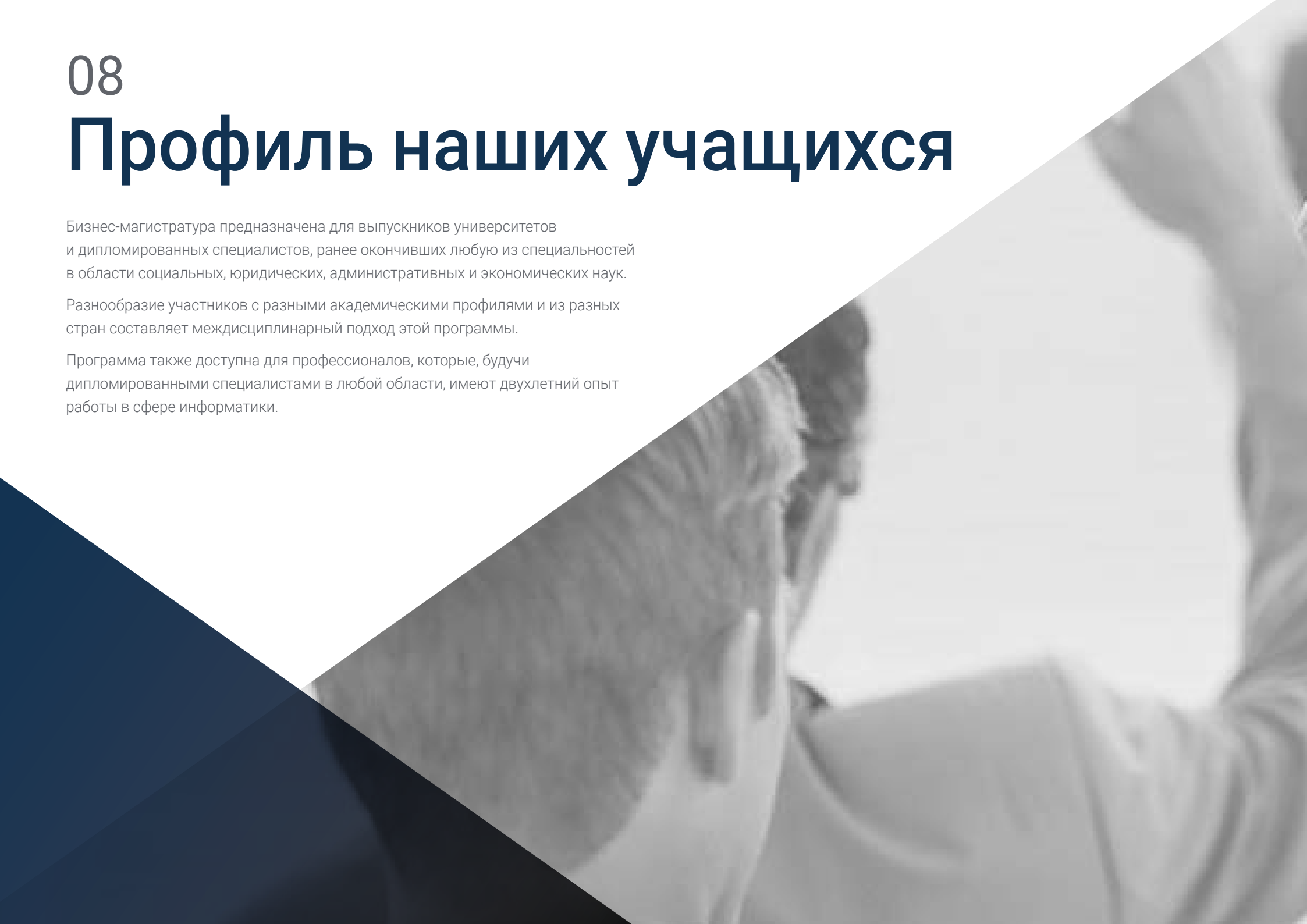
08

Профиль наших учащихся

Бизнес-магистратура предназначена для выпускников университетов и дипломированных специалистов, ранее окончивших любую из специальностей в области социальных, юридических, административных и экономических наук.

Разнообразие участников с разными академическими профилями и из разных стран составляет междисциплинарный подход этой программы.

Программа также доступна для профессионалов, которые, будучи дипломированными специалистами в любой области, имеют двухлетний опыт работы в сфере информатики.

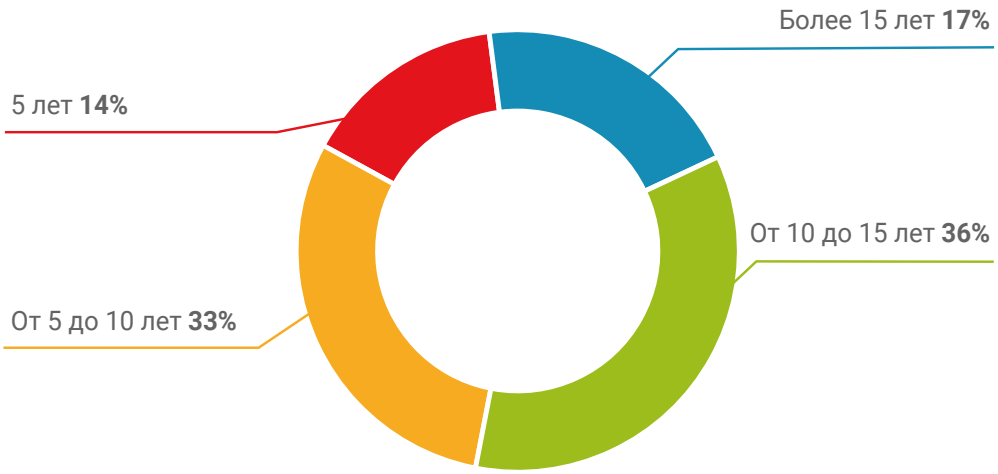


Если у вас есть опыт работы в области пентеста и Red Team, и вы ищете возможность интенсивного карьерного роста, продолжая при этом работать, то эта программа для вас"

Средний возраст

В возрасте от **35** до **45** лет

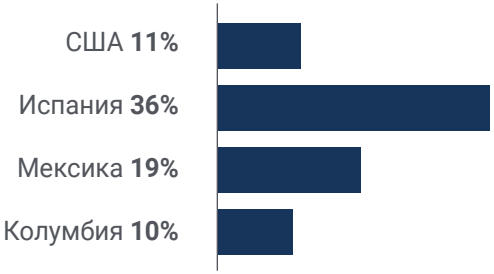
Годы практики



Обучение

Академический профиль

Географическое распределение



Саломон Гальвис

Аналитик по информационной безопасности

"Из этой программы я отмечаю, что мне удалось глубже понять важность регулярных оценок и то, насколько важно контролировать кибербезопасность. Это большая инвестиция в будущее благодаря ключевым инструментам, которые команда преподавателей внедряет в разработку программы"

09

Руководство курса

Бизнес-магистратура имеет в своем распоряжении команду преподавателей с большим международным признанием и обширными специализированными знаниями в области программного обеспечения, технологий информационного общества и кибербезопасности. Таким образом, престижное образование отражается в динамичном и инновационном подходе к учебной программе, реализующей последние тенденции в области кибербезопасности. Благодаря сочетанию моделирования и анализа реальных ситуаций студенты получают первоклассный практический опыт, позволяющий им решать различные профессиональные задачи на рабочем месте.

Ведущие эксперты в области пентеста и Red Team проведут эту инновационную и интенсивную программу"

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 курсов обучения высшего уровня профессионального образования 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 в Политехническом университете Мадрида

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 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 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

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

Уникальный, важный и значимый курс обучения для развития вашей карьеры"

10

Влияние на карьеру

Эта университетская программа была разработана с целью дать студенту знания, которые помогут ему справиться с любой ситуацией в области кибербезопасности. Таким образом, TECH сосредоточится на преподавании самого высокого качества, стремясь к эффективности в каждой из своих программ. Поэтому специалисту будет гарантировано специализированное обучение в области *пентеста* и *Red Team*.

Red Team и другие IT-аспекты кибербезопасности могут быть интегрированы в пентест благодаря этой интенсивной программе"

Продвинутые техники пивотирования — вот некоторые из навыков, которыми вы будете владеть после прохождения этой комплексной 12-месячной Специализированной магистратуры.

Готовы ли вы решиться на перемены? Вас ждет отличный профессиональный рост

Бизнес-магистратура в области пентеста и Red Team от TECH — это интенсивная программа, которая подготовит вас к решению задач и принятию бизнес-решений в области информатики. Главная цель — способствовать вашему личностному и профессиональному росту. Мы помогаем вам добиться успеха.

Если вы хотите усовершенствоваться, добиться положительных изменений на профессиональном уровне и пообщаться с лучшими, это место для вас.

Воспользуйтесь возможностью расширить свои навыки в области пентестинга в TECH, лучшем в мире онлайн-университете по версии Forbes.

Время перемен

Что изменится

Повышение заработной платы

Прохождение этой программы означает для наших студентов повышение заработной платы более чем на **25,55%**

11

Преимущества для вашей компании

Эта программа способствует раскрытию максимального потенциала талантов организации благодаря обучению руководителей высокого уровня.

Кроме того, прохождение этой университетской программы — уникальная возможность получить доступ к мощной сети контактов, в которой можно найти будущих профессиональных партнеров, клиентов или поставщиков.

В цифровую эпоху руководители должны интегрировать новые процессы и стратегии, которые приводят к значительным изменениям и организационному развитию. Это возможно только при условии университетского обучения и повышения квалификации"

Развитие и удержание талантов в компаниях – лучшая долгосрочная инвестиция.

01

Рост талантов и интеллектуального капитала

Профессионал привносит в компанию новые концепции, стратегии и перспективы, которые могут привести к соответствующим изменениям в организации.

02

Удержание руководителей с высоким потенциалом и избежание "утечки мозгов"

Эта программа укрепляет связь между компанией и специалистом и открывает новые возможности для профессионального роста внутри компании.

03

Создание агентов изменений

Вы сможете принимать решения в периоды неопределенности и кризиса, помогая организации преодолеть их.

04

Расширение возможностей для международной экспансии

Эта программа позволит компании установить контакт с основными рынками мировой экономики.

05

Разработка собственных проектов

Профессионал может работать над реальным проектом или разрабатывать новые проекты в области НИОКР или развития бизнеса своей компании.

06

Повышение конкурентоспособности

Данная программа предоставит специалистам необходимые навыки, чтобы они могли решать новые задачи и тем самым двигать организацию вперед.

12

Квалификация

Бизнес-магистратура в области пентеста и Red Team гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Бизнес-магистратура, выдаваемого TECH Технологическим университетом.

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

Данная **Бизнес-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 **Бизнес-магистратура** выданный **TECH Технологическим университетом.**

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

Диплом: **Бизнес-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

БИЗНЕС-МАГИСТРАТУРА

в области

пентеста и Red Team

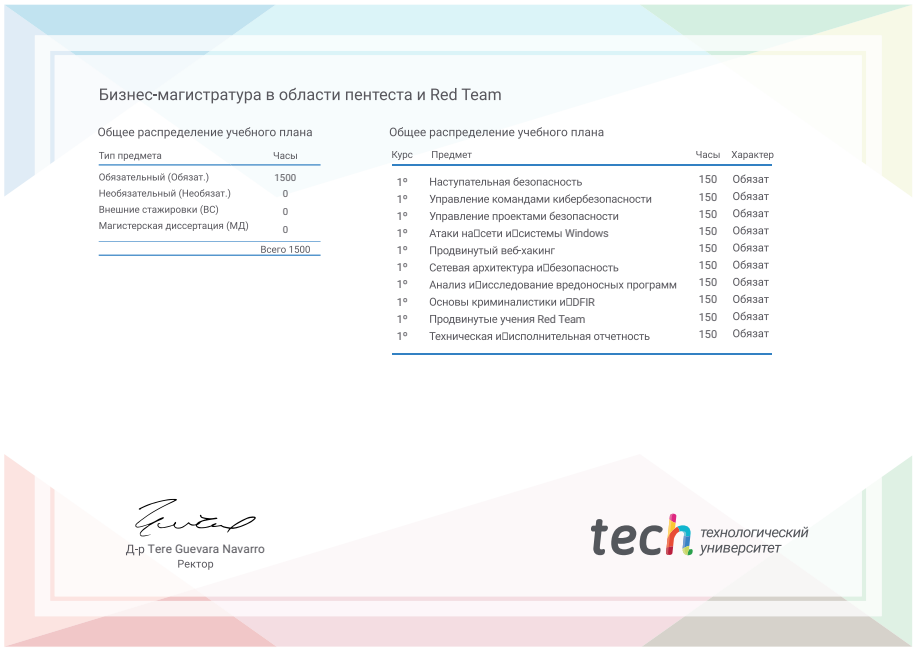
Данный диплом специализированной программы, присуждаемый Университетом, соответствует 1500 учебным часам, с датой начала дд/мм/гггг и датой окончания дд/мм/гггг.

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


Бизнес-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.

технологический университет

Бизнес-магистратура
Пентест и Red Team

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

Бизнес-магистратура

Пентест и Red Team

tech технологический университет