

Курс профессиональной подготовки

Оборонительная кибербезопасность



Курс профессиональной подготовки Оборонительная кибербезопасность

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

Веб-доступ: www.techitute.com/ru/school-of-business/postgraduate-diploma/postgraduate-diploma-defensive-cybersecurity

Оглавление

01

Добро пожаловать

стр. 4

02

Почему стоит учиться
в TESH?

стр. 6

03

Почему именно наша
программа?

стр. 10

04

Цели

стр. 14

05

Структура и содержание

стр. 20

06

Методология

стр. 28

07

Профиль наших учащихся

стр. 36

08

Руководство курса

стр. 40

09

Влияние на карьеру

стр. 46

10

Преимущества для
вашей компании

стр. 50

11

Квалификация

стр. 54

01

Добро пожаловать

Интернет является частью повседневной жизни наиболее развитых обществ. Его ежедневное использование означает, что граждане все больше привыкают к цифровым инструментам и используют их для любых повседневных действий. Кроме того, они способствовали большим достижениям в сфере бизнеса. Однако преступники нашли в сети новый способ действовать, подвергая риску практически все компании. В связи с этим возникает необходимость в том, чтобы руководители компаний и менеджеры среднего звена приобрели знания, которые позволят им действовать защитно перед лицом возможных атак, применяя превентивные меры, чтобы избежать нападения на их цифровую инфраструктуру. Чтобы удовлетворить эту потребность в специализации бизнес-профессионалов, TECH разработал специальную академическую программу "Оборонительная кибербезопасность", которая будет очень полезна для защиты их бизнеса.



Курс профессиональной подготовки в области оборонительной кибербезопасности
TECH Global University

“

Специализируйтесь на оборонительной кибербезопасности благодаря мастер-классам эксперта в области разведки, кибербезопасности и подрывных технологий”

02

Почему стоит учиться в ТЕСН?

ТЕСН — 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.



“

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

В TECH Технологическом университете



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 мультимедийной системы.



Высокие требования

Чтобы поступить в TECH, не потребуются 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 мультикультурном 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.



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.



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"

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 личного 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 Технологического университета.

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

04

Цели

Курс профессиональной подготовки в области оборонительной кибербезопасности от ТЕСН предназначен для укрепления профессиональных навыков руководителей компаний, желающих получить высшую специализацию в области кибербезопасности. В данном конкретном случае программа фокусируется на оборонительной кибербезопасности, чтобы они приобрели необходимые навыки для успешного управления в секторе, который становится все более популярным в бизнесе. Несомненно, это задача, которая становится все более важной в современном обществе.



“

Развивайте навыки,
необходимые для управления
цифровой безопасностью
вашего бизнеса”

Ваши цели – это наши цели

Мы работаем вместе, чтобы помочь вам их достичь

Курс профессиональной подготовки в области оборонительной кибербезопасности научит студента:

01

Определять политику резервного копирования
личных и рабочих данных

04

Проводить сканирование
оборудования на наличие вторжений

02

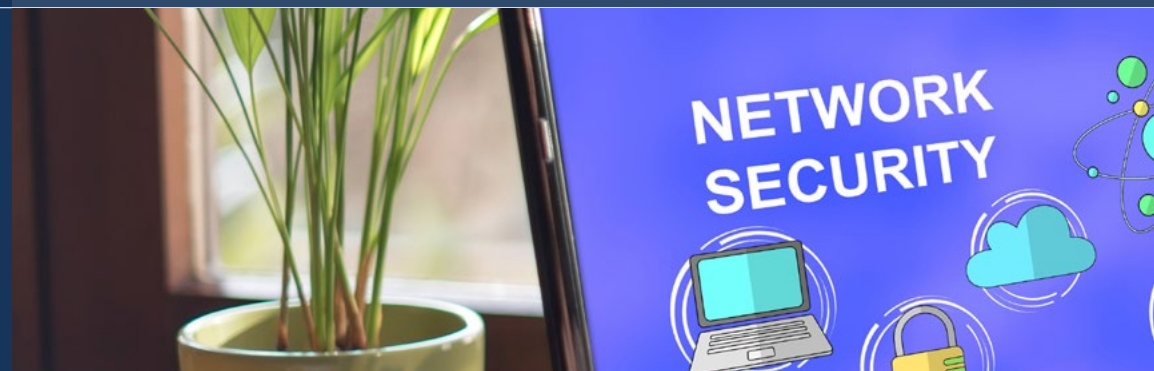
Оценивать различные инструменты для
решения конкретных проблем безопасности

03

Устанавливать механизмы для
актуализации системы

05

Определять правила доступа к системе



06

Проверять и классифицировать электронную почту для предотвращения мошенничества

08

Проанализировать текущие сетевые архитектуры для определения периметра защиты

09

Разрабатывать специальные конфигурации *брандмауэра* и Linux для защиты от наиболее распространенных атак

07

Генерировать списки разрешенного программного обеспечения

10

Изучить различные дополнительные уровни, предоставляемые *брандмауэрами* нового поколения и сетевыми функциями в облаке



11

Определять инструменты для защиты сети и демонстрировать, почему они являются основополагающими для многоуровневой защиты

12

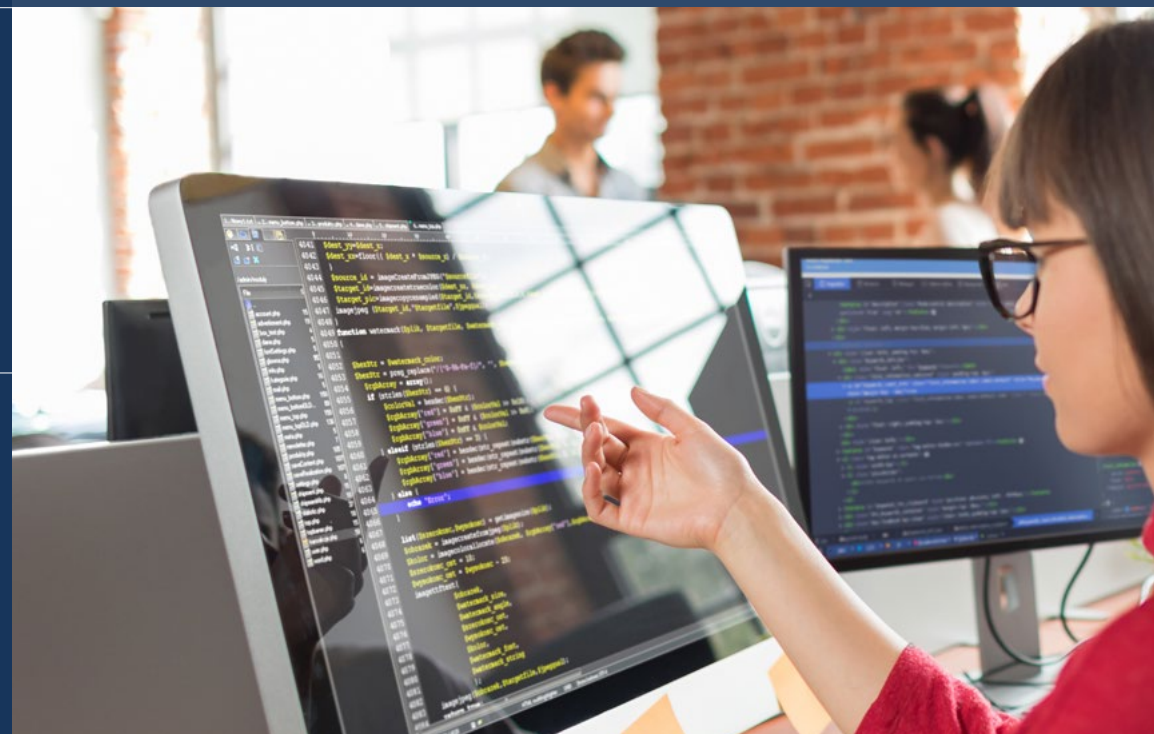
Определять основные атаки и типы вредоносных программ, которым подвергаются пользователи мобильных устройств

13

Проанализировать новейшие устройства для создания более безопасной конфигурации

14

Указывать основные шаги для проведения теста на проникновение на платформах iOS и Android



15

Расширять знания о различных инструментах защиты и безопасности

16

Проанализировать основные архитектуры IoT

17

Разрабатывать основные протоколы внедрения

18

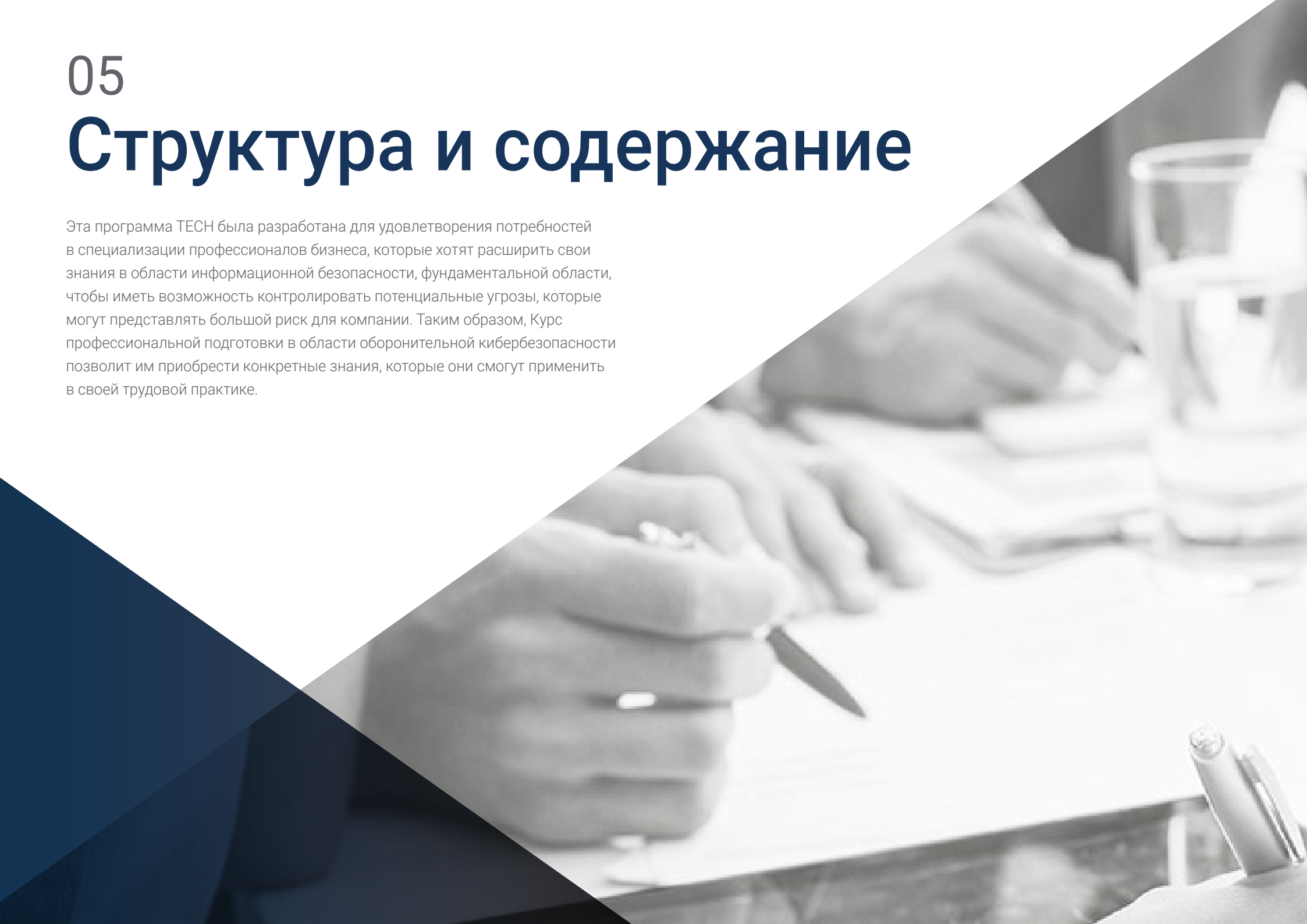
Оценивать уровни риска и существующие уязвимости



05

Структура и содержание

Эта программа TECH была разработана для удовлетворения потребностей в специализации профессионалов бизнеса, которые хотят расширить свои знания в области информационной безопасности, фундаментальной области, чтобы иметь возможность контролировать потенциальные угрозы, которые могут представлять большой риск для компании. Таким образом, Курс профессиональной подготовки в области оборонительной кибербезопасности позволит им приобрести конкретные знания, которые они смогут применить в своей трудовой практике.



“

*Учебный план, ориентированный
на то, чтобы способствовать
вашему обучению процессам
кибербезопасности”*

Учебный план

Курс профессиональной подготовки "Оборонительная кибербезопасность" от TECH Global University — это интенсивная программа, которая готовит студентов к решению проблем и принятию бизнес-решений в области ИТ-безопасности.

На протяжении 600 часов обучения вы разберете множество практических кейсов, что позволит вам приобрести необходимые навыки для успешного развития в вашей повседневной практике. Таким образом, это настоящее погружение в реальные деловые ситуации.

Данная программа углубленно рассматривает различные направления деятельности компании и разработана для руководителей, чтобы помочь им понимать кибербезопасность со стратегической, международной и инновационной точек зрения.

Кроме того, TECH предлагает студентам полноценные и эксклюзивные *мастер-классы*, которые проходят под руководством преподавателя-эксперта с большим

профессиональным опытом и международным авторитетом. Так, студент погрузится в тему "Оборонительная кибербезопасность", затрагивающую такие важные понятия, как безопасность хоста, сетей, смартфонов и IoT.

План, разработанный специально для студентов, ориентированный на их профессиональное совершенствование и готовящий их к достижению самых высоких позиций в области управления ИТ-безопасностью. Программа, которая понимает ваши потребности и потребности вашей компании благодаря инновационному содержанию, основанному на последних тенденциях, и поддерживается лучшей образовательной методологией и исключительным преподавательским составом, что позволит вам приобрести навыки решения критических ситуаций творческим и эффективным способом.

Модуль 1

Безопасность хоста

Модуль 2

Сетевая безопасность (периметр)

Модуль 3

Безопасность *смартфонов*

Модуль 4

Безопасность в IoT



Где, когда и как учиться?

TECH предлагает возможность пройти Курс профессиональной подготовки в области оборонительной кибербезопасности полностью в онлайн-формате. В течение 6 месяцев обучения студент сможет в любое время получить доступ ко всему содержанию данной программы, что позволит ему самостоятельно управлять учебным временем.

*Уникальный, ключевой
и решающий
образовательный опыт,
позволяющий повысить
свой профессиональный
уровень и сделать
решающий рывок.*

Модуль 1. Безопасность хоста

1.1. Резервные копии

- 1.1.1. Стратегии резервного копирования
- 1.1.2. Инструменты для Windows
- 1.1.3. Инструменты для Linux
- 1.1.4. Инструменты для MacOS

1.2. Пользовательский антивирус

- 1.2.1. Виды антивирусов
- 1.2.2. Антивирус для Windows
- 1.2.3. Антивирус для Linux
- 1.2.4. Антивирус для MacOS
- 1.2.5. Антивирусы для смартфонов

1.3. Детекторы вторжения - HIDS

- 1.3.1. Методы обнаружения вторжений
- 1.3.2. Sagan
- 1.3.3. Aide
- 1.3.4. Rkhunter

1.4. Локальный брандмауэр

- 1.4.1. Брандмауэры для Windows
- 1.4.2. Брандмауэры для Linux
- 1.4.3. Брандмауэры для MacOS

1.5. Менеджеры паролей

- 1.5.1. Password
- 1.5.2. LastPass
- 1.5.3. KeePass
- 1.5.4. StickyPassword
- 1.5.5. RoboForm

1.6. Детекторы фишинга

- 1.6.1. Обнаружение фишинга вручную
- 1.6.2. Антифишинговые средства

1.7. Шпионское программное обеспечение

- 1.7.1. Механизмы предотвращения
- 1.7.2. Антишпионские средства защиты

1.8. Трекеры

- 1.8.1. Меры по защите системы
- 1.8.2. Инструменты для борьбы с трекингом

1.9. EDR- End point Detection and Response

- 1.9.1. Поведение системы EDR
- 1.9.2. Различия между EDR и антивирусом
- 1.9.3. Будущее систем EDR

1.10. Контроль над установкой программного обеспечения

- 1.10.1. Репозитории и магазины программного обеспечения
- 1.10.2. Списки разрешенного или запрещенного программного обеспечения

1.10.3. Критерии обновлений

- 1.10.4. Права на установку программного обеспечения

Модуль 2. Сетевая безопасность (периметр)**2.1. Системы обнаружения и предотвращения угроз**

- 2.1.1. Общая нормативная база для инцидентов по безопасности
- 2.1.2. Современные системы защиты: *Глубокая защита* и SOC
- 2.1.3. Текущие сетевые архитектуры
- 2.1.4. Типы средств выявления и предотвращения инцидентов
 - 2.1.4.1. Сетевые системы
 - 2.1.4.2. Системы на базе хоста
 - 2.1.4.3. Централизованные системы
- 2.1.5. Связь и обнаружение экземпляров/хостов, контейнеров и бессерверных систем

2.2. Брандмауэр

- 2.2.1. Типы файрволов
- 2.2.2. Атаки и смягчение последствий
- 2.2.3. Лучший *брандмауэр* для Linux
 - 2.2.3.1. Uncomplicated Firewall
 - 2.2.3.2. *Nftables* и *iptables*
 - 2.2.3.3. *Firewalld*
- 2.2.4. Системы обнаружения на основе системных журналов
 - 2.2.4.1. TCP Wrappers
 - 2.2.4.2. BlockHosts и DenyHosts
 - 2.2.4.3. *Fai2ban*

2.3. Системы обнаружения и предотвращения вторжений (IDS/IPS)

- 2.3.1. Атаки на IDS/IPS
- 2.3.2. Системы IDS/IPS
 - 2.3.2.1. Snort
 - 2.3.2.2. Suricata

2.4. Брандмауэры следующего поколения (NGFW)

- 2.4.1. Различия между NGFW и традиционными брандмауэрами
- 2.4.2. Основные возможности
- 2.4.3. Коммерческие решения
- 2.4.4. Брандмауэры для *облачных* сервисов
 - 2.4.4.1. Архитектура Cloud VPC
 - 2.4.4.2. Cloud ACLs
 - 2.4.4.3. Security Group

2.5. Прокси

- 2.5.1. Виды *прокси*
- 2.5.2. Использование *прокси*. Преимущества и недостатки

2.6. Антивирусные системы

- 2.6.1. Общий контекст вредоносных программ и индикатор компрометации (IOCs)
- 2.6.2. Проблемы с антивирусным движком

2.7. Системы защиты почтовых сервисов

- 2.7.1. Антиспам
 - 2.7.1.1. Черные и белые списки
 - 2.7.1.2. Байесовская фильтрация спама
- 2.7.2. *Медиашлюз* (MGW)

2.8. SIEM

- 2.8.1. Компоненты и архитектура
- 2.8.2. Правила корреляции и примеры использования
- 2.8.3. Актуальные проблемы систем SIEM

2.9. SOAR

- 2.9.1. SOAR и SIEM: Враги или союзники
- 2.9.2. Будущее систем SOAR

2.10. Другие сетевые системы

- 2.10.1. WAF
- 2.10.2. NAC
- 2.10.3. HoneyPots и HoneyNets
- 2.10.4. CASB

Модуль 3. Безопасность смартфонов

3.1. Мир мобильных устройств

- 3.1.1. Виды мобильных платформ
- 3.1.2. iOS-устройства
- 3.1.3. Android-устройства

3.2. Управление безопасностью мобильных устройств

- 3.2.1. Проект по мобильной безопасности OWASP
 - 3.2.1.1. Топ-10 уязвимостей
- 3.2.2. Коммуникации, сети и режимы подключения

3.3. Мобильное устройство в бизнес-среде

- 3.3.1. Риски
- 3.3.2. Политики безопасности
- 3.3.3. Мониторинг устройств
- 3.3.4. Управление мобильными устройствами (MDM)

3.4. Конфиденциальность пользователей и безопасность данных

- 3.4.1. Состояние информации
- 3.4.2. Безопасное хранение данных
 - 3.4.2.1. Безопасное хранение данных на iOS
 - 3.4.2.2. Безопасное хранение данных на Android
- 3.4.3. Передовые методы разработки приложений

3.5. Уязвимости и векторы атак

- 3.5.1. Уязвимости
- 3.5.2. Векторы атак
 - 3.5.2.1. Вредоносное программное обеспечение
 - 3.5.2.2. Эксплуатация данных
 - 3.5.2.3. Манипуляции с данными

3.6. Основные угрозы

- 3.6.1. Непринужденный пользователь
- 3.6.2. Вредоносное программное обеспечение
 - 3.6.2.1. Виды вредоносного ПО
- 3.6.3. Социальная инженерия
- 3.6.4. Утечка данных
- 3.6.5. Кража информации
- 3.6.6. Незащищенные сети Wi-Fi
- 3.6.7. Устаревшее программное обеспечение

- 3.6.8. Вредоносные приложения
- 3.6.9. Ненадежные пароли
- 3.6.10. Слабые или отсутствующие настройки безопасности
- 3.6.11. Физический доступ к информации
- 3.6.12. Потеря или кража устройства
- 3.6.13. Подмена личности (интеграция)
- 3.6.14. Слабая или неработающая криптография
- 3.6.15. Отказ в обслуживании (DoS)

3.7. Основные атаки

- 3.7.1. Фишинговые атаки
- 3.7.2. Атаки, связанные со способами коммуникации
- 3.7.3. Смишинговые атаки
- 3.7.4. Атаки криптоджекинга
- 3.7.5. Man in the Middle

3.8. Хакинг

- 3.8.1. Rooting и Jailbreaking
- 3.8.2. Анатомия мобильной атаки
 - 3.8.2.1. Распространение угрозы
 - 3.8.2.2. Установка вредоносных программ на устройство
 - 3.8.2.3. Настойчивость
 - 3.8.2.4. Выполнение полезной нагрузки и извлечение информации
- 3.8.3. Хакинг устройств iOS: механизмы и средства
- 3.8.4. Хакинг устройств Android: механизмы и инструменты

3.9. Тестирование на проникновение

- 3.9.1. iOS PenTesting
- 3.9.2. Android PenTesting
- 3.9.3. Инструменты

3.10. Безопасность и защита

- 3.10.1. Настройки безопасности
 - 3.10.1.1. На устройствах iOS
 - 3.10.1.2. Android-устройства
- 3.10.2. Меры по обеспечению безопасности
- 3.10.3. Защитные средства

Модуль 4. Безопасность в IoT**4.1. Приборы**

- 4.1.1. Виды устройств
- 4.1.2. Стандартизированные архитектуры
 - 4.1.2.1. ONEM2M
 - 4.1.2.2. IoTWF
- 4.1.3. Протоколы применения
- 4.1.4. Технологии подключения

4.2. Устройства IoT. Области применения

- 4.2.1. *Умный дом*
- 4.2.2. *Умный город*
- 4.2.3. Транспорт
- 4.2.4. *Носимые приборы*
- 4.2.5. Сектор здравоохранения
- 4.2.6. IIoT

4.3. Протоколы коммуникации

- 4.3.1. MQTT
- 4.3.2. LWM2M
- 4.3.3. OMA-DM
- 4.3.4. TR-069

4.4. Умный дом

- 4.4.1. Бытовая автоматизация
- 4.4.2. Сети
- 4.4.3. Бытовая техника
- 4.4.4. Наблюдение и охрана

4.5. Умный город

- 4.5.1. Освещение
- 4.5.2. Метеорология
- 4.5.3. Безопасность

4.6. Транспорт

- 4.6.1. Локализация
- 4.6.2. Осуществление платежей и получение услуг
- 4.6.3. Подключение

4.7. Носимые приборы

- 4.7.1. Умная одежда
- 4.7.2. Умные ювелирные изделия
- 4.7.3. Умные часы

4.8. Сектор здравоохранения

- 4.8.1. Контроль физической нагрузки/частоты сердечных сокращений
- 4.8.2. Наблюдение за пациентами и пожилыми людьми
- 4.8.3. Имплантируемые
- 4.8.4. Хирургические роботы

4.9. Подключение

- 4.9.1. Wi-Fi/сетевой шлюз
- 4.9.2. Bluetooth
- 4.9.3. Встроенные возможности подключения

4.10. Секьюритизация

- 4.10.1. Выделенные сети
- 4.10.2. Менеджер паролей
- 4.10.3. Использование зашифрованных протоколов
- 4.10.4. Советы по применению

06

Методология

Данная учебная программа предлагает особый способ обучения. Наша методология разработана в режиме циклического обучения: **Relearning**.

Данная система обучения используется, например, в самых престижных медицинских школах мира и признана одной из самых эффективных ведущими изданиями, такими как **Журнал медицины Новой Англии**.





“

Откройте для себя методику *Relearning*, которая отвергает традиционное линейное обучение, чтобы показать вам циклические системы обучения: способ, который доказал свою огромную эффективность, особенно в предметах, требующих запоминания”

Бизнес-школа ТЕСН использует метод кейсов для контекстуализации всего содержания

Наша программа предлагает революционный метод развития навыков и знаний. Наша цель - укрепить компетенции в условиях меняющейся среды, конкуренции и высоких требований.

“

С ТЕСН вы сможете познакомиться со способом обучения, который опровергает основы традиционных методов образования в университетах по всему миру”



Эта программа подготовит вас к решению бизнес-задач в условиях неопределенности и достижению успеха в бизнесе.



Наша программа подготовит вас к решению новых задач в условиях неопределенности и достижению успеха в карьере.

Инновационный и отличный от других метод обучения

Эта программа TECH - интенсивная программа обучения, созданная с нуля для того, чтобы предложить менеджерам задачи и бизнес-решения на самом высоком уровне, на международной арене. Благодаря этой методологии ускоряется личностный и профессиональный рост, делая решающий шаг на пути к успеху.

Метод кейсов, составляющий основу данного содержания, обеспечивает следование самым современным экономическим, социальным и деловым реалиям.

“*В ходе совместной деятельности и рассмотрения реальных кейсов студент научится разрешать сложные ситуации в реальной бизнес-среде*”

Метод кейсов является наиболее широко используемой системой обучения в лучших бизнес-школах мира на протяжении всего времени их существования. Разработанный в 1912 году для того, чтобы студенты-юристы могли изучать право не только на основе теоретического содержания, метод кейсов заключается в том, что им представляются реальные сложные ситуации для принятия обоснованных решений и ценностных суждений о том, как их разрешить. В 1924 году он был установлен в качестве стандартного метода обучения в Гарвардском университете.

Что должен делать профессионал в определенной ситуации? Именно с этим вопросом мы сталкиваемся при использовании метода кейсов - метода обучения, ориентированного на действие. На протяжении всей программы студенты будут сталкиваться с многочисленными реальными случаями из жизни. Им придется интегрировать все свои знания, исследовать, аргументировать и защищать свои идеи и решения.

Методология *Relearning*

TECH эффективно объединяет метод кейсов с системой 100% онлайн-обучения, основанной на повторении, которая сочетает различные дидактические элементы в каждом уроке.

Мы улучшаем метод кейсов с помощью лучшего метода 100% онлайн-обучения: *Relearning*.

Наша онлайн-система позволит вам организовать свое время и темп обучения, адаптируя его к вашему графику. Вы сможете получить доступ к содержанию с любого стационарного или мобильного устройства с выходом в интернет.

В TECH вы будете учиться по передовой методике, разработанной для подготовки руководителей будущего. Этот метод, играющий ведущую роль в мировой педагогике, называется *Relearning*.

Наша Бизнес-школа - единственный вуз, имеющий лицензию на использование этого успешного метода. В 2019 году нам удалось повысить общий уровень удовлетворенности наших студентов (качество преподавания, качество материалов, структура курса, цели...) по отношению к показателям лучшего онлайн-университета.



В нашей программе обучение не является линейным процессом, а происходит по спирали (мы учимся, разучиваемся, забываем и заново учимся). Поэтому мы дополняем каждый из этих элементов по концентрическому принципу. Благодаря этой методике более 650 000 выпускников университетов добились беспрецедентного успеха в таких разных областях, как биохимия, генетика, хирургия, международное право, управленческие навыки, спортивная наука, философия, право, инженерное дело, журналистика, история, финансовые рынки и инструменты. Наша методология преподавания разработана в среде с высокими требованиями к уровню подготовки, с университетским контингентом студентов с высоким социально-экономическим уровнем и средним возрастом 43,5 года.

Методика Relearning позволит вам учиться с меньшими усилиями и большей эффективностью, все больше вовлекая вас в процесс обучения, развивая критическое мышление, отстаивая аргументы и противопоставляя мнения, что непосредственно приведет к успеху.

Согласно последним научным данным в области нейронауки, мы не только знаем, как организовать информацию, идеи, образы и воспоминания, но и знаем, что место и контекст, в котором мы что-то узнали, имеют фундаментальное значение для нашей способности запомнить это и сохранить в гиппокампе, чтобы удержать в долгосрочной памяти.

Таким образом, в рамках так называемого нейрокогнитивного контекстно-зависимого электронного обучения, различные элементы нашей программы связаны с контекстом, в котором участник развивает свою профессиональную практику.



В рамках этой программы вы получаете доступ к лучшим учебным материалам, подготовленным специально для вас:



Учебный материал

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

Затем вся информация переводится в аудиовизуальный формат, создавая дистанционный рабочий метод TECH. Все это осуществляется с применением новейших технологий, обеспечивающих высокое качество каждого из представленных материалов.



Мастер-классы

Существуют научные данные о пользе экспертного наблюдения третьей стороны.

Так называемый метод обучения у эксперта укрепляет знания и память, а также формирует уверенность в наших будущих сложных решениях.



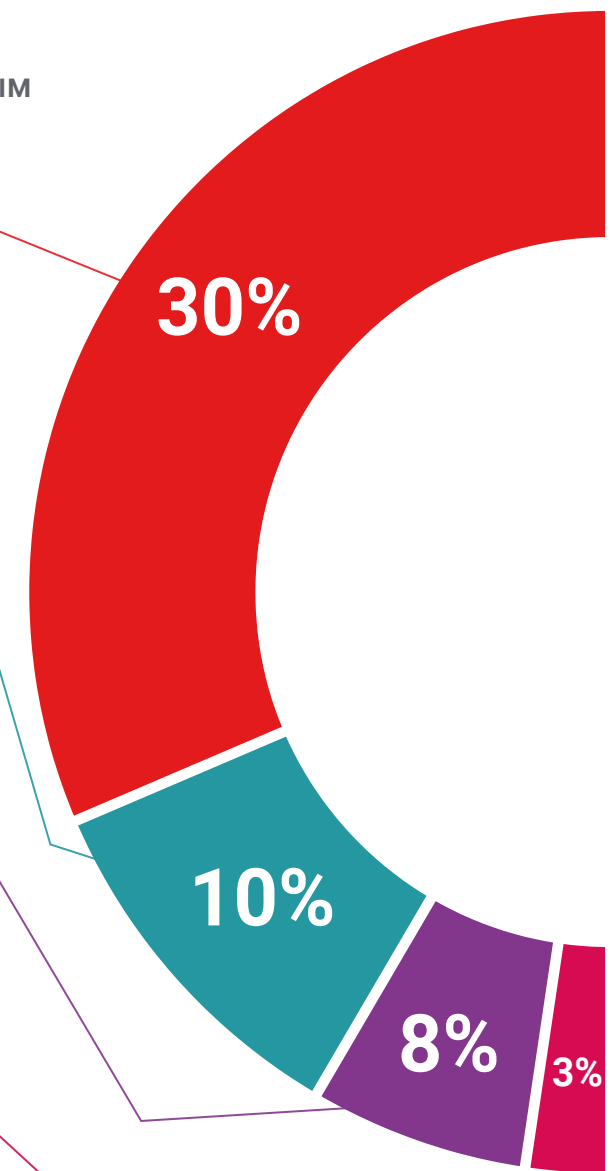
Практика управленческих навыков

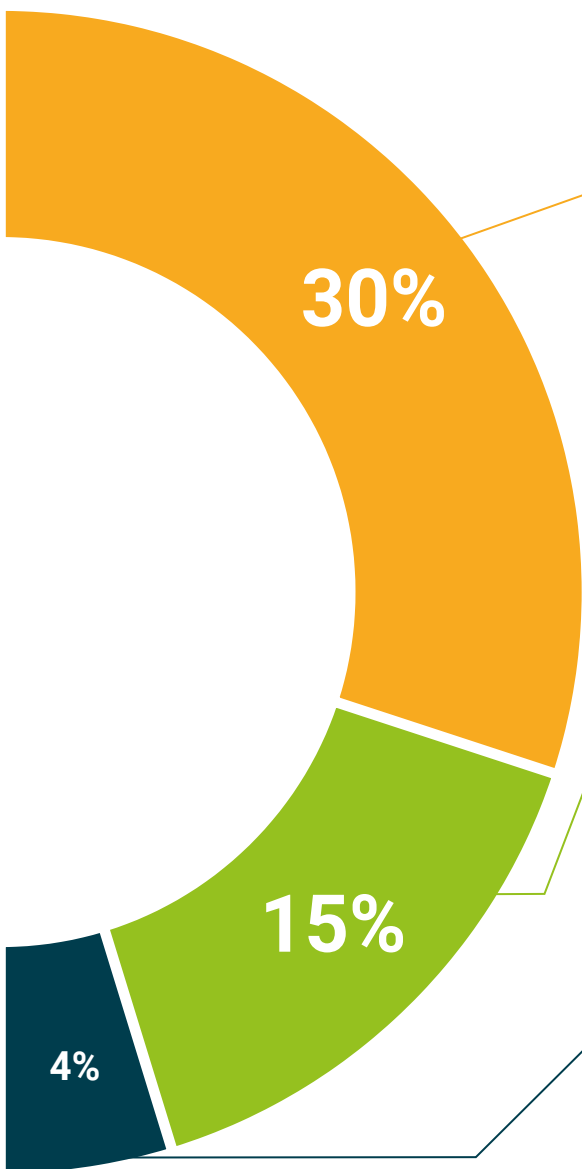
Студенты будут осуществлять деятельность по развитию конкретных управленческих компетенций в каждой предметной области. Практика и динамика приобретения и развития навыков и способностей, необходимых топ-менеджеру в условиях глобализации, в которой мы живем.



Дополнительная литература

Новейшие статьи, консенсусные документы и международные руководства включены в список литературы курса. В виртуальной библиотеке TECH студент будет иметь доступ ко всем материалам, необходимым для завершения обучения.





Метод кейсов

Метод дополнится подборкой лучших кейсов, выбранных специально для этой квалификации. Кейсы представляются, анализируются и преподаются лучшими специалистами в области высшего менеджмента на международной арене.



Интерактивные конспекты

Мы представляем содержание в привлекательной и динамичной мультимедийной форме, которая включает аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

Эта уникальная обучающая система для представления мультимедийного содержания была отмечена компанией Microsoft как "Европейская история успеха".



Тестирование и повторное тестирование

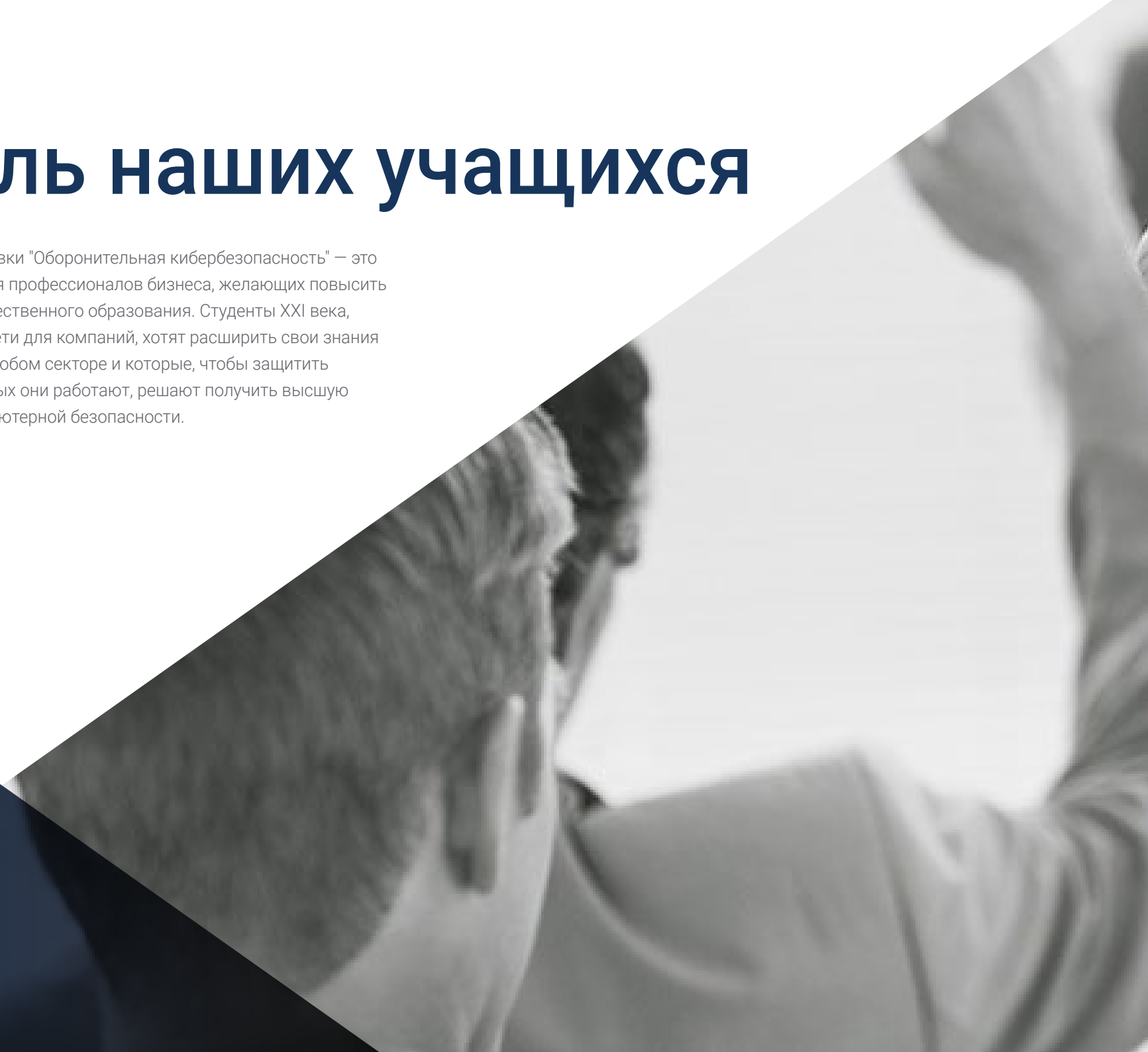
На протяжении всей программы мы периодически оцениваем и переоцениваем ваши знания с помощью оценочных и самооценочных упражнений: так вы сможете убедиться, что достигаете поставленных целей.



07

Профиль наших учащихся

Курс профессиональной подготовки "Оборонительная кибербезопасность" — это программа, предназначенная для профессионалов бизнеса, желающих повысить свою квалификацию за счет качественного образования. Студенты XXI века, которые, осознавая опасность сети для компаний, хотят расширить свои знания в соответствующих областях в любом секторе и которые, чтобы защитить свой бизнес и компании, в которых они работают, решают получить высшую специализацию в области компьютерной безопасности.



“

Студенты этой программы — опытные профессионалы, желающие расширить свои знания в сложной области кибербезопасности”

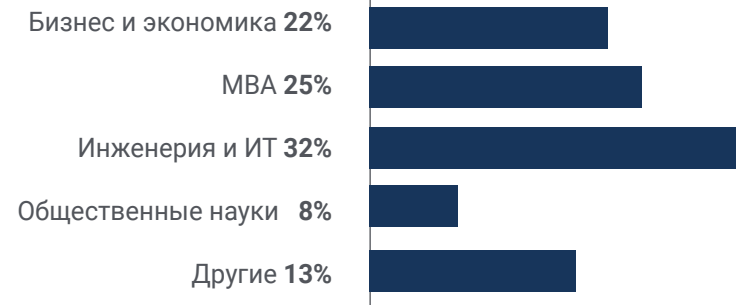
Средний возраст

В возрасте от **35** до **45** лет

Годы практики



Образование



Академический профиль



Географическое распределение



Хайме Диас

Директор по доходам

"Прохождение этой программы позволило мне повысить уровень подготовки в области оборонительной кибербезопасности — актуального аспекта ИТ-безопасности, который очень полезен для моего профессионального развития, поскольку в эпоху цифровых технологий умение предотвращать цифровые атаки является дополнительным преимуществом для любого специалиста"

08

Руководство курса

Преподаватели данного Курса профессиональной подготовки в области оборонительной кибербезопасности — профессионалы с большим опытом работы в данной сфере, как на профессиональном, так на образовательном уровне. Их специализация в этой области позволяет им обладать необходимой квалификацией, чтобы предложить студентам полное и качественное изучение предметов, которые будут полезны в их повседневной работе в мире бизнеса. Это, безусловно, люди, которые уверены в том, что повышение квалификации — это способ развития их профессии и повышения конкурентоспособности их бизнеса.



“

Опытные преподаватели помогут
вам специализироваться
в области кибербезопасности”

Приглашенный руководитель международного уровня

Доктор Фредерик Лемье признан во всем мире как инновационный эксперт и вдохновляющий лидер в области разведки, национальной безопасности, внутренней безопасности, кибербезопасности и инновационных технологий. Его постоянная преданность делу и значительный вклад в исследования и образование делают его ключевой фигурой в продвижении безопасности и понимании современных развивающихся технологий. За свою профессиональную карьеру он разработал концепцию и возглавил передовые академические программы в нескольких известных учебных заведениях, таких как Монреальский университет, Университет Джорджа Вашингтона и Джорджтаунский университет.

За свою обширную биографию он опубликовал множество актуальных книг, связанных с криминальной разведкой, полицейской деятельностью, киберугрозами и международной безопасностью. Он также внес значительный вклад в область кибербезопасности, опубликовав множество статей в научных журналах, посвященных борьбе с преступностью во время крупных катастроф, борьбе с терроризмом, сотрудничеству спецслужб и полиции. Кроме того, он выступал в качестве эксперта и основного докладчика на различных национальных и международных конференциях, зарекомендовав себя как ведущий ученый и практик.

Д-р Лемье занимал должности редактора и эксперта в различных научных, частных и правительственных организациях, что свидетельствует о его влиянии и стремлении к совершенству в своей области знаний. Благодаря своей престижной академической карьере он стал профессором-практиком и директором факультета по программам MPS в области прикладной разведки, управления рисками кибербезопасности, управления технологиями и управления информационными технологиями в Джорджтаунском университете.



Д-р Лемье, Фредерик

- Руководитель магистратуры по управлению рисками кибербезопасности в Джорджтауне, Вашингтон, США
- Руководитель магистратуры по управлению технологиями в Джорджтаунском университете
- Руководитель магистратуры по прикладной разведке в Джорджтаунском университете
- Преподаватель стажировок в Джорджтаунском университете
- Степень доктора криминологии Школы криминологии Монреальского университета
- Степень бакалавра социологии и степень бакалавра психологии в Университете Лавалья
- Член: New Program Roundtable Committee, Джорджтаунский университет

“

Благодаря TECH вы сможете учиться у лучших мировых профессионалов”

Руководство



Г-жа Фернандес Сапена, Соня

- Преподаватель по компьютерной безопасности и этическому взлому в Национальном справочном центре информационных технологий и телекоммуникаций Гетафе в Мадриде
- Сертифицированный инструктор E-Council
- Инструктор по проведению следующих сертификаций: EXIN Ethical Hacking Foundation и EXIN Cyber & IT Security Foundation. Мадрид
- Аккредитованный тренер-эксперт CAM в области следующих профессиональных сертификаций: Компьютерная безопасность (IFCT0190), Управление сетями передачи голоса и данных (IFCM0310), Управление ведомственными сетями (IFCT0410), Управление сигнализацией в телекоммуникационных сетях (IFCM0410), Оператор сетей передачи голоса и данных (IFCM0110) и Управление интернет-услугами (IFCT0509)
- Внешний сотрудник CSO/SSA (*главный специалист по безопасности/старший архитектор безопасности*) в Университете Балеарских островов
- Степень бакалавра в области компьютерной инженерии в Университете Алькала-де-Энарес в Мадриде
- Степень магистра в DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Technologies. E-Council

Преподаватели

Г-н Хименес Рамос, Альваро

- ♦ Аналитик по кибербезопасности
- ♦ Старший аналитик по вопросам безопасности в компании The Workshop
- ♦ Аналитик по кибербезопасности L1 в Axians
- ♦ Аналитик по кибербезопасности L2 в Axians
- ♦ Аналитик по кибербезопасности в SACYR S.A
- ♦ Степень инженера в области телематики Политехнического университета Мадрида
- ♦ Степень магистра в области кибербезопасности и этического взлома в CICE
- ♦ Продвинутый курс по кибербезопасности от Deusto Formación

Г-н Перальта Алонсо, Йон

- ♦ Старший консультант по защите данных и кибербезопасности в Altia
- ♦ Юрист / юрисконсульт в Arriaga Asociados Asesoramiento Jurídico y Económico S.L
- ♦ Юрисконсульт / стажер в профессиональной юридической фирме: Оскар Падур
- ♦ Степень бакалавра в области права в Государственном университете Страны Басков
- ♦ Степень магистра в области защиты данных Делегат инновационной школы EIS
- ♦ Степень магистра права Государственного университета Страны Басков
- ♦ Степень магистра в области гражданской судебной практики Международного университета Изабель I Кастильской
- ♦ Преподаватель магистратуры по защите персональных данных, кибербезопасности и праву ИКТ

Г-жа Маркос Сбарбаро, Виктория Алисия

- ♦ Разработчик мобильных приложений Native Android в B60. Великобритания
- ♦ Программист-аналитик для управления, координации и документирования виртуальной среды охранной сигнализации
- ♦ Программист-аналитик Java-приложений для банкоматов
- ♦ Специалист по разработке *программного обеспечения* для разработки приложений для проверки подлинности подписей и управления документами
- ♦ Системный техник по миграции оборудования и управлению, обслуживанию и обучению мобильных устройств PDA
- ♦ Технический инженер в области проектирования компьютерных систем Открытого университета Каталонии
- ♦ Степень магистра в области компьютерной безопасности и этического взлома
Официальная сертификация EC- Council и CompTIA в Профессиональной школе новых технологий CICE

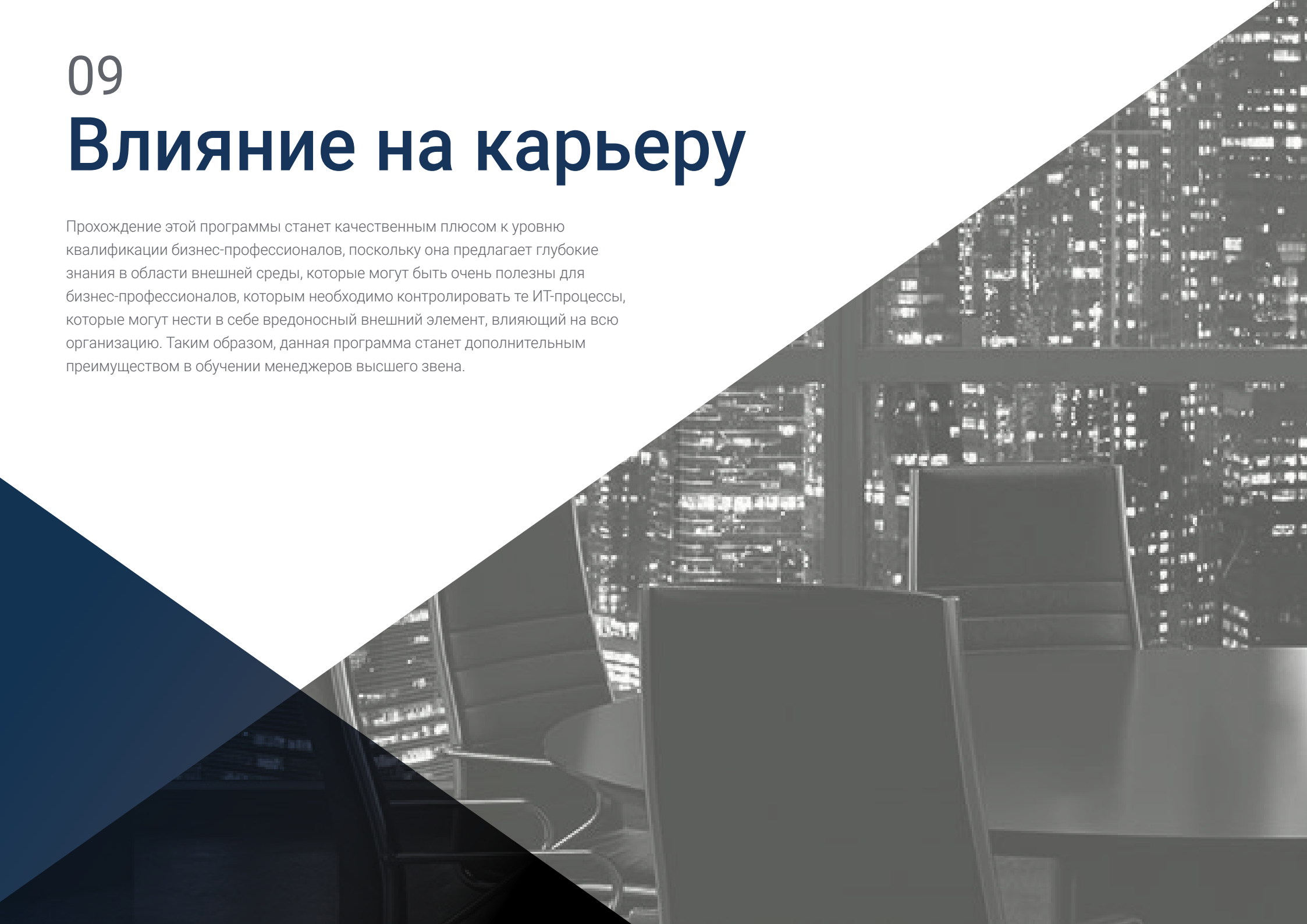
Г-н Катала Барба, Хосе Франсиско

- ♦ Специалист по электронике, Эксперт по кибербезопасности
- ♦ Разработчик приложений для мобильных устройств
- ♦ Специалист по электронике в промежуточном командовании министерства обороны Испании
- ♦ Специалист по электронике на заводе Ford Sita в Валенсии, Испания

09

Влияние на карьеру

Прохождение этой программы станет качественным плюсом к уровню квалификации бизнес-профессионалов, поскольку она предлагает глубокие знания в области внешней среды, которые могут быть очень полезны для бизнес-профессионалов, которым необходимо контролировать те ИТ-процессы, которые могут нести в себе вредоносный внешний элемент, влияющий на всю организацию. Таким образом, данная программа станет дополнительным преимуществом в обучении менеджеров высшего звена.



“

*Программа высокого уровня,
которая позволит вам кардинально
изменить свою профессию”*

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

Данная Курс профессиональной подготовки в области оборонительной кибербезопасности TECH Global University — это интенсивная и очень ценная программа, направленная на улучшение профессиональных навыков студентов в высококонкурентной сфере. Это, несомненно, уникальная возможность совершенствоваться не только в профессиональном плане, но и в личностном развитии, поскольку обучение требует усилий и самоотдачи.

Студенты, которые хотят самосовершенствоваться, внести позитивные изменения на профессиональном уровне и общаться с лучшими, найдут свое место в TECH.

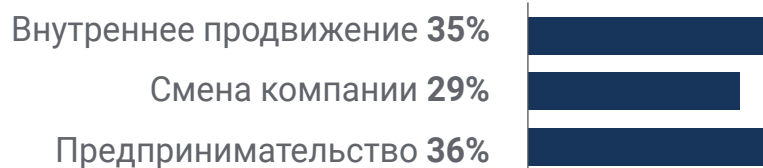
Прохождение этой программы позволит вам лучше контролировать безопасность цифровых процессов.

Уникальная программа для личного и профессионального совершенствования.

Время перемен



Что изменится



Повышение заработной платы

Прохождение этой программы означает для наших студентов повышение заработной платы более чем на **25,22%**



10

Преимущества для вашей компании

Курс профессиональной подготовки в области оборонительной кибербезопасности способствует повышению таланта организации до его максимального потенциала через специализацию лидеров высокого уровня. Таким образом, профессионалы бизнеса смогут привнести в свою компанию дополнительное качество, обладая необходимыми навыками для самостоятельного контроля процессов кибербезопасности. Программа, которая адаптируется под вас, позволяя вам получить необходимые навыки и в будущем применять их в своей повседневной практике, добиваясь больших преимуществ для своей компании.



“

Обязательная программа для профессионалов бизнеса, которые хотят отслеживать и управлять потенциальными проблемами кибербезопасности”

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.

11

Квалификация

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



“

*Успешно пройдите эту программу
и получите университетский диплом
без хлопот, связанных с поездками
и оформлением документов”*

Данный **Курс профессиональной подготовки в области оборонительной 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: **Курса профессиональной подготовки в области оборонительной кибербезопасности**

Формат: **онлайн**

Продолжительность: **6 месяцев**



Будущее

Здоровье Доверие Люди

Образование Информация Тьюторы

Гарантия Аккредитация Преподавание

Институты Технология Обучение

Сообщество Обязательство

Персональное внимание Инновации

Знания Настоящее Качество

Веб обучение кибербезопасность

Развитие Институты

Виртуальный класс Языки



Курс профессиональной подготовки

Оборонительная
кибербезопасность

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

Курс профессиональной подготовки

Оборонительная кибербезопасность

