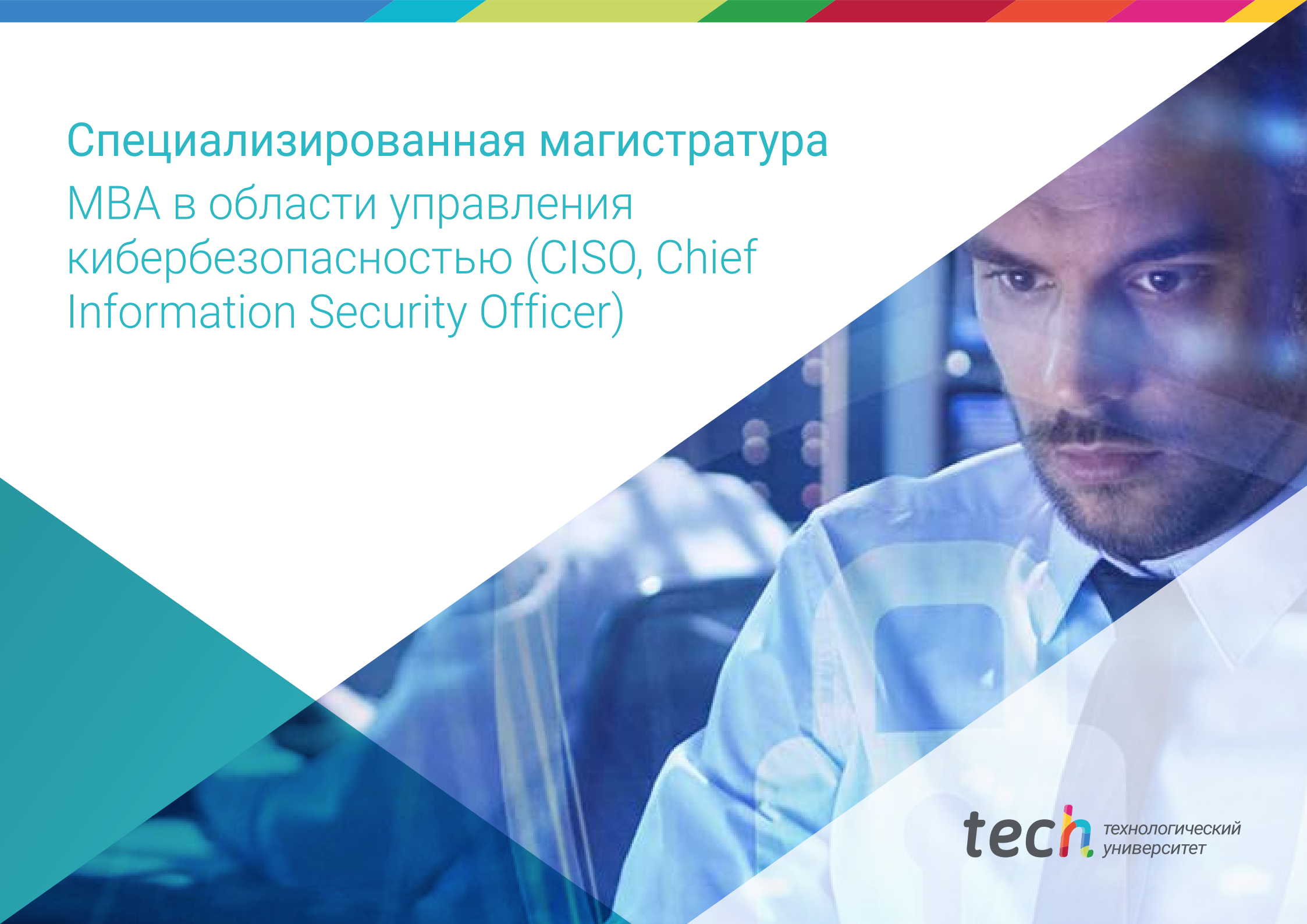
Специализированная магистратура

MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)



tech технологический университет

tech технологический университет

Специализированная магистратура

MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)

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

Веб-доступ: **www.techtitute.com/ru/information-technology/professional-master-degree/master-mba-cybersecurity-directorate-ciso-chief-information-security-officer**

Оглавление

01

Презентация

По мере развития технологий растет и количество угроз, совершенствуя свои методы атаки. Другими словами, возможности и способы достижения киберпреступниками своих целей растут. Именно в этом контексте TECH представляет программу, с помощью которой профессионалы смогут войти в курс дела и получить исчерпывающие знания по защите и обеспечению безопасности различных цифровых сред. Все это — с помощью революционной методологии relearning; в удобном и полностью онлайн-формате, который позволит студенту приобретать навыки и умения без заранее установленных сроков. Таким образом, по прохождении этой программы специалист получит необходимые навыки и компетенции для эффективной работы в качестве главного специалиста по информационной безопасности — руководящей должности с большим престижем, а также с высокими перспективами роста и расширения.

По мере развития технологий и возможностей подключения растет число и форма потенциальных угроз. Вот почему для будущих главных специалистов по информационной безопасности крайне важно обновлять свои знания, чтобы предлагать решения, более адаптированные к специфике компании"

Ни для кого не секрет, что мы живем в эпоху информации и коммуникаций, поскольку все мы подключены к сети как дома, так и в корпоративной среде. Таким образом, мы имеем доступ к множеству информации одним щелчком мыши, одним поиском в любой из имеющихся в нашем распоряжении систем, будь то смартфон, персональный или рабочий компьютер.

По мере развития технологий для рядовых граждан и сотрудников, растут угрозы и методы атак. Чем больше появляется новых функциональных возможностей и чем больше мы общаемся, тем больше увеличивается зона атак. Учитывая этот тревожный контекст, TECH представляет данную Специализированную программу MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer), которая была разработана командой с различными профессиональными специализациями в разных секторах, сочетающей международный профессиональный опыт в частной сфере в области исследований, разработок и технологических инноваций, а также обширный опыт преподавания.

Специализированная магистратура также предоставляет студентам отличные и полноценные дополнительные занятия, которые проводит специалист в области разведки, кибербезопасности и инновационных технологий, имеющий международный авторитет. Эти инновационные материалы будут доступны в виде 10 эксклюзивных *мастер-классов*, которые позволят студентам обновить свои знания в области кибербезопасности и управлять отделами, отвечающими за эти задачи в самых важных компаниях технологического сектора.

Программа включает в себя различные основные предметы в области кибербезопасности, тщательно отобранные, чтобы строго охватить широкий спектр технологий, применимых в различных сферах деятельности. Кроме того, программа охватывает и другие предметы, которых обычно мало в академическом каталоге других учебных заведений и которые глубоко обогатят учебный план специалиста. Таким образом, благодаря сквозным знаниям, предлагаемым TECH в рамках этой программы, студент приобретет навыки работы в качестве руководителя в области кибербезопасности (Chief Information Security Officer), тем самым увеличивая перспективы своего личного и профессионального роста.

Данная программа **MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных экспертами в области кибербезопасности
- Наглядное, схематичное и исключительно практическое содержание курса предоставляет научную и практическую информацию по тем дисциплинам, которые необходимы для осуществления профессиональной деятельности
- Практические упражнения для самооценки, контроля и улучшения успеваемости
- Особое внимание уделяется инновационным методологиям
- Теоретические занятия, вопросы эксперту, дискуссионные форумы по спорным темам и самостоятельная работа
- Учебные материалы курса доступны с любого стационарного или мобильного устройства, имеющего подключение к Интернету

Обучайтесь вместе с лучшими профессионалами! Воспользуйтесь преимуществами 10 мастер-классов, которые проводит всемирно признанный преподаватель"

Выделитесь в бурно развивающемся секторе и станьте экспертом в области кибербезопасности с помощью этой программы MBA от TECH. Программа является самой полноценной из представленных на образовательном рынке"

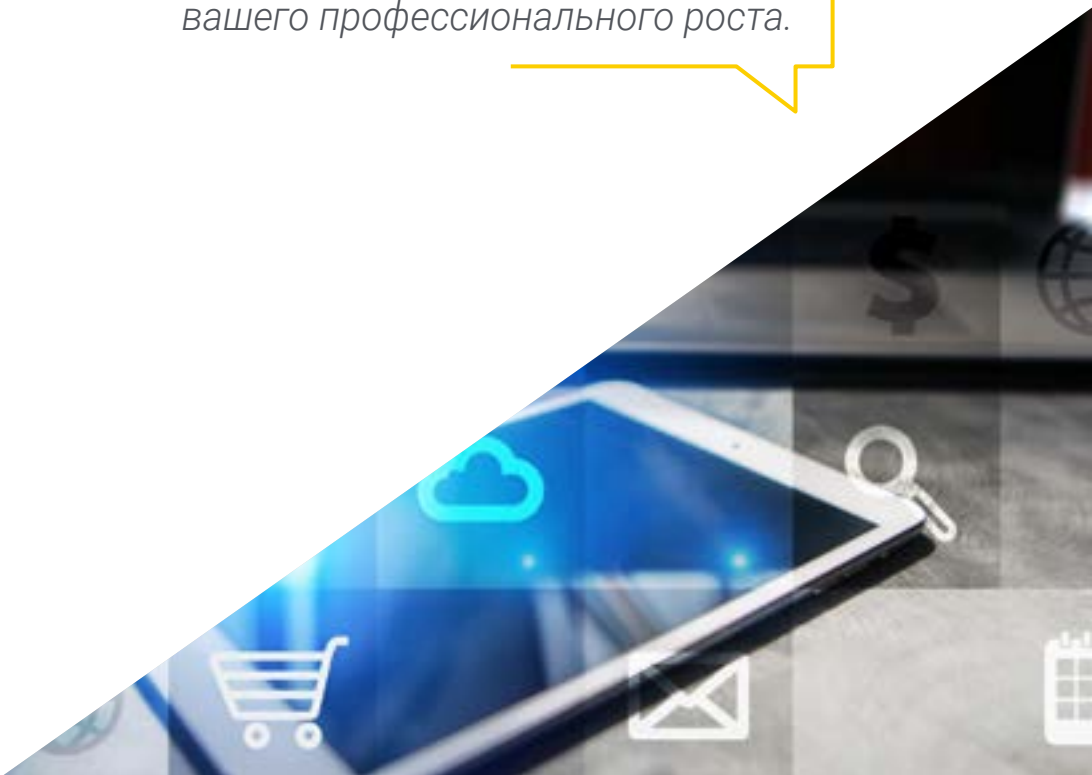
Средства, с помощью которых люди обмениваются информацией, быстро развиваются. Это требует новых методы киберзащиты для профессионалов.

Дистанционная программа 100% онлайн с исключительно практическим подходом, которая заложит основу для вашего профессионального роста.

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

Мультимедийное содержание программы, разработанное с использованием новейших образовательных технологий, позволит специалисту проходить обучение с учетом контекста и ситуации, т.е. в симулированной среде, обеспечивающей иммерсивный учебный процесс, запрограммированный на обучение в реальных ситуациях.

Структура этой программы основана на проблемно-ориентированном обучении, с помощью которого специалист должен попытаться разрешать различные ситуации из профессиональной практики, возникающие в течение учебного курса. В этом специалистам поможет инновационная интерактивная видеосистема, созданная признанными экспертами.



02

Цели

Полностью осознавая актуальность кибербезопасности для компаний и частных лиц, TECH разработал эту программу MBA, которая направлена на развитие и обновление знаний профессионалов в области обнаружения, защиты и предотвращения киберпреступлений. Таким образом, будущий выпускник станет ключевой фигурой в обеспечении сохранности данных и информации, минимизируя возможности злоумышленников воспользоваться существующими брешами в системе безопасности. Профессиональная квалификация, которую в TECH специалист сможет получить всего за 12 месяцев.

Это уникальная возможность воплотить свои мечты и цели в жизнь и стать экспертом в области управления кибербезопасностью"

Общие цели

- Проанализировать роль аналитика по кибербезопасности
- Углубить понимание социальной инженерии и ее методов
- Изучить методологии OSINT, HUMINT, OWASP, PTEC. OSSTM, OWISAM
- Проводить анализ рисков и понимать метрики рисков
- Определять, как правильно использовать анонимизацию и такие сети, как TOR, I2P и Freenet
- Формировать специализированные знания для проведения аудита безопасности
- Разрабатывать соответствующие политики использования
- Рассматривать системы обнаружения и предотвращения наиболее важных угроз
- Оценивать новые системы обнаружения угроз и их эволюцию по сравнению с более традиционными методами решений
- Анализировать основные современные мобильные платформы, их характеристики и использование
- Выявлять, анализировать и оценивать риски безопасности частей проекта IoT
- Оценивать полученную информацию и разработать механизмы предотвращения и взлома
- Уметь применять обратную инженерию в среде кибербезопасности
- Определять тесты, которые должны быть проведены на разработанном программном обеспечении
- Собирать все имеющиеся доказательства и данные для проведения криминалистической экспертизы
- Надлежащим образом представлять отчет о судебной экспертизе
- Анализировать текущее и будущее состояние ИТ-безопасности
- Изучить риски, связанные с новыми и развивающимися технологиями
- Компилировать различные технологии, связанные с ИТ-безопасностью

Конкретные цели

Модуль 1. Кибербезопасность и кибербезопасность

- Разрабатывать методологии, используемые в сфере кибербезопасности
- Изучить цикл разведки и установить его применение в кибербезопасности
- Определить роль разведывательного аналитика и препятствия на пути эвакуации
- Проанализировать методологии OSINT, OWISAM, OSSTM, PTES, OWASP
- Установить наиболее распространенные средства для производства разведданных
- Проводить анализ рисков и понимать используемые метрики
- Конкретизировать опции анонимизации и использования таких сетей, как TOR, I2P, FreeNet
- Подробно описать действующие нормативные акты по кибербезопасности

Модуль 2. Безопасность хоста

- Определить политику резервного *копирования* личных и рабочих данных
- Оценивать различные инструменты для решения конкретных проблем безопасности
- Устанавливать механизмы для актуализации системы
- Проводить сканирование оборудования на наличие вторжений
- Определять правила доступа к системе
- Проверять и классифицировать электронную почту для предотвращения мошенничества
- Генерировать списки разрешенного программного обеспечения

Модуль 3. Сетевая безопасность (периметр)

- Проанализировать текущие сетевые архитектуры для определения периметра защиты
- Разработать специальные конфигурации брандмауэра и Linux для защиты от наиболее распространенных атак
- Компилировать наиболее часто используемые решения, такие как Snort и Suricata, а также их конфигурацию.
- Изучить различные дополнительные уровни, предоставляемые *брандмауэрами* нового поколения и сетевыми функциями в облачных средах
- Определять инструменты для защиты сети и демонстрировать, почему они являются основополагающими для многоуровневой защиты

Модуль 4. Безопасность смартфонов

- Изучить различные векторы атак, чтобы не стать "легкой мишенью"
- Определять основные атаки и типы вредоносных программ, которым подвергаются пользователи мобильных устройств
- Проанализировать новейшие устройства для создания более безопасной конфигурации
- Указывать основные шаги для проведения теста на проникновение на платформах iOS и Android
- Расширять знания о различных инструментах защиты и безопасности
- Устанавливать передовые методы программирования для мобильных устройств

Модуль 5. Безопасность в IoT
- Анализировать основные архитектуры IoT
- Рассмотреть технологии подключения
- Разрабатывать основные протоколы внедрения
- Определять различные типы существующих устройств
- Оценивать уровни риска и существующие уязвимости
- Разработать политику безопасного использования
- Устанавливать соответствующие условия использования этих устройств

Модуль 6. Этичный хакинг
- Изучить методы IOSINT
- Собирать информацию, доступную в общественных СМИ
- Сканировать сети для получения информации об активном режиме
- Разрабатывать испытательные лаборатории
- Проанализировать инструменты для проведения *пентестов*
- Составлять каталоги и оценивать различные уязвимости систем
- Изучить различные методологий *хакинга*

Модуль 7. Реверс-инжиниринг
- Проанализировать этапы работы компилятора
- Проводить экспертизу архитектуры процессоров x86 и архитектуры процессоров ARM
- Проводить различные виды анализа
- Применять *технологии"песочницы"* в различных средах
- Разрабатывать различные методы анализа *вредоносных* программ
- Создавать инструменты, ориентированные на анализ *вредоносного* ПО

Модуль 8. Безопасная разработка
- Устанавливать требования, необходимые для корректной работы приложения в безопасном режиме
- Изучать *лог-файлы* для понимания сообщений об ошибках
- Проанализировать различные события и решить, что показать пользователю, а что оставить в *лог-файлах*
- Создавать санированный, легко проверяемый, качественный код
- Уметь оценивать необходимую документацию для каждой фазы разработки
- Определять поведение сервера для оптимизации системы
- Разрабатывать модульный, многократно используемый и сопровождаемый код.

Модуль 9. Судебная экспертиза
- Уметь определять различные элементы, раскрывающие правонарушение
- Получить конкретные знания для получения данных с различных носителей до их потери
- Уметь восстанавливать преднамеренно удаленные данные
- Проанализировать системные журналы и записи
- Определить способ дублирования данных, чтобы не изменять оригиналы
- Обосновывать доказательства, чтобы они имели последовательность
- Уметь создавать надежные и безукоризненные отчеты
- Предоставлять выводы последовательным образом
- Определить, как защитить отчет в компетентном органе
- Составлять стратегии для безопасной дистанционной работы

Модуль 10. Текущие и будущие проблемы в области кибербезопасности

- Изучить использование криптовалют, влияния на экономику и безопасность
- Проанализировать положение пользователей и степень их цифровой неграмотности
- Определить сферу использования *блокчейна*
- Представлять альтернативы IPv4 в сетевой адресации
- Разработать стратегии по обучению населения правильному использованию технологий
- Получить специальные знания для решения новых проблем
- Составлять стратегии для безопасной дистанционной работы

Модуль 11. Лидерство, этика и корпоративная социальная ответственность

- Анализировать влияние глобализации на управление и корпоративное управление
- Оценивать важность эффективного лидерства в управлении и успехе компаний
- Определять стратегии кросс-культурного менеджмента и их актуальность в различных бизнес-средах
- Развивать лидерские навыки и понимать современные проблемы, стоящие перед лидерами
- Определять принципы и практику деловой этики и их применение в принятии корпоративных решений
- Разрабатывать стратегии внедрения и совершенствования устойчивого развития и социальной ответственности в компаниях

Модуль 12. Управление персоналом и талантами

- Определять взаимосвязь между стратегическим направлением и управлением человеческими ресурсами
- Развивать компетенции, необходимые для эффективного управления человеческими ресурсами на основе компетенций
- Изучить методологии оценки и управления эффективностью работы
- Интегрировать инновации в управлении талантами и их влияние на удержание и лояльность персонала
- Разработать стратегии мотивации и развития высокоэффективных команд
- Предложить эффективные решения для управления изменениями и разрешения конфликтов в организациях

Модуль 13. Финансово-экономическое управление

- Анализировать макроэкономическую среду и ее влияние на национальную и международную финансовую систему
- Определять информационные системы и бизнес-аналитику для принятия финансовых решений
- Различать ключевые финансовые решения и управление рисками в финансовом менеджменте
- Оценивать стратегии финансового планирования и получения финансирования для бизнеса

Модуль 14. Коммерческий менеджмент и стратегический маркетинг

- Описать концептуальные основы и важность управления маркетингом в компаниях
- Изучить ключевые элементы и виды деятельности маркетинга и их влияние на организацию
- Определить этапы процесса стратегического маркетингового планирования
- Оценить стратегии по улучшению корпоративной коммуникации и цифровой репутации компании

Модуль 15. *Управленческий* менеджмент

- Определять концепцию общего менеджмента и ее значение для управления бизнесом
- Оценить роль и ответственность менеджмента в организационной культуре
- Проанализировать важность управления операциями и управления качеством в цепочке создания стоимости
- Развивать навыки межличностного общения и публичных выступлений для подготовки пресс-секретарей

Уникальная и идеальная программа, если вы хотите расширить свои знания в области кибербезопасности"

03

Компетенции

После прохождения аттестации данной магистратуры специалист приобретет ряд знаний, инструментов и навыков, которые гарантированно и с успехом позволят ему работать в данной отрасли. Таким образом, студент не только станет экспертом в области кибербезопасности, но и внесет положительный вклад в снижение уровня киберпреступности путем создания более безопасной и сильной сети для всех пользователей. Достижение высших руководящих должностей в качестве директора по информационной безопасности.

Сектор кибербезопасности требует постоянного обновления знаний. С помощью таких программ, как эта, профессионал достигнет цели быстро и эффективно"

Общие профессиональные навыки

- Ознакомиться с методологиями, используемыми в сфере кибербезопасности
- Уметь оценивать каждый тип угрозы, чтобы предложить оптимальное решение для каждого конкретного случая
- Уметь генерировать комплексные интеллектуальные решения для автоматизации поведения в случае инцидентов
- Уметь оценивать риски, связанные с уязвимостями как внутри компании, так и за ее пределами
- Ознакомиться с эволюцией и влиянием IoT за время его существования
- Уметь продемонстрировать, что система уязвима, атаковать ее проактивно и решать подобные проблемы
- Уметь применять *"песочницу"* в различных средах
- Знать руководящие принципы, которым должен следовать хороший разработчик, чтобы соответствовать необходимым требованиям безопасности

Совершенствование ваших навыков в сфере услуг для всех будет способствовать вашей профессиональной и личной карьере"

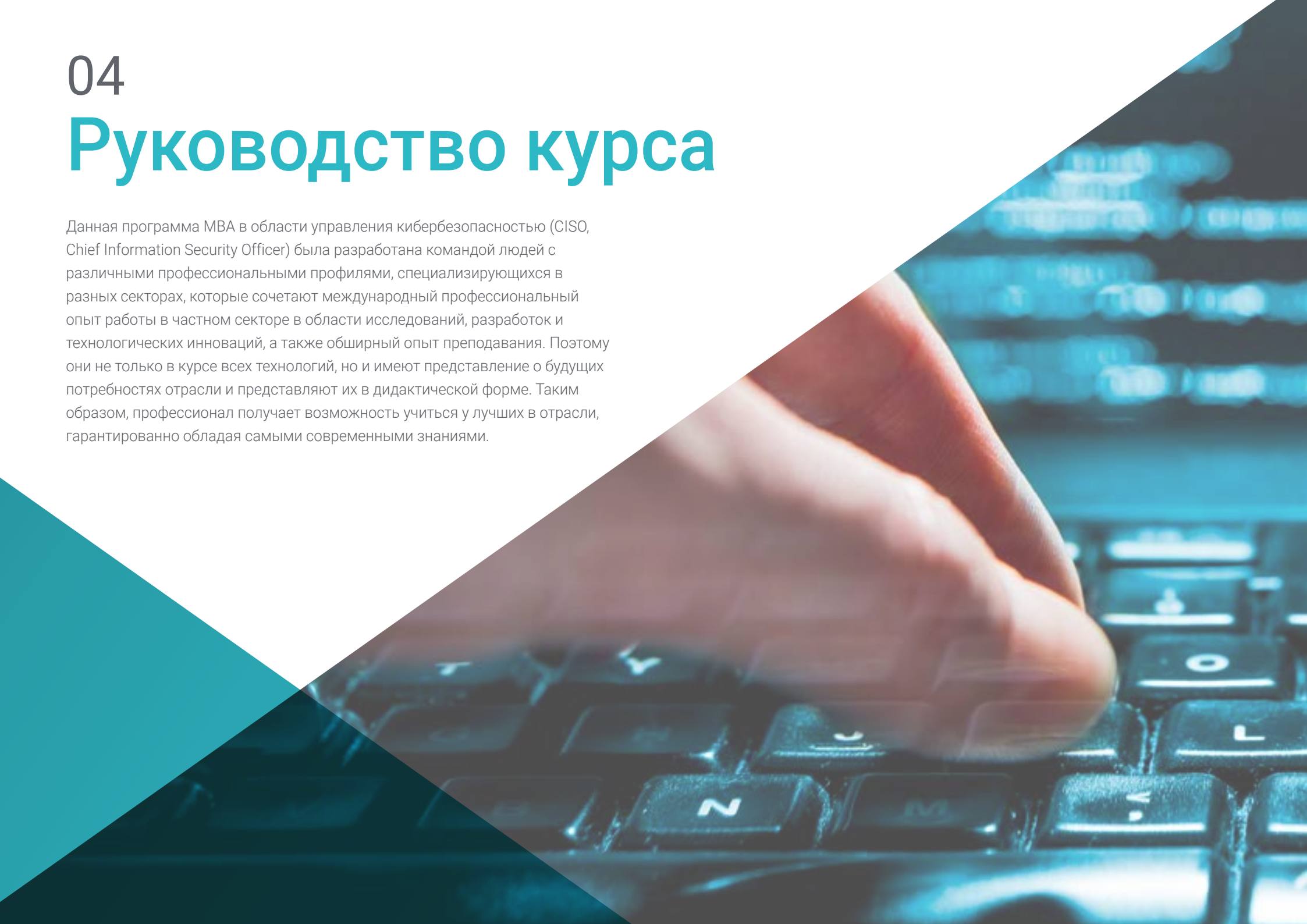
Профессиональные навыки

- Уметь проводить операции по обеспечению защитной безопасности
- Иметь глубокое и специализированное представление об ИТ-безопасности
- Обладать специализированными знаниями в области кибербезопасности и кибер разведки
- Обладать глубокими знаниями таких фундаментальных аспектов, как цикл разведки, источники разведывательных данных, социальная инженерия, методология OSINT, HUMINT, *анонимизация*, анализ рисков, существующие методологии (OWASP, OWISAM, OSSTM, PTES)
- Понять важность разработки многоуровневой защиты, также известной как *глубинная защита*, охватывающей все аспекты корпоративной сети, где некоторые концепции и системы, которые мы увидим, могут быть использованы и применены в домашней среде
- Уметь применять процессы обеспечения безопасности для смартфонов и портативных устройств
- Знать способы проведения так называемого этического хакинга и защиты компании от кибератаки
- Уметь расследовать инциденты, связанные с кибербезопасностью
- Овладеть различными доступными методами атаки и защиты
- Проанализировать роль аналитика по кибербезопасности
- Углубить понимание социальной инженерии и ее методов

04

Руководство курса

Данная программа MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer) была разработана командой людей с различными профессиональными профилями, специализирующихся в разных секторах, которые сочетают международный профессиональный опыт работы в частном секторе в области исследований, разработок и технологических инноваций, а также обширный опыт преподавания. Поэтому они не только в курсе всех технологий, но и имеют представление о будущих потребностях отрасли и представляют их в дидактической форме. Таким образом, профессионал получает возможность учиться у лучших в отрасли, гарантированно обладая самыми современными знаниями.



Во время прохождения данной программы MBA вас будет окружать ряд профессиональных экспертов, которые сделают ваш образовательный опыт уникальным"

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 Лаваля
- Член: New Program Roundtable Committee, Джорджтаунский университет

Благодаря TECH вы сможете учиться у лучших мировых профессионалов"

Приглашенный руководитель международного уровня

Обладая более чем 20-летним опытом создания и руководства глобальными командами по привлечению талантов, Дженнифер Дав является экспертом в области рекрутинга и технологической стратегии. На протяжении своей карьеры она занимала руководящие должности в нескольких технологических организациях в компаниях из списка Fortune 50, таких как NBCUniversal и Comcast. Ее послужной список позволил ей добиться успеха в конкурентной среде с высокими темпами роста.

В качестве вице-президента по привлечению талантов в Mastercard она курирует стратегию и реализацию программы привлечения талантов, сотрудничая с бизнес-лидерами и отделом кадров для достижения операционных и стратегических целей найма. В частности, она стремится создать разнообразные, инклюзивные и высокопроизводительные команды, которые будут способствовать инновациям и росту продуктов и услуг компании. Кроме того, она является экспертом в использовании инструментов для привлечения и удержания лучших специалистов со всего мира. Она также отвечает за усиление бренда и ценностного предложения Mastercard через публикации, мероприятия и социальные сети.

Дженнифер Дав демонстрирует свое стремление к постоянному профессиональному развитию, активно участвуя в работе сетей HR-специалистов и принимая участие в принятии на работу большого количества сотрудников в различных компаниях. Получив степень бакалавра в области организационных коммуникаций в Университете Майами, она занимала руководящие должности в сфере рекрутинга в компаниях различных направлений.

Она получила признание за способность руководить организационными преобразованиями, внедрять технологии в процессы подбора персонала и разрабатывать программы для руководителей, которые готовят учреждения к предстоящим испытаниям. Она также успешно реализовала оздоровительные программы, которые значительно повысили удовлетворенность сотрудников и их удержание.

Г-жа Дав, Дженнифер

- Вице-президент по поиску талантов в Mastercard, Нью-Йорк, США
- Директор по привлечению талантов в NBCUniversal, Нью-Йорк, США
- Руководитель отдела по подбору персонала в Comcast
- Директор по подбору персонала в Rite Hire Advisory
- Исполнительный вице-президент отдела продаж в Ardor NY Real Estate
- Директор по подбору персонала в Valerie August & Associates
- Исполнительный директор по работе с клиентами в BNC
- Менеджер по работе с клиентами в Vault
- Степень бакалавра в области организационная коммуникация Университета Майами

Благодаря TECH вы сможете учиться у лучших мировых профессионалов"

Приглашенный руководитель международного уровня

Лидер в области технологий с десятилетним опытом работы в **крупных транснациональных корпорациях**, Рик Готье занимает видное место в сфере **облачных услуг** и комплексного совершенствования процессов. Он признан как высокоэффективный лидер и руководитель команды, демонстрирующий природный талант обеспечивать высокий уровень вовлеченности своих сотрудников.

Он прекрасно разбирается в стратегии и инновациях, разрабатывает новые идеи и подкрепляет свои успехи качественными данными. Его опыт работы в **Amazon** позволил ему управлять и интегрировать ИТ-службы компании в США. В **Microsoft** он руководил командой из 104 человек, отвечая за обеспечение корпоративной ИТ-инфраструктуры и поддержку отделов разработки продуктов по всей компании.

Этот опыт позволил ему выделиться как высокоэффективному руководителю с выдающимися способностями к повышению эффективности, производительности и общей удовлетворенности клиентов.

Г-н Готье, Рик

- Региональный директор по ИТ в Amazon, Сиэтл, США
- Старший менеджер программ в Amazon
- Вице-президент компании Wimmer Solutions
- Старший директор по продуктивным инженерным услугам в Microsoft
- Степень по кибербезопасности в Университете Западных Губернаторов
- Профессиональный сертификат по *коммерческому дайвингу* от Технологического института дайверов
- Степень в области экологических исследований в Эвергринском государственном колледже

Используйте возможность ознакомиться с последними достижениями в этой области, чтобы применять их в вашей повседневной практике"

Приглашенный руководитель международного уровня

Роми Арман является известным международным экспертом с более чем двадцатилетним опытом работы в области **цифровой трансформации**, **маркетинга**, стратегии и **консалтинга**. На протяжении всей своей карьеры он не раз шел на риск и постоянно **выступал** за **инновации** и **изменения** в бизнес-среде. Благодаря этому опыту он работал с руководителями компаний и корпоративных организаций по всему миру, подталкивая их к отходу от традиционных бизнес-моделей. Благодаря этому он помог таким компаниям, как Shell Energy, стать **настоящими лидерами рынка,** ориентированными на своих **клиентов** и **цифровой мир.**

Стратегии, разработанные Арманом, имеют неоспоримое влияние, поскольку они позволили нескольким корпорациям **улучшить опыт как потребителей,** так и **сотрудников** и **акционеров.** Успех этого эксперта можно оценить с помощью таких осязаемых показателей, как **CSAT**, **вовлеченность сотрудников** в работу учреждений, в которых он работал, и рост **финансового показателя EBITDA** в каждом из них.

Кроме того, в своей профессиональной карьере он взращивал и **возглавлял высокоэффективные команды**, которые даже получали награды за свой **трансформационный потенциал**. В компании Shell он всегда стремился решить три задачи: удовлетворить сложные **требования** клиентов по **декарбонизации**, **поддержать** "**рентабельную декарбонизацию**" и **перестроить** фрагментированный ландшафт **данных**, **цифровых технологий и технологий.** Таким образом, его усилия показали, что для достижения устойчивого успеха необходимо исходить из потребностей потребителей и закладывать основы для трансформации процессов, данных, технологий и культуры.

С другой стороны, этот руководитель выделяется своим мастерством в области **бизнес-применения искусственного интеллекта,** по которому он получил степень в аспирантуре Лондонской школы бизнеса. В то же время он накопил опыт в области **IoT** и **Salesforce.**

Г-н Арман, Роми

- Директор по цифровой трансформации (CDO) в Shell Energy Corporation, Лондон, Великобритания
- Глобальный руководитель отдела электронной коммерции и обслуживания клиентов в Shell Energy Corporation, Лондон, Великобритания
- Национальный менеджер по работе с ключевыми клиентами (автомобильные комплектующие и розничная торговля) для компании Shell в Куала-Лумпуре, Малайзия
- Старший консультант по вопросам управления (сектор финансовых услуг) в компании Accenture в Сингапуре.
- Степень бакалавра от Университета Лидса
- Степень аспиранта Лондонской школы бизнеса по применению искусственного интеллекта в бизнесе для руководителей высшего звена
- Профессиональный сертификат CCXP Customer Experience
- Курс по цифровой трансформации для руководителей от IMD

Вы хотите обновить свои знания, получив образование высочайшего качества? TECH предлагает вам самый актуальный контент на академическом рынке, разработанный настоящими экспертами международного уровня"

Приглашенный руководитель международного уровня

Мануэль Аренс — **опытный специалист** по управлению данными и руководитель высококвалифицированной команды. В действительности Аренс занимает должность **менеджера по глобальным закупкам** в подразделении технической инфраструктуры и центров обработки данных компании Google, где он провел большую часть своей карьеры. Находясь в Маунтин-Вью (Калифорния), он занимался решением таких операционных задач технологического гиганта, как **обеспечение целостности основных данных, обновление данных о поставщиках** и определение их **приоритетности**. Он руководил планированием цепочки поставок центров обработки данных и оценкой рисков поставщиков, обеспечивая совершенствование процессов и управление рабочими процессами, что позволило добиться значительной экономии средств.

За более чем десятилетний опыт работы в области предоставления цифровых решений и руководства компаниями различных отраслей он обладает обширным опытом во всех аспектах предоставления стратегических решений, включая **маркетинг, медиааналитику, измерения** и **атрибуцию.** За свою работу он получил несколько наград, в том числе **BIM** Leadership Award, **Search Leadership Award, Export Lead Generation Programme Award** и **EMEA Best Sales Model Award**.

Аренс также занимал должность **менеджера по продажам** в Дублине, Ирландия. На этой должности он за три года сформировал команду из 4-14 человек и привел отдел продаж к достижению результатов и эффективному взаимодействию друг с другом и межфункциональными группами. Он также работал **старшим отраслевым аналитиком** в Гамбурге (Германия), создавая сторилайны для более чем 150 клиентов с использованием внутренних и сторонних инструментов для поддержки анализа. Разрабатывал и составлял подробные отчеты, демонстрирующие экспертные знания в предметной области, включая понимание **макроэкономических и политических/регуляторных факторов**, влияющих на внедрение и распространение технологий.

Он также возглавлял команды в таких компаниях, как **Eaton, Airbus и Siemens**, где приобрел ценный опыт управления клиентами и цепочками поставок. Его особенно отличает умение постоянно превосходить ожидания, **выстраивая ценные отношения с клиентами** и **беспрепятственно работая с людьми на всех уровнях организации**, включая заинтересованные стороны, руководство, членов команды и клиентов. Его подход, основанный на использовании данных, и способность разрабатывать инновационные и масштабируемые решения проблем отрасли сделали его выдающимся лидером в своей области.

Г-н Аренс, Мануэль

- Генеральный менеджер по глобальным закупкам в области Google, Маунтин-Вью, США
- Старший менеджер по аналитике и технологиям B2B в Google, США
- Директор по продажам в Google, Ирландия
- Старший отраслевой аналитик в Google, Германия
- Менеджер по работе с клиентами в Google, Ирландия
- Кредиторская задолженность в Eaton, Великобритания
- Менеджер по цепочке поставок в Airbus, Германия

Выбирайте TECH! Вы сможете получить доступ к лучшим учебным материалам, находящимся на передовой линии технологий и образования, которые разрабатываются всемирно известными специалистами в этой области"

Приглашенный руководитель международного уровня

Андреа Ла Сала – **опытный руководитель** отдела **маркетинга**, чьи проекты оказали **значительное влияние** на **индустрию моды**. На протяжении своей успешной карьеры он решал различные задачи, связанные с **продуктом**, **мерчендайзингом** и **коммуникациями**. Все это связано с такими престижными брендами, как **Giorgio Armani**, **Dolce&Gabbana**, **Calvin Klein** и другими.

Результаты работы этого **высокопоставленного руководителя международного уровня** связаны с его доказанной способностью **синтезировать информацию** в четкие схемы и осуществлять **конкретные действия** в соответствии с **конкретными бизнес-целями**. Кроме того, его признают за **проактивность** и **адаптацию к быстро меняющемуся ритму** работы. Ко всему этому он добавляет **сильное коммерческое понимание**, **видение рынка** и **искреннюю страсть** к **продукции**.

В качестве **директора по глобальному бренду и мерчандайзингу** в **Giorgio Armani** он курировал различные **маркетинговые стратегии** в области **одежды** и **аксессуаров**. Его тактика также была направлена на изучение **розничной торговли**, **потребностей** и **поведения потребителей**. В этой роли Ла Сала также отвечал за формирование маркетинга продукции на различных рынках, выступая в качестве **руководителя групп** в **отделах дизайна**, **коммуникаций** и **продаж**.

С другой стороны, в таких компаниях, как **Calvin Klein** или **Gruppo Coin**, он занимался проектами по улучшению **структуры**, **разработке** и **маркетингу различных коллекций**. Он также отвечал за создание **эффективных календарей** для **кампаний** по покупке и продаже. Андреа управлял **условиями**, **затратами**, **процессами** и **сроками поставки** для различных операций.

Этот опыт сделал Андреа Ла Сала одним из лучших и наиболее квалифицированных **корпоративных лидеров** в сфере **моды** и **роскоши**. Обладая высоким управленческим потенциалом, он сумел эффективно реализовать **позитивное позиционирование различных брендов** и переопределить их ключевые показатели эффективности (KPI).

Г-н Ла Сала, Андреа

- Директор по глобальному бренду и мерчандайзингу Armani Exchange в Giorgio Armani, Милан, Италия
- Директор по мерчандайзингу в компании Calvin Klein
- Управляющий брендом в Gruppo Coin
- Бренд-менеджер в Dolce&Gabbana
- Бренд-менеджер в Sergio Tacchini S.p.A.
- Маркетинговый аналитик в Fastweb
- Выпускник факультета бизнеса и экономики Восточного университета Пьемонта

Самые квалифицированные и опытные специалисты международного уровня ждут вас в TECH, чтобы предложить вам первоклассное обучение, обновленное и основанное на последних научных данных. Чего вы ждете, чтобы поступить?"

Приглашенный руководитель международного уровня

Мик Грэм является синонимом инноваций и передового опыта в области **бизнес-аналитики** на международном уровне. Его успешная карьера связана с руководящими должностями в таких транснациональных корпорациях, как **Walmart** и **Red Bull.** Он также известен своей способностью **определять новые технологии**, которые в долгосрочной перспективе окажут долгосрочное влияние на корпоративную среду.

С другой стороны, руководитель считается **первопроходцем** в **использовании методов визуализации данных**, которые упрощали сложные массивы, делая их доступными и облегчая принятие решений. Это умение стало основой его профессионального профиля, превратив его в желанного сотрудника для многих организаций, делающих ставку на **сбор информации** и **выработку конкретных действий** на ее основе.

Одним из его самых выдающихся проектов последних лет стала **платформа Walmart Data Cafe** - крупнейшая в мире платформа для **анализа *больших данных***, созданная на основе облачных технологий. Кроме того, он занимал должность **директора** по **бизнес-аналитике** в компании **Red Bull,** охватывая такие сферы, как **продажи, дистрибуция, маркетинг и управление цепочками поставок.** Недавно его команда была отмечена за постоянные инновации в использовании нового API Walmart Luminate для анализа покупателей и каналов сбыта.

Что касается образования, то руководитель имеет несколько магистерских и аспирантских степеней, полученных в таких престижных центрах, как **Университет Беркли** в США и **Копенгагенский университет** в Дании. Благодаря постоянному повышению квалификации эксперт добился передовых навыков. Таким образом, он стал считаться **прирожденным лидером новой глобальной экономики**, в центре которой - стремление к данным и их безграничным возможностям.

Г-н Грэм, Мик

- Директор по *бизнес-аналитике* и анализу в Red Bull, Лос-Анджелес, США
- Архитектор решений в области *бизнес-аналитики* в Walmart Data Cafe
- Независимый консультант по *бизнес-аналитике* и *науке о данных*
- Директор по бизнес-аналитике в *Capgemini*
- Руководитель аналитического отдела в Nordea
- Старший консультант *бизнес-аналитики для* SAS
- Образование для руководителей в области искусственного интеллекта и машинного обучения в Инженерном колледже Калифорнийского университета в Беркли
- Эксклюзивная программа MBA по электронной коммерции в Копенгагенском университете
- Бакалавриат и магистратура по математике и статистике в Копенгагенском университете

Учитесь в лучшем онлайн-университете мира по версии Forbes! На этой программе MBA вы получите доступ к обширной библиотеке мультимедийных ресурсов, разработанных всемирно известными профессорами"

Приглашенный руководитель международного уровня

Скотт Стивенсон - выдающийся эксперт в области **цифрового маркетинга**, который уже более 19 лет связан с одной из самых влиятельных компаний в индустрии развлечений, **Warner Bros. Discovery.** В этой должности он играл ключевую роль в **контроле за логистикой** и **творческими процессами** на различных цифровых платформах, включая социальные, поисковые, дисплейные и линейные медиа.

Его руководство сыграло решающую роль в разработке **стратегий производства платных медиа**, что привело к заметному **улучшению** показателей **конверсии** в компании. В то же время он занимал и другие должности, такие как директор по маркетинговым услугам и менеджер по трафику в той же транснациональной корпорации во время своей прежней работы в руководстве.

Стивенсон также участвовал в глобальной дистрибуции видеоигр и кампаниях по **продаже цифровой собственности**. Он также отвечал за внедрение операционных стратегий, связанных с формированием, завершением и доставкой звукового и графического контента для **телевизионных рекламных роликов** и ***трейлеров.***

Кроме того, он получил степень бакалавра в области телекоммуникаций в Университете Флориды и степень магистра в области творческого писательства в Калифорнийском университете, что свидетельствует о его мастерстве в области **коммуникации** и **подачи материала**. Кроме того, он участвовал в Школе профессионального развития Гарвардского университета в передовых программах по использованию **искусственного интеллекта** в **бизнесе**. Таким образом, его профессиональный профиль является одним из самых актуальных в современной сфере **маркетинга** и **цифровых медиа.**

Г-н Стивенсон, Скотт

- Директор по цифровому маркетингу в Warner Bros. Discovery, Бербанк, Соединенные Штаты Америки
- Менеджер по трафику в Warner Bros. Entertainment
- Степень магистра искусств в области творческого писательства Калифорнийского университета
- Степень бакалавра наук в области телекоммуникаций из Университета Флориды

Достигайте своих академических и карьерных целей с лучшими в мире экспертами! Преподаватели MBA будут сопровождать вас на протяжении всего процесса обучения"

Приглашенный руководитель международного уровня

Доктор Эрик Найквист – ведущий профессионал в **области международного спорта**, построивший впечатляющую карьеру, отмеченную его **стратегическим лидерством** и способностью управлять изменениями и **инновациями** в **спортивных организациях** высшего уровня.

Он занимал такие высокие должности, как **директор по коммуникациям и влиянию** в **NASCAR**, расположенном во **Флориде, США.** Имея за плечами многолетний опыт работы в NASCAR, доктор Найквист также занимал ряд руководящих должностей, в том числе старшего **вице-президента по стратегическому развитию** и **генерального директора по коммерческим вопросам**, управляя более чем десятком направлений - от **стратегического развития** до **маркетинга развлечений.**

Найквист также внес значительный вклад в развитие ведущих **спортивных франшиз** Чикаго. Будучи **исполнительным вице-президентом** клубов **Chicago Bulls** и **Chicago White Sox**, он продемонстрировал свою способность добиваться **делового** и **стратегического успеха** в мире **профессионального спорта**.

Наконец, он начал свою карьеру в **спорте**, работая в **Нью-Йорке** в **качестве старшего стратегического аналитика** для **Роджера Гуделла** в **Национальной футбольной лиге (НФЛ)**, а до этого - в качестве **стажера-юриста** в **Федерации футбола США.**

Д-р Найквист, Эрик

- Директор по коммуникациям и влиянию в NASCAR, Флорида, США
- Старший вице-президент по стратегическому развитию NASCAR
- Вице-президент по стратегическому планированию NASCAR
- Старший директор по деловым вопросам NASCAR
- Исполнительный вице-президент франшизы Chicago White Sox
- Исполнительный вице-президент франшизы Chicago Bulls
- Менеджер по бизнес-планированию в Национальной футбольной лиге (НФЛ)
- Стажер по деловым вопросам/юриспруденции в Федерации футбола США
- Доктор юриспруденции Чикагского университета
- Магистр делового администрирования-MBA в Школе бизнеса Бут Чикагского университета
- Степень бакалавра по международной экономике в Карлтонском колледже

Благодаря этой 100% онлайн-программе вы сможете совмещать учебу с повседневными обязанностями под руководством ведущих международных экспертов в интересующей вас области. Записывайтесь сейчас!"

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 Techonologies. E-Council

Преподаватели

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 Редондо, Хесус Серрано

- Веб-разработчик и специалист по кибербезопасности
- Веб-разработчик в Roams, Паленсия, Испания
- FrontEnd-разработчик в Telefónica, Мадрид
- FrontEnd-разработчик в Best Pro Consulting SL, Мадрид
- Установщик телекоммуникационного оборудования и услуг в Grupo Zener, Кастилья-и-Леон
- Установщик телекоммуникационного оборудования и услуг в Lican Comunicaciones SL, Кастилья-и-Леон
- Сертификат по компьютерной безопасности, CFTIC Getafe, Мадрид
- Профессиональное среднее образование в области телекоммуникаций и компьютерных систем, школа IES Trinidad Арройо, Паленсия
- Профессиональное среднее образование по электротехническим установкам среднего и низкого напряжения, школа IES Trinidad Arroyo, Паленсия, Испания
- Обучение реверс-инжинирингу, стенографии и шифрованию в Академии Hacker Incibe

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

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 Падура
- 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-н Хименес Рамос, Альваро

Г-н Хименес Рамос, Альваро

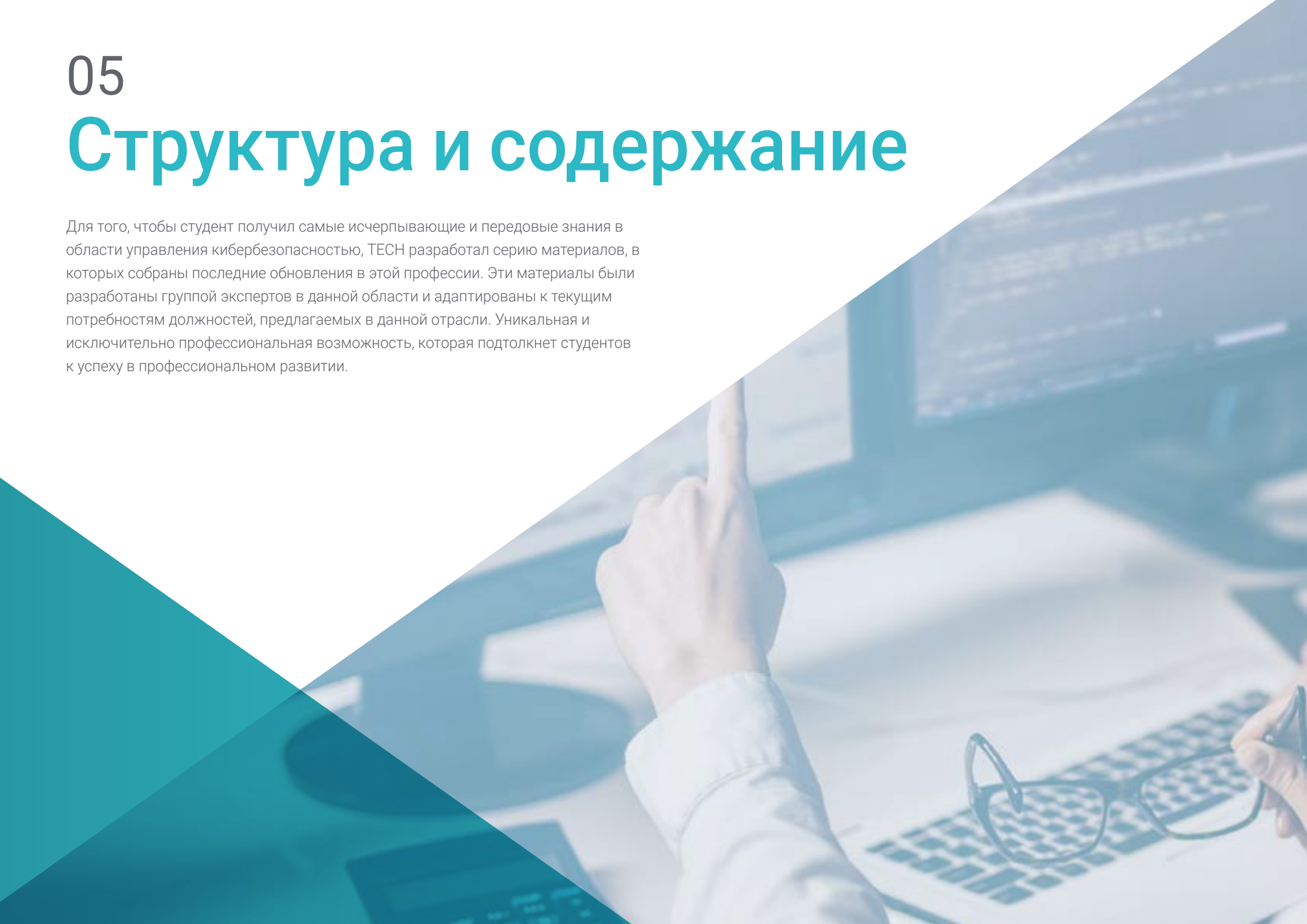
- Аналитик по кибербезопасности
- Старший аналитик по вопросам безопасности в компании The Workshop
- Аналитик по кибербезопасности L1 в Axians
- Аналитик по кибербезопасности L2 в Axians
- Аналитик по кибербезопасности в SACYR S.A.
- Степень инженера в области телематики Политехнического университета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

Воспользуйтесь возможностью узнать о последних достижениях в этой области, чтобы применить их в своей повседневной практике"

05

Структура и содержание

Для того, чтобы студент получил самые исчерпывающие и передовые знания в области управления кибербезопасностью, TECH разработал серию материалов, в которых собраны последние обновления в этой профессии. Эти материалы были разработаны группой экспертов в данной области и адаптированы к текущим потребностям должностей, предлагаемых в данной отрасли. Уникальная и исключительно профессиональная возможность, которая подтолкнет студентов к успеху в профессиональном развитии.



Учебный план высшего уровня, разработанный профессионалами высшего уровня и для профессионалов высшего: неужели вы хотите упустить эту возможность”

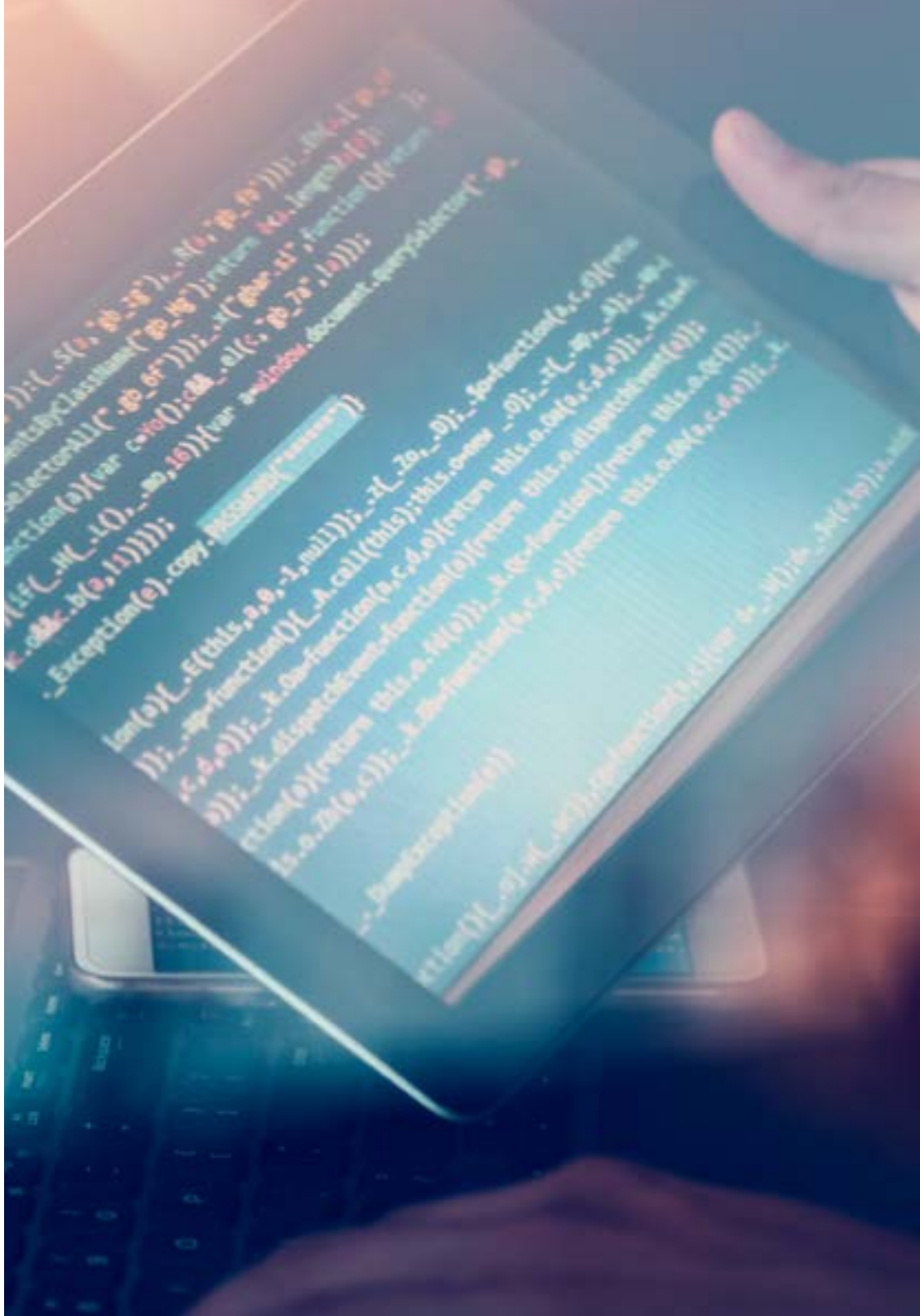
Модуль 1. Кибербезопасность

1.1. Кибербезопасность
- 1.1.1. Кибербезопасность
  - 1.1.1.1. Разведка
    - 1.1.1.1.1. Цикл разведки
  - 1.1.1.2. Кибербезопасность
  - 1.1.1.3. Кибербезопасность и кибербезопасность
- 1.1.2. Аналитик разведывательной службы
  - 1.1.2.1. Роль аналитика разведывательной службы
  - 1.1.2.2. Необъективность аналитика разведки в оценочной деятельности

1.2. Кибербезопасность
- 1.2.1. Уровни безопасности
- 1.2.2. Идентификация киберугроз
  - 1.2.2.1. Внешние угрозы
  - 1.2.2.2. Внутренние угрозы
- 1.2.3. Неблагоприятные действия
  - 1.2.3.1. Социальная инженерия
  - 1.2.3.2. Часто используемые методы

1.3. Инструменты и методы разведки
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Дистрибутивы и инструменты Linux
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. Методология оценки
- 1.4.1. Анализ разведывательной информации
- 1.4.2. Методы организации полученной информации
- 1.4.3. Надежность и достоверность источников информации
- 1.4.4. Методологии анализа
- 1.4.5. Представление результатов разведки



1.5. Аудиты и документация
  1.5.1. Аудит ИТ-безопасности
  1.5.2. Документация и разрешения на проведение аудита
  1.5.3. Виды аудита
  1.5.4. Результаты работы
    1.5.4.1. Технический отчет
    1.5.4.2. Исполнительный отчет
1.6. Анонимность в интернете
  1.6.1. Использование анонимизации
  1.6.2. Методы анонимизации (Proxy, VPN)
  1.6.3. Сети TOR, Freenet e IP2
1.7. Угрозы и виды безопасности
  1.7.1. Виды угроз
  1.7.2. Физическая безопасность
  1.7.3. Безопасность в сетях
  1.7.4. Логическая безопасность
  1.7.5. Безопасность веб-приложений
  1.7.6. Безопасность на мобильных устройствах
1.8. Регулирование и *комплаенс*
  1.8.1. Общий регламент по защите данных
  1.8.2. Семейство стандартов ISO 27000
  1.8.3. Система кибербезопасности NIST
  1.8.4. PIC
  1.8.5. ISO 27032
  1.8.6. Регулирование *Cloud*
  1.8.7. SOX
  1.8.8. PCI
1.9. Анализ рисков и метрики
  1.9.1. Масштабы рисков
  1.9.2. Активы
  1.9.3. Угрозы
  1.9.4. Уязвимости
  1.9.5. Оценка рисков
  1.9.6. Обработка риска
1.10. Важные органы по вопросам кибербезопасности
  1.10.1. NIST
  1.10.2. ENISA
  1.10.3. OEA
  1.10.4. UNASUR - PROSUR

Модуль 2. Безопасность хоста

2.1. Резервные копии
  2.1.1. Стратегии резервного копирования
  2.1.2. Инструменты для Windows
  2.1.3. Инструменты для Linux
  2.1.4. Инструменты для MacOS
2.2. Пользовательский антивирус
  2.2.1. Виды антивирусов
  2.2.2. Антивирус для Windows
  2.2.3. Антивирус для Linux
  2.2.4. Антивирус для MacOS
  2.2.5. Антивирусы для смартфонов
2.3. Детекторы вторжения - HIDS
  2.3.1. Методы обнаружения вторжений
  2.3.2. Sagan
  2.3.3. Aide
  2.3.4. Rkhunter
2.4. Локальный брандмауэр
  2.4.1. Брандмауэры для Windows
  2.4.2. Брандмауэры для Linux
  2.4.3. Брандмауэры для MacOS
2.5. Менеджеры паролей
  2.5.1. Password
  2.5.2. LastPass
  2.5.3. KeePass
  2.5.4. StickyPassword
  2.5.5. RoboForm

2.6. Детекторы *фишинга*
  2.6.1. Обнаружение *фишинга* вручную
  2.6.2. *Антифишинговые* инструменты
2.7. *Шпионское программное обеспечение*
  2.7.1. Механизмы предотвращения
  2.7.2. *Антишпионские* инструменты
2.8. Трекеры
  2.8.1. Меры по защите системы
  2.8.2. Инструменты для борьбы с трекингом
2.9. EDR - *Обнаружение и реагирование конечных точек*
  2.9.1. Поведение системы EDR
  2.9.2. Различия между EDR и антивирусом
  2.9.3. Будущее систем EDR
2.10. Контроль над установкой программного обеспечения
  2.10.1. Репозитории и магазины программного обеспечения
  2.10.2. Списки разрешенного или запрещенного программного обеспечения
  2.10.3. Критерии обновлений
  2.10.4. Права на установку программного обеспечения

Модуль 3. Сетевая безопасность (периметр)

3.1. Системы обнаружения и предотвращения угроз
  3.1.1. Общая нормативная база для инцидентов по безопасности
  3.1.2. Современные системы защиты: *Глубокая защита* и SOC
  3.1.3. Текущие сетевые архитектуры
  3.1.4. Типы средств выявления и предотвращения инцидентов
    3.1.4.1. Сетевые системы
    3.1.4.2. Системы на базе *хоста*
    3.1.4.3. Централизованные системы
  3.1.5. Связь и обнаружение экземпляров/хостов, контейнеров и бессерверных систем
3.2. Брандмауэр
  3.2.1. Типы файерволов
  3.2.2. Атаки и смягчение последствий
  3.2.3. Лучший *брандмауэр* для Linux
    3.2.3.1. Uncomplicated Firewall
    3.2.3.2. *Nftables* e *iptables*
    3.2.3.3. Firewalld
  3.2.4. Системы обнаружения на основе системных журналов
    3.2.4.1. TCP Wrappers
    3.2.4.2. BlockHosts и DenyHosts
    3.2.4.3. Fai2ban
3.3. Системы обнаружения и предотвращения вторжений (IDS/IPS)
  3.3.1. Атаки на IDS/IPS
  3.3.2. Системы IDS/IPS
    3.3.2.1. Snort
    3.3.2.2. Suricata
3.4. Брандмауэры следующего поколения (NGFW)
  3.4.1. Различия между NGFW и традиционными брандмауэрами
  3.4.2. Основные возможности
  3.4.3. Коммерческие решения
  3.4.4. Брандмауэры для *облачных сервисов*
    3.4.4.1. Архитектура Cloud VPC
    3.4.4.2. Cloud ACLs
    3.4.4.3. Security Group
3.5. *Прокси*
  3.5.1. Типы *прокси*
  3.5.2. Использование *прокси*. Преимущества и недостатки
3.6. Антивирусные системы
  3.6.1. Общий контекст *вредоносных программ* и IOCs
  3.6.2. Проблемы с антивирусным движком
3.7. Системы защиты почтовых сервисов
  3.7.1. Антиспам
    3.7.1.1. Черные и белые списки
    3.7.1.2. Байесовская фильтрация спама
  3.7.2. Mail Gateway (MGW)

3.8. SIEM
- 3.8.1. Компоненты и архитектура
- 3.8.2. Правила корреляции и примеры использования
- 3.8.3. Актуальные проблемы систем SIEM

3.9. SOAR
- 3.9.1. SOAR у SIEM: враги или союзники
- 3.9.2. Будущее систем SOAR

3.10. Другие сетевые системы
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. HoneyPots и HoneyNets
- 3.10.4. CASB

Модуль 4. Безопасность смартфонов

4.1. Мир мобильных устройств
- 4.1.1. Виды мобильных платформ
- 4.1.2. iOS-устройства
- 4.1.3. Android-устройства

4.2. Управление безопасностью мобильных устройств
- 4.2.1. Проект по мобильной безопасности OWASP
  - 4.2.1.1. Топ-10 уязвимостей
- 4.2.2. Коммуникации, сети и режимы подключения

4.3. Мобильное устройство в корпоративной среде
- 4.3.1. Риски
- 4.3.2. Мониторинг устройств
- 4.3.3. Управление мобильными устройствами (MDM)

4.4. Конфиденциальность пользователей и безопасность данных
- 4.4.1. Состояние информации
- 4.4.2. Безопасное хранение данных
  - 4.4.2.1. Безопасное хранение данных на iOS
  - 4.4.2.2. Безопасное хранение данных на Android
- 4.4.4. Передовые методы разработки приложений

4.5. Уязвимости и векторы атак
- 4.5.1. Уязвимости
- 4.5.2. Векторы атак
  - 4.5.2.1. Вредоносное программное обеспечение
  - 4.5.2.2. Эксфильтрация данных
  - 4.5.2.3. Манипуляции с данными

4.6. Основные угрозы
- 4.6.1. Непринужденный пользователь
- 4.6.2. *Вредоносное программное обеспечение*
  - 4.6.2.1. Виды *вредоносного* ПО
- 4.6.3. Социальная инженерия
- 4.6.4. Утечка данных
- 4.6.5. Кража информации
- 4.6.6. Незащищенные сети Wi-Fi
- 4.6.7. Устаревшее программное обеспечение
- 4.6.8. Вредоносные приложения
- 4.6.9. Ненадежные пароли
- 4.6.10. Слабые или отсутствующие настройки безопасности
- 4.6.11. Физический доступ к информации
- 4.6.12. Потеря или кража устройства
- 4.6.13. Подмена личности (целостность)
- 4.6.14. Слабая или неработающая криптография
- 4.6.15. Отказ в обслуживании (DoS)

4.7. Основные атаки
- 4.7.1. *Фишинговые* атаки
- 4.7.2. Атаки, связанные со способами коммуникации
- 4.7.3. *Смишинг*-атаки
- 4.7.4. Атаки *криптоджекинга*
- 4.7.5. *Man in The Middle*

4.8. Хакинг
- 4.8.1. *Рутинг и джейлбрейк*
- 4.8.2. Анатомия мобильной атаки
- 4.8.2.1. Распространение угрозы
- 4.8.2.2. Установка *вредоносных программ* на устройство
- 4.8.2.3. Настойчивость
- 4.8.2.4. Выполнение *полезной нагрузки* и извлечение информации
- 4.8.3. *Хакинг* устройств iOS: механизмы и средства
- 4.8.4. *Хакинг* устройств Android: механизмы и инструменты

4.9. Тестирование на проникновение
- 4.9.1. iOS *пентесты*
- 4.9.2. Android *PenTesting*
- 4.9.3. Инструменты

4.10. Безопасность и защита
- 4.10.1. Настройки безопасности
- 4.10.1.1. На устройствах IOS
- 4.10.1.2. Android-устройства
- 4.10.2. Меры по обеспечению безопасности
- 4.10.3. Защитные средства

Модуль 5. Безопасность в IoT

5.1. Приборы
- 5.1.1. Виды устройств
- 5.1.2. Стандартизированные архитектуры
- 5.1.2.1. ONEM2M
- 5.1.2.2. IoTWF
- 5.1.3. Протоколы внедрения
- 5.1.4. Технологии подключения

5.2. Устройства IoT. Области применения
- 5.2.1. *Умный дом*
- 5.2.2. *Умный город*
- 5.2.3. Транспорт
- 5.2.4. *Носимые приборы*
- 5.2.5. Сектор здравоохранения
- 5.2.6. IioT

5.3. Протоколы коммуникации
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *Умный дом*
- 5.4.1. Бытовая автоматизация
- 5.4.2. Сети
- 5.4.3. Бытовая техника
- 5.4.4. Наблюдение и охрана

5.5. *Умный город*
- 5.5.1. Освещение
- 5.5.2. Метеорология
- 5.5.3. Безопасность

5.6. Транспорт
- 5.6.1. Локализация
- 5.6.2. Осуществление платежей и получение услуг
- 5.6.3. Подключение

5.7. *Носимые приборы*
- 5.7.1. Умная одежда
- 5.7.2. Умные ювелирные изделия
- 5.7.3. Умные часы

5.8. Сектор здравоохранения
- 5.8.1. Контроль физической нагрузки/частоты сердечных сокращений
- 5.8.2. Наблюдение за пациентами и пожилыми людьми
- 5.8.3. Имплантируемые
- 5.8.4. Хирургические роботы

5.9. Подключение
- 5.9.1. Wi-Fi/сетевой шлюз
- 5.9.2. Bluetooth
- 5.9.3. Встроенные возможности подключения

5.10. Секьюритизация
- 5.10.1. Выделенные сети
- 5.10.2. Менеджер паролей
- 5.10.3. Использование зашифрованных протоколов
- 5.10.4. Советы по применению

Модуль 6. Этичный хакинг

6.1. Рабочая среда
- 6.1.1. Дистрибутивы Linux
  - 6.1.1.1. Kali Linux-Обеспечение безопасности
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Системы виртуализации
- 6.1.3. *Песочница*
- 6.1.4. Развертывание лабораторий

6.2. Методики
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. *Footprinting*
- 6.3.1. Разведка с открытым исходным кодом (OSINT)
- 6.3.2. Поиск утечек данных и уязвимостей
- 6.3.3. Использование пассивных средств

6.4. Сканирование сети
- 6.4.1. Средства сканирования
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Другие средства сканирования
- 6.4.2. Методы сканирования
- 6.4.3. Методы обхода брандмауэров и IDS
- 6.4.4. *Захват* баннера
- 6.4.5. Сетевые диаграммы

6.5. Перечисление
- 6.5.1. Перечисление SMTP
- 6.5.2. Перечисление DNS
- 6.5.3. Перечисление NetBIOS и Samba
- 6.5.4. Перечисление LDAP
- 6.5.5. Перечисление SNMP
- 6.5.6. Другие техники передачи

6.6. Анализ уязвимостей
- 6.6.1. Решения для сканирования уязвимостей
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2 Системы оценки уязвимостей
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Атаки на беспроводные сети
- 6.7.1. Методология взлома беспроводных сетей
  - 6.7.1.1. Wi-Fi *Discovery*
  - 6.7.1.2. Анализ трафика
  - 6.7.1.3. Атаки в *эйркрэк*
    - 6.7.1.3.1. Атаки WEP
    - 6.7.1.3.2. Атаки WPA/WPA2
  - 6.7.1.4. Атака *«злой двойник»*
  - 6.7.1.5. Атаки на WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Инструменты для обеспечения безопасности беспроводных сетей

6.8. Взлом веб-серверов
- 6.8.1. *Межсайтовый скриптинг*
- 6.8.2. CSRF
- 6.8.3. *Перехват сеанса*
- 6.8.4. *SQLinjection*

6.9. Эксплуатация уязвимостей
- 6.9.1. Использование известных *эксплойтов*
- 6.9.2. Использование *metasploit*
- 6.9.3. Использование вредоносного ПО
  - 6.9.3.1. Определение и сфера применения
  - 6.9.3.2. Генерация *вредоносных* программ
  - 6.9.3.3. Обход антивирусных решений

6.10. Настойчивость
- 6.10.1. Установка *руткитов*
- 6.10.2. Использование ncat
- 6.10.3. Использование запланированных задач для создания *бэкдоров*
- 6.10.4. Создание пользователей
- 6.10.5. Система обнаружения вторжений на хосте

Модуль 7. Реверс-инжиниринг

7.1. Компиляторы
- 7.1.1. Виды кодов
- 7.1.2. Этапы работы компилятора
- 7.1.3. Таблица символов
- 7.1.4. Менеджер ошибок
- 7.1.5. Компилятор GCC

7.2. Виды анализа в компиляторах
- 7.2.1. Лексический анализ
  - 7.2.1.1. Терминология
  - 7.2.1.2. Лексические компоненты
  - 7.2.1.3. Лексический анализ LEX
- 7.2.2. Синтактический анализ
  - 7.2.2.1. Бесконтекстная грамматика
  - 7.2.2.2. Виды синтаксического анализа
    - 7.2.2.2.1. Нисходящий анализ
    - 7.2.2.2.2. Восходящий анализ
  - 7.2.2.3. Синтаксические деревья и производные
  - 7.2.2.4. Виды синтаксических анализаторов
    - 7.2.2.4.1. Анализаторы LR (*Left To Right*)
    - 7.2.2.4.2. Анализаторы LALR
- 7.2.3. Семантический анализ
  - 7.2.3.1. Атрибутивная грамматика
  - 7.2.3.2. S-Attributed
  - 7.2.3.3. L-Attributed

7.3. Структуры данных ассемблера
- 7.3.1. Переменные
- 7.3.2. Arrays
- 7.3.3. Указатели
- 7.4.3. Конструкции
- 7.3.5. Предметы

7.4. Структуры кода ассемблера
- 7.1.4. Структуры отбора
  - 7.4.1.1. *If, else if, Else*
  - 7.4.1.2. *Switch*
- 7.4.2. Структуры итераций
  - 7.4.2.1. *For*
  - 7.4.2.2. *While*
  - 7.4.2.3. Использование *break*
- 7.3.4. Функции

7.5. Архитектура аппаратного обеспечения x86
- 7.5.1. Архитектура процессоров в x86
- 7.5.2. Структуры данных в x86
- 7.5.3. Структуры данных в x86
- 7.5.3. Структуры данных в x86

7.6. Архитектура аппаратного обеспечения ARM
- 7.6.1. Архитектура процессоров ARM
- 7.6.2. Структуры данных в ARM
- 7.6.3. Структуры данных в ARM

7.7. Анализ статического кода
- 7.7.1. Дизассемблеры
- 7.7.2. IDA
- 7.7.3. Реконструкторы кодов

7.8. Анализ динамического кода
- 7.8.1. Поведенческий анализ
  - 7.8.1.1. Коммуникация
  - 7.8.1.2. Мониторинг
- 7.8.2. Отладчики кода в Linux
- 7.8.3. Отладчики кода в Windows

7.9. Песочница
- 7.9.1. Архитектура *песочницы*
- 7.9.2. Обход *песочницы*
- 7.9.3. Методы обнаружения
- 7.9.4. Методы избегания
- 7.9.5. Контрмеры
- 7.9.6. Песочница в Linux
- 7.9.7. Песочница в Windows
- 7.9.8. Песочница в MacOS
- 7.9.9. Песочница в Android

7.10. Анализ *вредоносного ПО*
- 7.10.1. Методы анализа *вредоносного ПО*
- 7.10.2. Методы обфускации *вредоносного ПО*
  - 7.10.2.1. Обфускация исполняемых файлов
  - 7.10.2.2. Ограничение среды исполнения
  - 7.10.3. Инструменты анализа *Вредоносного ПО*

Модуль 8. Безопасная разработка

8.1. Безопасная разработка
- 8.1.1. Качество, функциональность и безопасность
- 8.1.2. Конфиденциальность, целостность и доступность
- 8.1.3. Жизненный цикл разработки *программного обеспечения*

8.2. Этап требований
- 8.2.1. Контроль аутентификации
- 8.2.2. Контроль ролей и привилегий
- 8.2.3. Риск-ориентированные требования
- 8.2.4. Утверждение привилегий

8.3. Этапы анализа и проектирования
- 8.3.1. Доступ к компонентам и системное администрирование
- 8.3.2. Контрольные журналы
- 8.3.3. Управление сессиями
- 8.3.4. Исторические данные
- 8.3.5. Правильная обработка ошибок
- 8.3.6. Разделение функций

8.4. Этап внедрения и кодификации
- 8.4.1. Обеспечение безопасности среды разработки
- 8.4.2. Подготовка технической документации
- 8.4.3. Безопасное кодирование
- 8.4.4. Безопасность коммуникаций

8.5. Надлежащая практика безопасного кодирования
- 8.5.1. Валидация входных данных
- 8.5.2. Кодирование выходных данных
- 8.5.3. Стиль программирования
- 8.5.4. Ведение журнала изменений
- 8.5.5. Криптографические практики
- 8.5.6. Управление ошибками и журналами
- 8.5.7. Управление архивами
- 8.5.8. Управление памятью
- 8.5.9. Стандартизация и повторное использование функций безопасности

8.6. Подготовка сервера и *укрепление*
- 8.6.1. Управление пользователями, группами и ролями на сервере
- 8.6.2. Установка ПО
- 8.6.3. *Укрепление* сервера
- 8.6.4. Надежная конфигурация среды приложения

8.7. Подготовка БД и *укрепление*
- 8.7.1. Оптимизация движка БД
- 8.7.2. Создание собственного пользователя для приложения
- 8.7.3. Назначение необходимых привилегий пользователю
- 8.7.4. *Укрепление* БД

8.8. Этап тестирования
- 8.8.1. Контроль качества в управлении безопасностью
- 8.8.2. Поэтапная проверка кода
- 8.8.3. Проверка управления конфигурации
- 8.8.4. Тестирование методом «черного ящика»

8.9. Подготовка к переходу на производство
- 8.9.1. Осуществлять контроль за изменениями
- 8.9.2. Выполнять процедуры переналадки производства
- 8.9.3. Выполните процедуру *отката*
- 8.9.4. Предпроизводственное тестирование

8.10. Фаза технического обслуживания
- 8.10.1. Обеспечение на основе рисков
- 8.10.2. Тестирование обслуживания системы безопасности «белого ящика»
- 8.10.3. Тестирование обслуживания системы безопасности «черного ящика»

Модуль 9. Судебная экспертиза

9.1. Сбор и воспроизведение данных
- 9.1.1. Сбор волатильных данных
  - 9.1.1.1. Системная информация
  - 9.1.1.2. Сетевая информация
  - 9.1.1.3. Порядок волатильности
- 9.1.2. Сбор статистических данных
  - 9.1.2.1. Создание дублирующего изображения
  - 9.1.2.2. Подготовка документа о цепочке поставок
- 9.1.3. Методы валидации полученных данных
  - 9.1.3.1. Методы для Linux
  - 9.1.3.2. Методы для Windows

9.2. Оценка и преодоление антикриминалистических методов
- 9.2.1. Цели анктикриминалистических методов
- 9.2.2. Удаление данных
  - 9.2.2.1. Удаление данных и файлов
  - 9.2.2.2. Восстановление файлов
  - 9.2.2.3. Восстановление удаленных разделов
- 9.2.3. Защита с помощью пароля
- 9.2.4. Стеганография
- 9.2.5. Безопасное удаление данных с устройств
- 9.2.6. Шифрование

9.3. Судебная экспертиза операционных систем
- 9.3.1. Судебная экспертиза Windows
- 9.3.2. Судебная экспертиза Linux
- 9.3.3. Судебная экспертиза Mac

9.4. Судебная экспертиза сети
- 9.4.1. Анализ журнала
- 9.4.2. Корреляция данных
- 9.4.3. Расследование сети
- 9.4.4. Шаги, необходимые для проведения криминалистической экспертизы сети

9.5. Судебная экспертиза Web
- 9.5.1. Расследование веб-атак
- 9.5.2. Обнаружение атак
- 9.5.3. Локализация IP-адресов

9.6. Криминалистическая экспертиза баз данных
- 9.6.1. Судебная экспертиза MSSQL
- 9.6.2. Судебная экспертиза MySQL
- 9.6.3. Судебная экспертиза PostgreSQL
- 9.6.4. Судебная экспертиза MongoDB

9.7. Судебная экспертиза *облачного сервиса*
- 9.7.1. Виды преступлений в облаке
  - 9.7.1.1. Облако как субъект
  - 9.7.1.2. Облако как объект
  - 9.7.1.3. Облако как средство
- 9.7.2. Трудности судебной экспертизы в облаке
- 9.7.3. Исследование услуг по хранению данных в облаке
- 9.7.4. Средства проведения криминалистической экспертизы в облаке

9.8. Расследования преступлений, связанных с электронной почтой
- 9.8.1. Почтовые системы
  - 9.8.1.1. Почтовые клиенты
  - 9.8.1.2. Почтовые серверы
  - 9.8.1.3. Сервер SMTP
  - 9.8.1.4. Сервер POP3
  - 9.8.1.5. Сервер IMAP4
- 9.8.2. Преступления, связанные с электронной почтой
- 9.8.3. Сообщение на почте
  - 9.8.3.1. Стандартные заголовки
  - 9.8.3.2. Расширенные заголовки
- 9.8.4. Шаги по расследованию этих преступлений
- 9.8.5. Средства криминалистической экспертизы электронной почты

9.9. Судебная экспертиза мобильных устройств
- 9.9.1. Сотовые сети
  - 9.9.1.1. Виды сетей
  - 9.9.1.2. Содержимое хранилища клинических данных
- 9.9.2. *Модуль идентификации абонента* (SIM)
- 9.9.3. Логическое получение
- 9.9.4. Физическое получение
- 9.9.5. Получение файловой системы

9.10. Составление и представление отчетов о судебной экспертизе
- 9.10.1. Важные аспекты заключения судебной экспертизы
- 9.10.2. Классификация и виды отчетов
- 9.10.3. Руководство по написанию отчета
- 9.10.4. Презентация отчета
  - 9.10.4.1. Предварительная подготовка к даче показаний
  - 9.10.4.2. Изложение
  - 9.10.4.3. Общение с прессой

Модуль 10. Текущие и будущие проблемы в области кибербезопасности

10.1. Технология *блокчейна*
- 10.1.1. Области применения
- 10.1.2. Гарантия конфиденциальности
- 10.1.3. Гарантия отсутствия отказа от претензий

10.2. Цифровая валюта
- 10.2.1. Биткойны
- 10.2.2. Криптомонеты
- 10.2.3. Майнинг криптовалюты
- 10.2.4. Пирамидальные схемы
- 10.2.5. Другие потенциальные преступления и проблемы

10.3. *Дипфейк*
- 10.3.1. Влияние СМИ
- 10.3.2. Опасность для общества
- 10.3.3. Механизмы обнаружения

10.4. Будущее искусственного интеллекта
- 10.4.1. Искусственный интеллект и когнитивные вычисления
- 10.4.2. Применение в упрощении обслуживания клиентов

10.5. Цифровая конфиденциальность
- 10.5.1. Ценность данных в сети
- 10.5.2. Использование данных в сети
- 10.5.3. Конфиденциальность и управление цифровой идентичностью

10.6. Киберконфликты, киберпреступники и кибератаки
- 10.6.1. Влияние кибербезопасности на международные конфликты
- 10.6.2. Последствия кибератак для населения в целом
- 10.6.3. Виды киберпреступников. Защитные мероприятия

10.7. Удаленная работа
- 10.7.1. Революция дистанционной работы во время и после Covid19
- 10.7.2. Узкие места при доступе
- 10.7.3. Изменение площади атаки
- 10.7.4. Потребности работников

10.8. Новые *беспроводные технологии*
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Миллиметровые волны
- 10.8.4. Тенденция Get Smart вместо *Get more*

10.9. Будущая адресация в сетях
- 10.9.1. Актуальные проблемы IP-адресации
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Преимущества IPv4+ в сравнении с IPv4
- 10.9.5. Преимущества IPv6 в сравнении с IPv4

10.10. Задача повышения осведомленности населения о своевременном и непрерывном образовании
- 10.10.1. Текущие стратегии правительства
- 10.10.2. Сопротивляемость населения обучению
- 10.10.3. Планы обучения, которые должны быть внедрены компаниями

Модуль 11. Лидерство, этика и корпоративная социальная ответственность

11.1. Глобализация и руководство
- 11.1.1. Руководство и корпоративное управление
- 11.1.2. Основы корпоративного управления в компаниях
- 11.1.3. Роль совета директоров в рамках корпоративного управления

11.2. Лидерство
- 11.2.1. Лидерство. Концептуальный подход
- 11.2.2. Лидерство в бизнесе
- 11.2.3. Значение лидера в управлении бизнесом

11.3. *Кросс-культурный менеджмент*
- 11.3.1. Концепция *кросс-культурного менеджмента*
- 11.3.2. Вклад в познание национальных культур
- 11.3.3. Управление разнообразием

11.4. Развитие менеджмента и лидерства
- 11.4.1. Концепция развития менеджмента
- 11.4.2. Концепция лидерства
- 11.4.3. Теории лидерства
- 11.4.4. Стили лидерства
- 11.4.5. Интеллект в лидерстве
- 11.4.6. Проблемы лидерства сегодня

11.5. Деловая этика
- 11.5.1. Этика и мораль
- 11.5.2. Деловая этика
- 11.5.3. Лидерство и этика в компаниях

11.6. Устойчивость
- 11.6.1. Устойчивость и устойчивое развитие
- 11.6.2. Повестка дня на 2030 год
- 11.6.3. Устойчивые предприятия

11.7. Корпоративная социальная ответственность
- 11.7.1. Международное измерение корпоративной социальной ответственности
- 11.7.2. Реализация корпоративной социальной ответственности
- 11.7.3. Влияние и измерение корпоративной социальной ответственности

11.8. Системы и инструменты ответственного управления
- 11.8.1. КСО: Корпоративная социальная ответственность
- 11.8.2. Ключевые вопросы реализации стратегии ответственного управления
- 11.8.3. Шаги по внедрению системы управления корпоративной социальной ответственностью
- 11.8.4. Инструменты и стандарты КСО

11.9. Транснациональные компании и права человека
- 11.9.1. Глобализация, многонациональные компании и права человека
- 11.9.2. Транснациональные компании и международное право
- 11.9.3. Правовые инструменты для транснациональных корпораций в области прав человека

11.10. Правовое регулирование и *корпоративное управление*
- 11.10.1. Международные стандарты импорта и экспорта
- 11.10.2. Интеллектуальная и промышленная собственность
- 11.10.3. Международное трудовое право

Модуль 12. Управление персоналом и талантами

12.1. Стратегическое управление персоналом
- 12.1.1. Стратегическое управление и человеческие ресурсы
- 12.1.2. Стратегическое управление персоналом

12.2. Управление человеческими ресурсами на основе компетенций
- 12.2.1. Анализ потенциала
- 12.2.2. Политика вознаграждения
- 12.2.3. Планирование карьеры/повышения

12.3. Оценка производительности и управление эффективностью
- 12.3.1. Управление производительностью
- 12.3.2. Управление эффективностью: цели и процесс

12.4. Инновации в управлении талантами и людьми
- 12.4.1. Модели стратегического управления талантами
- 12.4.2. Выявление, обучение и развитие талантов
- 12.4.3. Лояльность и удержание
- 12.4.4. Проактивность и инновации

12.5. Воля
- 12.5.1. Природа мотивации
- 12.5.2. Теория ожиданий
- 12.5.3. Теории потребностей
- 12.5.4. Мотивация и финансовое вознаграждение

12.6. Развитие высокоэффективных команд
- 12.6.1. Высокоэффективные команды: самоуправляемые команды
- 12.6.2. Методики управления высокоэффективными самоуправляемыми командами

12.7. Управление изменениями
- 12.7.1. Управление изменениями
- 12.7.2. Тип процессов управления изменениями
- 12.7.3. Этапы или фазы управления изменениями

12.8. Переговоры и управление конфликтами
- 12.8.1. Переговоры
- 12.8.2. Управление конфликтами
- 12.8.3. Антикризисное управление

12.9. Управленческая коммуникация
- 12.9.1. Внутренняя и внешняя коммуникация в бизнесе
- 12.9.2. Департаменты коммуникации
- 12.9.3. Менеджер по связям с общественностью компании. Профиль менеджера по коммуникациям

12.10. Производительность, привлечение, удержание и активизация талантов
- 12.10.1. Производительность
- 12.10.2. Рычаги привлечения и удержания талантов

Модуль 13. Финансово-экономическое управление

13.1. Экономическая среда
- 13.1.1. Макроэкономическая среда и внутренняя финансовая система
- 13.1.2. Финансовые учреждения
- 13.1.3. Финансовые рынки
- 13.1.4. Финансовые активы
- 13.1.5. Прочие организации финансового сектора

13.2. Управленческий учет
- 13.2.1. Основные понятия
- 13.2.2. Активы компании
- 13.2.3. Обязательства компании
- 13.2.4. Чистая стоимость компании
- 13.2.5. Счет прибылей и убытков

13.3. Информационные системы и *бизнес-аналитика*
- 13.3.1. Основы и классификация
- 13.3.2. Этапы и методы распределения затрат
- 13.3.3. Выбор центра затрат и эффекта

13.4. Бюджет и управленческий контроль
- 13.4.1. Модель бюджета
- 13.4.2. Капитальный бюджет
- 13.4.3. Операционный бюджет
- 13.4.5. Бюджет казначейства
- 13.4.6. Мониторинг бюджета

13.5. Финансовый менеджмент
- 13.5.1. Финансовые решения компании
- 13.5.2. Финансовый отдел
- 13.5.3. Денежные излишки
- 13.5.4. Риски, связанные с управлением финансами
- 13.5.5. Управление рисками в финансовом менеджменте

13.6. Финансовое планирование
- 13.6.1. Определение финансового планирования
- 13.6.2. Действия, которые необходимо предпринять при финансовом планировании
- 13.6.3. Создание и разработка бизнес-стратегии
- 13.6.4. Таблица *движения денежных средств*
- 13.6.5. Таблица оборотных активов

13.7. Корпоративная финансовая стратегия
- 13.7.1. Корпоративная стратегия и источники финансирования
- 13.7.2. Продукты корпоративного финансирования

13.8. Стратегическое финансирование
- 13.8.1. Самофинансирование
- 13.8.2. Увеличение собственных средств
- 13.8.3. Гибридные ресурсы
- 13.8.4. Финансирование через посредников

13.9. Финансовый анализ и планирование
- 13.9.1. Анализ бухгалтерского баланса
- 13.9.2. Анализ отчета о прибылях и убытках
- 13.9.3. Анализ рентабельности

13.10. Анализ и решение кейсов/проблем
- 13.10.1. Финансовая информация о компании Industria de Diseño y Textil, S.A. (INDITEX)

Модуль 14. Коммерческий менеджмент и стратегический маркетинг

14.1. Управление продажами
- 14.1.1. Концептуальные основы управления бизнесом
- 14.1.2. Коммерческая стратегия и планирование
- 14.1.3. Роль коммерческих менеджеров

14.2. Маркетинг
- 14.2.1. Концепция маркетинга
- 14.2.2. Основы маркетинга
- 14.2.3. Маркетинговая деятельность компании

14.3. Управление стратегическим маркетингом
- 14.3.1. Концепция стратегического маркетинга
- 14.3.2. Концепция стратегического маркетингового планирования
- 14.3.3. Этапы процесса стратегического маркетингового планирования

14.4. Цифровой маркетинг и электронная коммерция
- 14.4.1. Цели цифрового маркетинга и электронной коммерции
- 14.4.2. Цифровой маркетинг и средства массовой информации, которые он использует
- 14.4.3. Электронная коммерция. Общий контекст
- 14.4.4. Категории электронной коммерции
- 14.4.5. Преимущества и недостатки *электронной коммерции* по сравнению с традиционной торговлей

14.5. Цифровой маркетинг для укрепления бренда
- 14.5.1. Онлайн-стратегии для улучшения репутации вашего бренда
- 14.5.2. *Брендированный контент* и *сторителлинг*

14.6. Цифровой маркетинг для привлечения и удержания клиентов
- 14.6.1. Стратегии лояльности и вовлечения через интернет
- 14.6.2. *Управление взаимоотношениями с посетителями*
- 14.6.3. Гиперсегментация

14.7. Управление цифровыми кампаниями
- 14.7.1. Что такое цифровая рекламная кампания?
- 14.7.2. Шаги по запуску маркетинговой кампании в Интернете
- 14.7.3. Ошибки при проведении цифровых рекламных кампаний

14.8. Стратегия продаж
- 14.8.1. Стратегия продаж
- 14.8.2. Методы продаж

14.9. Корпоративная коммуникация
- 14.9.1. Понятие
- 14.9.2. Важность коммуникации в организации
- 14.9.3. Тип коммуникации в организации
- 14.9.4. Функции коммуникации в организации
- 14.9.5. Элементы коммуникации
- 14.9.6. Проблемы коммуникации
- 14.9.7. Сценарии коммуникации

14.10. Коммуникация и цифровая репутация
- 14.10.1. Онлайн-репутация
- 14.10.2. Как измерить цифровую репутацию?
- 14.10.3. Инструменты для создания онлайн-репутации
- 14.10.4. Отчет о репутации в Интернете
- 14.10.5. *Брендинг* онлайн

Модуль 15. *Управленческий* менеджмент

15.1. Общий менеджмент
- 15.1.1. Концепция общего менеджмента
- 15.1.2. Действия генерального директора
- 15.1.3. Генеральный директор и его функции
- 15.1.4. Трансформация работы менеджмента

15.2. Менеджер и его функции. Организационная культура и подходы к ней
- 15.2.1. Менеджер и его функции. Организационная культура и подходы к ней

15.3. Управление операциями
- 15.3.1. Важность управления
- 15.3.2. Цепочка создания стоимости
- 15.3.3. Управление качеством

15.4. Публичные выступления и тренинги для пресс-секретарей
- 15.4.1. Межличностная коммуникация
- 15.4.2. Коммуникативные навыки и влияние
- 15.4.3. Барьеры коммуникации

15.5. Средства личной и организационной коммуникации
- 15.5.1. Межличностная коммуникация
- 15.5.2. Инструменты межличностной коммуникации
- 15.5.3. Коммуникация в организации
- 15.5.4. Инструменты в организации

15.6. Кризисная коммуникация
- 15.6.1. Кризис
- 15.6.2. Фазы кризиса
- 15.6.3. Сообщения: содержание и моменты

15.7. Подготовка кризисного плана
- 15.7.1. Анализ потенциальных проблем
- 15.7.2. Планирование
- 15.7.3. Адекватность персонала

15.8. Эмоциональный интеллект
- 15.8.1. Эмоциональный интеллект и коммуникация
- 15.8.2. Ассертивность, эмпатия и активное слушание
- 15.8.3. Самооценка и эмоциональная коммуникация

15.9. Личный *брендинг*
- 15.9.1. Стратегии личного брендинга
- 15.9.2. Законы личного брендинга
- 15.9.3. Инструменты для создания личного бренда

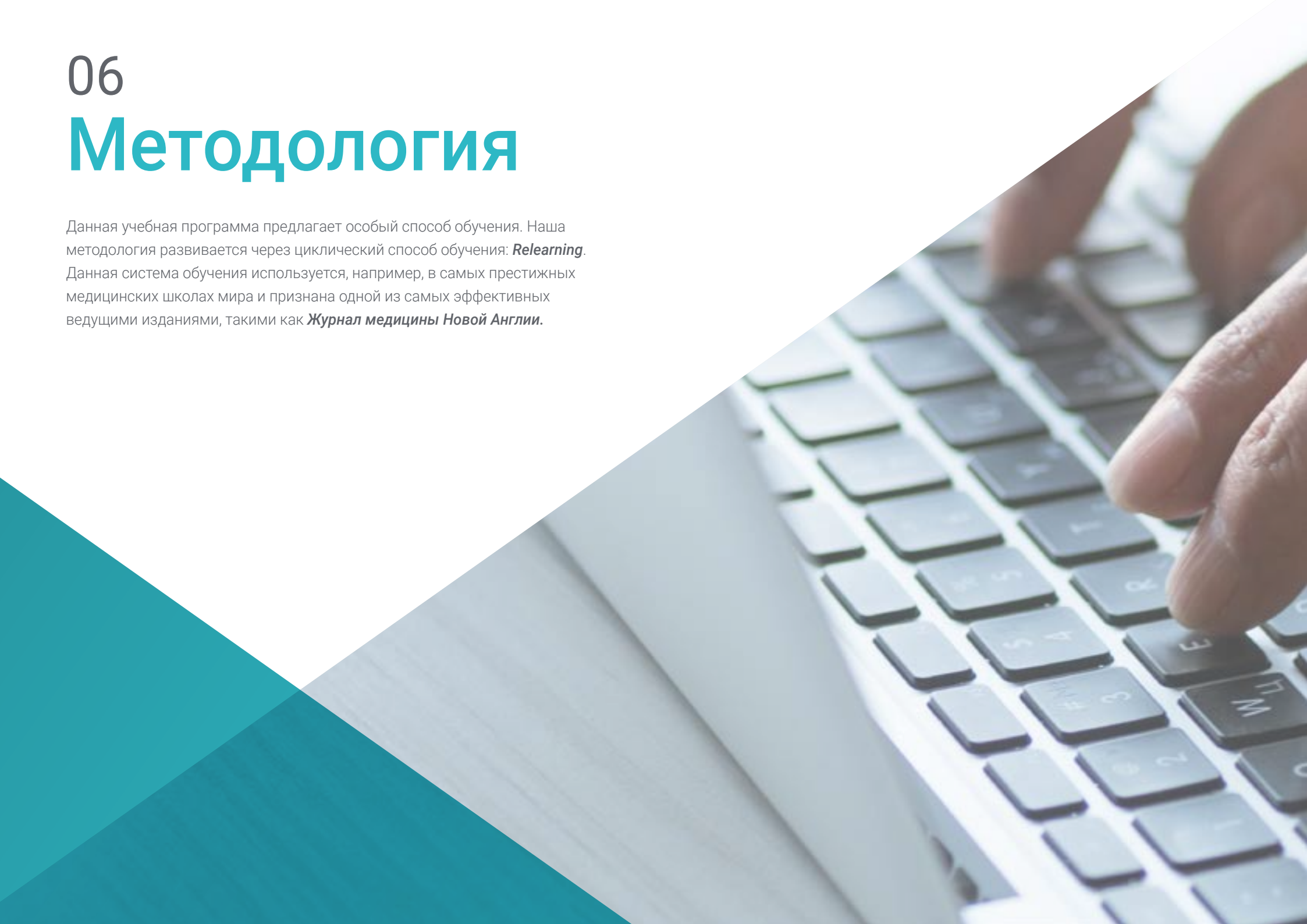
15.10. Лидерство и управление командой
- 15.10.1. Лидерство и стили лидерства
- 15.10.2. Возможности и проблемы лидеров
- 15.10.3. Управление процессами изменений
- 15.10.4. Управление мультикультурными командами

Ваше будущее начинается здесь. Поступайте сегодня и станьте главным информационным директором крупных компаний"

06

Методология

Данная учебная программа предлагает особый способ обучения. Наша методология развивается через циклический способ 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 циклический подход: способ, который доказал свою эффективность, особенно в предметах, требующих запоминания”

Метод кейс-стади предназначен 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.

В TECH вы сможете познакомиться со способом обучения, который опровергает основы традиционных методов, применяемых в университетах по всему миру.

Вы получите доступ к системе обучения, основанной на повторении, с естественным и прогрессивным обучением по всему учебному плану.

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

Инновационный и отличный от других метод обучения

Данная программа TECH — это интенсивная программа обучения, созданная с нуля, которая предлагает самые сложные задачи и решения в этой области на международном уровне. Благодаря этой методологии ускоряется личностный и профессиональный рост, что позволяет сделать решающий шаг на пути к успеху. Метод кейс-стади, составляющий основу данного содержания, обеспечивает соответствие самым современным экономическим, социальным и профессиональным реалиям.

> *Наша программа готовит вас к решению новых задач в условиях неопределенности и достижению успеха в карьере"*

Кейс-метод является наиболее широко используемой системой обучения лучшими преподавателями в мире. Разработанный в 1912 году для того, чтобы студенты-юристы могли изучать право не только на основе теоретического содержания, метод кейс-стади заключается в том, что учащимся 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 кейс-стади — метода обучения, ориентированного на действие. На протяжении всей курса 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*

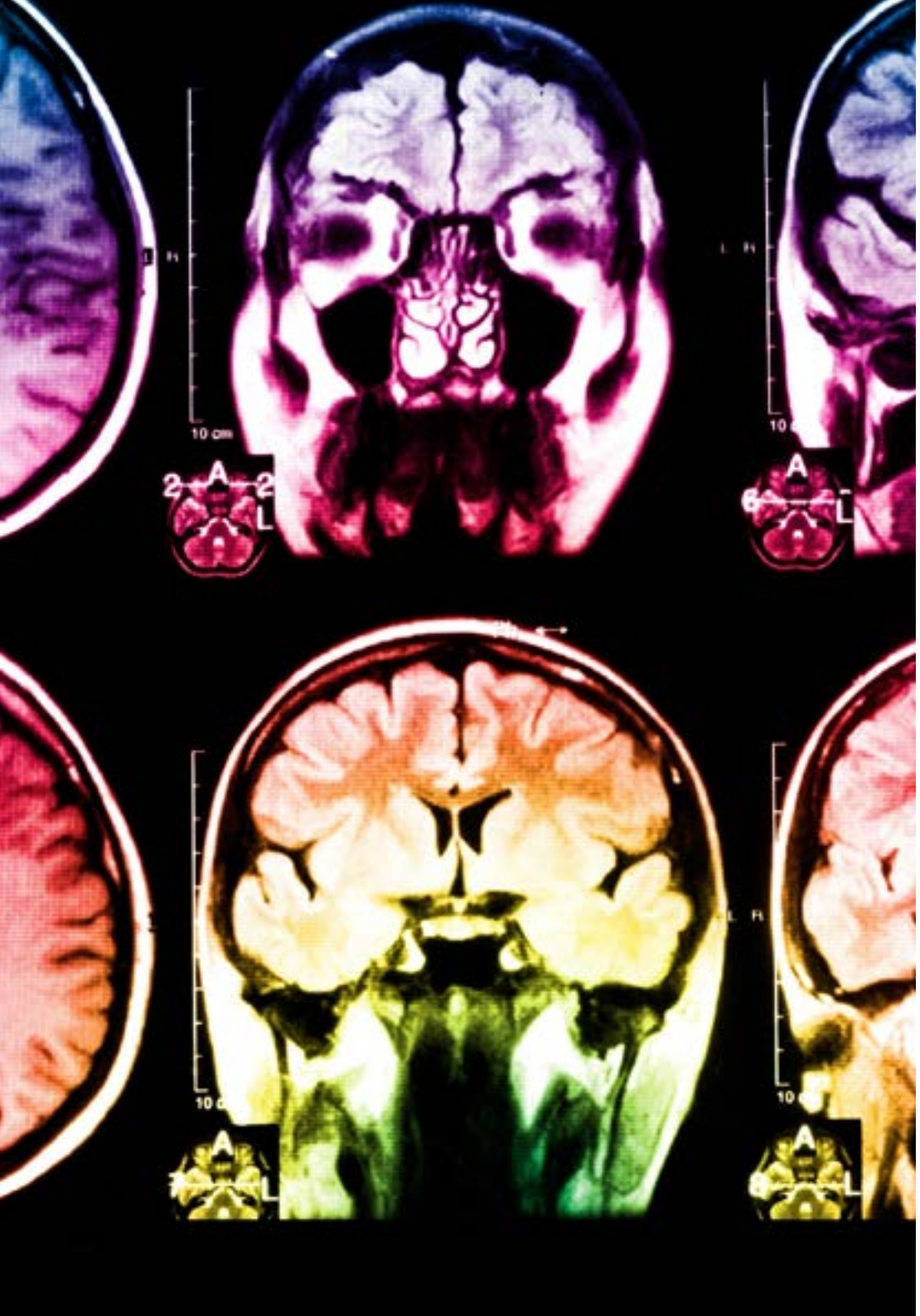
TECH эффективно объединяет метод кейс-стади с системой 100% онлайн-обучения, основанной на повторении, которая сочетает различные дидактические элементы в каждом уроке.

Мы улучшаем методику кейс-стади с помощью лучшего метода 100% онлайн-обучения: *Relearning*.

В 2019 году мы достигли лучших результатов обучения среди всех испаноязычных онлайн-университетов мира.

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

Наш университет — 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 испаноязычного 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, инженерия, журналистика, история, финансовые рынки и инструменты. Наша методология преподавания разработана в среде с высокими требованиями к уровню подготовки, с университетским контингентом студентов с социально-экономическим уровнем выше среднего 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 получите 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.

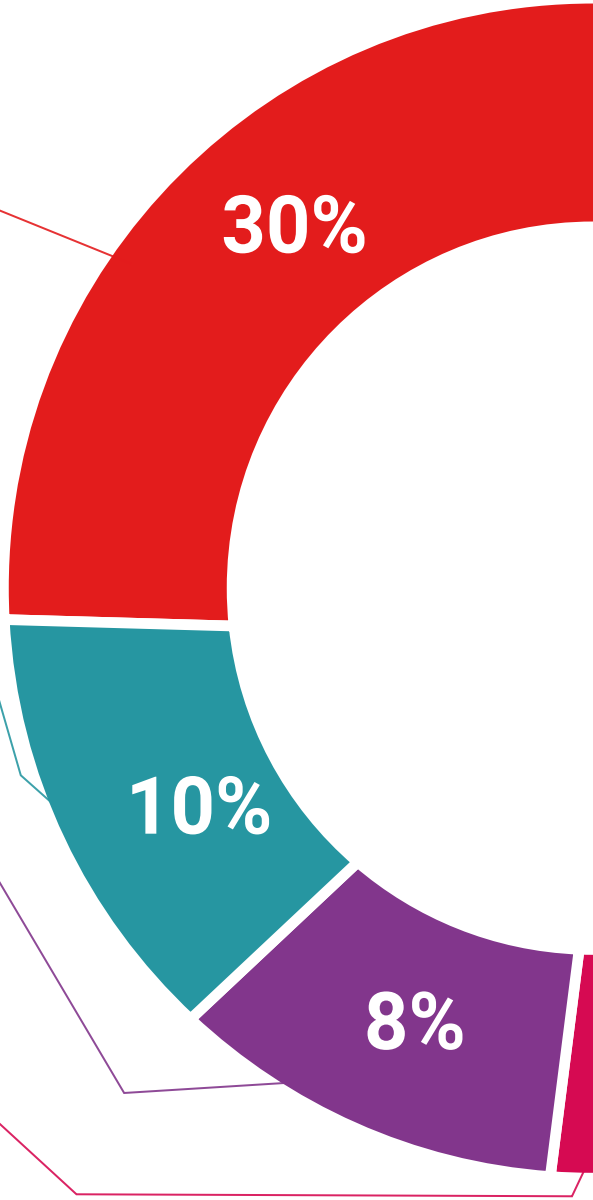
Так называемый метод обучения у эксперта укрепляет знания и память, а также формирует уверенность в принятии будущих сложных решений.

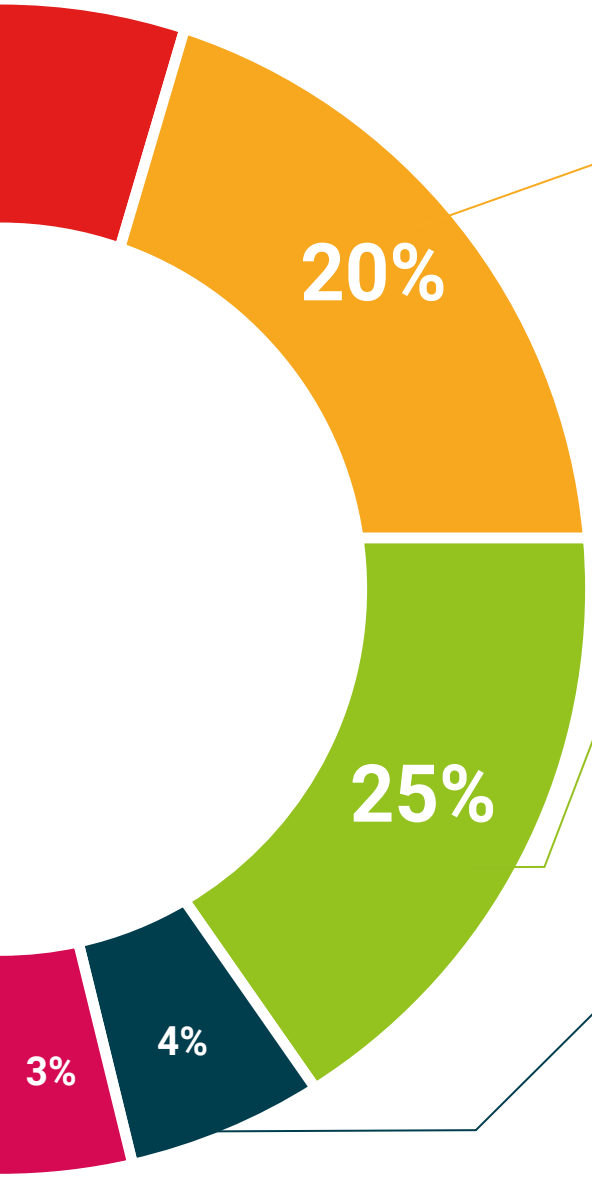
Практика навыков и компетенций

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.

Дополнительная литература

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





Метод кейс-стади

Метод дополняется подборкой лучших кейсов, выбранных специально для этой специальности. Кейсы представляются, анализируются и преподаются лучшими специалистами на международной арене.

Интерактивные конспекты

Мы представляем содержание в привлекательной и динамичной мультимедийной форме, которая включает в себя 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 самопроверочных упражнений: так вы сможете убедиться, что достигаете поставленных целей.

07

Квалификация

Специализированная магистратура в области MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer) гарантирует, помимо самого строгого и современного обучения, получение диплома об окончании Специализированной магистратуры, выдаваемого TECH Технологическим университетом.

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

Данная **Специализированная магистратура в области MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)** содержит самую полную и современную программу на рынке.

После прохождения аттестации студент получит по почте* с подтверждением получения соответствующий диплом **Специализированной магистратуры,** выданный **TECH Технологическим университетом.**

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

Диплом: **Специализированная магистратура в области MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)**

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

СПЕЦИАЛИЗИРОВАННАЯ МАГИСТРАТУРА

в области

MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)

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


Специализированная магистратура в области MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)

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
1°	Кибеpразведка и кибербезопасность	100	Обязат
1°	Безопасность хоста	100	Обязат
1°	Сетевая безопасность (периметр)	100	Обязат
1°	Безопасность смартфонов	100	Обязат
1°	Безопасность в IoT	100	Обязат
1°	Этичный хакинг	100	Обязат
1°	Реверс-инжиниринг	100	Обязат
1°	Безопасная разработка	100	Обязат
1°	Судебная экспертиза	100	Обязат
1°	Текущие и будущие проблемы в области кибербезопасности	100	Обязат
1°	Лидерство, этика и корпоративная социальная ответственность	100	Обязат
1°	Управление персоналом и талантами	100	Обязат
1°	Финансово-экономическое управление	100	Обязат
1°	Коммерческий менеджмент и стратегический маркетинг	100	Обязат
1°	Управленческий менеджмент	100	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.

tech технологический университет

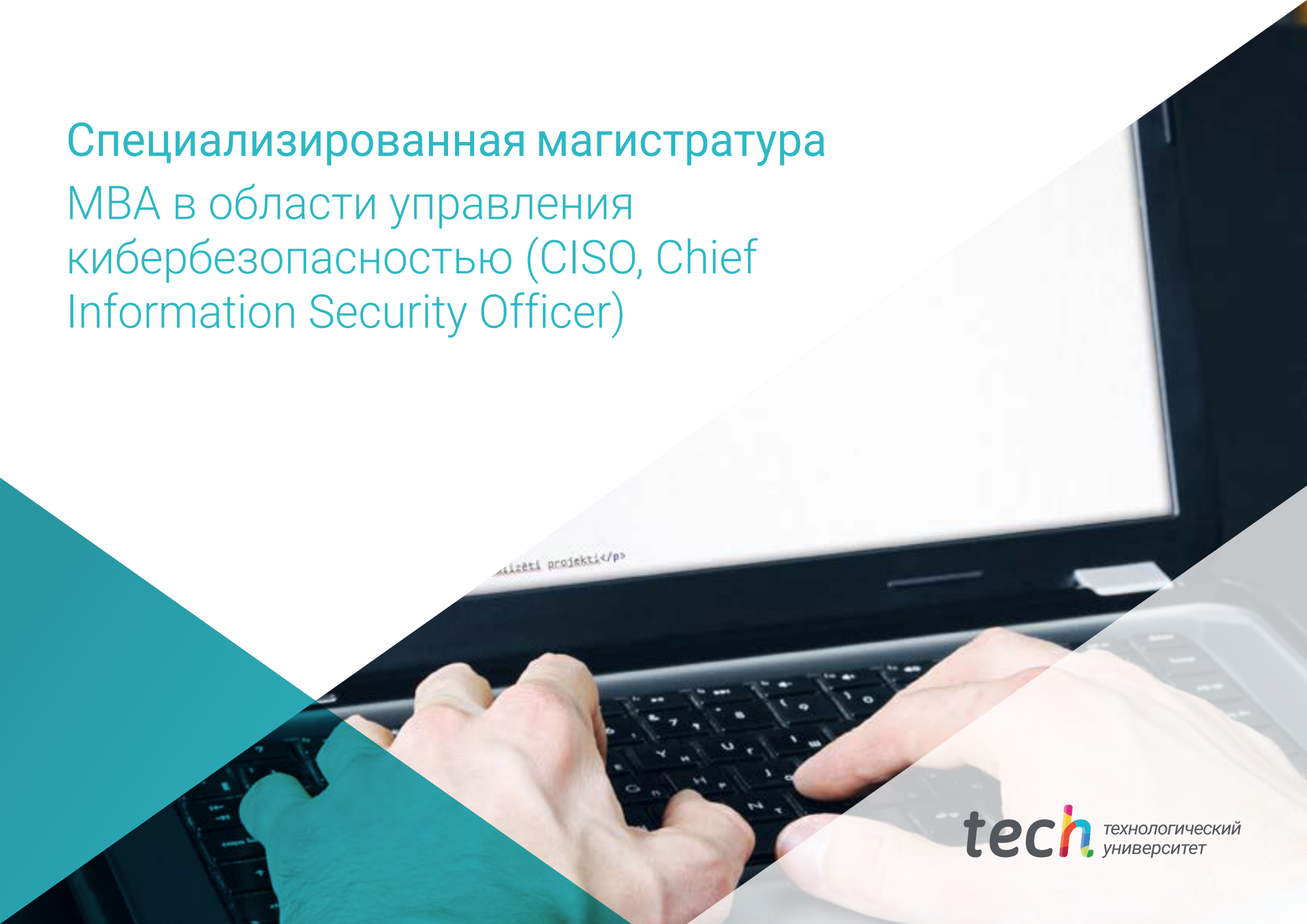
Специализированная магистратура

MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)

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

Специализированная магистратура

MBA в области управления кибербезопасностью (CISO, Chief Information Security Officer)



tech технологический университет