# Специализированная магистратура

## MBA в области управления усовершенствованной кибербезопасностью (CISO)

tech технологический университет

tech технологический университет

# Специализированная магистратура

## MBA в области управления усовершенствованной кибербезопасностью (CISO)

- 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-advanced-cybersecurity-management**

# Оглавление

01

# Презентация

Современный мир движется в сторону полной дигитализации. Все больше базовых процессов, операций и задач разного рода выполняются с помощью электронных устройств. Но этот прогресс также сопровождается определенными рисками, поскольку компьютеры, *смартфоны*,, *планшеты* и всевозможные цифровые приложения могут быть подвержены кибератакам. По этой причине многие компании ищут специалистов, способных эффективно руководить и управлять кибербезопасностью своих услуг. Этот новый профессиональный профиль пользуется большим спросом, поэтому данная программа была разработана для предоставления новейших знаний и методик специалисту в области компьютерных технологий, который будет готов стать директором по кибербезопасности в любой компании, где это требуется.

*Данная программа интенсивно подготовит вас к специализации в области управления кибербезопасностью — наиболее востребованной сегодня профессии в сфере информатики"*

В последние годы процесс дигитализации ускорился благодаря постоянному прогрессу в области информационных технологий. Таким образом, не только технологии претерпели значительные улучшения, но также и сами цифровые инструменты, с помощью которых сегодня выполняются многие задачи. Например, благодаря этим разработкам многие банковские операции можно осуществлять с помощью мобильного приложения. Также произошли изменения в секторе здравоохранения, в системах записи на прием к врачу и в доступе к медицинской документации. Кроме того, благодаря этим технологиям можно ознакомиться со счетами или запросить услуги у компаний в таких областях, как телефония.

Однако, эти достижения также привели к росту уязвимости компьютеров. Таким образом, несмотря на расширение возможностей для выполнения различных действий и задач, пропорционально увеличилось количество атак на безопасность устройств, приложений и веб-сайтов. В результате все больше компаний ищут специалистов по кибербезопасности, способных обеспечить им надлежащую защиту от всех видов кибератак.

Таким образом, профиль директора по кибербезопасности является одним из самых востребованных среди компаний, которые работают в Интернете или оказывают услуги в цифровой среде. И для удовлетворения данного спроса, TECH разработал данную MBA в области управления усовершенствованной кибербезопасностью (CISO), которая предоставит специалисту в области компьютерных технологий все необходимые инструменты для эффективной работы на этой должности с учетом последних разработок в области защиты и уязвимостей в этой технологической области.

В рамках этой программы вы сможете углубленно изучить такие аспекты, как безопасность при разработке и проектировании систем, лучшие криптографические методы и безопасность в средах облачных вычислений. Для этого вы будете использовать 100% онлайн-методику, которая позволит вам совмещать вашу профессиональную деятельность с учебой, без строгого расписания и неудобных поездок в образовательный центр. Вы также сможете воспользоваться многочисленными мультимедийными учебными ресурсами, которые преподают самые престижные и специализированные преподаватели в области кибербезопасности.

Данная программа **Специализированная магистратура в области MBA в области управления усовершенствованной кибербезопасностью (CISO)** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных экспертами в области информатики и 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 самопроверки, контроля и улучшения успеваемости
- Особое внимание уделяется инновационным методологиям
- Теоретические занятия, вопросы эксперту, дискуссионные форумы по спорным темам и самостоятельная работа
- Учебные материалы курса доступны с любого стационарного или мобильного устройства с выходом в интернет

*Узнайте из первых рук о лучших методах обеспечения безопасности, применяемых в средах облачных вычислений или технологии блокчейн"*

*Вы сможете воспользоваться многочисленными мультимедийными материалами для ускорения процесса обучения, получая при этом поддержку высокопрестижного преподавательского состава в области кибербезопасности"*

*Онлайн-методология TECH позволит вам выбрать время и место для занятий, не мешая вашей профессиональной деятельности.*

*Вы сможете стать директором по кибербезопасности в лучших компаниях вашего региона.*

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

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

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

02

# Цели

Стремительное развитие информационных технологий принесло большие успехи, предоставляя многочисленные услуги широким слоям населения. Однако количество уязвимостей и кибератак также возросло, поэтому основная цель данной программы — превратить специалиста по информационным технологиям в настоящего специалиста по управлению кибербезопасностью, гарантируя огромный и немедленный профессиональный прогресс. Ваши новые навыки дадут вам возможность получить доступ к крупным компаниям, которые активно используют цифровые технологии в различных отраслях.

*Цель данной программы — сделать из вас профессионала, готового возглавить отдел кибербезопасности крупной компании"*

## Общие цели

- Сформировать специализированные знания об информационной системе, типах и аспектах безопасности, которые необходимо учитывать
- Выявлять уязвимости в информационных системах
- Разрабатывать базу для правового регулирования и криминализации преступлений, связанных с атаками на информационные системы
- Оценивать различные модели архитектуры безопасности, чтобы определять наиболее подходящую модель для организации
- Определять применимые нормативно-правовые акты и нормативную базу для них
- Анализировать организационную и функциональную структуру в области информационной безопасности (офис CISO)
- Анализировать и развивать концепцию риска, неопределенности в среде, в которой мы живем
- Изучить модель управления рисками на основе ISO 31.000
- Изучить науку криптологию и ее связь с отраслями: криптографией, криптоанализом, стеганографией и стегоанализом
- Проанализировать виды криптографии в соответствии с видом алгоритма и его использованием
- Изучить цифровые сертификаты
- Изучить инфраструктуру открытых ключей (PKI)
- Разработать концепцию управления идентификацией
- Определять методы аутентификации
- Генерировать специализированные знания об экосистеме ИТ-безопасности
- Оценивать знания в области кибербезопасности
- Определять сферы безопасности в *облачных сервисах*
- Провести анализ услуг и инструментов в каждом из областей безопасности
- Разрабатывать спецификации безопасности для каждой технологии LPWAN
- Провести сравнительный анализ безопасности технологий LPWAN

*Ваши профессиональные цели теперь в пределах досягаемости благодаря данной Специализированной магистратуре, которая предлагает самые передовые знания в области кибербезопасности"*



## Конкретные цели

### Модуль 1. Безопасность при проектировании и разработке систем

- Оценивать безопасность информационной системы во всех ее компонентах и слоях
- Определять виды современных угроз безопасности и тенденции их развития
- Устанавливать руководящие принципы безопасности, определив политику и планы безопасности и действий в чрезвычайных ситуациях
- Анализировать стратегии и инструменты для обеспечения целостности и безопасности информационных систем
- Применять конкретные методы и инструменты для каждого вида атак или уязвимостей безопасности
- Защищать конфиденциальную информацию, хранящуюся в информационной системе
- Иметь правовую базу и типизацию преступлений, дополняя ее типизацией преступника и его жертвы

### Модуль 2. Архитектуры и модели информационной безопасности

- Согласовывать генеральный план безопасности со стратегическими целями организации
- Создать систему непрерывного управления рисками как неотъемлемую часть генерального плана безопасности
- Определять соответствующие показатели для мониторинга внедрения системы менеджмента информационной безопасности (СМИБ)
- Создавать стратегию безопасности на основе политики
- Проанализировать цели и процедуры, связанные с планом повышения осведомленности сотрудников, поставщиков и партнеров
- Определять в рамках нормативно-правовой базы нормативные акты, сертификаты и законы, применимые к каждой организации
- Разрабатывать фундаментальные элементы, требуемые стандартом ISO 27001:2013
- Внедрять модель управления конфиденциальностью в соответствии с европейским регламентом GDPR

### Модуль 3. Управление информационной безопасностью

- Определять различные структуры, которые может иметь область информационной безопасности
- Разрабатывать модель безопасности на основе трех линий защиты
- Представлять различные регулярные и чрезвычайные комитеты, в которых участвует область кибербезопасности
- Указать технологические инструменты, которые поддерживают основные функции группы операционной безопасности (SOC)
- Оценивать меры контроля уязвимостей, соответствующие каждому сценарию
- Разрабатывать структуру операций безопасности на основе NIST CSF
- Определять объем различных видов аудита (*Red Team*, *Pentesting*, *Bug Bounty*, и т.д.)
- Предлагать мероприятия, которые должны быть проведены после инцидента, связанного с информационной безопасностью
- Создавать командный центр информационной безопасности, охватывающий все соответствующие заинтересованные стороны (руководство, клиенты, поставщики и т.д.).

### Модуль 4. Анализ рисков и среды информационной безопасности

- Изучить с точки зрения комплексного подхода окружающую среду, в которой мы живем
- Определить основные риски и возможности, которые могут повлиять на достижение наших целей
- Анализировать риски на основе лучших и доступных методов
- Проводить оценку потенциального влияния этих рисков и возможностей
- Разрабатывать методы работы с рисками и возможностями таким образом, чтобы максимизировать выгоду
- Изучить углубленно различные методы передачи риска, а также передачи стоимости
- Получать прибыль от разработки собственных моделей для гибкого управления рисками
- Анализировать результаты, чтобы предлагать постоянные улучшения в управлении проектами и процессами на основе риск-ориентированных моделей управления
- Внедрять инновации и преобразовывать общие данные в актуальную информацию для принятия решений на основе рисков

### Модуль 5. Криптография в ИТ

- Составлять фундаментальные операции (XOR, большие числа, подстановка и транспонирование) и различные компоненты (односторонние функции, хэш, генераторы случайных чисел)
- Анализировать криптографические методы
- Разрабатывать различные криптографические алгоритмы
- Демонстрировать использование цифровых подписей и их применение в цифровых сертификатах
- Оценивать системы управления ключами и важность длины криптографических ключей
- Изучить алгоритмы получения ключей
- Проанализировать жизненный цикл ключей
- Оценивать режимы работы блочного и потокового шифров
- Определять генераторы псевдослучайных чисел
- Разрабатывать реальные кейсы криптографических приложений, таких как Kerberos, PGP или смарт-карты
- Изучить соответствующие ассоциации и организации, такие как ISO, NIST или NCSC
- Определять задачи в криптографии квантовых вычислений

### Модуль 6. Управление идентификацией и доступом в ИТ-безопасности

- Разрабатывать концепцию цифровой идентификации
- Оценивать контроль физического доступа к информации
- Провести обоснование биометрической аутентификации и многофакторной аутентификации MFA
- Оценивать атаки, связанные с конфиденциальностью информации
- Анализировать федеративные удостоверения
- Устанавливать контроль за доступом к сети

### Модуль 7. Безопасность в сфере коммуникации и эксплуатации программного обеспечения

- Развивать знания в области физической и логической безопасности
- Демонстрировать знание коммуникаций и сетей
- Выявлять основные вредоносные атаки
- Создавать безопасную основу для разработки
- Демонстрировать знание основных положений системы управления информационной безопасностью
- Учреждать операционный центр в сфере кибербезопасности
- Демонстрировать важность практики кибербезопасности для организационных сбоев

### Модуль 8. Безопасность в облачных средах

- Определять риски развертывания инфраструктуры открытого *облачного* пространства
- Определять требования к безопасности
- Разрабатывать план безопасности для развертывания в *облачных сервисах*
- Определять облачные *сервисы,* которые необходимо развернуть для выполнения плана безопасности
- Определять необходимые оперативные меры для превентивных механизмов
- Устанавливать руководящие принципы для системы *ведения журнала* и мониторинга
- Предлагать действия по реагированию на инцидент

### Модуль 9. Безопасность коммуникаций устройств IoT

- Иметь представление об упрощенной архитектуре IoT
- Обосновывать различия между технологиями подключения общего назначения и технологиями подключения для IoT
- Разрабатывать концепцию "железного треугольника" для подключения IoT
- Анализировать спецификации безопасности технологии LoRaWAN, технологии NB-IoT и технологии WiSUN
- Обосновывать выбор правильной технологии IoT для каждого проекта

### Модуль 10. План по обеспечению непрерывности бизнеса, связанный с безопасностью

- Представлять ключевые элементы каждого этапа и анализировать характеристики плана обеспечения непрерывности бизнеса (ПНБ)
- Обосновывать необходимость ПНБ
- Определять карты успеха и риска для каждого этапа плана непрерывности бизнеса
- Определять, как составляется план действий по внедрению
- Оценивать полноценность плана обеспечения непрерывности бизнеса (ПНБ)
- Разрабатывать план успешной реализации плана непрерывности бизнеса

### 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

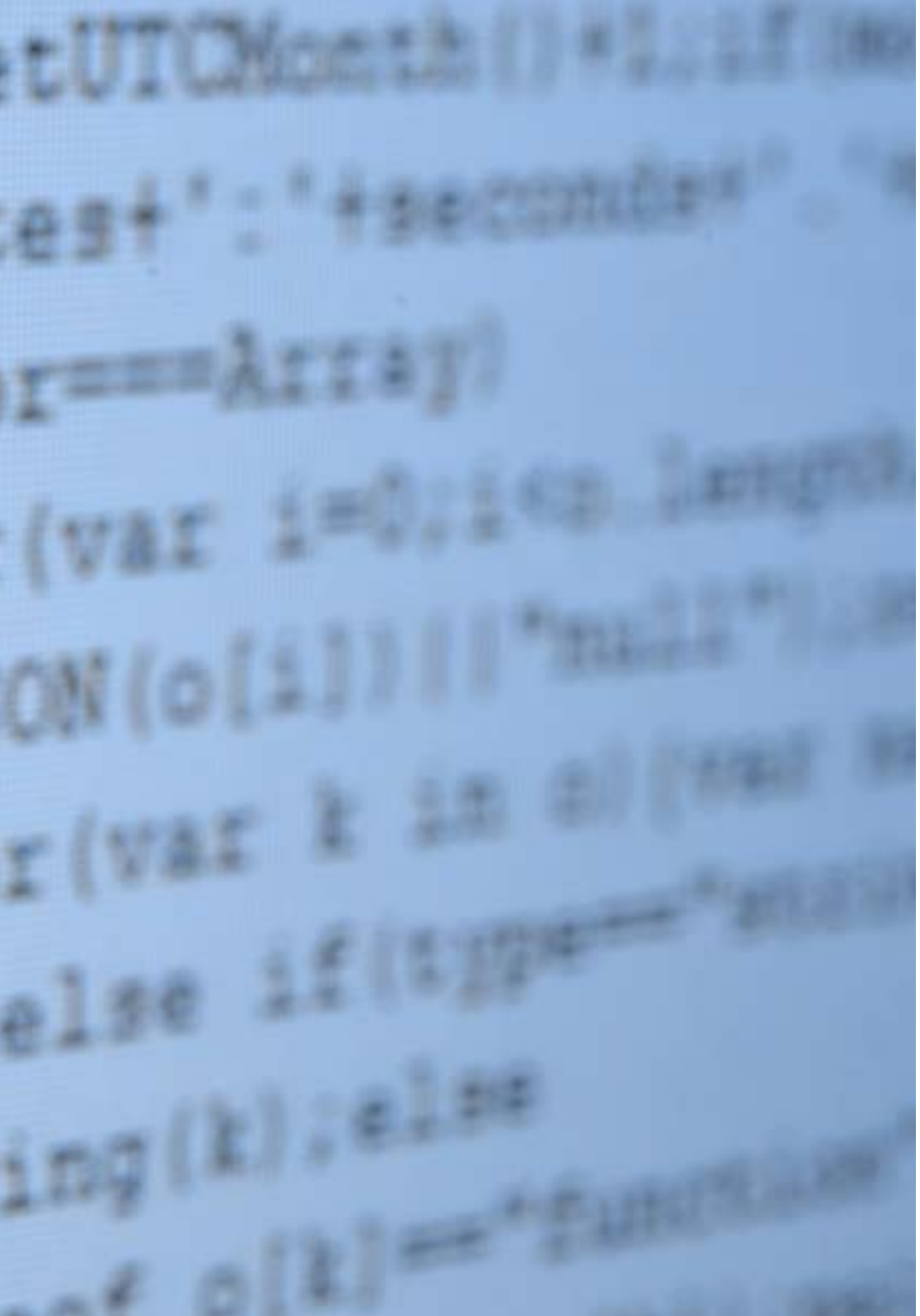
- Анализировать макроэкономическую среду и ее влияние на национальную и международную финансовую систему
- Определять информационные системы и бизнес-аналитику для принятия финансовых решений
- Различать ключевые финансовые решения и управление рисками в финансовом менеджменте
- Оценивать стратегии финансового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

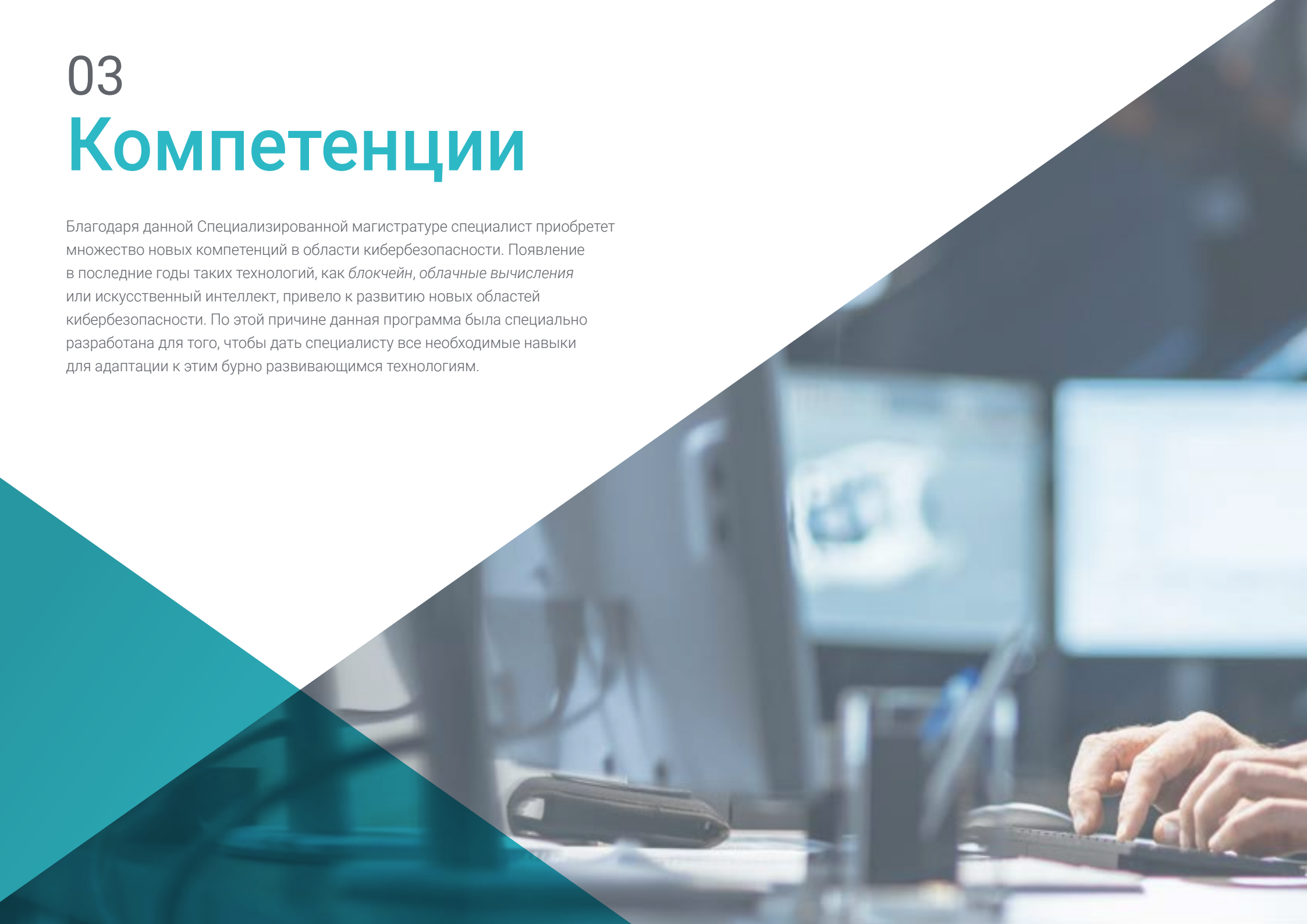


*Ваши профессиональные цели теперь в пределах досягаемости благодаря данной Специализированной магистратуре, которая предлагает самые передовые знания в области кибербезопасности"*

03

# Компетенции

Благодаря данной Специализированной магистратуре специалист приобретет множество новых компетенций в области кибербезопасности. Появление в последние годы таких технологий, как *блокчейн*, *облачные вычисления* или искусственный интеллект, привело к развитию новых областей кибербезопасности. По этой причине данная программа была специально разработана для того, чтобы дать специалисту все необходимые навыки для адаптации к этим бурно развивающимся технологиям.



*Компетенции, которые даст данная программа, позволят вам обновить и адаптироваться к новой ИТ-среде, где на сцену вырвались такие технологии, как блокчейн или искусственный интеллект"*

## Общие профессиональные навыки

- Применять наиболее подходящие меры безопасности в зависимости от конкретных видов угроз
- Определять политику и план безопасности информационной системы компании, завершая разработку и реализацию плана действий в чрезвычайных ситуациях
- Составить программу аудита, отвечающую потребностям самооценки кибербезопасности организации
- Разработать программу сканирования и мониторинга уязвимостей и план реагирования на инциденты кибербезопасности
- Использовать максимально представленные возможности и устранять все потенциальные риски, связанные с самим проектом
- Составлять системы управления ключами
- Оценивать информационную безопасность компании
- Анализировать систему доступа к информации
- Создавать передовой опыт в области безопасного развития
- Предоставлять информацию о возможных рисках для компаний, связанных с отсутствием среды ИТ-безопасности

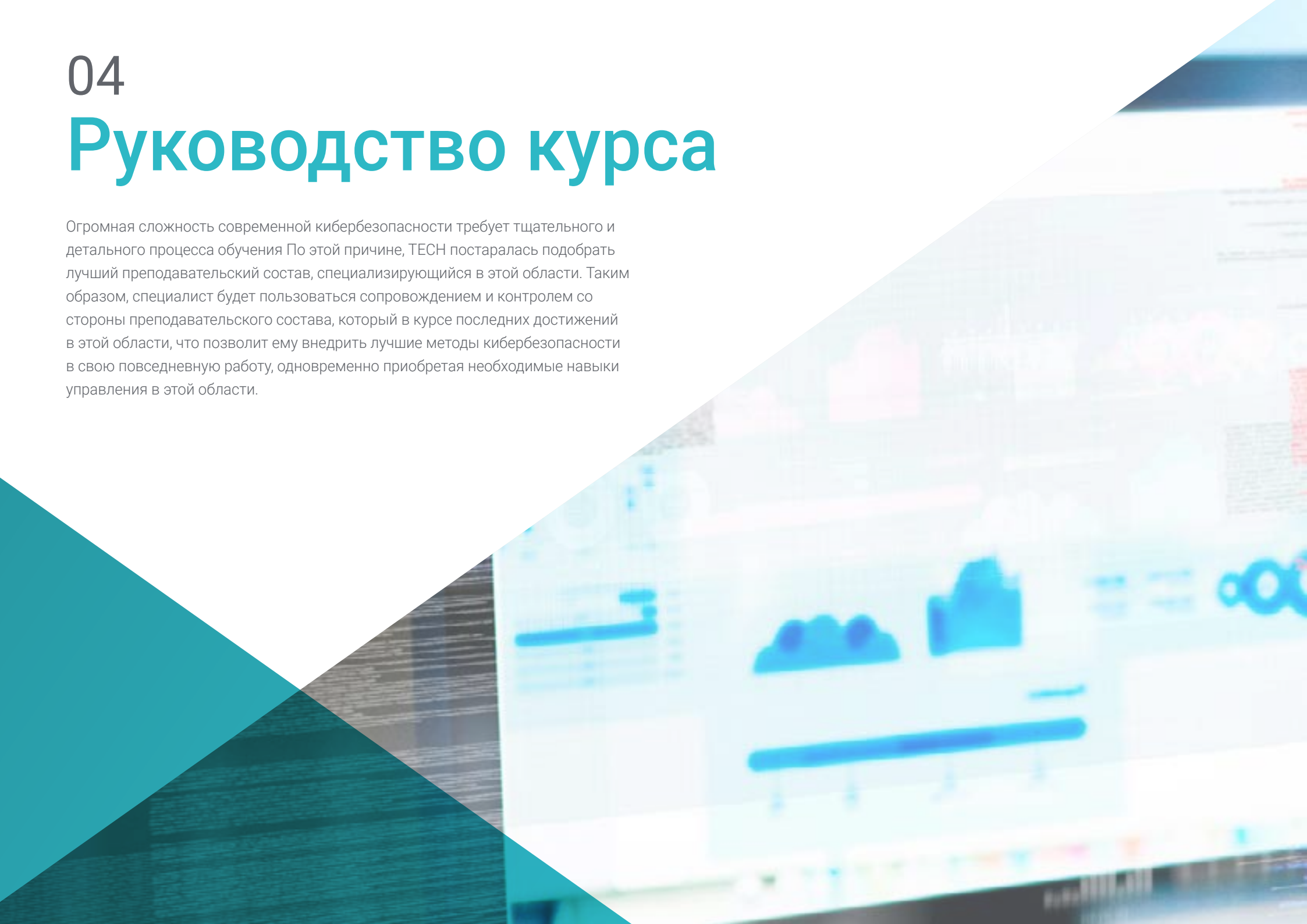
## Профессиональные навыки

- Разрабатывать систему управления информационной безопасностью (СУИБ)
- Определять ключевые элементы, из которых состоит СУИБ
- Применять методологию MAGERIT для развития модели и развиваться в профессии в этом направлении
- Разрабатывать новые методологии управления рисками на основе концепции *гибкого управления рисками*
- Выявлять, анализировать, оценивать и справляться с рисками, с которыми сталкивается профессионал, с новой точки зрения бизнеса на основе модели *Risk-Driven* или модель, управляемая рисками, которая позволяет не только выжить в своей среде, но и увеличить вклад собственной ценности
- Изучить процесс разработки стратегии безопасности при развертывании корпоративных *облачных* сервисов
- Оценивать различия в конкретных реализациях разных поставщиков *публичного* облачного пространства
- Оценивать варианты подключения к IoT для решения задач проекта, уделяя особое внимание технологиям LPWAN
- Представлять базовые характеристики основных технологий LPWAN для IoT

04

# Руководство курса

Огромная сложность современной кибербезопасности требует тщательного и детального процесса обучения По этой причине, TECH постаралась подобрать лучший преподавательский состав, специализирующийся в этой области. Таким образом, специалист будет пользоваться сопровождением и контролем со стороны преподавательского состава, который в курсе последних достижений в этой области, что позволит ему внедрить лучшие методы кибербезопасности в свою повседневную работу, одновременно приобретая необходимые навыки управления в этой области.



*В вашем распоряжении будут настоящие специалисты по кибербезопасности. Это та возможность, которую вы искали"*

## 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-н Олайа Бональ, Мартин

- Старший менеджер практики блокчейн в компании EY
- Технический специалист по блокчейн-клиентам в IBM
- Директор по архитектуре компании Blocknitive
- Координатор о группы по нереляционным распределенным базам данных в WedoIT, дочернее предприятие IBM
- Архитектор инфраструктуры в Bankia
- Руководитель отдела вертски в компании T-Systems
- Координатор отдела Bing Data España SL

## Преподаватели

### Д-р Ногалес Авила, Хавьер

- Старший консультант по корпоративным облакам и сорсингу. Quint
- Консультант по облакам и технологиям. Indra
- Младший консультант по технологиям. Accenture
- Степень бакалавра Университет Хаэна и Университет технологии и экономики Будапешта
- Степень в области инженерии промышленной организации

### Г-н Родриго Эстебанес, Хуан Мануэль

- Соучредитель компании Ismet Tech
- Менеджер по информационной безопасности в Ecix Group
- *Сотрудник по операционной безопасности* в Atos IT Solutions and Services A/S
- Преподаватель по управлению кибербезопасностью в университете
- Степень бакалавра в области инженерии Университета Вальядолида
- Степень магистра в области интегрированных систем управления в Университете CEU Сан-Пабло

## Преподаватели

### Д-р Гомес Родригес, Антонио

- Главный инженер по облачным решениям для Oracle
- Соорганизатор Malaga Developer Meetup
- Специалист-консультант для Sopra Group и Everis
- Руководитель команды в компании System Dynamics
- Разработчик программного обеспечения в компании SGO Software
- Степень магистра в области электронного бизнеса в бизнес-школе Ла-Салье
- Последипломное образование в области информационных технологий и систем в Каталонском технологическом институте
- Степень бакалавра в области высшей телекоммуникационной инженерии в Политехническом университете Каталонии

### Д-р дель Валье Ариас, Хорхе

- Smart City Solutions & Software Business Development Manager Испания. Itron, Inc Консультант по IoT
- Временный директор по бизнесу IoT. TCOMET
- Руководитель бизнес-подразделения IoT, Индустрия 4.0. Diode Испания
- Региональный менеджер по продажам в области IoT и телекоммуникаций. Aicox Soluciones
- Главный технический директор (CTO) и менеджер по развитию бизнеса. Консалтинг TELYC
- Основатель и генеральный директор компании Sensor Intelligence
- Руководитель отдела операций и проектов. Codio
- Главный операционный директор в компании Codium Networks
- Главный инженер по разработке аппаратного и микропрограммного обеспечения. AITEMIN
- Региональный руководитель отдела радиочастотного планирования и оптимизации - сеть LMDS 3,5 ГГц. Clearwire
- Диплом инженера в области телекоммуникаций в Политехническом университете Мадрида
- Бизнес-магистратура в Международной высшей школе Ла-Салье в Мадриде
- Степень магистра в области возобновляемых источников энергии. CEPYME

### Г-н Гонсало Алонсо, Феликс

- Генеральный директор и учредитель компании Smart REM Solutions
- Партнер-основатель и руководитель отдела проектирования рисков и инноваций Dynargy
- Директор и партнер-учредитель. Risknova (экспертное бюро, специализирующееся на технологиях)
- Степень бакалавра в области организации производства в Папском университете Комильяс
- Степень бакалавра в области промышленной электроники в Папском университете Комильяс
- Степень магистра в области управления страхованием в Институте сотрудничества страховых компаний

### Д-р Энтренас, Алехандро

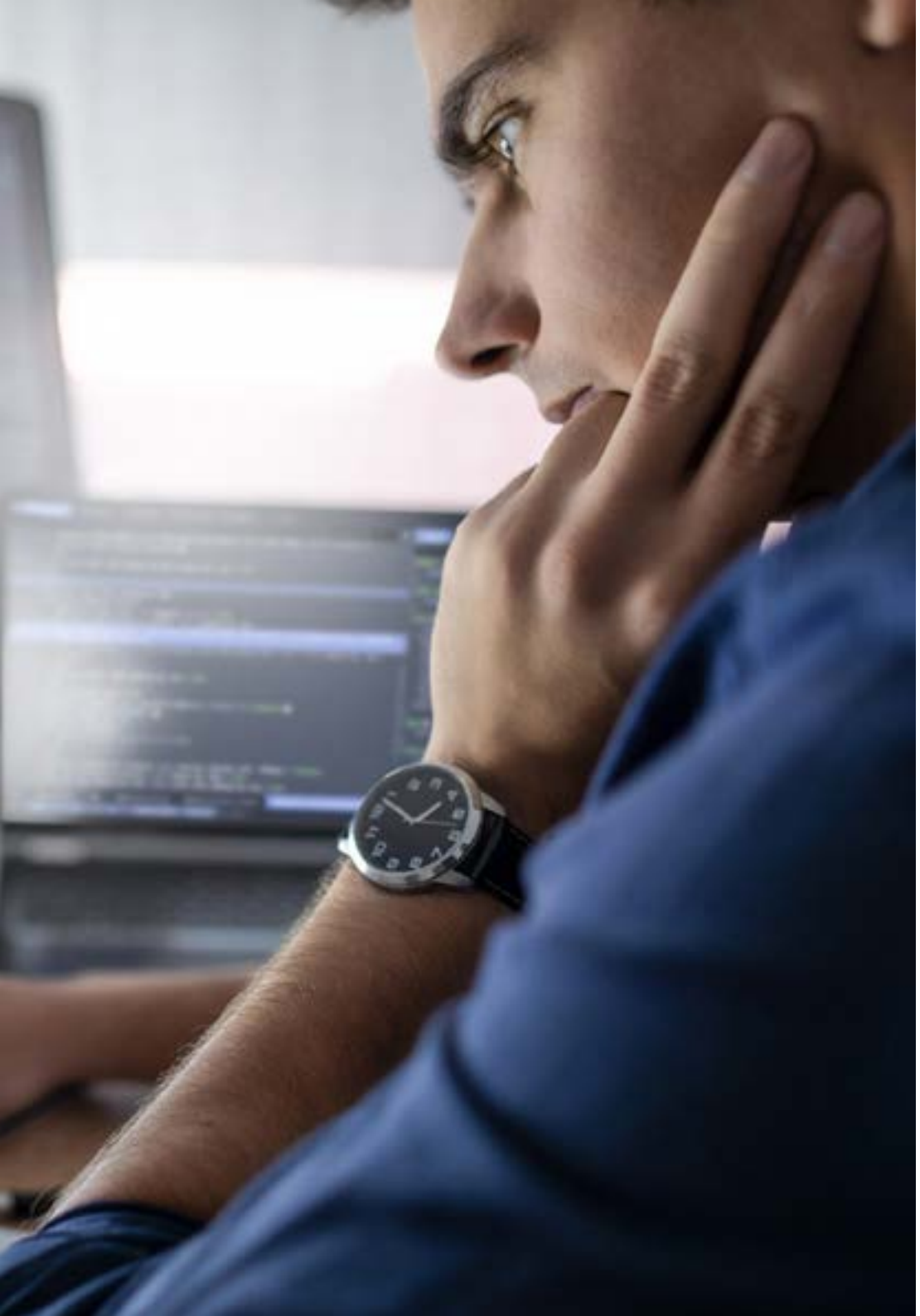
- Руководитель проекта по кибербезопасности. Entelgy Innotec Security
- Консультант по кибербезопасности. Entelgy
- Аналитик информационной безопасности. Innovery, Испания
- Аналитик по информационной безопасности. Atos
- Степень технического инженера в области компьютерных систем в Университете Кордовы
- Степень магистра в области управления информационной безопасностью в Мадридском политехническом университете
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified

**Г-н Ортега, Октавио**

- Специалист по маркетингу и веб-разработке
- Внештатный программист компьютерных приложений и *веб-разработчик*
- *Операционный директор* в Smallsquid SL
- Администратор электронной коммерции в компании Ortega y Serrano
- Преподаватель курсов по получению сертификата специалиста в области компьютерных технологий и коммуникаций
- Преподаватель курсов по компьютерной безопасности
- Степень бакалавра психологии Открытого университета Каталонии
- Профессиональное среднее образование в области анализа, проектирования и решения *программного обеспечения*
- Старший технический специалист в области перспективного программирования

**Г-н Эмбид Руис, Марио**

- Юрист, специализирующийся на ИКТ и защите данных в Martínez-Echevarría Abogados
- Менеджер по правовым вопросам в Branddocs SL
- Аналитик по рискам в сегменте малого и среднего бизнеса BBVA
- Преподаватель в университетской аспирантуре, связанной с правом
- Степень бакалавра в области права в Университете короля Хуана Карлоса
- Степень магистра в области делового администрирования и менеджмента в Университете короля Хуана Карлоса
- Степень магистра права со специализацией в области новых технологий, Интернета и аудиовизуального права от Центра университетских исследований Вильянуэва (Centro de Estudios Universitarios Villanueva)





**Д-р Госало Фернандес, Хуан Луис**

- Менеджер по продуктам на основе блокчейна для Open Canarias
- Директор по блокчейн DevOps в Аластрии
- Директор по технологиям уровня обслуживания в Santander, Испания
- Руководитель направления разработки мобильных приложений Tinkerlink в компании Cronos Telecom
- Директор по технологиям управления ИТ-услугами в Barclays Bank Spain
- Степень бакалавра в области высшей компьютерной инженерии в UNED
- Специализация в области *глубокого обучения* в DeepLearning.ai

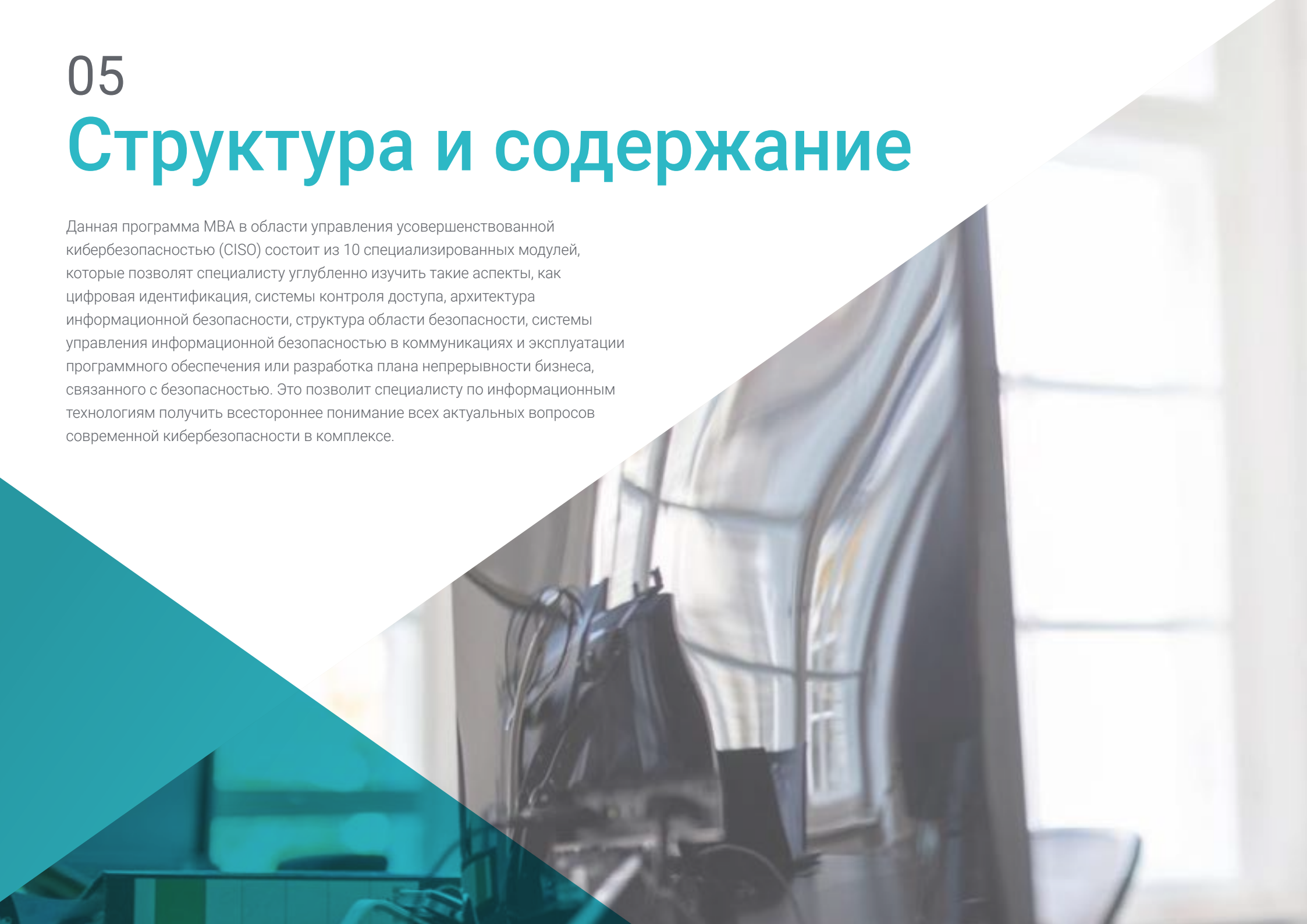
**Д-р Хурадо Хабонеро, Лорена**

- Ответственная за информационную безопасность (CISO) в компании Grupo Pascual
- Менеджер по кибербезопасности в KPMG. Испания
- Консультант по контролю и управлению проектами в области ИТ-процессов и инфраструктуры в Bankia
- Инженер по средствам эксплуатации в Dalkia
- Разработчик в Banco Popular Group
- Разработчик приложений в Мадридском политехническом университете
- Степень бакалавра в области компьютерной инженерии в Университете Альфонсо X Мудрого
- Профессиональное среднее образование в области инженерии со специализацией по компьютерному менеджменту Мадридского политехнического университета Сертифицированный инженер по решениям в области конфиденциальности данных (CDPSE) от ISACA

05

# Структура и содержание

Данная программа MBA в области управления усовершенствованной кибербезопасностью (CISO) состоит из 10 специализированных модулей, которые позволят специалисту углубленно изучить такие аспекты, как цифровая идентификация, системы контроля доступа, архитектура информационной безопасности, структура области безопасности, системы управления информационной безопасностью в коммуникациях и эксплуатации программного обеспечения или разработка плана непрерывности бизнеса, связанного с безопасностью. Это позволит специалисту по информационным технологиям получить всестороннее понимание всех актуальных вопросов современной кибербезопасности в комплексе.



*Вы не найдете более полного и инновационного содержания, чем данное, чтобы специализироваться в продвинутом управлении кибербезопасностью"*

## **Модуль 1.** Безопасность при проектировании и разработке систем

1.1. Информационные системы
- 1.1.1. Домены информационной системы
- 1.1.2. Компоненты информационных систем
- 1.1.3. Виды деятельности информационной системы
- 1.1.4. Жизненный цикл информационной системы
- 1.1.5. Ресурсы информационной системы

1.2. Информационные системы. Типология
- 1.2.1. Виды информационных систем
  - 1.2.1.1. Бизнес-системы
  - 1.2.1.2. Стратегические
  - 1.2.1.3. В зависимости от сферы применения
  - 1.2.1.4. Специфические
- 1.2.2. Информационные системы. Реальные примеры
- 1.2.3. Эволюция информационных систем: этапы
- 1.2.4. Методологии информационных систем

1.3. Безопасность информационных систем. Правовые последствия
- 1.3.1. Доступ к данным
- 1.3.2. Угрозы безопасности: уязвимости
- 1.3.3. Правовые последствия: уголовные преступления
- 1.3.4. Процедуры по техническому обслуживанию информационной системы

1.4. Безопасность информационных систем. Протоколы безопасности
- 1.4.1. Безопасность информационных систем
  - 1.4.1.1. Целостность
  - 1.4.1.2. Конфиденциальность
  - 1.4.1.3. Доступность
  - 1.4.1.4. Аутентификация
- 1.4.2. Услуги по обеспечению безопасности
- 1.4.3. Протоколы информационной безопасности. Типология
- 1.4.4. Чувствительность информационных систем

1.5. Безопасность информационных систем. Меры и системы контроля доступа
- 1.5.1. Меры по обеспечению безопасности
- 1.5.2. Вид мер по обеспечению безопасности
  - 1.5.2.1. Профилактика
  - 1.5.2.2. Обнаружение
  - 1.5.2.3. Правильность
- 1.5.3. Системы контроля доступа. Типология
- 1.5.4. Криптография

1.6. Безопасность сети и интернета
- 1.6.1. Файрволы
- 1.6.2. Цифровая идентификация
- 1.6.3. Вирусы и черви
- 1.6.4. *Хакинг*
- 1.6.5. Примеры и реальные кейсы

1.7. Компьютерные преступления
- 1.7.1. Компьютерное преступление
- 1.7.2. Компьютерные преступления. Типология
- 1.7.3. Компьютерное преступление Атака. Типологии
- 1.7.4. Случай в виртуальной реальности
- 1.7.5. Профили правонарушителей и жертв. Типизация преступлений
- 1.7.6. Компьютерные преступления. Примеры и реальные кейсы

1.8. План по обеспечению безопасности информационной системы
- 1.8.1. План по обеспечению безопасности. Цели
- 1.8.2. План по обеспечению безопасности. Планирование
- 1.8.3. План по рискам. Анализ
- 1.8.4. Политика безопасности. Внедрение в организацию
- 1.8.5. План по обеспечению безопасности. Внедрение в организацию
- 1.8.6. Процедуры по обеспечению безопасности. Типы
- 1.8.7. План по обеспечению безопасности. Примеры

1.9. План действий в чрезвычайных ситуациях
- 1.9.1. План действий в непредвиденных ситуациях. Функции
- 1.9.2. План действий в чрезвычайных ситуациях: Элементы и цели
- 1.9.3. План непредвиденных в организации. Реализация
- 1.9.4. План действий в непредвиденных ситуациях. Примеры

1.10. Управление безопасностью информационных систем
- 1.10.1. Правовые нормы
- 1.10.2. Стандарты
- 1.10.3. Сертификация
- 1.10.4. Технологии

## **Модуль 2.** Архитектуры и модели информационной безопасности

2.1. Архитектура информационной безопасности
- 2.1.1. SGSI/PDS
- 2.1.2. Стратегическая согласованность
- 2.1.3. Управление рисками
- 2.1.4. Измерение результативности

2.2. Модели информационной безопасности
- 2.2.1. На основе политик безопасности
- 2.2.2. На основе инструментов защиты
- 2.2.3. На основе вовлеченных в работу команд

2.3. Модель безопасности. Ключевые компоненты
- 2.3.1. Определение рисков
- 2.3.2. Определение средств контроля
- 2.3.3. Постоянная оценка уровня риска
- 2.3.4. План информирования сотрудников, поставщиков, партнеров и т.д.

2.4. Процесс управления рисками
- 2.4.1. Определение активов
- 2.4.2. Определение угроз
- 2.4.3. Оценка рисков
- 2.4.4. Определение приоритетов контроля
- 2.4.5. Переоценка и остаточный риск

2.5. Бизнес-процессы и информационная безопасность
- 2.5.1. Бизнес-процессы
- 2.5.2. Оценка рисков на основе параметров бизнеса
- 2.5.3. Анализ влияния на бизнес
- 2.5.4. Деловые операции и информационная безопасность

2.6. Процесс непрерывного улучшения
- 2.6.1. Цикл Деминга
  - 2.6.1.1. План
  - 2.6.1.2. Создание
  - 2.6.1.3. Верификация
  - 2.6.1.4. Действовать

2.7. Архитектура безопасности
- 2.7.1. Выбор и гомогенизация технологий
- 2.7.2. Управление идентификацией. Аутентификация
- 2.7.3. Управление доступом. Полномочия
- 2.7.4. Безопасность сетевой инфраструктуры
- 2.7.5. Технологии и решения в области шифрования
- 2.7.6. Защита конечных точек, EDR

2.8. Нормативно-правовая база
- 2.8.1. Отраслевые нормативные акты
- 2.8.2. Сертификация
- 2.8.3. Законодательство

2.9. Стандарт ISO 27001
- 2.9.1. Реализация
- 2.9.2. Сертификация
- 2.9.3. Аудиты и тесты на вторжение
- 2.9.4. Непрерывное управление рисками
- 2.9.5. Классификация информации

2.10. Законодательство о конфиденциальности. GDPR
- 2.10.1. Сфера действия Общего положения о защите данных (GDPR)
- 2.10.2. Персональные данные
- 2.10.3. Роли в обработке персональных данных
- 2.10.4. Права ARCO
- 2.10.5. Должностное лицо по защите данных (DPO). Функции

## **Модуль 3.** Управление информационной безопасностью

3.1. Управление безопасностью
- 3.1.1. Операции по обеспечению безопасности
- 3.1.2. Правовые и нормативные аспекты
- 3.1.3. Расширение возможностей бизнеса
- 3.1.4. Управление рисками
- 3.1.5. Управление идентификацией и доступом

3.2. Структура зоны безопасности. Офис CISO
- 3.2.2. Организационная структура. Место CISO в структуре
- 3.2.2. Линии защиты
- 3.2.3. Организационная схема офиса CISO
- 3.2.4. Управление бюджетом

3.3. Управление в сфере безопасности
- 3.3.1. Комитет по безопасности
- 3.3.2. Комитет по мониторингу рисков
- 3.3.3. Комитет по аудиту
- 3.3.4. Кризисный комитет

3.4. Управление в сфере безопасности. Функции
- 3.4.1. Политики и стандарты
- 3.4.2. Генеральный план по обеспечению безопасности
- 3.4.3. Приборные панели
- 3.4.4. Повышение осведомленности и обучение
- 3.4.5. Безопасность цепи поставок

3.5. Операции по обеспечению безопасности
- 3.5.1. Управление идентификацией и доступом
- 3.5.2. Конфигурация правил сетевой безопасности. *Файрволы*
- 3.5.3. Управление платформами IDS/IPS
- 3.5.4. Анализ уязвимостей

3.6. Рамки кибербезопасности. NIST CSF
- 3.6.1. Методология NIST
  - 3.6.1.1. Идентификация
  - 3.6.1.2. Защита
  - 3.6.1.3. Обнаружение
  - 3.6.1.4. Ответить
  - 3.6.1.5. Восстановление

3.7. Операционный центр безопасности (SOC). Функции
- 3.7.1. Защита *Red Team, пентестинг, разведка угроз*
- 3.7.2. Выявление. SIEM, *аналитика поведения пользователей, предотвращение мошенничества*
- 3.7.3. Ответ

3.8. Аудиты безопасности
- 3.8.1. Тест на вторжение
- 3.8.2. Упражнения по *red team*
- 3.8.3. Аудит исходного кода. Безопасная разработка
- 3.8.4. Безопасность компонентов (*цепочка поставок программного обеспечения*)
- 3.8.5. Судебная экспертиза

3.9. Реагирование на инциденты
- 3.9.1. Подготовка
- 3.9.2. Выявление, анализ и отчетность
- 3.9.3. Сдерживание, искоренение и восстановление
- 3.9.4. Деятельность после инцидента
  - 3.9.4.1. Сохранение доказательств
  - 3.9.4.2. Судебная экспертиза
  - 3.9.4.3. Управление разрывами
- 3.9.5. Официальное руководство по управлению киберинцидентами

3.10. Управление уязвимостями
- 3.10.1. Анализ уязвимостей
- 3.10.2. Оценка уязвимости
- 3.10.3. Системное базирование
- 3.10.4. Уязвимость нулевого дня. *Нулевой день*

## **Модуль 4.** Анализ рисков и среды информационной безопасности

4.1. Анализ среды
- 4.1.1. Анализ экономического положения
  - 4.1.1.1. VUCA-среды
    - 4.1.1.1.1. Волатильность
    - 4.1.1.1.2. Неопределенность
    - 4.1.1.1.3. Сложность
    - 4.1.1.1.4. Неоднозначность
  - 4.1.1.2. BANI-среды
    - 4.1.1.2.1. Хрупкость
    - 4.1.1.2.2. Тревожность
    - 4.1.1.2.3. Нелинейность
    - 4.1.1.2.4. Непонятность
- 4.1.2. Анализ общей среды. PESTEL
  - 4.1.2.1. Политический
  - 4.1.2.2. Экономический
  - 4.1.2.3. Социальный
  - 4.1.2.4. Технологичный
  - 4.1.2.5. Экологичный
  - 4.1.2.6. Юридический
- 4.1.3. Анализ внутреннего положения. SWOT-анализ
  - 4.1.3.1. Цели
  - 4.1.3.2. Угрозы
  - 4.1.3.3. Возможности
  - 4.1.3.4. Преимущества

4.2. Риск и неопределенность
- 4.2.1. Риск
- 4.2.2. Управление рисками
- 4.2.3. Стандарты управления рисками

4.3. Руководства по управлению рисками ISO 31.000:2018
- 4.3.1. Цель
- 4.3.2. Принципы
- 4.3.3. Система координат
- 4.3.4. Процесс

4.4. Методология анализа и управления рисками информационных систем (MAGERIT)
- 4.4.1. Методология MAGERIT
  - 4.4.1.1. Цели
  - 4.4.1.2. Методика
  - 4.4.1.3. Элементы
  - 4.4.1.4. Техники
  - 4.4.1.5. Доступные инструменты (PILAR)

4.5. Передача киберрисков
- 4.5.1. Передача рисков
- 4.5.2. Кибериски. Типология
- 4.5.3. Страхование от киберрисков

4.6. Agile-методологии для управления рисками
- 4.6.1. Методологии Agile
- 4.6.2. Scrum для управления рисками
- 4.6.3. *Управление рисками в Agile*

4.7. Технологии для управления рисками
- 4.7.1. Применение искусственного интеллекта в управлении рисками
- 4.7.2. *Блокчейн* и криптография. Методы сохранения стоимости
- 4.7.3. Квантовые вычисления. Возможности или угрозы

4.8. Составление карт ИТ-рисков на основе Agile-методологий
- 4.8.1. Представление вероятности и последствий в Agile-средах
- 4.8.2. Риск как угроза стоимости
- 4.8.3. Революция в управлении проектами и Agile-процессами на основе KRI

4.9. *Риск-ориентированное* управление
- 4.9.1. *Ориентирование на риск*
- 4.9.2. *Риск-ориентированное* управление
- 4.9.3. Разработка модели управления бизнесом с учетом рисков

4.10. Инновации и цифровая трансформация в управлении ИТ-рисками
- 4.10.1. Agile-управление рисками как источник инноваций в бизнесе
- 4.10.2. Преобразование данных в полезную для принятия решений информацию
- 4.10.3. Целостный взгляд на предприятие через призму риска

## **Модуль 5.** Криптография в ИТ

5.1. Криптография
- 5.1.1. Криптография
- 5.1.2. Математические основы

5.2. Криптология
- 5.2.1. Криптология
- 5.2.2. Криптоанализ
- 5.2.3. Стеганография и стегоанализ

5.3. Криптографические протоколы
- 5.3.1. Базовые блоки
- 5.3.2. Базовые протоколы
- 5.3.3. Промежуточные протоколы
- 5.3.4. Расширенные протоколы
- 5.5.3. Экзотерические протоколы

5.4. Криптографические методы
- 5.4.1. Длина ключа
- 5.4.2. Управление ключами
- 5.4.3. Типы алгоритмов
- 5.4.4. Агрегатные функции. *Хеш-функция*
- 5.4.5. Генераторы псевдослучайных чисел
- 5.4.6. Использование алгоритмов



5.5. Симметричная криптография
- 5.5.1. Блочные шифры
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. Алгоритм RC4
- 5.5.4. AES (*Advanced Encryption Standard*)
- 5.5.5. Комбинация блочных шифров
- 5.5.6. Получение ключей

5.6. Асимметричная криптография
- 5.6.1. Протокол Диффи — Хеллмана
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Ривест, Шамир и Адлеман)
- 5.6.4. Эллиптическая кривая
- 5.6.5. Асимметричная криптография. Типология

5.7. Цифровые сертификаты
- 5.7.1. Цифровая подпись
- 5.7.2. Сертификаты X509
- 5.7.3. Инфраструктура открытых ключей (PKI)

5.8. Способы реализации
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL и TLS
- 5.8.6. Смарт-карты в платежных средствах (EMV)
- 5.8.7. Протоколы мобильной связи
- 5.8.8. *Блокчейн*

5.9. Стеганография
- 5.9.1. Стеганография
- 5.9.2. Стегоанализ
- 5.9.3. Применение и использование

5.10. Квантовая криптография
- 5.10.1. Квантовые алгоритмы
- 5.10.2. Защита алгоритмов от квантовых вычислений
- 5.10.3. Квантовое распределение ключей

## **Модуль 6.** Управление идентификацией и доступом в ИТ-безопасности

6.1. Управление идентификацией и доступом (IAM)
- 6.1.1. Цифровая идентичность
- 6.1.2. Управление идентификацией
- 6.1.3. Федеративные удостоверения

6.2. Управление физическим доступом
- 6.2.1. Системы защиты
- 6.2.2. Безопасность территорий
- 6.2.3. Восстановительные комплексы

6.3. Управление логическим доступом
- 6.3.1. Аутентификация: типология
- 6.3.2. Протоколы аутентификации
- 6.3.3. Атаки на аутентификацию

6.4. Управление логическим доступом. Многофакторная аутентификация (MFA)
- 6.4.1. Управление логическим доступом. Многофакторная аутентификация (MFA)
- 6.4.2. Пароли. Важность
- 6.4.3. Атаки на аутентификацию

6.5. Управление логическим доступом. Биометрическая аутентификация
- 6.5.1. Контроль логического доступа. Биометрическая аутентификация
  - 6.5.1.1. Биометрическая аутентификация. Требования
- 6.5.2. Функционирование
- 6.5.3. Модели и методы

6.6. Системы управления аутентификацией
- 6.6.1. *Единая регистрация*
- 6.6.2. Kerberos
- 6.6.3. Системы AAA

6.7. Системы управления аутентификацией: Системы AAA
- 6.7.1. TACACS
- 6.7.2. RADIUS
- 6.7.3. DIAMETER

6.8. Службы по управлению доступом
- 6.8.1. Файрволы — Межсетевые экраны
- 6.8.2. VPN — виртуальные частные сети
- 6.8.3. IDS — система обнаружения вторжений

6.9. Системы управления доступом к сети
- 6.9.1. NAC
- 6.9.2. Архитектура и элементы
- 6.9.3. Эксплуатация и стандартизация

6.10. Доступ к беспроводным сетям
- 6.10.1. Виды беспроводных сетей
- 6.10.2. Безопасность в беспроводных сетях
- 6.10.3. Атаки на беспроводные сети

## **Модуль 7.** Безопасность в сфере коммуникации и эксплуатации программного обеспечения

7.1. Информационная безопасность в сфере коммуникаций и эксплуатации программного обеспечения
- 7.1.1. Информационная безопасность
- 7.1.2. Кибербезопасность
- 7.1.3. Облачная безопасность

7.2. Информационная безопасность в сфере коммуникаций и эксплуатации программного обеспечения. Типология
- 7.2.1. Физическая безопасность
- 7.2.2. Логическая безопасность

7.3. Безопасность в сфере коммуникаций
- 7.3.1. Основные элементы
- 7.3.2. Сетевая безопасность
- 7.3.3. Передовая практика

7.4. Кибербезопасность
- 7.4.1. Социальная инженерия
- 7.4.2. *Глубокий веб*
- 7.4.3. *Фишинг*
- 7.4.4. *Вредоносное программное обеспечение*

7.5. Безопасная разработка в сфере коммуникации и эксплуатации программного обеспечения
- 7.5.1. Безопасная разработка. Протокол HTTP
- 7.5.2. Безопасная разработка. Жизненный цикл
- 7.5.3. Безопасная разработка. Безопасность PHP
- 7.5.4. Безопасная разработка. Безопасность NET
- 7.5.5. Безопасная разработка. Передовая практика

7.6. Системы управления информационной безопасностью в сфере коммуникации и эксплуатации программного обеспечения
- 7.6.1. GDPR
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/18

7.7. SIEM-технологии
- 7.7.1. SIEM-технологии
- 7.7.2. Деятельность SOC
- 7.7.3. SIEM *Поставщики*

7.8. Роль в обеспечении безопасности в организациях
- 7.8.1. Роли в организациях
- 7.8.2. Роль специалистов в области IoT в компаниях
- 7.8.3. Признанные на рынке сертификаты

7.9. Судебная экспертиза
- 7.9.1. Судебная экспертиза
- 7.9.2. Криминалистическая экспертиза. Методология
- 7.9.3. Криминалистическая экспертиза. Инструменты и внедрение

7.10. Кибербезопасность сегодня
- 7.10.1. Крупные кибернетические атаки
- 7.10.2. Прогнозы по трудоустройству
- 7.10.3. Задачи

## **Модуль 8.** Безопасность в облачных средах

8.1. Безопасность в среде *облачных вычислений*
- 8.1.1. Безопасность в среде *облачных вычислений*
- 8.2.1. Безопасность в среде *облачных вычислений*. Угрозы и риски безопасности
- 8.3.1. Безопасность в среде *облачных вычислений*. Ключевые аспекты безопасности

8.2. Виды *облачной инфраструктуры*
- 8.2.1. Публичная
- 8.2.2. Частная
- 8.2.3. Гибридная

8.3. Модель совместного управления
- 8.3.1. Элементы безопасности, управляемые поставщиком
- 8.3.2. Элементы, управляемые клиентом
- 8.3.3. Определение стратегии безопасности

8.4. Профилактические механизмы
- 8.4.1. Системы управления аутентификацией
- 8.4.2. Система управления авторизацией: политики доступа
- 8.4.3. Системы управления ключами

8.5. Секьюритизация систем
- 8.5.1. Секьюритизация систем хранения
- 8.5.2. Защита систем баз данных
- 8.5.3. Секьюризация данных при передаче

8.6. Защита инфраструктуры
- 8.6.1. Проектирование и внедрение безопасных сетей
- 8.6.2. Безопасность вычислительных ресурсов
- 8.6.3. Инструменты и ресурсы для защиты инфраструктуры

8.7. Обнаружение угроз и атак
- 8.7.1. Системы аудита, *регистрации* и мониторинга
- 8.7.2. Системы событий и сигнализации
- 8.7.3. Системы SIEM

8.8. Реагирование на инциденты
- 8.8.1. План по реагированию на инциденты
- 8.8.2. Непрерывность бизнеса
- 8.8.3. Криминалистический анализ и устранение последствий инцидентов аналогичного характера

8.9. Безопасность в публичных *облаках*
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Регулирование и соблюдение
- 8.10.1. Соблюдение норм безопасности
- 8.10.2. Управление рисками
- 8.10.3. Люди и процессы в организациях

## **Модуль 9.** Безопасность коммуникаций устройств IoT

9.1. От телеметрии к IoT
- 9.1.1. Телеметрия
- 9.1.2. Межмашинное взаимодействие (M2M)
- 9.1.3. Демократизация телеметрии

9.2. Эталонные модели IoT
- 9.2.1. Эталонные модели IoT
- 9.2.2. Упрощенная архитектура IoT

9.3. Уязвимости безопасности IoT
- 9.3.1. IoT-устройства
- 9.3.2. Устройства IoT. Примеры использования
- 9.3.3. Устройства IoT. Уязвимости

9.4. IoT-соединение
- 9.4.1. Сети PAN, LAN, WAN
- 9.4.2. Беспроводные технологии, не относящиеся к IoT
- 9.4.3. Беспроводные технологии LPWAN

9.5. LPWAN-технологии
- 9.5.1. "Железный треугольник" сетей LPWAN
- 9.5.2. Свободные частотные диапазоны vs. Лицензированные диапазоны
- 9.5.3. Возможности технологии LPWAN

9.6. Технология LoRaWAN
- 9.6.1. Технология LoRaWAN
- 9.6.2. Варианты использования LoRaWAN. Экосистема
- 9.6.3. Безопасность LoRaWAN

9.7. Технология Sigfox
- 9.7.1. Технология Sigfox
- 9.7.2. Варианты использования Sigfox. Экосистема
- 9.7.3. Безопасность Sigfox

9.8. Сотовая технология IoT
- 9.8.1. Сотовая технология IoT (NB-IoT и LTE-M)
- 9.8.2. Случаи использования сотового IoT. Экосистема
- 9.8.3. Безопасность сотовой технологии IoT

9.9. Технология WiSUN
- 9.9.1. Технология WiSUN
- 9.9.2. Случаи использования WiSUN. Экосистема
- 9.9.3. Безопасность WiSUN

9.10. Другие виды технологий IoT
- 9.10.1. Другие виды технологий IoT
- 9.10.2. Примеры использования и экосистема других технологий IoT
- 9.10.3. Безопасность других технологий IoT

## **Модуль 10.** План по обеспечению непрерывности бизнеса, связанный с безопасностью

10.1. План обеспечения непрерывности бизнеса
- 10.1.1. Планы обеспечения непрерывности бизнеса (Business Continuity Plan — BCP)
- 10.1.2. План обеспечения непрерывности бизнеса (BCP). Основные вопросы
- 10.1.3. План обеспечения непрерывности бизнеса (BCP) для оценки компании

10.2. Метрические данные плана обеспечения непрерывности бизнеса (BCP)
- 10.2.1. *Цель по времени восстановления* (RTO) и *Цель по точке восстановления* (RPO)
- 10.2.2. Максимально допустимое время (MTD)
- 10.2.3. Минимальные уровни восстановления (ROL)
- 10.2.4. Цель точки восстановления (RPO)

10.3. Проекты непрерывного действия. Типология
- 10.3.1. План обеспечения непрерывности бизнеса (BCP)
- 10.3.2. План по обеспечению непрерывности ИКТ
- 10.3.3. План аварийного восстановления (DRP)

10.4. Управление рисками, связанными с BCP
- 10.4.1. Анализ влияния на бизнес
- 10.4.2. Преимущества внедрения BCP
- 10.4.3. Менталитет, основанный на риске

10.5. Жизненный цикл бизнеса плана обеспечения непрерывности
- 10.5.1. Фаза 1: Анализ организации
- 10.5.2. Фаза 2: Определение стратегии обеспечения непрерывности
- 10.5.3. Фаза 3: Ответ на непредвиденные ситуации
- 10.5.4. Фаза 4: Испытание, обслуживание и осмотр

10.6. Фаза организационного анализа BCP
- 10.6.1. Идентификация процессов, входящих в сферу действия BCP
- 10.6.2. Определение критических областей бизнеса
- 10.6.3. Выявление зависимостей между областями и процессами
- 10.6.4. Определение адекватного MTD
- 10.6.5. Результаты. Создание плана

10.7. Фаза определения стратегии непрерывности в рамках BCP
- 10.7.1. Роли в фазе определения стратегии
- 10.7.2. Задачи в фазе определения стратегии
- 10.7.3. Результаты работы

10.8. Фаза реагирования на непредвиденные обстоятельства в рамках BCP
- 10.8.1. Роли в фазе реагирования
- 10.8.2. Задачи в этой фазе
- 10.8.3. Результаты работы

10.9. Фаза тестирования, обслуживания и ревизии BCP
- 10.9.1. Роли в фазе тестирования, обслуживания и ревизии
- 10.9.2. Задачи в фазе тестирования, обслуживания и ревизии
- 10.9.3. Результаты работы

10.10. Нормы ISO, связанные с планом обеспечения непрерывности бизнеса (BCP)
- 10.10.1. ISO 22301, ISO 2019
- 10.10.2. ISO 22313, ISO 2020
- 10.10.3. Другие соответствующие стандарты ISO и международные стандарты

## **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.** *Исполнительный* 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

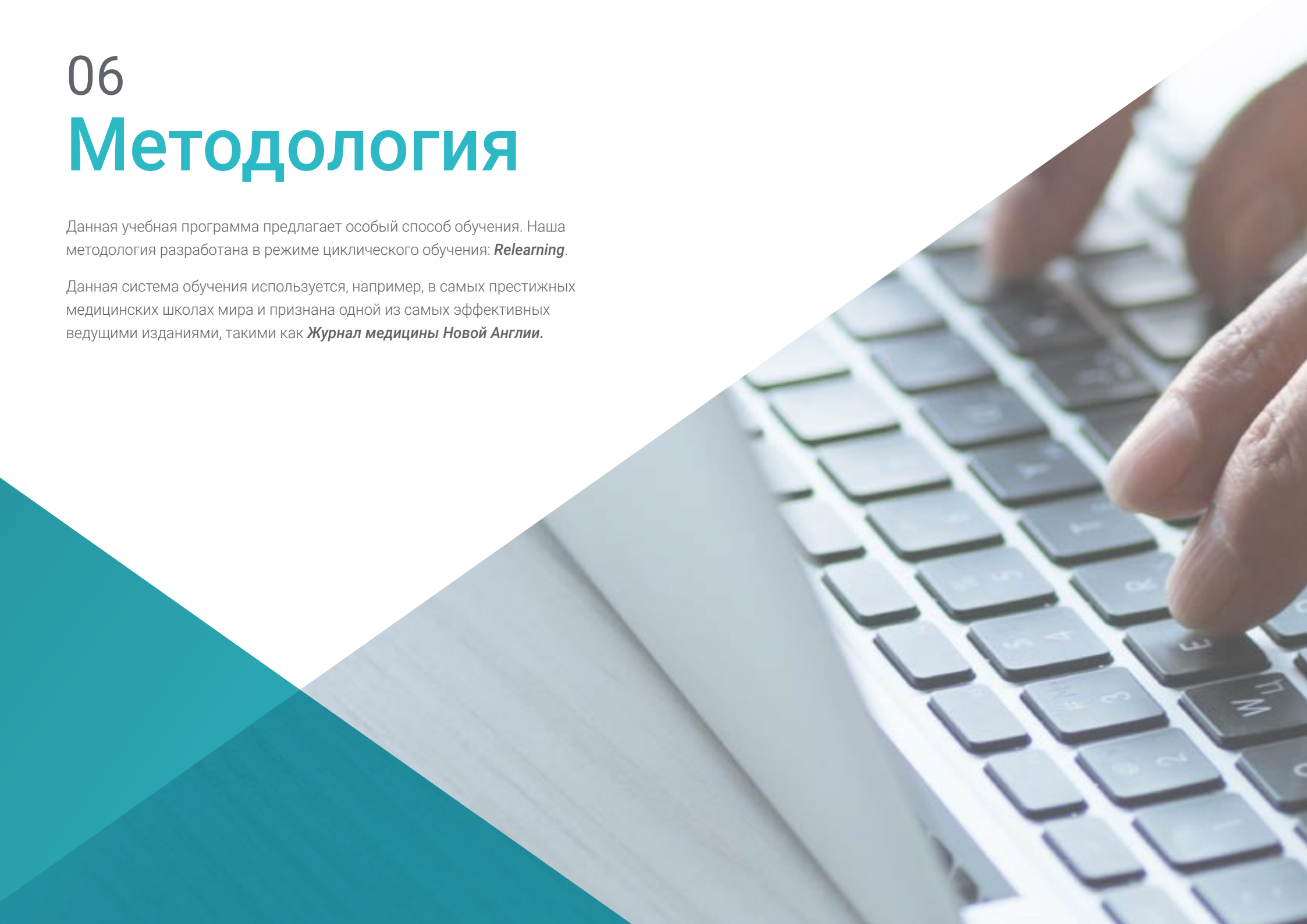
*Лучший преподавательский состав и инновационная система обучения в сочетании с наиболее полным и современным учебным планом: у вас есть прекрасная возможность продвинуться как специалист в области информатики"*

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"*

## Исследование 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 TECH вы сможете познакомиться со способом обучения, который опровергает основы традиционных методов образования 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

Эта программа TECH - 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, делая решающий шаг на пути к успеху. Метод кейсов, составляющий основу данного содержания, обеспечивает следование 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 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 кейс-метода - 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*

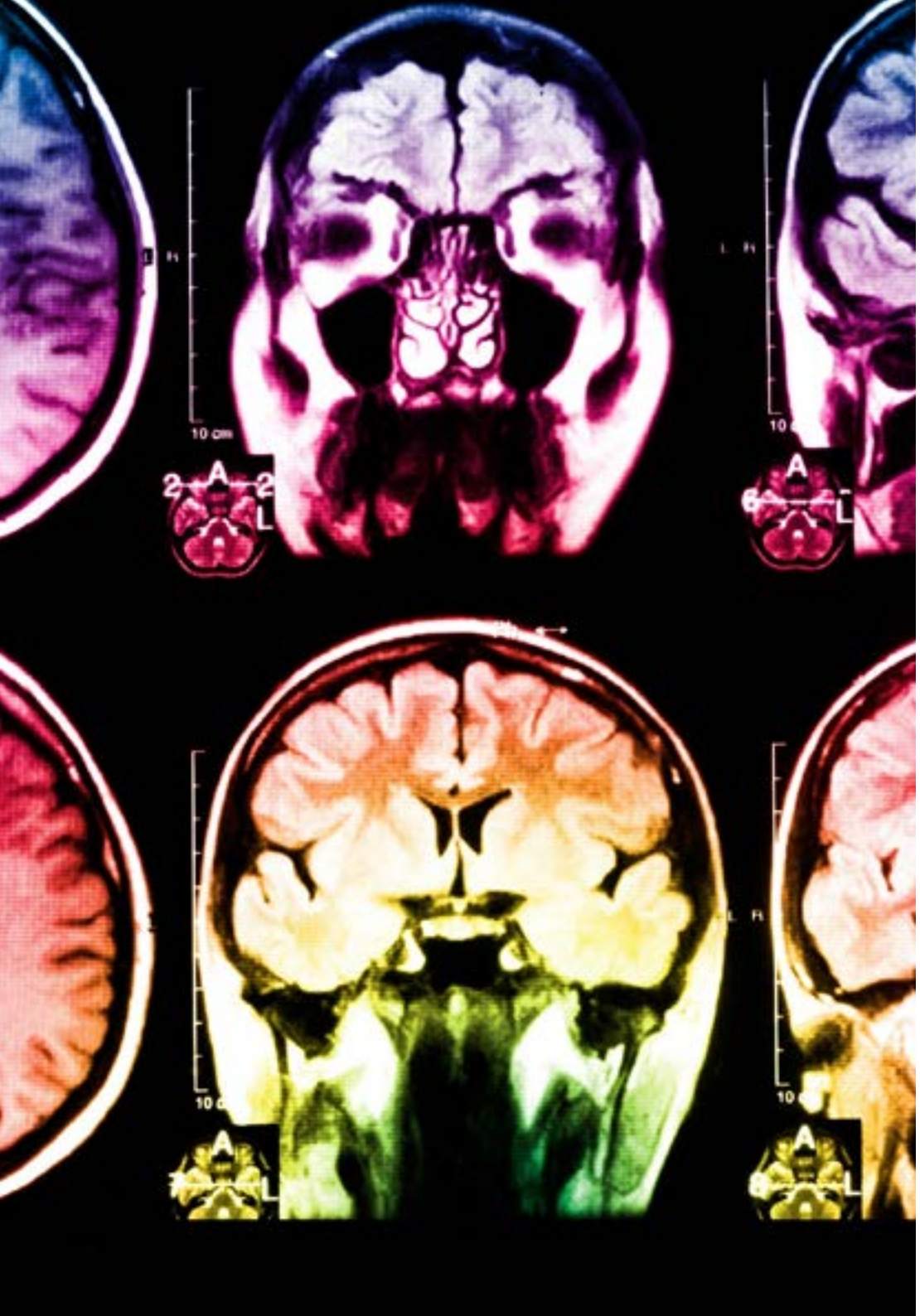
TECH эффективно объединяет метод кейсов с системой 100% онлайн-обучения, основанной на повторении, которая сочетает различные дидактические элементы в каждом уроке.

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

*В 2019 году мы достигли лучших результатов обучения среди всех онлайн-университетов в мире.*


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 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.

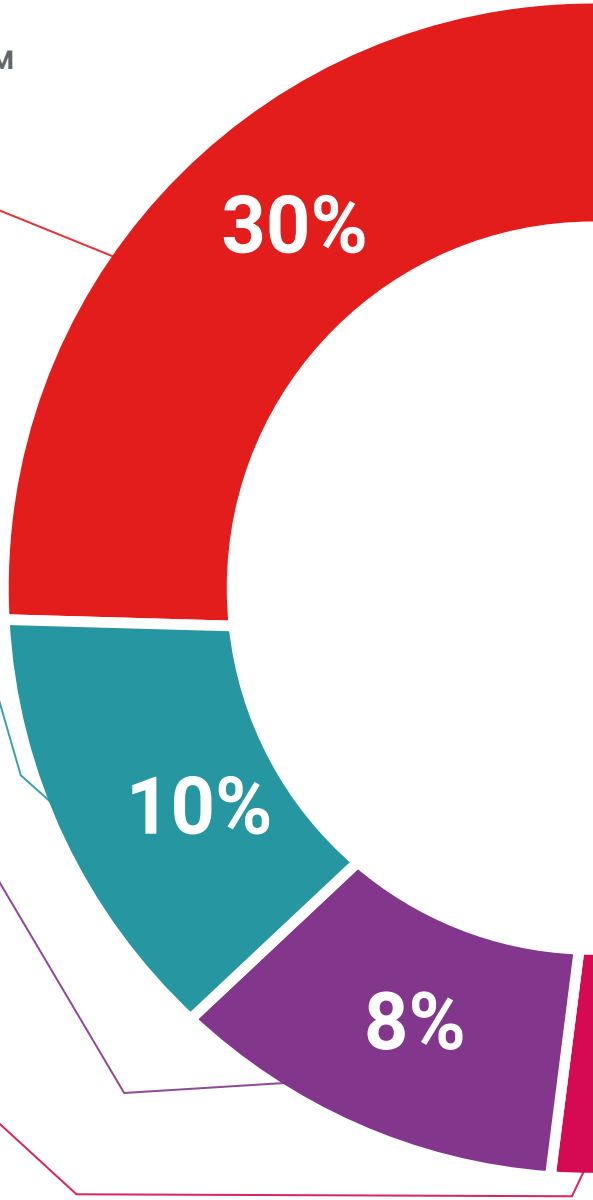
Так называемый метод обучения у эксперта укрепляет знания и память, а также формирует уверенность в наших будущих сложных решениях.

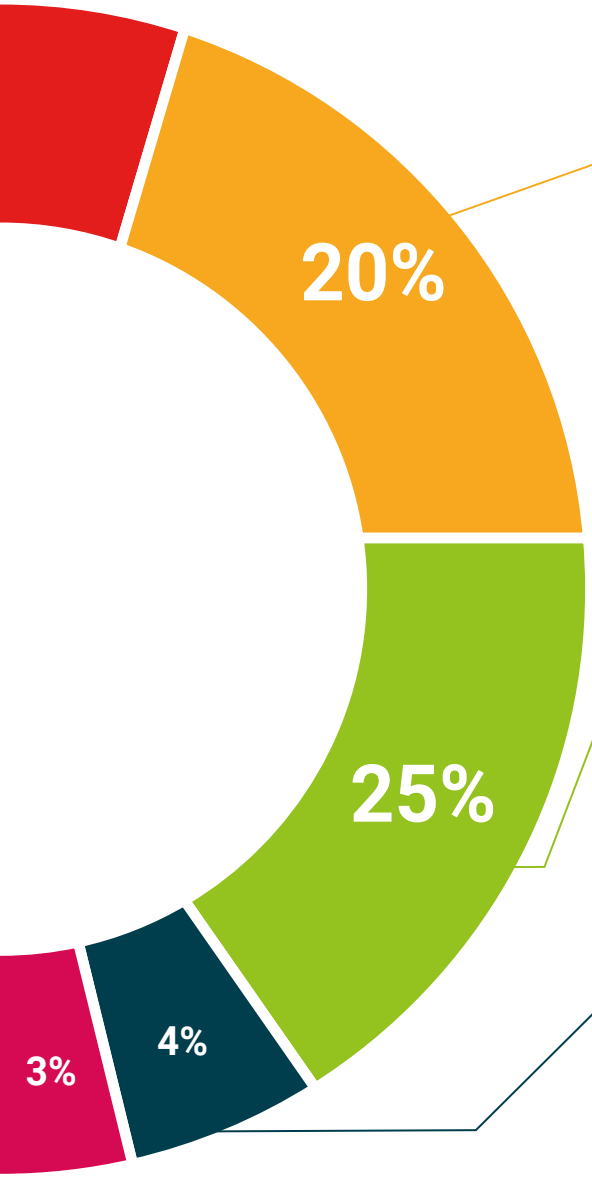
### Практика навыков и компетенций

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 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 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".

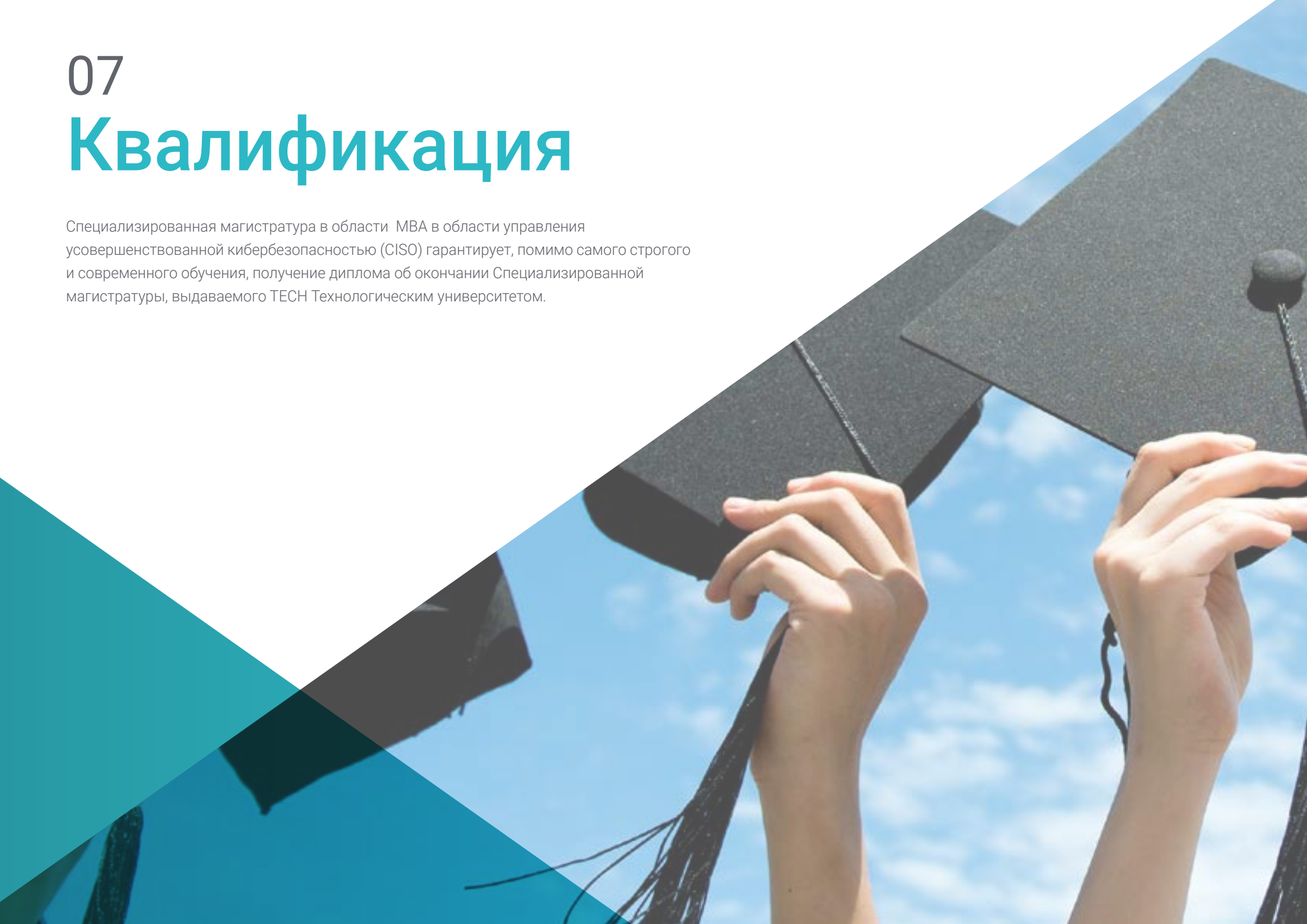
### Тестирование и повторное тестирование

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

# Квалификация

Специализированная магистратура в области  MBA в области управления усовершенствованной кибербезопасностью (CISO) 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 усовершенствованной кибербезопасностью (CISO)** содержит самую полную и современную программу на рынке.

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

Диплом, выданный **ТЕСН 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 усовершенствованной кибербезопасностью (CISO)**

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 усовершенствованной кибербезопасностью (CISO)

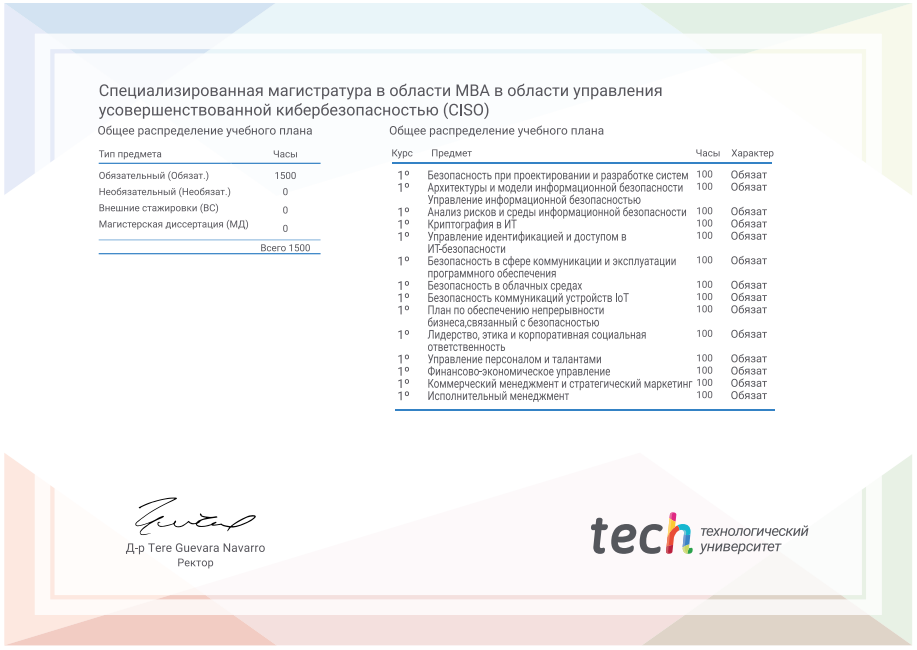
Данный диплом специализированной программы, присуждаемый Университетом, соответствует 1500 учебным часам, с датой начала дд/мм/гггг и датой окончания дд/мм/гггг.

ТЕСН 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 усовершенствованной кибербезопасностью (CISO)

Общее распределение учебного плана

| Тип предмета | Часы |
|---|---|
| Обязательный (Обязат.) | 1500 |
| Необязательный (Необязат.) | 0 |
| Внешние стажировки (ВС) | 0 |
| Магистерская диссертация (МД) | 0 |
| Всего 1500 | |

Общее распределение учебного плана

| Курс | Предмет | Часы | Характер |
|---|---|---|---|
| 1º | Безопасность при проектировании и разработке систем | 100 | Обязат |
| 1º | Архитектуры и модели информационной безопасности | 100 | Обязат |
| 1º | Управление информационной безопасностью | 100 | Обязат |
| 1º | Анализ рисков и среды информационной безопасности | 100 | Обязат |
| 1º | Криптография в ИТ | 100 | Обязат |
| 1º | Управление идентификацией и доступом в ИТ-безопасности | 100 | Обязат |
| 1º | Безопасность в сфере коммуникации и эксплуатации программного обеспечения | 100 | Обязат |
| 1º | Безопасность в облачных средах | 100 | Обязат |
| 1º | Безопасность коммуникаций устройств IoT | 100 | Обязат |
| 1º | План по обеспечению непрерывности бизнеса,связанный с безопасностью | 100 | Обязат |
| 1º | Лидерство, этика и корпоративная социальная ответственность | 100 | Обязат |
| 1º | Управление персоналом и талантами | 100 | Обязат |
| 1º | Финансово-экономическое управление | 100 | Обязат |
| 1º | Коммерческий менеджмент и стратегический маркетинг | 100 | Обязат |
| 1º | Исполнительный 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 усовершенствованной кибербезопасностью (CISO)

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

# Специализированная магистратура

## MBA в области управления усовершенствованной кибербезопасностью (CISO)

tech технологический университет