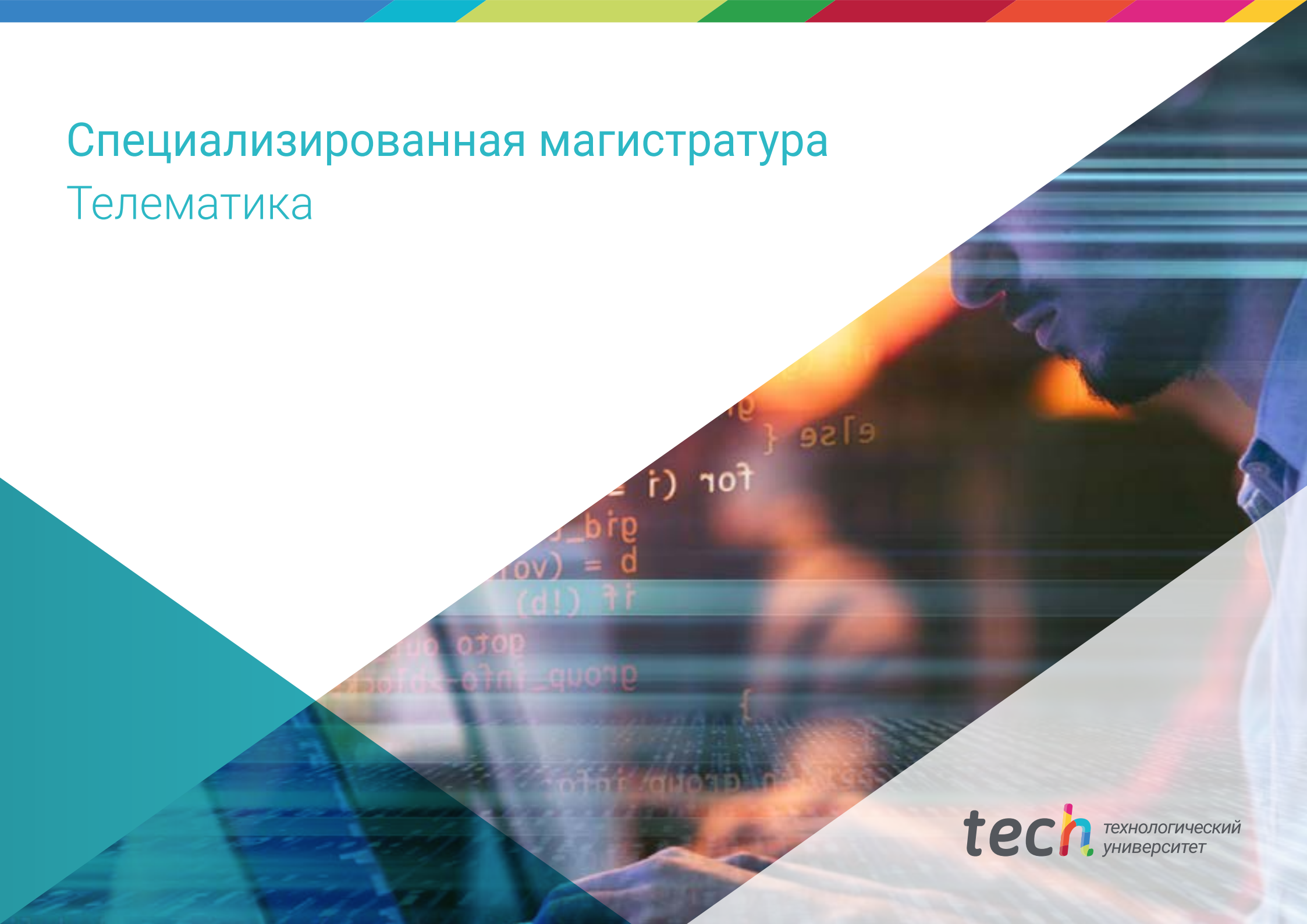
Специализированная магистратура

Телематика



tech технологический университет

tech технологический университет

Специализированная магистратура
Телематика

- Формат: **онлайн**
- Продолжительность: **12 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Режим обучения: **16ч./неделя**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

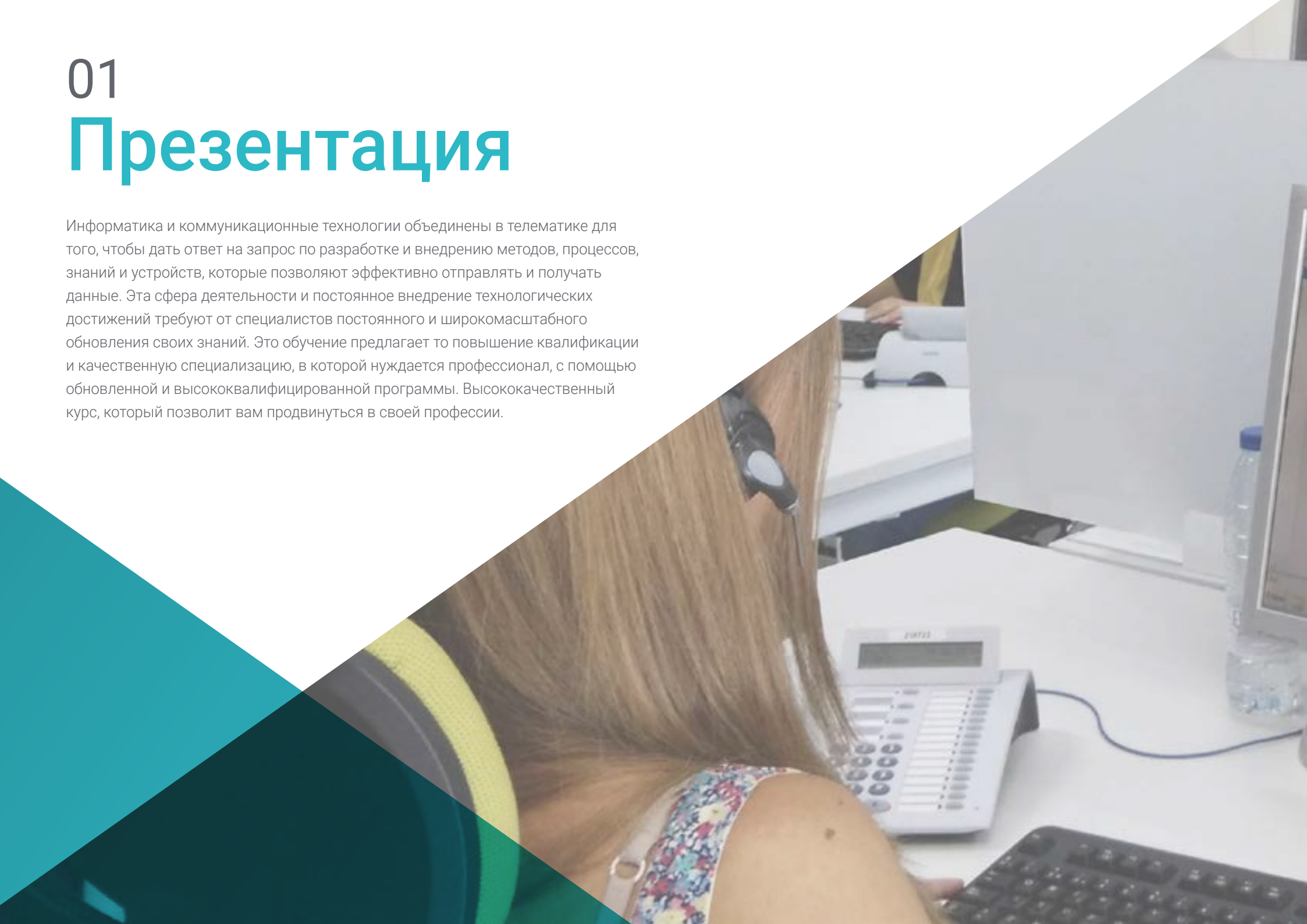
Веб-доступ: www.techtitute.com/ru/information-technology/professional-master-degree/master-telematics

Оглавление

01

Презентация

Информатика и коммуникационные технологии объединены в телематике для того, чтобы дать ответ на запрос по разработке и внедрению методов, процессов, знаний и устройств, которые позволяют эффективно отправлять и получать данные. Эта сфера деятельности и постоянное внедрение технологических достижений требуют от специалистов постоянного и широкомасштабного обновления своих знаний. Это обучение предлагает то повышение квалификации и качественную специализацию, в которой нуждается профессионал, с помощью обновленной и высококвалифицированной программы. Высококачественный курс, который позволит вам продвинуться в своей профессии.



Комплексная, полностью обновленная и адаптируемая к вашим возможностям, эта программа является высококачественным инструментом для специалиста по информатике, желающего расширить свои реальные навыки"

Развитие телекоммуникаций происходит постоянно, поскольку это одна из наиболее быстро развивающихся областей. Поэтому необходимо иметь в команде ИТ-экспертов, которые могут адаптироваться к этим изменениям и из первых рук знают о новых инструментах и методах, появляющихся в этой области.

Программа по телематике охватывает все предметы, связанные с этой сферой. Ее изучение имеет явное преимущество перед другими программами магистратуры, которые сосредоточены на конкретных блоках, что не позволяет студенту понять взаимосвязь с другими областями, входящими в междисциплинарную область телекоммуникаций. Кроме того, команда преподавателей этой программы провела тщательный отбор каждого из предметов этого курса, чтобы предложить студенту возможность пройти наиболее комплексное обучение с наиболее актуальной информацией.

Эта программа предназначена для тех, кто заинтересован в достижении более высокого уровня знаний в области телематики. Основная цель — научить студентов на практике применять знания, полученные в рамках этой программы, в той среде, которая отражает реальность, с которой они могут столкнуться в будущем, в условиях строгой и реальной работы.

Более того, поскольку это 100% онлайн-программа, студент не обусловлен фиксированным расписанием или необходимостью переезда в другое физическое место, а может получить доступ к материалам в любое время суток, совмещая свою работу или личную жизнь с учебой.

Данная **Специализированная магистратура в области Телематика** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор кейсов из реальной практики, представленных экспертами в области телематики
- Наглядное, схематичное и исключительно практичное содержание курса предоставляет научную и практическую информацию по тем дисциплинам, которые необходимы для осуществления профессиональной деятельности
- Практические упражнения для самооценки, контроля и улучшения успеваемости
- Особое внимание уделяется инновационным методикам в области телематики
- 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

Включите в свои компетенции способность работать в различных областях телематики, пройдя путь обучения, который будет способствовать вашему профессиональному развитию"

Данная программа — это лучшая инвестиция, которую вы можете сделать, выбрав программу повышения квалификации для актуализации своих знаний в области телематики"

Дидактический материал, с помощью которого вы будете проходить обучение, представляет собой сборник высокого качества, который позволит вам учиться в удобной и простой форме.

Эта 100% онлайн-программа позволит вам совмещать учебу с профессиональной деятельностью.

В преподавательский состав входят профессионалы в области телекоммуникаций, которые вносят свой опыт работы в эту программу, а также признанные специалисты, принадлежащие к ведущим научным сообществам.

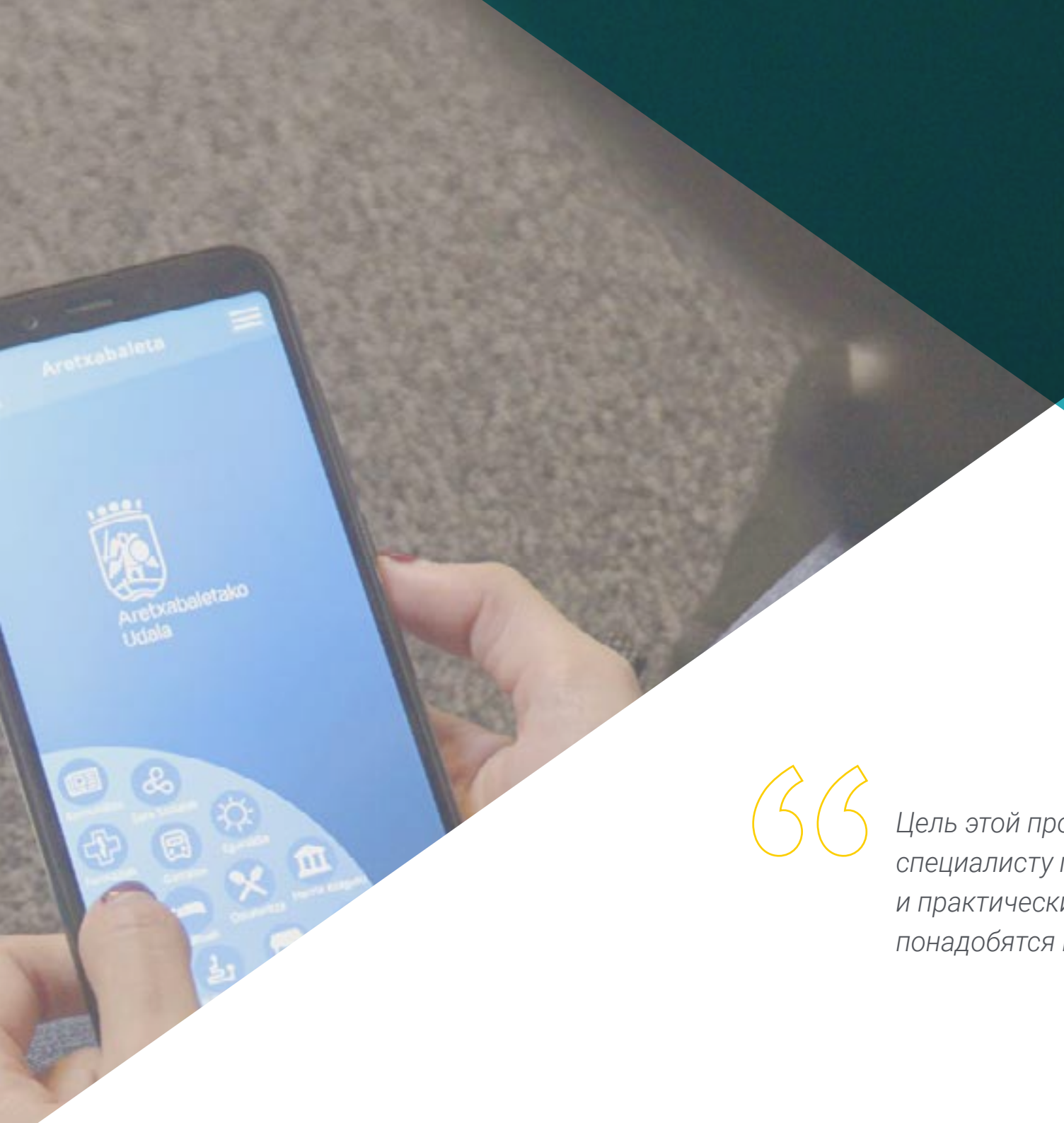
Мультимедийное содержание программы, разработанное с использованием новейших образовательных технологий, позволит специалисту проходить обучение с учетом контекста и ситуации, т.е. в симулированной среде, обеспечивающей иммерсивный учебный процесс, запрограммированный на обучение в реальных ситуациях.

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

02

Цели

Программа в области телематики призвана предложить ИТ-специалистам полное и современное изучение всех областей, связанных с телематикой, с гарантией и качеством программы, созданной с критерием абсолютного передового опыта.



Цель этой программы — предоставить специалисту полный спектр теоретических и практических знаний, которые ему/ей понадобятся в области телематики"

Общая цель

- Подготовить студентов, чтобы они могли разрабатывать телематические приложения, анализировать данные или выполнять задачи по обеспечению цифровой безопасности, среди прочих аспектов

Возможность, созданная для профессионалов, которые ищут интенсивный и эффективный курс, чтобы сделать значительный шаг вперед в своей профессии"

Конкретные цели

Модуль 1. Компьютерные сети

- Приобрести необходимые знания о компьютерных сетях в Интернете
- Понимать функционирование различных уровней, определяющих сетевую систему, таких как прикладной, транспортный, сетевой и канальный уровни
- Понимать состав локальных сетей (LAN), их топологию и элементы сети и межсетевого взаимодействия
- Узнать, как работает IP-адресация и подсети
- Понять структуру беспроводных и мобильных сетей, включая новую сеть 5G
- Знать различные механизмы сетевой безопасности, а также различные протоколы безопасности Интернета

Модуль 2. Распределенные системы

- Освоить основные принципы работы распределенных систем
- Научиться определять характеристики и классифицировать распределенные системы по ряду основных параметров
- Понять различные типы моделей, используемых в распределенных системах
- Знать современные архитектуры, реализующие концепцию распределенных файловых систем
- Уметь анализировать алгоритмы синхронизации процессов и объектов, определение логических часов и временной согласованности информации
- Понять систему именования, используемую в Интернете, известную как DNS (Domain Name System)
- Узнать, как работает IP-адресация и подсети

Модуль 3. Безопасность систем и сетей связи

- Получить глобальное представление о безопасности, криптографии и классическом криптоанализе
- Понять основы симметричной и асимметричной криптографии, а также их основные алгоритмы
- Проанализировать природу сетевых атак и различные типы архитектур безопасности
- Сформировать понимание различных методов защиты системы и разработки безопасного кода
- Сформировать понимание основных компонентов ботнетов и спама, а также вредоносных программ и вредоносного кода
- Заложить основы судебной экспертизы в мире ПО и ИТ-аудита

Модуль 4. Корпоративные сети и инфраструктуры

- Освоить передовые аспекты взаимосвязи инфраструктуры, необходимые для проектирования и планирования высокоскоростных сетей
- Знать основные характеристики и технологии транспортных сетей
- Понимать классические архитектуры WAN, All-Ethernet, MPLS, VPN
- Проанализировать фундаментальные аспекты эволюции сетей до NGN (сетей следующего поколения)
- Понимать передовые требования к QoS, маршрутизации и управлению перегрузками и надежностью
- Знать и уметь применять международные сетевые стандарты

Модуль 5. Архитектура безопасности

- Понимать основные принципы информационной безопасности
- Освоить стандарты ИТ-безопасности и процессы сертификации
- Анализировать организационные и криптографические основы, на которых базируются технологии безопасности
- Определять основные угрозы и уязвимости различных элементов, задействованных в ИКТ, а также их причины
- Обладать глубокими знаниями об инструментах сетевой безопасности и их специфических функциях
- Знать, как применять технологии, составляющие архитектуру безопасности ИКТ, в ее различных перспективах

Модуль 6. Центры обработки данных, эксплуатация сетей и услуги

- Уметь проектировать, эксплуатировать, управлять и поддерживать сети, услуги и контент, предоставляемые через центр обработки данных
- Знать все основные элементы, из которых состоит центр обработки данных, а также существующие стандарты и сертификаты
- Анализировать экономическое воздействие инфраструктуры центра обработки данных с точки зрения производительности и эффективности
- Идентифицировать в реальных инфраструктурах элементы hardware центра обработки данных
- Понять последствия для безопасности различных решений, предлагаемых поставщиками услуг на рынке
- Понять, как работает процесс виртуализации
- Понять преимущества, выгоды и модели внедрения облачных технологий (Cloud)

Модуль 7. Расширенное программирование

- Углубить свои знания в области программирования, особенно в отношении объектно-ориентированного программирования и различных видов отношений между существующими классами
- Знать различные шаблоны проектирования для решения объектно-ориентированных задач
- Изучить событийно-управляемое программирование и разработку пользовательского интерфейса с помощью Qt
- Получить необходимые знания о параллельном программировании, процессах и потоках
- Узнайте, как управлять использованием потоков и синхронизацией, а также как решать общие задачи в параллельном программировании
- Понимать важность документации и тестирования при разработке программного обеспечения

Модуль 8. Системный инжиниринг и сетевые услуги

- Освоить фундаментальные концепции сервисного инжиниринга
- Понять основные принципы управления конфигурацией развивающихся систем software
- Знать технологии и инструменты для предоставления телематических услуг
- Знать различные архитектурные стили программной системы, понимать их различия и уметь выбрать наиболее подходящий в соответствии с требованиями системы
- Понимать процессы валидации и верификации и их взаимосвязь с другими фазами жизненного цикла
- Уметь интегрировать системы для захвата, представления, обработки, хранения, управления и презентации мультимедийной информации для построения телекоммуникационных услуг и телематических приложений
- Знать общие элементы для детального проектирования программной системы
- Приобрести навыки программирования, моделирования и проверки для телематических, сетевых и распределенных услуг и приложений
- Сформировать понимание процессов и действий по переходу, конфигурации, развертыванию и эксплуатации
- Понимать процессы управления, автоматизации и оптимизации сети

Модуль 9. Аудит информационных систем

- Освоить основные концепции, стандарты и методологии системного аудита
- Знать организационные элементы и правовые основы аудита
- Получить справочное руководство по разработке новых систем внутреннего ИТ-контроля
- Понимать и определять риски, связанные с технологическим развитием
- Определить, как различные информационные системы соответствуют или не соответствуют желаемым требованиям безопасности
- Уметь осуществлять процесс постоянного совершенствования кибербезопасности

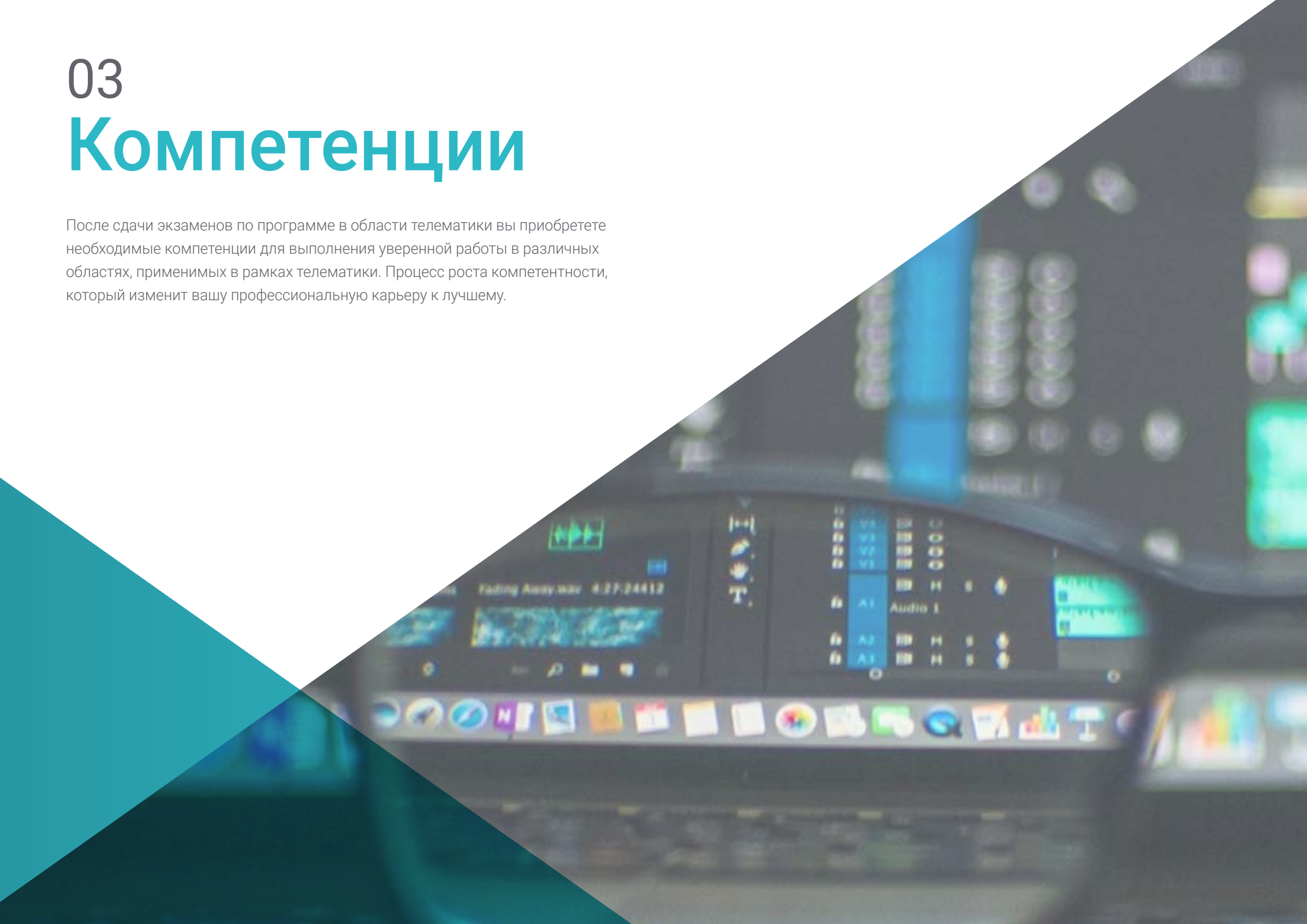
Модуль 10. Управление проектами

- Понимать фундаментальные концепции управления проектами и жизненного цикла управления проектами
- Понять различные этапы управления проектами, такие как инициация, планирование, управление *заинтересованными сторонами* и определение объема работ
- Изучить разработку хронограммы для управления временем, составления бюджета и реагирования на риски
- Понимать функционирование менеджмента качества в проектах, включая планирование, обеспечение, контроль, статистические концепции и доступные инструменты
- Понимать функционирование процессов закупки, выполнения, мониторинга, контроля и закрытия проекта
- Приобрести основные знания, связанные с профессиональной ответственностью в области управления проектами

03

Компетенции

После сдачи экзаменов по программе в области телематики вы приобретете необходимые компетенции для выполнения уверенной работы в различных областях, применимых в рамках телематики. Процесс роста компетентности, который изменит вашу профессиональную карьеру к лучшему.



Приобретите навыки специалиста по телематике и начните работать в этой области с позиции самого современного профессионала"

Общий профессиональный навык

- Разрабатывать телематические приложения и выполнять задачи по обеспечению цифровой безопасности

Специализируйтесь с лучшими и получите место среди лидеров профессиональной работы"

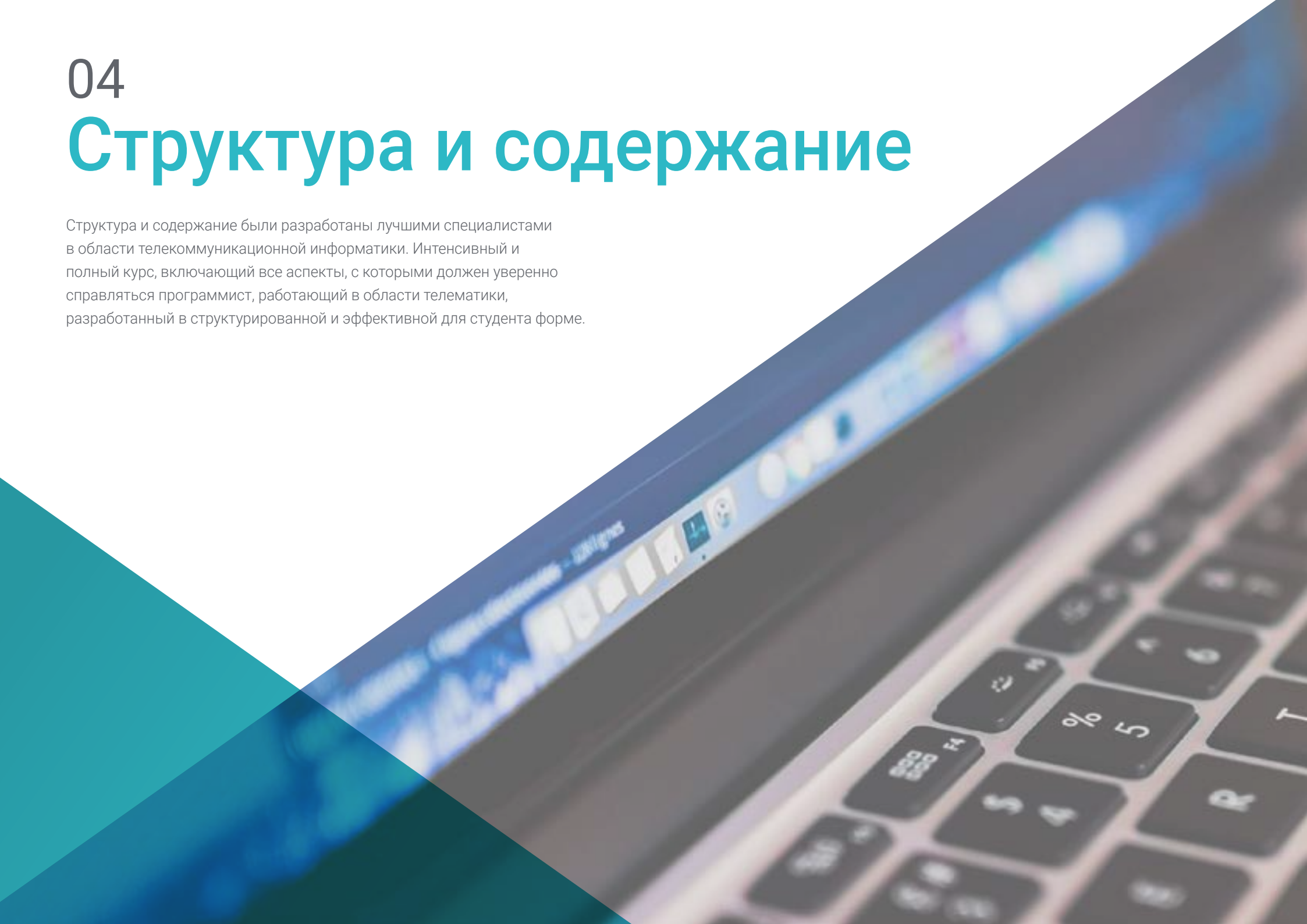
Профессиональные навыки

- Знать всю структуру компьютерных сетей
- Освоить распределенные системы и уметь их классифицировать
- Выполнять задачи по обеспечению безопасности систем и сетей коммуникации
- Применять международные стандарты для сетей
- Освоить все процедуры по обеспечению безопасности ИТ
- Проектировать и управлять центрами обработки данных
- Программировать, выявлять проблемы и устранять неисправности
- Понимать весь процесс проектирования систем
- Проводить системные аудиты и повышать уровень кибербезопасности
- Знать все этапы управления проектом и его жизненный цикл, чтобы уметь управлять ими

04

Структура и содержание

Структура и содержание были разработаны лучшими специалистами в области телекоммуникационной информатики. Интенсивный и полный курс, включающий все аспекты, с которыми должен уверенно справляться программист, работающий в области телематики, разработанный в структурированной и эффективной для студента форме.



Это самая комплексная и современная программа на рынке. Мы стремимся к совершенству и хотим, чтобы вы тоже его достигли"

Модуль 1. Компьютерные сети

1.1. Компьютерные сети в интернете
  1.1.1. Сети и интернет
  1.1.2. Архитектура протокола
1.2. Уровень приложений
  1.2.1. Модель и протоколы
  1.2.2. FTP- и SMTP-сервисы
  1.2.3. DNS-сервис
  1.2.4. Операционная модель HTTP
  1.2.5. Форматы HTTP-сообщений
  1.2.6. Взаимодействие с передовыми методами
1.3. Транспортный уровень
  1.3.1. Коммуникация между процессами
  1.3.2. Транспорт, ориентированный на соединение: TCP и SCTP
1.4. Сетевой уровень
  1.4.1. Коммутация цепей и пакетов
  1.4.2. Протокол IP (v4 и v6)
  1.4.3. Алгоритмы маршрутизации
1.5. Уровень каналов
  1.5.1. Каналы соединения и методы обнаружения и исправления ошибок
  1.5.2. Каналы и протоколы множественного доступа
  1.5.3. Адресация на уровне канала
1.6. Сети LAN
  1.6.1. Топологии сетей
  1.6.2. Сетевые и межсетевые элементы
1.7. IP-адресация
  1.7.1. IP-адресация и *Subnetting*
  1.7.2. Обзор: запрос по протоколу HTTP
1.8. Беспроводные и мобильные сети
  1.8.1. Мобильные сети и услуги 2G, 3G и 4G
  1.8.2. 5G-сети
1.9. Безопасность в сетях
  1.9.1. Основы безопасности в сфере коммуникаций
  1.9.2. Контроль доступа
  1.9.3. Системная безопасность
  1.9.4. Основы криптографии
  1.9.5. Цифровая подпись
1.10. Протоколы интернет-безопасности
  1.10.1. IP-безопасность и виртуальные частные сети (VPN)
  1.10.2. Веб-безопасность с помощью SSL/TLS

Модуль 2. Распределенные системы

2.1. Введение в распределенные вычисления
  2.1.1. Основные понятия
  2.1.2. Монолитные, распределенные, параллельные и кооперативные вычисления
  2.1.3. Преимущества, недостатки и проблемы распределенных систем
  2.1.4. Основы операционных систем: процессы и параллелизм
  2.1.5. Первичный опыт работы с сетями
  2.1.6. Опыт работы в области разработки программного обеспечения
  2.1.7. Организация данного справочника
2.2. Парадигмы распределенных вычислений и межпроцессное взаимодействие
  2.2.1. Коммуникация между процессами
  2.2.2. Синхронизация событий
    2.2.2.1. Сценарий 1: синхронная отправка и синхронный прием
    2.2.2.2. Сценарий 2: асинхронная отправка и синхронный прием
    2.2.2.3. Сценарий 3: синхронная отправка и асинхронный прием
    2.2.2.4. Сценарий 4: асинхронная отправка и асинхронный прием
  2.2.3. Блокировки и таймеры
  2.2.4. Представление и кодирование данных
  2.2.5. Классификация и описание парадигм распределенных вычислений
  2.2.6. Java как среда разработки для распределенных систем

2.3. API *сокеты*
- 2.3.1. API сокеты, типы и различия
- 2.3.2. Датаграммные сокеты
- 2.3.3. Сокеты типа *Stream*
- 2.3.4. Решение проблемы блокировок: таймеры и неблокирующие события
- 2.3.5. Безопасность *сокетов*

2.4 Парадигма связи клиент-сервер
- 2.4.1. Ключевые особенности и концепции распределенных систем клиент-сервер
- 2.4.2. Процесс проектирования и внедрения системы клиент-сервер
- 2.4.3. Проблемы адресации, не ориентированной на соединение с анонимными клиентами
- 2.4.4. Итеративные и параллельные серверы
- 2.4.5. Информация о состоянии и сессии
  - 2.4.5.1. Информация о сессии
  - 2.4.5.2. Информация о глобальном статусе
- 2.4.6. Сложные клиенты, получающие асинхронные ответы со стороны сервера
- 2.4.7. Сложные серверы, выступающие в качестве посредников между несколькими клиентами

2.5. Групповая коммуникация
- 2.5.1. Введение в многоадресную рассылку и общие способы ее использования
- 2.5.2. Надежность и упорядочивание в многоадресных системах
- 2.5.3. Java-реализация многоадресных систем
- 2.5.4. Пример использования одноранговой групповой коммуникации
- 2.5.5. Реализация надежной многоадресной рассылки
- 2.5.6. Многократная передача на уровне приложений

2.6. Распределенные объекты
- 2.6.1. Введение в распределенные объекты
- 2.6.2. Архитектура распределенного объектно-ориентированного приложения
- 2.6.3. Технологии распределенных объектных систем
- 2.6.4. Программные уровни Java RMI на стороне клиента и на стороне сервера
- 2.6.5. Java RMI API для распределенных объектов
- 2.6.6. Шаги по созданию RMI-приложения
- 2.6.7. Использование *Callback* в RMI
- 2.6.8. Динамическая разгрузка кэшей удаленных объектов и менеджер безопасности RMI

2.7. Интернет-приложения I: HTML, XML, HTTP
- 2.7.1. Введение в Интернет-приложения I
- 2.7.2. Язык HTML
- 2.7.3. Язык XML
- 2.7.4. Интернет-протокол HTTP
- 2.7.5. Использование динамического контента: обработка форм и CGI
- 2.7.6. Обработка данных о состоянии и сеансах в Интернете

2.8. CORBA
- 2.8.1. Введение в CORBA
- 2.8.2. Архитектура CORBA
- 2.8.3. Язык описания интерфейсов в CORBA
- 2.8.4. Протоколы операционной совместимости GIOP
- 2.8.5. Ссылки на удаленные объекты IOR
- 2.8.6. Сервис наименования CORBA
- 2.8.7. Пример в IDL Java
- 2.8.8. Этапы проектирования, компиляции и выполнения в IDL Java

2.9. Интернет-приложения II: Applets, Servlets y SOA
- 2.9.1. Введение в интернет-приложения II
- 2.9.2. Applets
- 2.9.3. Введение в сервлет
- 2.9.4. Сервелет HTTP и принцип его работы
- 2.9.5. Ведение информации о состоянии в сервлетах
  - 2.9.5.1. Скрытые поля формы
  - 2.9.5.2. *Файлы cookies*
  - 2.9.5.3. Переменные сервлета
  - 2.9.5.4. Объектная сессия
- 2.9.6. Веб-сервисы
- 2.9.7. Протокол SOAP
- 2.9.8. Краткий обзор архитектуры REST

2.10. Продвинутые парадигмы
- 2.10.1. Введение в продвинутые парадигмы
- 2.10.2. Парадигма MOM
- 2.10.3. Парадигма мобильных программных агентов
- 2.10.4. Парадигма объектного пространства
- 2.10.5. Совместные вычисления
- 2.10.6. Будущие тенденции в распределенных вычислениях

Модуль 3. Безопасность систем и сетей связи

3.1. Глобальное представление о безопасности, криптографии и классическом криптоанализе
- 3.1.1. Компьютерная безопасность: историческая перспектива
- 3.1.2. Но что именно подразумевается под безопасностью?
- 3.1.3. История возникновения криптографии
- 3.1.4. Заменяющие шифровальщики
- 3.1.5. Пример из практики: машина Энигма

3.2. Симметричная криптография
- 3.2.1. Введение и основная терминология
- 3.2.2. Симметричное шифрование
- 3.2.3. Режимы работы
- 3.2.4. DES
- 3.2.5. Новый стандарт AES
- 3.2.6. Потоковый шифр
- 3.2.7. Криптоанализ

3.3. Асимметричная криптография
- 3.3.1. Истоки криптографии с открытым ключом
- 3.3.2. Основные понятия и функционирование
- 3.3.3. RSA-алгоритм
- 3.3.4. Цифровые сертификаты
- 3.3.5. Хранение и управление ключами

3.4. Атаки на сети
- 3.4.1. Сетевые угрозы и атаки
- 3.4.2. Перечисление
- 3.4.3. Перехват трафика: *Снифферы (sniffers)*
- 3.4.4. Атаки типа "отказ в обслуживании"
- 3.4.5. Атаки с отравлением ARP-адресов

3.5. Архитектура безопасности
- 3.5.1. Традиционные архитектуры безопасности
- 3.5.2. Secure Socket Layer: SSL
- 3.5.3. Протокол SSH
- 3.5.4. Виртуальные частные сети (VPN)
- 3.5.5. Механизмы защиты внешних запоминающих устройств
- 3.5.6. Механизмы защиты аппаратного обеспечения

3.6. Методы защиты системы и разработка безопасного кода
- 3.6.1. Безопасность в операционной деятельности
- 3.6.2. Ресурсы и средства контроля
- 3.6.3. Наблюдение
- 3.6.4. Системы обнаружения интрузии
- 3.6.5. Система обнаружения вторжений (СОВ) в *Host*
- 3.6.6. СОВ в сети
- 3.6.7. СОВ на основе сигнатур
- 3.6.8. Системы приманок
- 3.6.9. Основные принципы безопасности при разработке кода
- 3.6.10. Управление неисправностями
- 3.6.11. Враг общества номер 1: переполнение буфера
- 3.6.12. Криптографические боты

3.7. Ботнеты и *спам*
- 3.7.1. Истоки проблемы
- 3.7.2. Процесс рассылки спама
- 3.7.3. Рассылка спама
- 3.7.4. Усовершенствование списков рассылки
- 3.7.5. Методы защиты
- 3.7.6. Сервисы *Antispam,* предлагаемые третьими лицами
- 3.7.7. Практические случаи
- 3.7.8. Экзотический спам

3.8. Веб-аудит и атаки
- 3.8.1. Сбор информации
- 3.8.2. Методы атаки
- 3.8.3. Инструменты

3.9. Вредоносное ПО и вредоносный код
- 3.9.1. Что такое вредоносное ПО?
- 3.9.2. Виды вредоносного ПО
- 3.9.3. Вирус
- 3.9.4. Криптовирус
- 3.9.5. Черви
- 3.9.6. *Adware*
- 3.9.7. *Шпионское программное обеспечение*
- 3.9.8. *Hoaxes*
- 3.9.9. *Фишинг*
- 3.9.10. Трояны
- 3.9.11. Экономика вредоносных программ
- 3.9.12. Возможные решения

3.10. Криминалистическая экспертиза
- 3.10.1. Сбор доказательств
- 3.10.2. Анализ доказательств
- 3.10.3. Антикриминалистические методы
- 3.10.4. Пример из практики

Модуль 4. Корпоративные сети и инфраструктуры

4.1. Транспортные сети
- 4.1.1. Функциональная архитектура транспортных сетей
- 4.1.2. Интерфейс сетевого узла в SDH
- 4.1.3. Элемент сети
- 4.1.4. Качество и доступность сети
- 4.1.5. Управление транспортными сетями
- 4.1.6. Эволюция транспортных сетей

4.2. Классические WAN-архитектуры
- 4.2.1. Глобальные вычислительные сети WAN
- 4.2.2. Стандарты WAN
- 4.2.3. Протоколы инкапсуляции WAN
- 4.2.4. Устройства WAN
  - 4.2.4.1. Роутер
  - 4.2.4.2. Модем
  - 4.2.4.3. *Switch*
  - 4.2.4.4. Коммуникационные серверы
  - 4.2.4.5. *Шлюзы*
  - 4.2.4.6. *Брандмауэр*
  - 4.2.4.7. *Прокси*
  - 4.2.4.8. NAT
- 4.2.5. Типы соединений
  - 4.2.5.1. Соединение точка-точка
  - 4.2.5.2. Переключение цепей
  - 4.2.5.3. Коммутация пакетов
  - 4.2.5.4. Виртуальные схемы WAN

4.3. Сети на базе ATM
- 4.3.1. Введение, характеристики и модель слоев
- 4.3.2. Физический уровень доступа к ATM
  - 4.3.2.1. Подуровень, зависящий от физической среды PM
  - 4.3.2.2. Подуровень конвергенции передачи, TC
- 4.3.3. Ячейка ATM
  - 4.3.3.1. Заголовок
  - 4.3.3.2. Виртуальное соединение
  - 4.3.3.3. Коммутационный узел ATM
  - 4.3.3.4. Управление потоком (загрузка ссылок)
- 4.3.4. Адаптация ячеек AAL
  - 4.3.4.1. Виды AAL-услуг

4.4. Расширенные модели очередей
- 4.4.1. Введение
- 4.4.2. Основы теории очередей
- 4.4.3. Теория базовой системы с очередями
  - 4.4.3.1. Системы M/M/1, M/M/m и M/M/∞
  - 4.4.3.2. Системы M/M/1/k и M/M/m/m
- 4.4.4. Теория продвинутой системы с очередями
  - 4.4.4.1. Система M/G/1
  - 4.4.4.2. Система M/G/1 с приоритетами
  - 4.4.4.3. Сети очередей
  - 4.4.4.4. Моделирование коммуникационных сетей

4.5. Качество обслуживания в корпоративных сетях
- 4.5.1. Основы
- 4.5.2. Факторы QoS в конвергентных сетях
- 4.5.3. Концепции в QoS
- 4.5.4. Политики в QoS

4.5.5. Методы реализации QoS
4.5.6. QoS-модели
4.5.7. Механизмы для развертывания DiffServ QoS
4.5.8. Примеры применения
4.6. Корпоративные сети и инфраструктуры All-Ethernet
4.6.1. Топологии сетей Ethernet
4.6.1.1. Топология Шина
4.6.1.2. Топология Звезда
4.6.2. Формат фрейма Ethernet и IEEE 802.3
4.6.3. Коммутируемая сеть Ethernet
4.6.3.1. Виртуальные сети VLAN
4.6.3.2. Агрегация портов
4.6.3.3. Избыточность соединений
4.6.3.4. Управление QoS
4.6.3.5. Функции безопасности
4.6.4. Fast Ethernet
4.6.5. Gigabit Ethernet
4.7. MPLS-инфраструктуры
4.7.1. Введение
4.7.2. MPLS
4.7.2.1. Предшественники MPLS и его эволюция
4.7.2.2. Архитектура MPLS
4.7.2.3. Повторная отправка маркированных посылок
4.7.2.4. Протокол распределения меток (LDP)

4.7.3. VPN MPLS
- 4.7.3.1. Определение VPN
- 4.7.3.2. Модели VPN
- 4.7.3.3. Модели VPN MPLS
- 4.7.3.4. Архитектура VPN MPLS
- 4.7.3.5. *Virtual Routing Forwarding* (VRF)
- 4.7.3.6. RD
- 4.7.3.7. Route Target (RT)
- 4.7.3.8. Распространение маршрутов VPNv4 в MPLS VPN
- 4.7.3.9. Пересылка пакетов в сети VPN MPLS
- 4.7.3.10. BGP
- 4.7.3.11. Расширенное BGP-сообщество: RT
- 4.7.3.12. Транспортировка меток с помощью BGP
- 4.7.3.13. Route Reflector (RR)
- 4.7.3.14. Группа RR
- 4.7.3.15. Выбор маршрута BGP
- 4.7.3.16. Экспедирование посылок

4.7.4. Общие протоколы *Маршрутизации* в средах MPLS
- 4.7.4.1. Протоколы дистанционно-векторной маршрутизации
- 4.7.4.2. Протоколы маршрутизации состояния каналов связи
- 4.7.4.3. OSPF
- 4.7.4.4. ISIS

4.8. Услуги операторов связи и VPN
- 4.8.1. Введение
- 4.8.2. Основные требования к VPN
- 4.8.3. Типы VPN
  - 4.8.3.1. VPN для удаленного доступа
  - 4.8.3.2. VPN точка-точка
  - 4.8.3.3. Внутренний VPN (через LAN)
- 4.8.4. Протоколы, используемые в VPN
- 4.8.5. Реализации и типы соединений

4.9. NGN (Next Generation Networks)
- 4.9.1. Введение
- 4.9.2. Предыстория
  - 4.9.2.1. Определение и характеристики сети NGN
  - 4.9.2.2. Миграция к сетям следующего поколения
- 4.9.3. Архитектура NGN
  - 4.9.3.1. Первичный уровень подключения
  - 4.9.3.2. Уровень доступа
  - 4.9.3.3. Уровень обслуживания
  - 4.9.3.4. Уровень управления
- 4.9.4. IMS
- 4.9.5. Организации по установлению стандартов
- 4.9.6. Регуляторные тенденции

4.10. Экспертиза стандартов МСЭ и IETF
- 4.10.1. Введение
- 4.10.2. Нормализация
- 4.10.3. Некоторые типовые организации
- 4.10.4. Протоколы и стандарты физического уровня WAN
- 4.10.5. Примеры средоориентированных протоколов

Модуль 5. Архитектура безопасности

5.1. Основные принципы компьютерной безопасности
- 5.1.1. Что понимается под компьютерной безопасностью
- 5.1.2. Цели ИТ-безопасности
- 5.1.3. Услуги по обеспечению ИТ-безопасности
- 5.1.4. Последствия недостаточной безопасности
- 5.1.5. Принцип защиты безопасности
- 5.1.6. Политики, планы и процедуры в области безопасности
  - 5.1.6.1. Управление учетными записями пользователей
  - 5.1.6.2. Идентификация и аутентификация пользователя
  - 5.1.6.3. Авторизация и логическое управление доступом
  - 5.1.6.4. Мониторинг серверов
  - 5.1.6.5. Защита данных
  - 5.1.6.6. Безопасность при удаленных соединениях
- 5.1.7. Важность человеческого фактора

5.2. Стандартизация и сертификация ИТ-безопасности
- 5.2.1. Стандарты безопасности
  - 5.2.1.1. Цель стандартов
  - 5.2.1.2. Ответственные организации
- 5.2.2. Американские стандарты
  - 5.2.2.1. TCSEC
  - 5.2.2.2. Federal Criteria
  - 5.2.2.3. FISCAM
  - 5.2.2.4. NIST SP 800
- 5.2.3. Европейские стандарты
  - 5.2.3.1. ITSEC
  - 5.2.3.2. ITSEM
  - 5.2.3.3. Европейское агентство по сетевой и информационной безопасности
- 5.2.4. Международные стандарты
- 5.2.5. Процесс сертификации

5.3. Угрозы компьютерной безопасности: уязвимости и вредоносные ПО
- 5.3.1. Введение
- 5.3.2. Уязвимости системы
  - 5.3.2.1. Инциденты сетевой безопасности
  - 5.3.2.2. Причины уязвимости ИТ-систем
  - 5.3.2.3. Типы уязвимостей
  - 5.3.2.4. Ответственность производителей ПО
  - 5.3.2.5. Инструменты для оценки уязвимости
- 5.3.3. Угрозы ИТ-безопасности
  - 5.3.3.1. Классификация сетевых взломщиков
  - 5.3.3.2. Мотивы взломщиков
  - 5.3.3.3. Фазы атаки
  - 5.3.3.4. Типы атак
- 5.3.4. Компьютерные вирусы
  - 5.3.4.1. Общие характеристики
  - 5.3.4.2. Типы вирусов
  - 5.3.4.3. Ущерб, наносимый вирусами
  - 5.3.4.4. Как бороться с вирусами

5.4. Кибертерроризм и реагирование на инциденты
- 5.4.1. Введение
- 5.4.2. Угроза кибертерроризма и кибервойн
- 5.4.3. Последствия сбоев и атак на предприятия
- 5.4.4. Шпионаж в компьютерных сетях

5.5. Идентификация пользователя и биометрические системы
- 5.5.1. Введение в аутентификацию, авторизацию и регистрацию пользователей
- 5.5.2. Модель безопасности AAA
- 5.5.3. Контроль доступа
- 5.5.4. Идентификация пользователя
- 5.5.5. Верификация пароля
- 5.5.6. Аутентификация с помощью цифровых сертификатов
- 5.5.7. Удаленная идентификация пользователя
- 5.5.8. Однократный вход в систему
- 5.5.9. Менеджеры паролей
- 5.5.10. Биометрические системы
  - 5.5.10.1. Общие характеристики
  - 5.5.10.2. Типы биометрических систем
  - 5.5.10.3. Внедрение систем

5.6. Основы криптографии и криптографических протоколов
- 5.6.1. Введение в криптографию
  - 5.6.1.1. Криптография, криптоанализ и криптология
  - 5.6.1.2. Работа криптографической системы
  - 5.6.1.3. История криптографических систем
- 5.6.2. Криптоанализ
- 5.6.3. Классификация криптографических систем
- 5.6.4. Симметричные и асимметричные криптографические системы
- 5.6.5. Аутентификация с помощью криптографических систем

5.6.6. Электронная подпись
5.6.6.1. Что такое электронная подпись?
5.6.6.2. Характеристики электронной подписи
5.6.6.3. Органы по сертификации
5.6.6.4. Цифровые сертификаты
5.6.6.5. Системы, основанные на доверии третьих лиц
5.6.6.6. Использование электронных подписей
5.6.6.7. Электронное удостоверение личности
5.6.6.8. Электронные счета-фактуры
5.7. Инструменты сетевой безопасности
5.7.1. Проблема безопасности интернет-соединения
5.7.2. Безопасность во внешней сети
5.7.3. Роль *Прокси*-серверов
5.7.4. Роль брандмауэров
5.7.5. Серверы аутентификации для удаленных подключений
5.7.6. Анализ записей о деятельности
5.7.7. Системы обнаружения вторжений
5.7.8. Приманки
5.8. Безопасность беспроводных и виртуальных частных сетей
5.8.1. Безопасность виртуальных частных сетей
5.8.1.1 Роль VPN
5.8.1.2 Протоколы для VPN
5.8.2. Традиционная безопасность беспроводных сетей
5.8.3. Возможные атаки на беспроводные сети
5.8.4. Протокол WEP
5.8.5. Стандарты безопасности беспроводных сетей
5.8.6. Рекомендации по усилению безопасности
5.9. Безопасность при использовании интернет-услуг
5.9.1. Безопасный веб-серфинг
5.9.1.1. Сервис www
5.9.1.2. Вопросы безопасности www
5.9.1.3. Рекомендации по безопасности
5.9.1.4. Защита конфиденциальности в интернете
5.9.2. Безопасность электронной почты
5.9.2.1. Характеристики электронной почты
5.9.2.2. Вопросы безопасности электронной почты
5.9.2.3. Рекомендации по обеспечению безопасности электронной почты
5.9.2.4. Расширенные услуги электронной почты
5.9.2.5. Использование электронной почты сотрудниками
5.9.3. Спам
5.9.4. *Фишинг*
5.10. Контроль содержания
5.10.1. Распространение контента через интернет
5.10.2. Правовые меры по борьбе с нелегальным контентом
5.10.3. Фильтрация, каталогизация и блокировка контента
5.10.4. Ущерб имиджу и репутации

Модуль 6. Центры обработки данных, эксплуатация сетей и услуги

6.1. Дата-центры: основные понятия и компоненты
6.1.1. Введение
6.1.2. Основные понятия
6.1.2.1. Определение дата-центра
6.1.2.2. Классификация и значение
6.1.2.3. Катастрофы и потери
6.1.2.4. Эволюционная тенденция
6.1.2.5. Издержки, связанные со сложностью
6.1.2.6. Столпы и уровни избыточности
6.1.3. Философия дизайна
6.1.3.1. Цели
6.1.3.2. Выбор местоположения
6.1.3.3. Доступность
6.1.3.4. Критические элементы
6.1.3.5. Оценка и анализ издержек
6.1.3.6. ИТ-бюджет

6.1.4. Базовые компоненты
6.1.4.1. Технический этаж
6.1.4.2. Виды плитки
6.1.4.3. Общие положения
6.1.4.4. Размер центра обработки данных
6.1.4.5. *Телекоммуникационные стойки*
6.1.4.6. Серверы и коммуникационное оборудование
6.1.4.7. Наблюдение

6.2. *Дата-центры:* системы управления
6.2.1. Введение
6.2.2. Электропитание
6.2.2.1. Электрическая сеть
6.2.2.2. Электрическая энергия
6.2.2.3. Стратегии распределения электроэнергии
6.2.2.4. UPS
6.2.2.5. Генераторы
6.2.2.6. Проблемы с электрикой
6.2.3. Мониторинг окружающей среды
6.2.3.1. Температура
6.2.3.2. Влажность
6.2.3.3. Кондиционер
6.2.3.4. Оценка тепловой выработки
6.2.3.5. Стратегии охлаждающей системы
6.2.3.6. Дизайн коридоров. Циркуляция воздуха
6.2.3.7. Датчики и техническое обслуживание
6.2.4. Безопасность и предотвращение пожаров
6.2.4.1. Физическая безопасность
6.2.4.2. Возгорание и его классификация
6.2.4.3. Классификация и типы систем пожаротушения

6.3. *Дата-центры:* проектирование и организация
6.3.1. Введение
6.3.2. Проектирование сети
6.3.2.1. Типологии
6.3.2.2. Структурированная кабельная система
6.3.2.3. Магистральные линии
6.3.2.4. Сетевые кабели UTP и STP
6.3.2.5. Телефонные провода
6.3.2.6. Клеммные элементы
6.3.2.7. Оптоволоконные кабели
6.3.2.8. Коаксиальный кабель
6.3.2.9. Беспроводная передача
6.3.2.10. Рекомендации и маркировка
6.3.3. Организация
6.3.3.1. Введение
6.3.3.2. Основные меры
6.3.3.3. Стратегии управления кабелями
6.3.3.4. Принципы и процедуры
6.3.4. Управление центром обработки данных
6.3.5. Стандарты в *Дата-центрах*

6.4. *Дата-центры*: бизнес-модели и устойчивое развитие
6.4.1. Введение
6.4.2. Оптимизация
6.4.2.1. Методы оптимизации
6.4.2.2. Экологические *дата-центры*
6.4.2.3. Актуальные проблемы
6.4.2.4. Модульные *дата-центры*
6.4.2.5. Housing
6.4.2.6. Консолдиация *дата-центров*
6.4.2.7. Наблюдение

6.4.3. Непрерывность бизнес-деятельности
6.4.3.1. BCP. План по обеспечению непрерывности бизнеса. Ключевые моменты
6.4.3.2. DR. План аварийного восстановления (DRP)
6.4.3.3. Внедрение DR
6.4.3.4. *Backup* и стратегии
6.4.3.5. Резервный *дата-центр*
6.4.4. Передовая практика
6.4.4.1. Рекомендации
6.4.4.2. Использование методологии ITIL
6.4.4.3. Показатели доступности
6.4.4.4. Мониторинг окружающей среды
6.4.4.5. Управление рисками
6.4.4.6. Ответственный за дата-центр
6.4.4.7. Инструменты
6.4.4.8. Советы по внедрению
6.4.4.9. Характеристика
6.5. *Облачные вычисления:* введение и основы
6.5.1. Введение
6.5.2. Основные понятия и терминология
6.5.3. Цели и преимущества
6.5.3.1. Доступность
6.5.3.2. Надежность
6.5.3.3. Масштабируемость
6.5.4. Риски и задачи
6.5.5. Роли. Провайдер. Потребитель
6.5.6. Характеристики облака
6.5.7. Модели предоставления услуг
6.5.7.1. IaaS
6.5.7.2. PaaS
6.5.7.3. SaaS
6.5.8. Виды облачных систем
6.5.8.1. Общественные
6.5.8.2. Частные
6.5.9.3. Гибридные

6.5.9. Технологии, позволяющие использовать облако
6.5.9.1. Сетевые архитектуры
6.5.9.2. Широкополосные сети. Взаимосвязь
6.5.9.3. Технологии дата-центров
6.5.9.3.1. *Computing*
6.5.9.3.2. *Storage*
6.5.9.3.3. *Networking*
6.5.9.3.4. Высокая доступность
6.5.9.3.5. Системы *Backup*
6.5.9.3.6. Балансировщики
6.5.9.4. Виртуализация
6.5.9.5. Веб-технологии
6.5.9.6. Технология Multitenant
6.5.9.7. Технология предоставления услуг
6.5.9.8. Облачная безопасность
6.5.9.8.1. Термины и понятия
6.5.9.8.2. Целостность и аутентификация
6.5.9.8.3. Механизмы безопасности
6.5.9.8.4. Угрозы безопасности
6.5.9.8.5. Атаки на безопасность облака
6.5.9.8.6. Кейс-стади

6.6. *Облачные вычисление*: технологии и безопасность в облаке
6.6.1. Введение
6.6.2. Механизмы облачной инфраструктуры
6.6.2.1. Граница сети
6.6.2.2. Хранение
6.6.2.3. Серверная среда
6.6.2.4. Мониторинг облака
6.6.2.5. Высокая доступность
6.6.3. Механизмы обеспечения безопасности в облаке (часть I)
6.6.3.1. Автоматизация
6.6.3.2. Балансировщики нагрузки
6.6.3.3. Мониторинг SLA
6.6.3.4. Механизмы оплаты по факту
6.6.4. Механизмы обеспечения безопасности в облаке (часть II)
6.6.4.1. Системы отслеживания и аудита
6.6.4.2. Системы Failover
6.6.4.3. Гипервизор
6.6.4.4. Кластеризация
6.6.4.5. Системы Multitenant

6.7. *Облачные вычисления*: инфраструктура. Механизмы контроля и безопасности
6.7.1. Введение в механизмы управления облаком
6.7.2. Системы удаленного администрирования
6.7.3. Системы управления ресурсами
6.7.4. Системы управления соглашениями об уровне обслуживания
6.7.5. Системы управления биллингом
6.7.6. Механизмы обеспечения безопасности облаков
6.7.6.1. Шифрование
6.7.6.2. *Hashing*
6.7.6.3. Цифровая подпись
6.7.6.4. PKI
6.7.6.5. Управление идентификацией и доступом
6.7.6.6. SSO
6.7.6.7. Группы безопасности на основе облачных технологий
6.7.6.8. Бастионные системы

6.8. *Облачные вычисления*: архитектура облака
6.8.1. Введение
6.8.2. Основные облачные архитектуры
6.8.2.1. Архитектуры распределения рабочей нагрузки
6.8.2.2. Архитектуры использования ресурсов
6.8.2.3. Масштабируемые архитектуры
6.8.2.4. Архитектуры балансировки нагрузки
6.8.2.5. Избыточные архитектуры
6.8.2.6. Примеры

6.8.3. Усовершенствованные облачные архитектуры
6.8.3.1. Кластерные архитектуры гипервизоров
6.8.3.2. Виртуальные архитектуры балансировки нагрузки
6.8.3.3. Архитектуры *non-stop*
6.8.3.4. Архитектуры высокой доступности
6.8.3.5. Архитектуры Bare metal
6.8.3.6. Избыточные архитектуры
6.8.3.7. Гибридные архитектуры
6.8.4. Специализированные облачные архитектуры
6.8.4.1. Архитектуры прямого доступа к вводу/выводу
6.8.4.2. Архитектуры прямого доступа LUN
6.8.4.3. Эластичные сетевые архитектуры
6.8.4.4. Архитектура SDDC
6.8.4.5. Специальные архитектуры
6.8.4.6. Примеры
6.9. *Облачные вычисления*: модели предоставления услуг
6.9.1. Введение
6.9.2. Предоставление облачных услуг
6.9.3. Взгляд поставщика услуг
6.9.4. Потребительский взгляд на эти услуги
6.9.5. Практические случаи
6.10. *Облачные вычисления*: модели заключения контрактов, показатели и поставщики услуг
6.10.1. Введение в биллинговые модели и метрики
6.10.2. Модели выставления счетов-фактур
6.10.3. Метрики оплаты по факту использования
6.10.4. Соображения по управлению затратами
6.10.5. Введение в метрики QoS и SLA
6.10.6. Показатели качества обслуживания
6.10.7. Показатели эффективности обслуживания
6.10.8. Показатели масштабируемости услуг
6.10.9. SLA модели обслуживания
6.10.10. Практические случаи

Модуль 7. Расширенное программирование

7.1. Введение в объектно-ориентированное программирование
7.1.1. Введение в объектно-ориентированное программирование
7.1.2. Разработка классов
7.1.3. Введение в унифицированный язык моделирования (UML) для моделирования задач
7.2. Отношения между классами
7.2.1. Абстракция и наследование
7.2.2. Расширенные концепции наследования
7.2.3. Полиморфизм
7.2.4. Состав и агрегация
7.3. Введение в паттерны проектирования для объектно-ориентированных задач
7.3.1. Что такое паттерны проектирования?
7.3.2. Паттерн Фабрика
7.3.3. Паттерн Одиночка
7.3.4. Паттерн Наблюдатель
7.3.5. Паттерн Компоновщик
7.4. Исключения
7.4.1. Что такое исключения?
7.4.2. Перехват и обработка исключений
7.4.3. Запуск исключений
7.4.4. Создание исключений
7.5. Пользовательские интерфейсы
7.5.1. Введение во фреймворк Qt
7.5.2. Расположение
7.5.3. Что такое события?
7.5.4. События: определение и захват
7.5.5. Разработка пользовательского интерфейса

7.6. Введение в параллельное программирование
- 7.6.1. Введение в параллельное программирование
- 7.6.2. Концепция процесса и потока
- 7.6.3. Взаимодействие между процессами или потоками
- 7.6.4. Потоки в C++
- 7.6.5. Преимущества и недостатки параллельного программирования

7.7. Управление потоками и синхронизация
- 7.7.1. Жизненный цикл потока
- 7.7.2. Класс Thread
- 7.7.3. Планирование потоков
- 7.7.4. Группы потоков
- 7.7.5. Демонические потоки
- 7.7.6. Синхронизация
- 7.7.7. Механизмы блокировки
- 7.7.8. Механизмы коммуникации
- 7.7.9. Мониторы

7.8. Распространенные задачи в параллельном программировании
- 7.8.1. Задача "производитель – потребитель"
- 7.8.2. Задача о читателях — писателях
- 7.8.3. Задача об обедающих философах

7.9. Документация и тестирование программного обеспечения
- 7.9.1. Почему важно документировать программное обеспечение?
- 7.9.2. Проектная документация
- 7.9.3. Использование инструментов для документирования

7.10. Тестирование программного обеспечения
- 7.10.1. Введение в тестирование программного обеспечения
- 7.10.2. Виды тестирования
- 7.10.3. Единичное тестирование
- 7.10.4. Интеграционное тестирование
- 7.10.5. Валидационное тестирование
- 7.10.6. Тестирование системы

Модуль 8. Системный инжиниринг и сетевые услуги

8.1. Введение в проектирование систем и сетевых услуг
- 8.1.1. Концепция компьютерных систем и компьютерный инжиниринг
- 8.1.2. Программное обеспечение и его возможности
  - 8.1.2.1. Характеристики ПО
- 8.1.3. Эволюция ПО
  - 8.1.3.1. Рассвет разработки ПО
  - 8.1.3.2. Кризис ПО
  - 8.1.3.3. Разработка ПО
  - 8.1.3.4. Трагедия ПО
  - 8.1.3.5. Актуальное положение ПО
- 8.1.4. Мифы о ПО
- 8.1.5. Новые задачи перед ПО
- 8.1.6. Профессиональная деонтология разработки ПО
- 8.1.7. SWEBOK. Совокупность знаний в области программной инжиниринга

8.2. Процесс разработки
- 8.2.1. Процесс решения проблем
- 8.2.2. Процесс разработки ПО
- 8.2.3. Программный процесс в сравнении с жизненным циклом
- 8.2.4. Жизненные циклы. Модели процессов (традиционные)
  - 8.2.4.1. Каскадная модель
  - 8.2.4.2. Модели, основанные на прототипах
  - 8.2.4.3. Инкрементная модель разработки
  - 8.2.4.4. Быстрая разработка приложений (RAD)
  - 8.2.4.5. Спиральная модель
  - 8.2.4.6. Унифицированный процесс разработки или Rational Unified Process (RUP)
  - 8.2.4.7. Разработка ПО на основе компонентов
- 8.2.5. Манифест Agile. Методы Agile
  - 8.2.5.1. Экстремальное программирование (XP)
  - 8.2.5.2. Scrum
  - 8.2.5.3. Feature Driven Development (FDD)
- 8.2.6. Стандарты процессов ПО
- 8.2.7. Определение процесса ПО
- 8.2.8. Зрелость ПО

8.3. Планирование и управление проектами Agile
- 8.3.1. Что такое Agile?
  - 8.3.1.1. История Agile
  - 8.3.1.2. Манифест Agile
- 8.3.2. Основы Agile
  - 8.3.2.1. Мышление Agile
  - 8.3.2.2. Согласование с Agile
  - 8.3.2.3. Жизненный цикл разработки продукта
  - 8.3.2.4. Железный треугольник
  - 8.3.2.5. Работа с неопределенностью и неустойчивостью
  - 8.3.2.6. Определенные процессы и эмпирические процессы
  - 8.3.2.7. Мифы об Agile
- 8.3.3. Среда Agile
  - 8.3.3.1. Операционная модель
  - 8.3.3.2. Роли Agile
  - 8.3.3.3. Техники Agile
  - 8.3.3.4. Agile-практики
- 8.3.4. Agile-фреймворки
  - 8.3.4.1. e-Xtreme Programming (XP)
  - 8.3.4.2. Scrum
  - 8.3.4.3. Dynamic Systems Development Method (DSDM)
  - 8.3.4.4. Agile Project Management
  - 8.3.4.5. Kanban
  - 8.3.4.6. Lean software Development
  - 8.3.4.7. Lean Start-up
  - 8.3.4.8. Scaled Agile Framework (SAFe)

8.4. Управление конфигурацией и совместные репозитории
- 8.4.1. Основы управления конфигурацией ПО
  - 8.4.1.1. Что такое управление конфигурацией ПО?
  - 8.4.1.2. Конфигурация ПО и элементы конфигурации ПО
  - 8.4.1.3. Базовые линии
  - 8.4.1.4. Версии, ревизии, варианты и *Releases*

8.4.2. Деятельность по управлению конфигурацией
8.4.2.1. Идентификация конфигурации
8.4.2.2. Управление изменениями конфигурации
8.4.2.3. Формирование отчетов о состоянии
8.4.2.4. Аудит конфигурации
8.4.3. План управления конфигурацией
8.4.4. Инструменты по управлению конфигурацией
8.4.5. Управление конфигурацией в методологии Metrics v.3
8.4.6. Управление конфигурацией в SWEBOK
8.5. Тестирование систем и услуг
8.5.1. Общие концепции проверки
8.5.1.1. Проверяйте и подтверждайте
8.5.1.2. Определение доказательств
8.5.1.3. Принципы доказательств
8.5.2. Подходы к проверке
8.5.2.1. Тестирование методом «белого ящика»
8.5.2.2. Тестирование методом «черного ящика»
8.5.3. Статические тесты или ревизионные тесты
8.5.3.1. Формальные технические проверки
8.5.3.2. *Walkthroughs*
8.5.3.3. Проверки кодов
8.5.4. Динамическое тестирование
8.5.4.1. Единичное или модульное тестирование
8.5.4.2. Интеграционное тестирование
8.5.4.3. Тестирование системы
8.5.4.4. Тестирование принятия
8.5.4.5. Тестирование регрессии
8.5.5. Альфа-тестирование и бета-тестирование
8.5.6. Процесс тестирования
8.5.7. Ошибка, дефект и неудача
8.5.8. Инструменты автоматического тестирования
8.5.8.1. Junit
8.5.8.2. LoadRunner

8.6. Моделирование и проектирование сетевых архитектур
- 8.6.1. Введение
- 8.6.2. Характеристики систем
  - 8.6.2.1. Описание систем
  - 8.6.2.2. Описание и характеристики услуг
  - 8.6.2.3. Требования к эксплуатационной пригодности
- 8.6.3. Анализ требований
  - 8.6.3.1. Требования к пользователю
  - 8.6.3.2. Требования к применению
  - 8.6.3.3. Требования к сети
- 8.6.4. Проектирование сетевых архитектур
  - 8.6.4.1. Референсная архитектура и компоненты
  - 8.6.4.2. Архитектурные модели
  - 8.6.4.3. Системные и сетевые архитектуры

8.7. Моделирование и проектирование распределенных систем
- 8.7.1. Введение
- 8.7.2. Архитектура адресации и *Routing*
  - 8.7.2.1. Стратегия адресации
  - 8.7.2.2. Стратегия маршрутизации
  - 8.7.2.3. Проектные соображения
- 8.7.3. Концепции проектирования сетей
- 8.7.4. Процесс проектирования

8.8. Платформы и среды развертывания
- 8.8.1. Введение
- 8.8.2. Распределенные компьютерные системы
  - 8.8.2.1. Основные понятия
  - 8.8.2.2. Компьютерные модели
  - 8.8.2.3. Преимущества, недостатки и проблемы
  - 8.8.2.4. Основы операционных систем
- 8.8.3. Развертывание виртуализированных сетей
  - 8.8.3.1. Необходимость изменений
  - 8.8.3.2. Трансформация сетей: от "all-IP" к облаку
  - 8.8.3.3. Развертывание облачной сети
- 8.8.4. Пример: архитектура сети в Azure

8.9. Производительность E2E: задержка и пропускная способность. QoS
- 8.9.1. Введение
- 8.9.2. Анализ производительности
- 8.9.3. QoS
- 8.9.4. Приоритизация и управление трафиком
- 8.9.5. Соглашения об уровне обслуживания
- 8.9.6. Проектные соображения
  - 8.9.6.1. Оценка эффективности
  - 8.9.6.2. Взаимоотношения и взаимодействия

8.10. Автоматизация и оптимизация сетей
- 8.10.1. Введение
- 8.10.2. Управление сетью
  - 8.10.2.1. Протоколы управления и конфигурации
  - 8.10.2.2. Архитектуры управления сетями
- 8.10.3. Оркестровка и автоматизация
  - 8.10.3.1. Архитектура ONAP
  - 8.10.3.2. Регуляторы и функции
  - 8.10.3.3. Политика
  - 8.10.3.4. Инвентаризация сети
- 8.10.4. Оптимизация

Модуль 9. Аудит информационных систем

9.1. Аудит информационных систем. Стандарты надлежащей практики
- 9.1.1. Введение
- 9.1.2. Аудит и COBIT
- 9.1.3. Аудит систем управления ИКТ
- 9.1.4. Сертификация

9.2. Концепции и методологии аудита систем
- 9.2.1. Введение
- 9.2.2. Методологии оценки систем: количественная и качественная
- 9.2.3. Методологии ИТ-аудита
- 9.2.4. План аудита

9.3. Договор о проведении аудита
- 9.3.1. Правовая природа договора
- 9.3.2. Стороны договора о проведении аудита
- 9.3.3. Предмет договора о проведении аудита
- 9.3.4. Аудиторское заключение

9.4. Организационные элементы аудита
- 9.4.1. Введение
- 9.4.2. Миссия отдела аудита
- 9.4.3. Планирование аудита
- 9.4.4. Методология аудита ИС

9.5. Правовая база для проведения аудита
- 9.5.1. Защита персональных данных
- 9.5.2. Правовая защита ПО
- 9.5.3. Технологические преступления
- 9.5.4. Прием на работу, подпись и электронный ID

9.6. Аудит аутсорсинга и системы отсчета
- 9.6.1. Введение
- 9.6.2. Основные принципы аутсорсинга
- 9.6.3. Аудит ИТ-аутсорсинга
- 9.6.4. Системы отсчета: CMMI, ISO27001, ITIL

9.7. Аудит информационной безопасности
- 9.7.1. Введение
- 9.7.2. Физическая и логическая безопасность
- 9.7.3. Безопасность среды
- 9.7.4. Планирование и проведение аудита физической безопасности

9.8. Аудит сети и интернета
- 9.8.1. Введение
- 9.8.2. Уязвимости в сети
- 9.8.3. Принципы и права в интернете
- 9.8.4. Контроль и обработка данных

9.9. Аудит IT-приложений и систем
- 9.9.1. Введение
- 9.9.2. Эталонные модели
- 9.9.3. Оценка качества приложений
- 9.9.4. Аудит организации и управления зоной развития и обслуживания

9.10. Аудит персональных данных
- 9.10.1. Введение
- 9.10.2. Законы и нормативные акты о защите данных
- 9.10.3. Разработка аудиторской проверки
- 9.10.4. Нарушения и санкции

Модуль 10. Управление проектами

10.1. Фундаментальные концепции управления проектами и жизненного цикла управления проектами
- 10.1.1. Что такое проект?
- 10.1.2. Общая методология
- 10.1.3. Что такое управление проектами?
- 10.1.4. Что такое план проекта?
- 10.1.5. Преимущества
- 10.1.6. Жизненные циклы проекта
- 10.1.7. Группы процессов или жизненный цикл управления проектами
- 10.1.8. Взаимосвязь между группами процессов и областями знаний
- 10.1.9. Взаимосвязи между жизненным циклом продукта и проекта

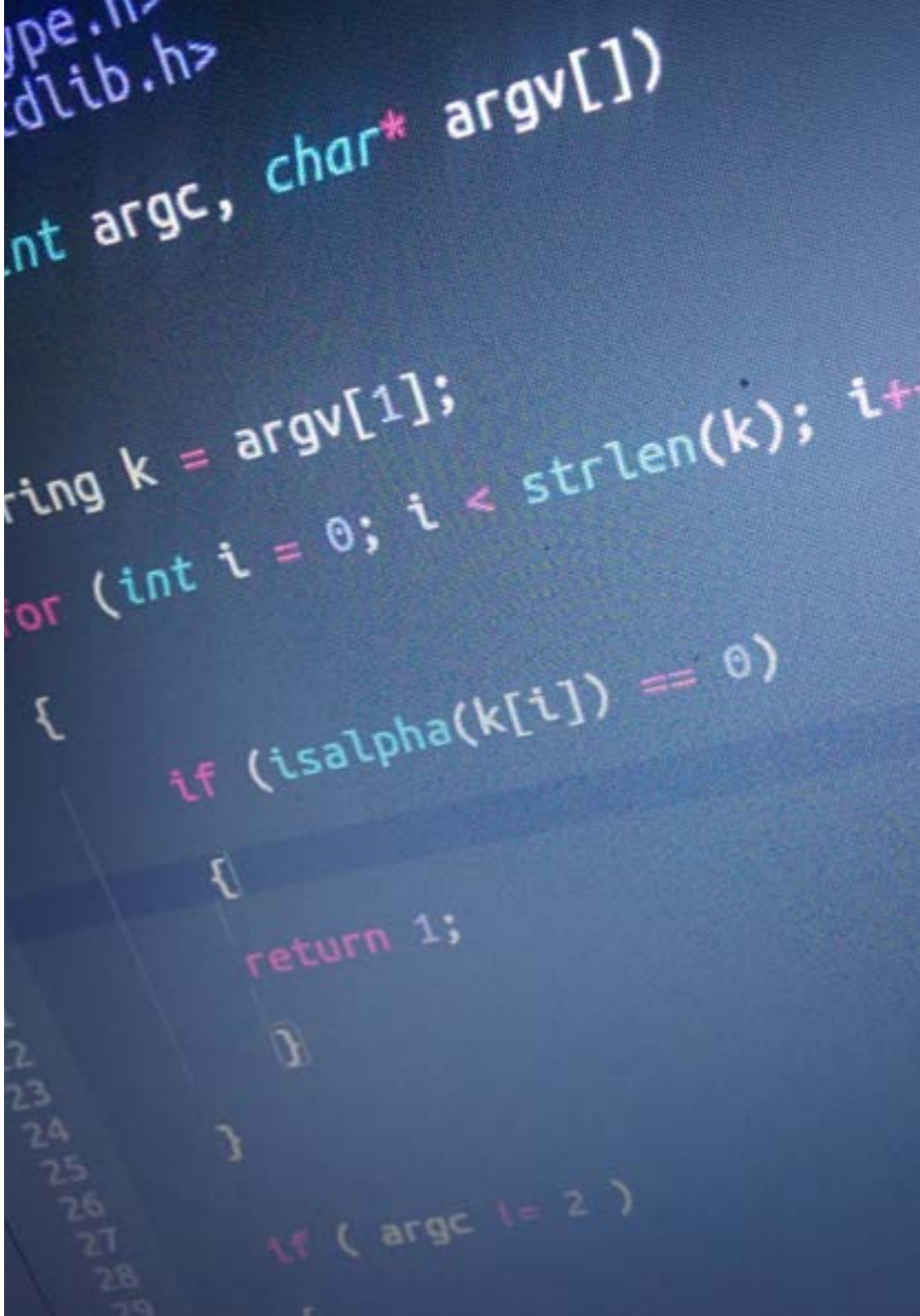
10.2. Запуск и планирование
- 10.2.1. От идеи до реализации проекта
- 10.2.2. Разработка акта проекта
- 10.2.3. Начальное совещание по проекту
- 10.2.4. Задачи, знания и навыки в процессе запуска
- 10.2.5. План проекта
- 10.2.6. Разработка основного плана Шаги
- 10.2.7. Задачи, знания и навыки в процессе планирования

10.3. Управление *заинтересованными сторонами* и масштабами деятельности
- 10.3.1. Выявление заинтересованных сторон
- 10.3.2. Разработка плана по управлению заинтересованными сторонами
- 10.3.3. Управление взаимодействием между заинтересованными сторонами
- 10.3.4. контроль взаимодействия между заинтересованными сторонами
- 10.3.5. Цель проекта
- 10.3.6. Управление аутрич-работой и ее план
- 10.3.7. Сбор информации о требованиях
- 10.3.8. Определение сферы применения
- 10.3.9. Создание WBS (EDT)
- 10.3.10. Утверждение и контроль масштаба

10.4. Разработка расписания
- 10.4.1. Управление временем и его планирование
- 10.4.2. Определение деятельности
- 10.4.3. Составление последовательности деятельности
- 10.4.4. Оценка ресурсов деятельности
- 10.4.5. Предполагаемая продолжительность деятельности
- 10.4.6. Разработка графика и расчет критического пути
- 10.4.7. Контроль расписания

10.5. Составление бюджета и реагирование на риски
- 10.5.1. Оценка затрат
- 10.5.2. Разработка бюджета и S-образной кривой
- 10.5.3. Контроль затрат и метод оценки стоимости
- 10.5.4. Понятие риска
- 10.5.5. Как проводить анализ рисков
- 10.5.6. Разработка плана реагирования

10.6. Управление качеством
- 10.6.1. Планирование качества
- 10.6.2. Обеспечение качества
- 10.6.3. Контроль качества
- 10.6.4. Основные статистические концепции
- 10.6.5. Инструменты в области управления качеством



10.7. Коммуникация и человеческие ресурсы
- 10.7.1. Планирование управления коммуникациями
- 10.7.2. Анализ требований к коммуникациям
- 10.7.3. Коммуникационные технологии
- 10.7.4. Модели коммуникации
- 10.7.5. Методы коммуникации
- 10.7.6. План управления коммуникациями
- 10.7.7. Управление коммуникациями
- 10.7.8. Управление человеческими ресурсами
- 10.7.9. Основные участники и их роли в проектах
- 10.7.10. Типы организаций
- 10.7.11. Организация проекта
- 10.7.12. Рабочая группа

10.8. Закупка
- 10.8.1. Процесс закупок
- 10.8.2. Планирование
- 10.8.3. Поиск поставщиков и запрос на тендеры
- 10.8.4. Заключение контракта
- 10.8.5. Администрирование контракта
- 10.8.6. Контракты
- 10.8.7. Виды контрактов
- 10.8.8. Ведение переговоров по контракту

10.9. Выполнение, мониторинг и контроль и закрытие
- 10.9.1. Группы процессов
- 10.9.2. Осуществление проекта
- 10.9.3. Наблюдение и контроль проекта
- 10.9.4. Завершение проекта

10.10. Профессиональная ответственность
- 10.10.1. Профессиональная ответственность
- 10.10.2. Характеристики социальной и профессиональной ответственности
- 10.10.3. Кодекс этических норм руководителя проекта
- 10.10.4. Ответственность vs. PMP®
- 10.10.5. Примеры ответственности
- 10.10.6. Преимущества профессионализации

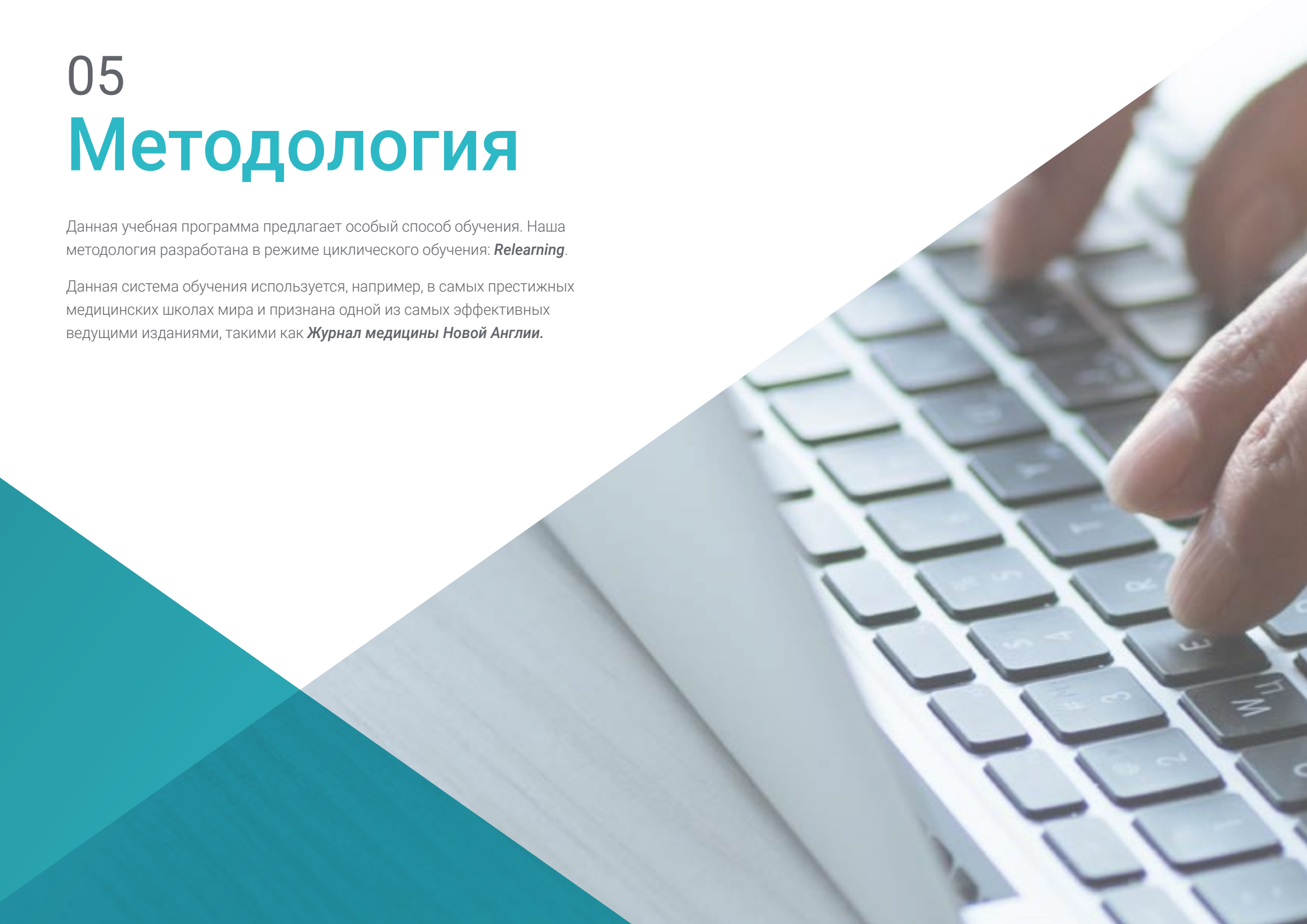
Процесс профессионального и личностного роста, который станет огромным толчком к повышению вашей конкурентоспособности"

05

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*

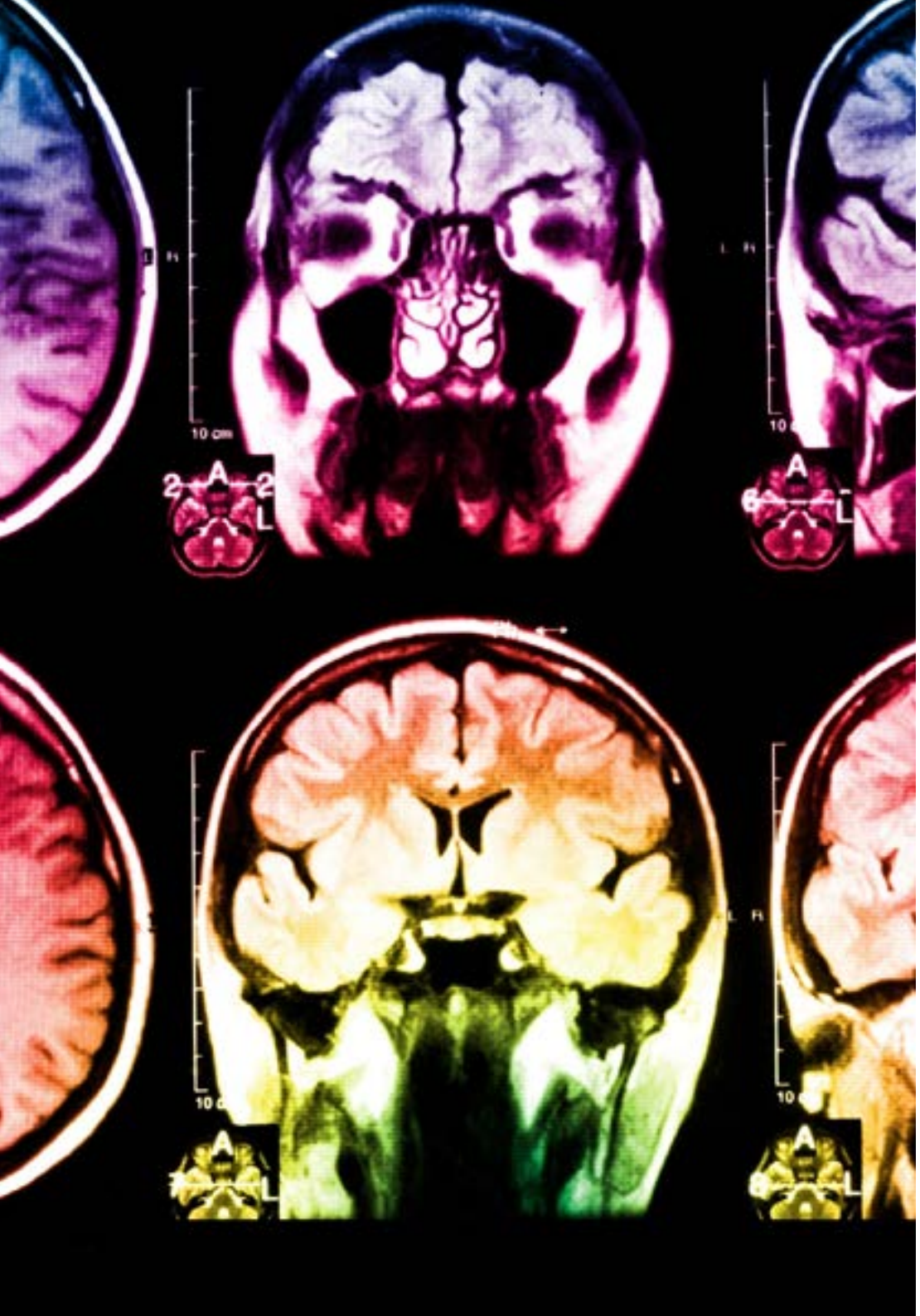
TECH эффективно объединяет метод кейсов с системой 100% онлайн-обучения, основанной на повторении, которая сочетает различные дидактические элементы в каждом уроке.

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.

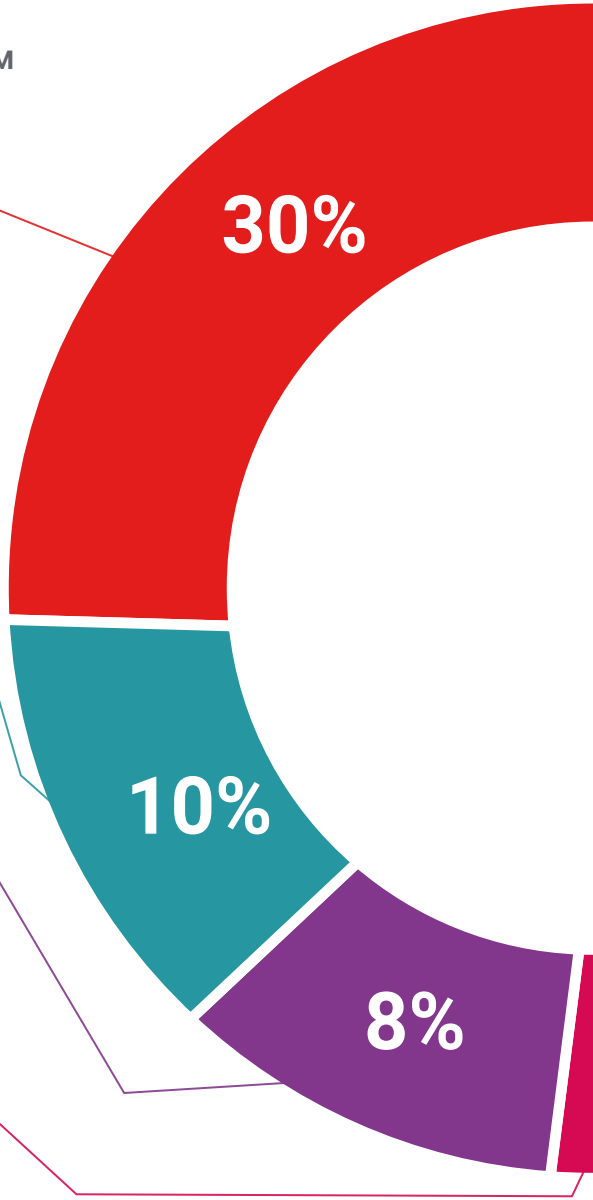
Так называемый метод обучения у эксперта укрепляет знания и память, а также формирует уверенность в наших будущих сложных решениях.

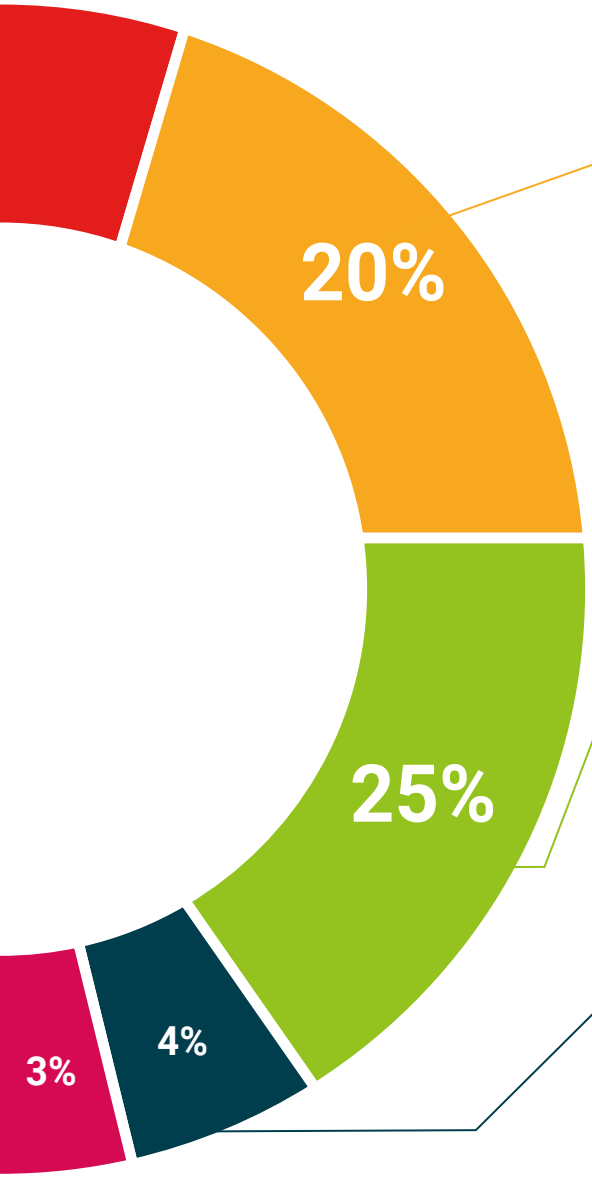
Практика навыков и компетенций

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.

06

Квалификация

Специализированная магистратура в области Телематика 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 оформлением документов"

Данная **Специализированная магистратура в области Телематика** содержит самую полную и современную программу на рынке.

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

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

Диплом: **Специализированная магистратура в области Телематика**

Количество учебных часов: **1500 часов**


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

Телематика

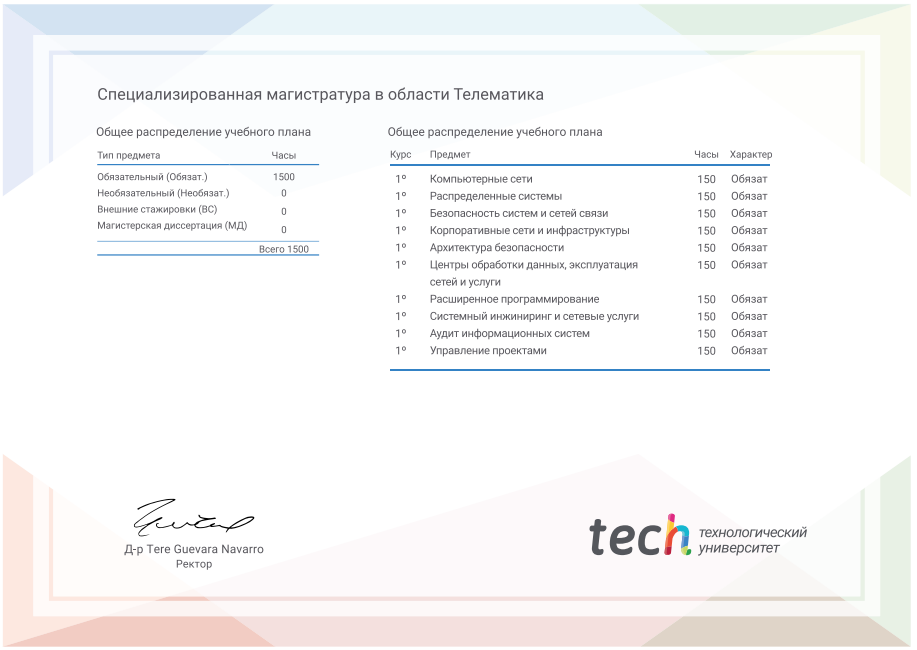
Данный диплом специализированной программы, присуждаемый Университетом, соответствует 1500 учебным часам, с датой начала дд/мм/гггг и датой окончания дд/мм/гггг.

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

17 июня 2020 г.

Д-р Tere Guevara Navarro
Ректор

unique TECH code: AFWOR23S techtitute.com/certificates


Специализированная магистратура в области Телематика

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	Компьютерные сети	150	Обязат
1º	Распределенные системы	150	Обязат
1º	Безопасность систем и сетей связи	150	Обязат
1º	Корпоративные сети и инфраструктуры	150	Обязат
1º	Архитектура безопасности	150	Обязат
1º	Центры обработки данных, эксплуатация сетей и услуги	150	Обязат
1º	Расширенное программирование	150	Обязат
1º	Системный инжиниринг и сетевые услуги	150	Обязат
1º	Аудит информационных систем	150	Обязат
1º	Управление проектами	150	Обязат

Д-р Tere Guevara Navarro
Ректор

tech технологический университет

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

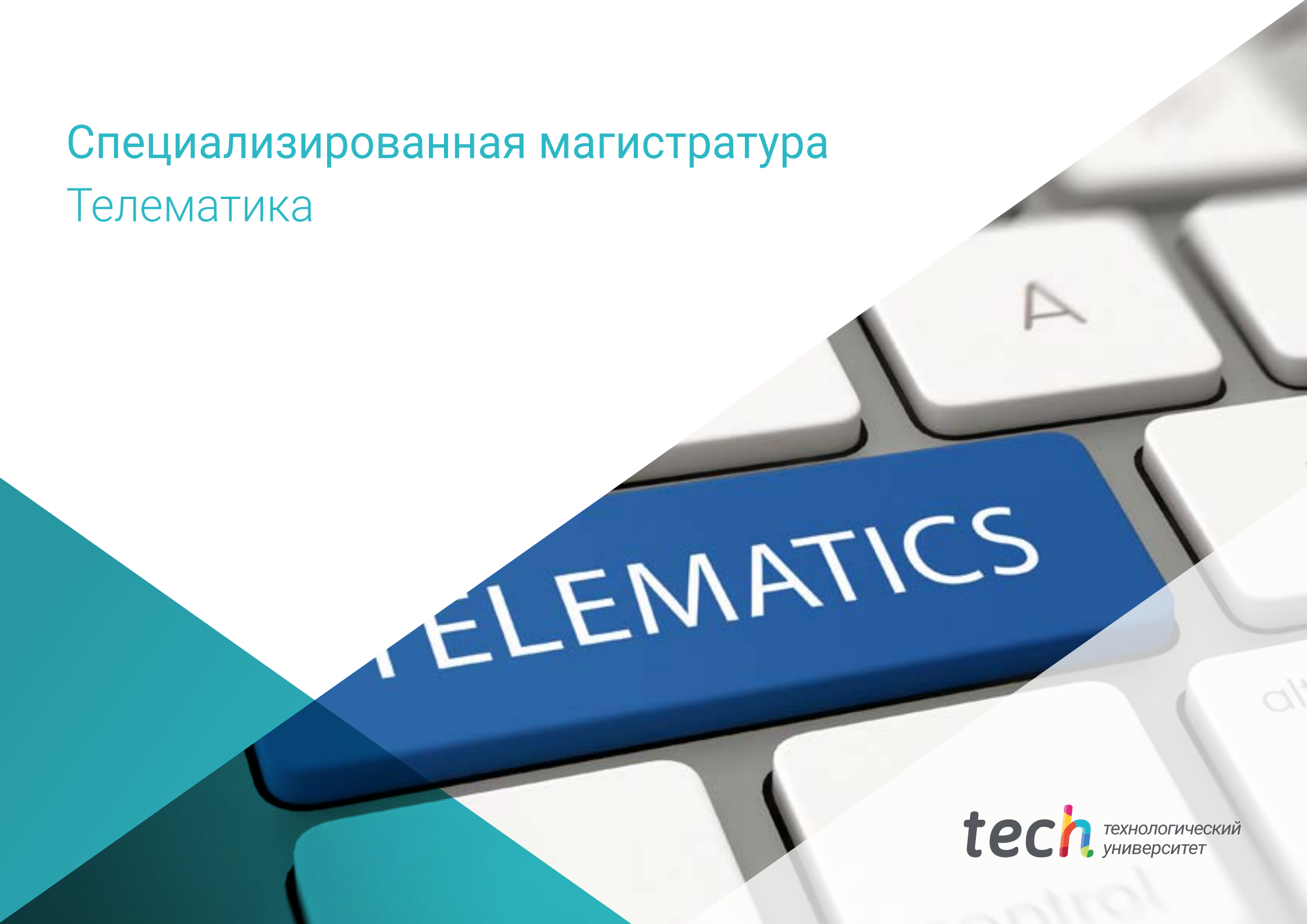
tech технологический университет

Специализированная магистратура

Телематика

- Формат: **онлайн**
- Продолжительность: **12 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Режим обучения: **16ч./неделя**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

Специализированная магистратура
Телематика



tech технологический университет