

Профессиональная магистерская специализация

Компьютерные науки,
кибербезопасность и
аналитика данных





Профессиональная магистерская специализация

Компьютерные науки,
кибербезопасность и
аналитика данных

- » Формат: **онлайн**
- » Продолжительность: 2 года
- » Учебное заведение: **TECH Технологический университет**
- » Режим обучения: 16ч./неделя
- » Расписание: по своему усмотрению
- » Экзамены: **онлайн**

Веб-доступ: www.techtitute.com/ru/informatica/information-technology/advanced-master-degree/advanced-master-degree-computer-science-cybersecurity-data-analysis

Оглавление

01

Презентация

стр. 4

02

Цели

стр. 8

03

Компетенции

стр. 20

04

Руководство курса

стр. 24

05

Структура и содержание

стр. 32

06

Методология

стр. 60

07

Квалификация

стр. 68

01

Презентация

В современном мире, движущемся к полной цифровизации, ИТ-специалистам необходимо постоянно обновлять свои навыки, чтобы продолжать полноценно работать в области своих компетенций, а также быть в курсе последних инноваций которые сегодня внедряются в эту область с головокружительной скоростью. Появление новых систем генерации данных и информации стало центральным фактором развития многих отраслей промышленности и отдельных компаний. Все больше базовых процессов, операций и задач разного рода выполняются с помощью электронных устройств. Но подобный технический прогресс также сопровождается определенными рисками, поскольку все виды цифровых устройств и приложений могут быть подвержены кибератакам. По этой причине была разработана эта 100% онлайн-программа, в которой фокус обучения сосредоточен на направлениях знаний, необходимых для обработки и сбора данных, формирования собственного подхода к кибербезопасности, а также углубления знаний в области *компьютерных наук*, как с теоретической, так и с практической точки зрения.



“

Станьте экспертом в области кибербезопасности, освоив компьютерные науки и аналитику данных, и значительно увеличьте ваши шансы на трудоустройство в динамично развивающемся секторе”

Благодаря непрерывному прогрессу в области вычислительной техники значительно улучшились не только технологии, но и сами цифровые инструменты, с помощью которых сегодня выполняются многие задачи. Обратная сторона медали заключается в том, что подобные достижения также привели к росту ИТ-уязвимостей. По этой причине все больше компаний ищут профессионалов, специализирующихся на кибербезопасности, которые могут обеспечить им адекватную защиту от всех видов кибератак.

В рамках этой Профессиональной магистерской специализации в области компьютерных наук, кибербезопасности и аналитики данных ИТ-специалист сможет углубиться в такие вопросы, как безопасность при разработке и проектировании систем, лучшие криптографические методы или безопасность при *облачных вычислениях*. Кроме того, в этой программе основное внимание уделяется основам программирования и структурам данных, алгоритмам и сложности систем, а также продвинутому проектированию алгоритмов, продвинутому программированию, языковым процессорам и компьютерной графике и др. Все это дополняется многочисленными мультимедийными учебными ресурсами, которые преподаются самыми престижными и профессиональными преподавателями в этой области.

С другой стороны, эта Профессиональная магистерская специализация рассматривает науку о данных с технической и деловой точки зрения, предлагая необходимые сведения для получения знаний, заключенных в данных материалах. Таким образом, ИТ-специалисты смогут детально проанализировать различные алгоритмы, платформы и современные инструменты для исследования, визуализации, манипулирования, обработки и анализа данных. Все вышеперечисленное дополняется развитием деловых навыков, необходимых для достижения рабочего профиля на руководящем уровне, с которым студент сможет принимать ключевые решения в компании.

Таким образом, обучение на данной программе даст специалисту конкретные инструменты и навыки для успешного развития своей профессиональной деятельности в масштабной среде вычислительной техники. Студент будет работать над ключевыми компетенциями, такими как получение актуальных знаний и освоение ежедневной практики в различных областях ИТ, а также развитие ответственности в вопросах отслеживания и контроля за своей работой, а также над конкретными навыками в каждой области.

Окончив эту программу, ИТ-специалисты смогут специализироваться в области компьютерных наук, кибербезопасности и аналитики данных, что сделает данную Профессиональную магистерскую специализацию идеальной возможностью для развития их профессиональной карьеры. Все это станет реальностью благодаря 100% онлайн-программе, которая адаптируется к ежедневным потребностям специалистов, поэтому для начала работы над полноценным профессиональным профилем с международной перспективой достаточно иметь устройство с выходом в интернет.

Данная **Профессиональная магистерская специализация в области компьютерных наук, кибербезопасности и аналитики данных** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- ♦ Разработка практических кейсов, представленных экспертами в области информатики
- ♦ Наглядное, схематичное и исключительно практичное 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 в области кибербезопасности и аналитики данных
- ♦ 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



Получите необходимые знания в удобной и простой форме в области компьютерных наук, кибербезопасности и аналитики данных для качественного программирования"

“

TECH предоставляет к вашим услугам широкий и понятный дидактический материал, который включает в себя все актуальные темы, необходимые для того, чтобы вы могли продолжать развиваться в области вычислительной техники”

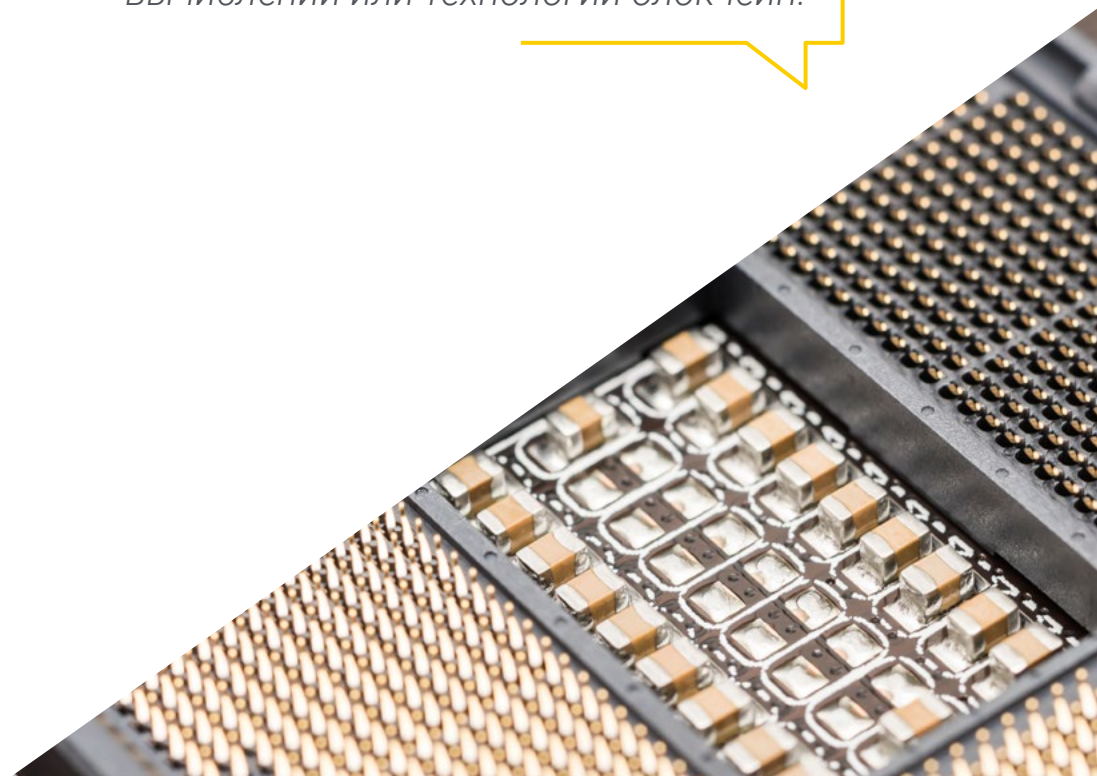
В преподавательский состав входят профессионалы в области информатики, которые вносят свой опыт работы в эту программу, а также признанные специалисты, принадлежащие к ведущим научным сообществам и престижным университетам.

Мультимедийное содержание, разработанное с использованием новейших образовательных технологий, позволит профессионалам проходить обучение в симулированной среде, обеспечивающей иммерсивный учебный процесс, основанный на обучении в реальных ситуациях.

В центре этой программы — проблемно-ориентированное обучение, с помощью которого студент попытается решить различные ситуации из профессиональной практики, возникающие в течение учебного курса. В этом студенту будет помогать инновационная интерактивная видеосистема, созданная известными и опытными специалистами.

Ускорьте развитие своей карьеры за счет создания системы показателей и KPI, в зависимости от отдела, в котором вы работаете.

Узнайте от специалистов о лучших методах обеспечения безопасности, применяемых в средах облачных вычислений или технологии блокчейн.



02

Цели

Профессиональная магистерская специализация в области компьютерных наук, кибербезопасности и аналитики данных создана специально для ИТ-специалистов, желающих быстро и качественно продвинуться в этой сфере. Поэтому данная программа основана на достижении реалистичных и высоких целей, которые позволят вам перейти на новый уровень работы в этой области. Специалист будет сосредоточен на изучении различных методов, технологий и этапов, необходимых для вычислительной техники, с прорывной, комплексной и современной точки зрения.





“

TECH предлагает высококачественную специализацию, которая позволит вам уверенно работать с вычислительной техникой с гарантией безопасности для вашей компании”



Общие цели

- ♦ Быть современным в научном и технологическом плане, а также подготовиться к профессиональной практике межотраслевым и разносторонним образом в области вычислительной техники и языков программирования и быть адаптированным к новым технологиям и инновациям в этой области
- ♦ Сформировать специализированные знания об информационных системах, видах 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
- ♦ Проанализировать организационную и функциональную структуру области информационной безопасности (офис CISO)
- ♦ Анализировать и развивать концепцию риска, неопределенности в среде, в которой мы живем
- ♦ Изучить модель управления рисками на основе стандарта ISO 31000
- ♦ 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
- ♦ Сформировать специализированные знания об экосистеме кибербезопасности
- ♦ Оценить знания в области кибербезопасности
- ♦ Определять области безопасности в облаке
- ♦ Провести анализ услуг и инструментов в каждом из областей безопасности
- ♦ Разрабатывать спецификации безопасности для каждой технологии LPWAN
- ♦ Провести сравнительный анализ безопасности технологий LPWAN
- ♦ Проанализировать эффективность применения методов анализа данных в каждом отделе компании
- ♦ Разработать основу для понимания потребностей и приложений каждого отдела
- ♦ Получить специализированные знания для выбора подходящего инструмента
- ♦ Предложить методы и задачи, чтобы быть максимально продуктивным в соответствии с требованиями отдела



Конкретные цели

Модуль 1. Основы программирования

- ◆ Понимать базовую структуру компьютера, программного обеспечения и языки программирования общего назначения
- ◆ Научиться разрабатывать и интерпретировать алгоритмы, которые являются необходимой основой для разработки программного обеспечения
- ◆ Знать основные элементы компьютерных программ, такие как различные типы данных, операторы, выражения, операторы ввода-вывода и управляющие операторы
- ◆ Знать различные структуры данных, доступные в языках программирования общего назначения, как статических, так и динамических, а также приобрести необходимые знания по работе с файлами
- ◆ Знать различные методы тестирования программного обеспечения, а также понимать важность создания хорошей документации вместе с хорошим исходным кодом
- ◆ Изучить основы языка программирования C++, одного из самых распространенных языков программирования в мире

Модуль 2. Структура данных

- ◆ Изучить основы программирования на языке C++, включая классы, переменные, условные выражения и объекты
- ◆ Понимать, что такое абстрактные типы данных, линейные типы структур данных, простые и сложные иерархические структуры данных и как их реализовать на C++
- ◆ Понимать работу расширенных структур данных, отличных от обычных
- ◆ Понимать теорию и практику, связанную с использованием кучи и очереди с приоритетом

- ♦ Изучить, как работают *хеш-таблицы*, используемые в качестве абстрактных типов данных и функций
- ♦ Понимать теорию графов, а также продвинутые алгоритмы и концепции, основанные на графах

Модуль 3. Алгоритм и вычислительная сложность

- ♦ Изучить основные стратегии проектирования алгоритмов, а также различные методы и меры для вычисления
- ♦ Знать основные алгоритмы сортировки, используемые при разработке программного обеспечения
- ♦ Понимать, как различные алгоритмы работают с деревьями, кучами и графами
- ♦ Понимать, как работают *жадные алгоритмы*, их стратегию, а также изучить примеры их использования в основных известных проблемах Узнать об использовании *жадных* алгоритмов на графах
- ♦ Изучить основные стратегии поиска минимального пути, с приближением к основным задачам в данной области и алгоритмам их решения
- ♦ Понимать технику поиска с возвратом *Backtracking* и ее основные виды применения, а также альтернативные техники

Модуль 4. Продвинутая разработка алгоритмов

- ♦ Углубиться в продвинутую разработку алгоритмов, анализируя рекурсивные алгоритмы и алгоритмы "разделяй и властвуй", а также выполняя амортизационный анализ
- ♦ Понимать концепции динамического программирования и алгоритмы для NP-задач
- ♦ Понимать, как работает комбинаторная оптимизация, а также различные алгоритмы рандомизации и параллельные алгоритмы
- ♦ Знать и понимать, как работают различные методы локального поиска и с использованием кандидатов
- ♦ Изучить механизмы формальной проверки программ и итеративной проверки программ, включая логику первого порядка и формальную систему Хоара
- ♦ Изучить работу некоторых основных численных методов, таких как метод бисекции, метод Ньютона — Рафсона и метод секущих

Модуль 5. Продвинутое 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
- ♦ Научиться событийно-управляемому программированию и разработке *пользовательских интерфейсов* с помощью Qt
- ♦ Получить необходимые знания о параллельном программировании, процессах и потоках
- ♦ Узнать, 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 6. Теоретическая информатика

- ♦ Понимать основные теоретические математические концепции, лежащие в основе компьютерных наук, такие как пропозициональная логика, теория множеств, числовые и нечисловые множества
- ♦ Понимать концепции формальных языков и грамматик, а также машин Тьюринга в их различных вариантах
- ♦ Узнать о различных видах неразрешимых и неразрешимых задач, включая различные их варианты и подходы к ним
- ♦ Понимать, как функционируют различные виды языков, основанные на рандомизации и других видах классов и грамматик
- ♦ Узнать о других передовых вычислительных системах, таких как мембранные вычисления, вычисления с помощью ДНК и квантовые вычисления

Модуль 7. Теория автоматов и формальных языков

- ◆ Понимать теорию автоматов и формальных языков, изучить понятия алфавитов, строк и языков, а также научиться реализовывать формальные демонстрации
- ◆ Углубить знания о различных видах конечных автоматов, как детерминированных, так и недетерминированных
- ◆ Изучить основные и расширенные понятия, связанные с регулярными языками и регулярными выражениями, а также с применением леммы о накачке и замкнутостью регулярных языков
- ◆ Понимать контекстно-независимые грамматики, а также функционирование автоматов с магазинной памятью
- ◆ Углубить свои знания в области нормальных форм, леммы о накачке контекстно-свободных грамматик и свойств контекстно-независимых языков

Модуль 8. Языковые процессоры

- ◆ Получить представление о понятиях, связанных с процессом компиляции и различными видами анализа: лексическим, синтаксическим и семантическим
- ◆ Знать, как работает лексический анализатор, как его применяют и устраняют ошибки
- ◆ Углубить свои знания в области синтаксического анализа, как нисходящего, так и восходящего, но с особым акцентом на различные типы нисходящих синтаксических анализаторов
- ◆ Понимать, как работают семантические анализаторы, какие существуют традиции в области синтаксиса, как устроены таблицы символов и какие бывают их виды
- ◆ Изучить различные механизмы генерации кода, как в среде выполнения, так и для генерации промежуточного кода
- ◆ Заложить основы знаний в области оптимизации кода, включая переупорядочивание выражений и оптимизацию циклов

Модуль 9. Компьютерная графика и визуализация

- ◆ Получить представление о понятиях, связанных с компьютерной графикой и компьютерной визуализацией, такими как теория цвета и ее модели, а также свойства света
- ◆ Понимать, как функционируют примитивы вывода и их алгоритмы, как для рисования линий, так и для рисования окружностей и заливок
- ◆ Изучить углубленно различные виды 2D- и 3D-преобразований и их системы координат, а также компьютерную визуализацию
- ◆ Научиться делать 3D-проекции и разрезы, а также удалять скрытые поверхности
- ◆ Изучите теорию, связанную с интерполяцией и параметрическими кривыми, а также кривыми Безье и *B-сплайнами*

Модуль 10. Биоинспирированные алгоритмы

- ◆ Получить представление о понятии биоинспирированных алгоритмов, а также понять, как функционируют различные виды алгоритмов социальной адаптации и генетических алгоритмов
- ◆ Углубленно изучить различные модели эволюционных вычислений, узнать их стратегии, программирование, алгоритмы и модели, основанные на оценке распределений
- ◆ Понимать, как устроены основные стратегии исследования и освоения пространства для генетических алгоритмов
- ◆ Понимать, как функционирует эволюционное программирование в применении к задачам обучения и многоцелевым задачам
- ◆ Изучить основные понятия, связанные с нейронными сетями, и понять, как они работают в реальных случаях в таких разных областях, как медицинские исследования, экономика и компьютерное зрение

Модуль 11. 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 12. 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 13. Управление информационной безопасностью

- ◆ Определять различные структуры, которые может иметь область информационной безопасности
- ◆ Разрабатывать модель безопасности на основе трех линий защиты
- ◆ Представлять в различных временных и чрезвычайных комитетах, связанных с кибербезопасностью
- ◆ Определять технологические инструменты, которые поддерживают основные функции центра мониторинга информационной безопасности (SOC)
- ◆ Оценивать меры контроля уязвимостей, соответствующие каждому сценарию
- ◆ Разрабатывать структуру операций безопасности на основе NIST CSF
- ◆ Определять объем различных видов аудита (*RedTeam, Pentesting, Bug Bounty* и т. д.)
- ◆ Предлагать мероприятия, которые должны быть проведены после инцидента, связанного с информационной безопасностью
- ◆ Научиться создавать командный центр информационной безопасности, охватывающий все соответствующие стороны (органы власти, клиенты, поставщики и т. д.)

Модуль 14. Анализ рисков и среды информационной безопасности

- ◆ Изучить с точки зрения комплексного подхода окружающую среду, в которой мы живем
- ◆ Определять 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, позволяющие справляться с рисками и возможностями таким образом, чтобы максимально увеличить вклад в создание стоимости
- ♦ Углубленно изучить 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 моделей управления рисками, так называемых *риск-ориентированных моделей*
- ♦ Внедрять инновации и преобразовывать общие данные в актуальную информацию для принятия решений на основе рисков

Модуль 15. Криптография в ИТ

- ♦ Использовать фундаментальные операции (XOR, большие числа, подстановка и транспонирование) и различные компоненты (функции *односторонние*, *хеш*, 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 16. 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 17. Безопасность в сфере коммуникаций 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 понимание основных положений, связанных с системой управления информационной безопасностью
- ♦ Изучить основы функционирования операционного центра кибербезопасности
- ♦ Показывать важность методов кибербезопасности при организационных катастрофах

Модуль 18. Безопасность в среде облака

- ♦ Определять риски развертывания инфраструктуры в облаке публичных сервисов
- ♦ Определять требования к безопасности
- ♦ Разрабатывать планы безопасности для развертывания облака
- ♦ Определять облачные сервисы, которые необходимы для реализации 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 19. Безопасность в коммуникациях между устройствами интернета вещей (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
- ♦ Проанализировать спецификации безопасности технологий LoRaWAN, NB-IoT и WiSUN
- ♦ Обосновывать выбор правильной технологии IoT для каждого проекта

Модуль 20. 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 ПНБ
- ♦ Знать, как составляется план действий по реализации проекта
- ♦ Оценивать полноценность ПНБ
- ♦ Разрабатывать план успешной реализации ПНБ для конкретного предприятия

Модуль 21. Аналитика данных в организации бизнеса

- ♦ Развивать аналитические навыки для принятия качественных решений
- ♦ Изучить эффективные маркетинговые и коммуникационные кампании
- ♦ Определять порядок создания системы показателей и KPI для конкретных отделов
- ♦ Получить специализированные знания для разработки предиктивной аналитики
- ♦ Предлагать бизнес-планы и планы лояльности на основе изучения рынка
- ♦ Развивать умение слушать клиента
- ♦ Применять статистические, количественные и технические знания в реальных ситуациях

Модуль 22. Управление данными, обработка данных и составление отчетов согласно науке о данных

- ♦ Проводить анализ данных
- ♦ Объединять разнообразные данные: добиться согласованности информации
- ♦ Разрабатывать актуальную, эффективную информацию для принятия решений
- ♦ Определять лучшие практики управления данными в зависимости от типа данных и их использования
- ♦ Создавать политику доступа к данным и их повторного использования
- ♦ Обеспечивать безопасность и доступность: доступность, целостность и конфиденциальность информации
- ♦ Изучать инструменты для управления данными с использованием языков программирования

Модуль 23. IoT-устройства и платформы как основа для науки о данных

- ♦ Определить, что такое IoT (*Интернет вещей*) и IIoT (*Промышленный Интернет вещей*)
- ♦ Изучить, как устроен консорциум промышленного интернета
- ♦ Проанализировать, что представляет собой эталонная архитектура IoT

- ♦ Изучить датчики и устройства IoT, а также их классификацию
- ♦ Определять протоколы и технологии коммуникаций, используемые в IoT
- ♦ Изучить различные *облачные платформы* в IoT: общего назначения, промышленные, с открытым исходным кодом
- ♦ Разрабатывать механизмы для обмена данными
- ♦ Устанавливать требования и стратегии безопасности
- ♦ Представлять различные области применения IoT и IIoT

Модуль 24. Графическое представление для анализа данных

- ♦ Представлять графики для анализа данных
- ♦ Получить специальные знания в области представления данных и аналитики
- ♦ Изучить наиболее используемые графические представления в различных областях
- ♦ Определять принципы проектирования в визуализации данных
- ♦ Представлять визуальный нарратив как инструмент
- ♦ Проанализировать различные программные средства для построения графиков и анализа исследовательских данных

Модуль 25. Инструменты науки о данных

- ♦ Развивать навыки преобразования данных в информацию, из которой можно извлечь знания
- ♦ Определять основные характеристики *набора данных*, его структуру, компоненты и последствия распространения набора данных при моделировании
- ♦ Информировать о принятии решений путем проведения тщательного предварительного анализа данных
- ♦ Развивать навыки решения конкретных примеров с использованием методов науки о данных

- ♦ Определять наиболее подходящие общие инструменты и методы для моделирования каждого *набора данных* на основе проведенной предварительной обработки
- ♦ Оценивать аналитические результаты, понимая, как влияет выбранная стратегия на различные показатели
- ♦ Демонстрировать способность критически оценивать результаты, полученные после применения методов предварительной обработки или моделирования

Модуль 26. Добыча данных. Отбор, предварительная обработка и преобразование

- ♦ Получить специализированные знания о статистических предпосылках для любого анализа и оценки данных
- ♦ Развить необходимые навыки для идентификации, подготовки и преобразования данных
- ♦ Оценивать различные представленные методологии и определять их преимущества и недостатки
- ♦ Изучить задачи в среде данных высокой размерности
- ♦ Разрабатывать методы реализации алгоритмов, используемых для предварительной обработки данных
- ♦ Демонстрировать способность интерпретировать визуализацию данных для описательного анализа
- ♦ Развивать передовые знания о различных существующих методах подготовки данных для очистки, нормализации и преобразования данных

Модуль 27. Предсказуемость и стохастический анализ

- ♦ Анализировать временные ряды
- ♦ Разрабатывать формулировку и основные свойства моделей одномерных временных рядов
- ♦ Изучить методологию моделирования и прогнозирования реальных временных рядов

- ♦ Определять одномерные модели, включая аномалии
- ♦ Применять динамические регрессионные модели и методику построения таких моделей на основе наблюдаемых рядов
- ♦ Изучить спектральный анализ одномерных временных рядов, а также фундаментальных аспектов, связанных с выводами на основе периодограмм и их интерпретацией
- ♦ Оценивать вероятность и тенденцию временного ряда для заданного временного горизонта

Модуль 28. Проектирование и разработка интеллектуальных систем

- ♦ Анализировать переход от информации к знаниям
- ♦ Разрабатывать различные типы методов машинного обучения
- ♦ Изучить метрики и баллы для количественной оценки качества моделей
- ♦ Внедрять различные алгоритмы машинного обучения
- ♦ Определять модели вероятностных рассуждений
- ♦ Изучить основы глубокого обучения
- ♦ Демонстрировать полученные навыки для понимания различных алгоритмов машинного обучения

Модуль 29. Архитектуры и системы с интенсивным использованием данных

- ♦ Определять требования к системам с интенсивным использованием данных
- ♦ Изучить различные модели данных и анализировать базы данных
- ♦ Анализировать ключевые функциональные возможности распределенных систем и их важность для различных видов систем
- ♦ Оценить, какие широко применяемые приложения используют основы распределенных систем при проектировании своих систем
- ♦ Анализировать, как базы данных хранят и извлекают информацию

- ♦ Определять различные модели репликации и связанные с ними задачи
- ♦ Разрабатывать формы разделения и распределенных транзакций
- ♦ Определять системы пакетного и (почти) реального времени

Модуль 30. Практическое применение науки о данных в различных секторах бизнеса

- ♦ Анализировать состояние искусственного интеллекта (ИИ) и аналитики данных
- ♦ Расширить знания о наиболее используемых технологиях
- ♦ Добиться лучшего понимания технологии с помощью конкретных примеров применения
- ♦ Анализировать выбранные стратегии, чтобы выбрать наилучшие технологии для внедрения
- ♦ Определять области применения
- ♦ Изучить фактические и потенциальные риски применяемой технологии
- ♦ Предлагать выгоды, получаемые от использования
- ♦ Определять будущие тенденции в конкретных секторах



Достигните совершенства, окончив программу, содержащую специализированные знания в области компьютерных наук, кибербезопасности и аналитики данных"

03

Компетенции

После сдачи экзаменов в рамках этой программы ИТ-специалист приобретет необходимые навыки для понимания фундаментальных принципов вычислений, а также для работы с языками программирования и данными. Это позволит вам улучшить качество своей повседневной работы в этой области специализации и даст возможность использовать ценные знания при принятии решений, влияющих на функционирование подразделений компании.



“

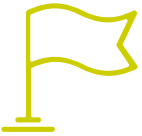
Приобретите необходимые навыки, чтобы вывести свою профессию на высокий уровень, благодаря этой Профессиональной магистерской специализации, которая позволит вам обновить свои знания и адаптироваться к новой ИТ-среде”



Общие профессиональные навыки

- ♦ Корректно выполнять работу, связанную с компьютерами и компьютерным языком
- ♦ Применять наиболее подходящие меры безопасности в зависимости от конкретных видов угроз
- ♦ Определять политику и план безопасности информационной системы компании, а также завершать разработку и реализовывать план действий в чрезвычайных ситуациях
- ♦ Создавать программу аудита, которая отвечает потребностям организации в самооценке уровня кибербезопасности
- ♦ Разрабатывать программу сканирования и мониторинга уязвимостей, а также план реагирования на инциденты в области 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
- ♦ Представлять риски для компаний, связанные с отсутствием безопасной ИТ-среды
- ♦ Развивать техническую и бизнес-перспективу в области аналитики данных
- ♦ Понимать новейшие алгоритмы, платформы и инструменты для изучения, визуализации, манипулирования, обработки и анализа данных
- ♦ Внедрять такое видение бизнеса, которое необходимо для создания добавленной стоимости, в качестве ключевого элемента в вопросах принятия решений
- ♦ Уметь решать проблемы, связанные с анализом данных





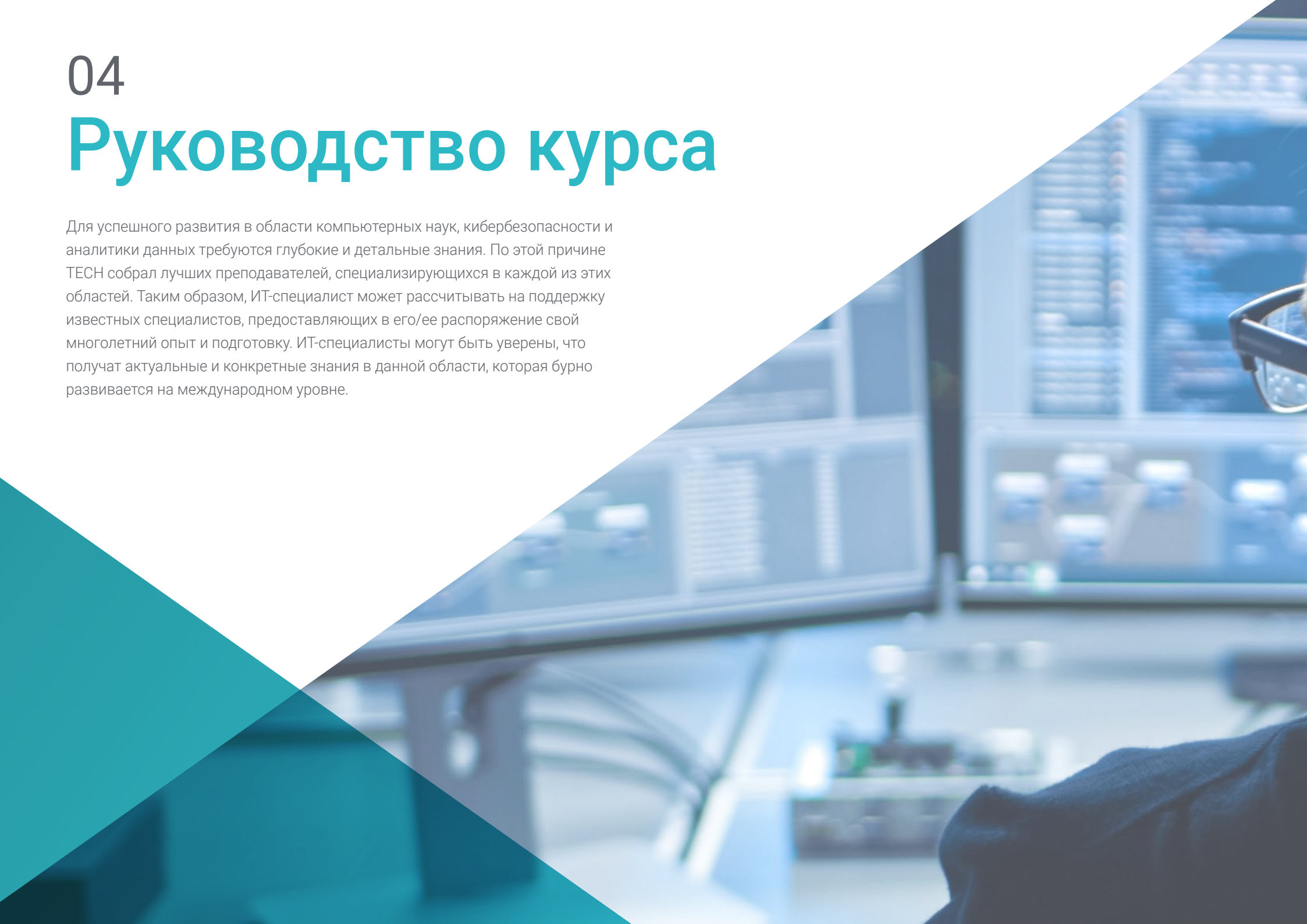
Профессиональные навыки

- ◆ Проектировать алгоритмы для разработки компьютерных программ и применять язык программирования
- ◆ Понимать и использовать структуру компьютерных данных
- ◆ Использовать алгоритмы, необходимые для решения компьютерных задач
- ◆ Иметь глубокие знания в области разработки передовых алгоритмов и методов поиска
- ◆ Выполнять задачи в области компьютерного программирования
- ◆ Понимать и применять теорию, лежащую в основе компьютерных наук, например, математику
- ◆ Знать теорию автоматов и применять компьютерный язык
- ◆ Знать теоретические основы языков программирования и связанные с ними лексические, синтаксические и семантические методы обработки
- ◆ Понимать основные концепции из математики и вычислительной сложности, чтобы применять их для решения вычислительных задач
- ◆ Знать и применять фундаментальные принципы вычислительной техники для осуществления новых компьютерных разработок
- ◆ 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 *Agile Risk Management*
- ◆ Выявлять, анализировать, оценивать и устранять риски, с которыми сталкивается специалист, с новой точки зрения бизнеса, основанной на *риск-ориентированной* модели, которая позволяет не только выжить в своей среде, но и вносить вклад в себестоимость
- ◆ Изучить процесс разработки стратегии безопасности при развертывании корпоративных служб в *облаке*
- ◆ Оценивать различия в конкретных реализациях сервисов от различных поставщиков публичных *облаков*
- ◆ Оценивать варианты подключения IoT для решения задач проекта, уделяя особое внимание технологиям LPWAN
- ◆ Представлять основные характеристики основных технологий LPWAN для IoT
- ◆ Специализироваться в области *науки о данных* с технической и деловой точки зрения
- ◆ Визуализировать данные наиболее подходящим способом, чтобы облегчить их совместное использование и понимание различными специалистами
- ◆ Обращаться к ключевым функциональным областям организации, где наука о данных может принести наибольшую пользу
- ◆ Разрабатывать жизненный цикл данных, их типологию, а также технологии и этапы, необходимые для управления ими
- ◆ Обращивать и управлять данными с помощью специальных языков и библиотек
- ◆ Развивать передовые знания в области фундаментальных методов добычи данных для отбора, предварительной обработки и преобразования данных
- ◆ Специализироваться на основных алгоритмах *машинного обучения* для извлечения скрытых знаний из данных
- ◆ Получить знания в области архитектуры программного обеспечения и систем, необходимых для интенсивного использования данных
- ◆ Определить, как IoT может стать источником генерации данных и ключевой информации, на основе которой можно применять науку о данных для извлечения знаний
- ◆ Анализировать различные способы применения науки о данных в различных отраслях или вертикалях на реальных примерах

04

Руководство курса

Для успешного развития в области компьютерных наук, кибербезопасности и аналитики данных требуются глубокие и детальные знания. По этой причине ТЕСН собрал лучших преподавателей, специализирующихся в каждой из этих областей. Таким образом, ИТ-специалист может рассчитывать на поддержку известных специалистов, предоставляющих в его/ее распоряжение свой многолетний опыт и подготовку. ИТ-специалисты могут быть уверены, что получат актуальные и конкретные знания в данной области, которая бурно развивается на международном уровне.



“

Вы будете учиться под руководством и контролем со стороны преподавательского состава, который находится в курсе последних событий в области кибербезопасности и аналитики данных”

Руководство



Г-н Олая Бональ, Мартин

- ♦ Технический специалист в области *блокчейна* в IBM SPGI
- ♦ Технический специалист по продажам в области *блокчейна*. IBM
- ♦ Директор по проектированию. *Blocknitive*
- ♦ Технический специалист в области цифровой электроники
- ♦ *Блокчейн Архитектор* – Архитектор ИТ-инфраструктуры – Руководитель ИТ-проектов. Области деятельности: Программное обеспечение, инфраструктура, телекоммуникации



Д-р Перальта Мартин-Паломино, Артуро

- ♦ CEO и CTO в Prometheus Global Solutions
- ♦ CTO в Korporate Technologies
- ♦ CTO в AI Shephers GmbH
- ♦ Степень доктора наук в области компьютерной инженерии в Университете Кастилии-Ла-Манчи
- ♦ Степень доктора наук в области экономики, бизнеса и финансов в Университете Камило Хосе Села. Получил премию за выдающуюся докторскую степень
- ♦ Степень доктора в области психологии в Университете Кастилии-Ла-Манчи
- ♦ Степень магистра в области передовых информационных технологий в Университете Кастилии-Ла-Манчи
- ♦ Степень магистра MBA+E (магистр в области делового администрирования и организационной инженерии) в Университете Кастилии-Ла-Манчи
- ♦ Доцент, преподающий в Университете Кастилии-Ла-Манчи программы бакалавриата и магистратуры в области компьютерной инженерии
- ♦ Преподаватель магистратуры в области больших данных и науки о данных в Международном университете Валенсии

Преподаватели

Г-н Тобаль Редондо, Хавьер

- ◆ Руководитель программы инноваций в области приложений в HUAWEI
- ◆ Руководитель отдела информационной безопасности в департаменте платежных средств. Amadeus IT Group
- ◆ Директор по информационной безопасности FINTONIC, Servicios Financieros
- ◆ Сервисный инженер и архитектор в области планирования и архитектуры служб и безопасности в Amena / Orange España
- ◆ Степень бакалавра в области компьютерных наук в Университете Деусто (Бильбао, Испания)
- ◆ Послевузовское образование в области промышленной информатики. Школа промышленной инженерии. Бильбао

Г-н Гонсало Алонсо, Феликс

- ◆ Управляющий директор и основатель. Smart REM Solutions
- ◆ Партнер-основатель и руководитель отдела проектирования рисков и инноваций. Dunargo
- ◆ Руководитель и партнер-основатель. Risknova (Технологический консалтинг, специализирующийся на технологиях)
- ◆ Степень бакалавра в области организации производства в Папском университете Комильяс
- ◆ Степень в области промышленной электроники в Папском университете Комильяс
- ◆ Степень магистра в области управления страхованием в Институте сотрудничества страховых компаний

Г-н Севильяно Искьердо, Хавьер

- ◆ Архитектор глобальной кибербезопасности в компании Vodafone España
- ◆ Главный офис технологической безопасности (CTSO) в Vodafone España
- ◆ Менеджер по технологической безопасности в компании Bankia
- ◆ Менеджер по технологической безопасности в компании Caja Madrid

- ◆ Менеджер по безопасности в компании Sistema 4B
- ◆ SEINCA — старший аналитик
- ◆ Старший технический специалист в области бизнес-информатики в Институте Cibernos

Г-н Энтренас, Алехандро

- ◆ Entelgy Innotec
- ◆ Степень технического инженера в области компьютерных систем в Университете Кордовы
- ◆ Степень магистра в области управления информационной безопасностью в Мадридском политехническом университете

Г-н Ногалес Авила, Хавьер

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

Г-н Гомес Родригес, Антонио

- ◆ Инженер по облачным решениям в компании Oracle
- ◆ Руководитель проектов в компании Sopra Group
- ◆ Руководитель проектов в компании Everis
- ◆ Руководитель проектов в государственной компании по управлению культурными программами при Министерстве культуры Андалусии
- ◆ Аналитик информационных систем в компании Sopra Group
- ◆ Степень бакалавра в области высшей телекоммуникационной инженерии Политехнического университета Каталонии
- ◆ Послевузовское образование в области информационных технологий и систем в Каталонском технологическом институте
- ◆ *E-Business* магистратура в Бизнес-школе Ла-Салье

Г-н Дель Валье Ариас, Хорхе

- ◆ Руководитель подразделения IoT в компании Diode España
- ◆ Менеджер по развитию бизнеса в умных городах Испании в компании Itron Inc
- ◆ Консультант по вопросам IoT
- ◆ Менеджер по продажам IoT и сотовой связи в компании Aicoh Solutions
- ◆ Основатель и генеральный директор компании Sensor Intelligence
- ◆ Главный операционный директор в компании Codium Networks
- ◆ Руководитель направления электроники в компании Aitemin
- ◆ Диплом инженера в области телекоммуникаций в Политехническом университете Мадрида
- ◆ Бизнес-магистратура в Международной высшей школе Ла-Салье в Мадриде

Г-н Госало Фернандес, Хуан Луис

- ◆ Компьютерный инженер.
- ◆ Доцент кафедры DevOps и блокчейна в Международном университете Ла-Риоха
- ◆ Бывший директор направления блокчейна и DevOps в компании Alastria
- ◆ Руководитель направления разработки мобильных приложений Tinkerlink в компании Cronos Telecom
- ◆ Директор по ИТ в банке Santander
- ◆ Директор по технологиям управления ИТ-услугами в Barclays Bank Spain
- ◆ Степень бакалавра в области компьютерной инженерии в Национальном университете дистанционного образования (UNED)

Г-жа Хурадо Хабонеро, Лорена

- ◆ Ответственная за информационную безопасность (CISO) в компании Grupo Pascual
- ◆ Степень в области компьютерной инженерии в Университете Альфонсо X Мудрого

- ◆ Технический инженер в области компьютерного менеджмента в Политехническом университете Мадрида
- ◆ Навыки: ISO 27001, ISO 27701, ISO 22301, ISO 20000, LOPDGDD, NIST CSF, CSA, ITIL, PCI и т. д.

Г-н Армеро Фернандес, Рафаэль

- ◆ Консультант по бизнес-аналитике в компании SDG Group
- ◆ Цифровой инженер в компании Mi-GSO
- ◆ Инженер по логистике в компании Torrecid S.A.
- ◆ Специалист по качеству в INDRA
- ◆ Степень бакалавра в области аэрокосмической инженерии в Политехническом университете Валенсии
- ◆ Степень магистра в области профессионального развития 4.0 в Университете Алькала-де-Энарес

Г-н Перис Морильо, Луис Хавьер

- ◆ Технический руководитель в компании Capitole Consulting. Возглавляет команд в подразделении логистики открытой платформы компании Inditex
- ◆ Старший технический руководитель и руководитель службы поддержки в компании HCL
- ◆ Коуч по гибким технологиям и операционный менеджер в компании Mirai Advisory
- ◆ Член координационного комитета, операционный директор
- ◆ Разработчик, руководитель группы, Scrum-мастер, Agile-коуч, менеджер по продукту в компании DocPath
- ◆ Специалист в области компьютерной инженерии в Высшей школы информации в Сьюдад-Реаль
- ◆ Послевузовское профессиональное образование в области управления проектами в CEOE — Испанской конфедерации бизнес-организаций

- ◆ Пройдено +50 MOOC, преподаваемых в известных университетах, таких как Стэнфордский университет, Мичиганский университет, Университет Ёнсе, Мадридский политехнический университет и др.
- ◆ Имеет множество сертификатов, из наиболее заметных или недавних — Azure Fundamentals

Г-жа Педрахас Параба, Елена

- ◆ Бизнес-аналитик в области управленческих решений в Мадриде
- ◆ Научный сотрудник на кафедре компьютерных наук и численного анализа в Университете Кордовы
- ◆ Научный сотрудник Сингулярного центра исследований в области интеллектуальных технологий в Сантьяго-де-Компостела
- ◆ Степень бакалавра в области компьютерной инженерии. Степень магистра в области науки о данных и компьютерной инженерии

Г-н Монторо Монтарросо, Андрес

- ◆ Исследователь в группе SMILe в Университете Кастилии-Ла-Манчи
- ◆ Специалист в области анализа данных в компании Prometheus Global Solutions
- ◆ Степень в области компьютерной инженерии в Университете Кастилии-Ла-Манчи
- ◆ Степень магистра в области науки о данных и компьютерной инженерии в Университете Гранады
- ◆ Приглашенный преподаватель для курса "Системы, основанные на знаниях" в Высшей школе информатики в Сьюдаде-Реале, читает следующую лекцию: "Продвинутые методы искусственного интеллекта: Поиск и анализ потенциальных радикалов в социальных сетях"
- ◆ Приглашенный преподаватель для курса "Добыча данных" в Высшей школе информатики в Сьюдад-Реаль, читает следующую лекцию: "Приложения для обработки естественного языка: Нечеткая логика для анализа сообщений в социальных сетях"

- ◆ Докладчик на семинаре "Предотвращение коррупции в органах государственного управления и искусственный интеллект". Факультет права и социальных наук в Толедо. Конференция "Методы искусственного интеллекта". Докладчик на Первом международном семинаре по административному праву и искусственному интеллекту (DAIA). Организован Центром европейских исследований им. Луиса Ортеги Альвареса и Институтом исследований TransJus. Конференция "Анализ настроений для предотвращения языка ненависти в социальных сетях"

Г-н Фондон Алькальде, Рубен

- ◆ Бизнес-аналитик для сегмента малого и среднего бизнеса в компании Vodafone España
- ◆ Бизнес-аналитик для рынка Южной Европы в Vodafone Global Enterprise
- ◆ Старший консультант по процессам в Unisys в компании Telefónica Global Solutions
- ◆ Лидер по интеграции услуг в Entelgy в компании Telefónica Global Solutions
- ◆ Степень бакалавра в области телекоммуникационной инженерии в Европейском университете Мадрида
- ◆ Степень магистра в области *больших данных* и аналитики в Международном университете Валенсии

Г-жа Фернандес Мелендес, Галина

- ◆ Аналитик данных в компании ADN Mobile Solution
- ◆ Процессы ETL, добыча данных, анализ и визуализация данных, установление KPI, разработка и внедрение систем показателей, управленческий контроль. Также обладает навыками разработки на языке R и управления SQL
- ◆ Определения закономерностей, прогностического моделирования и машинного обучения
- ◆ Степень бакалавра в области делового администрирования. Университет Бисентариа Арагуа-Каракас
- ◆ Диплом в области планирования и государственных финансов. Венесуэльская школа планирования и школа финансов

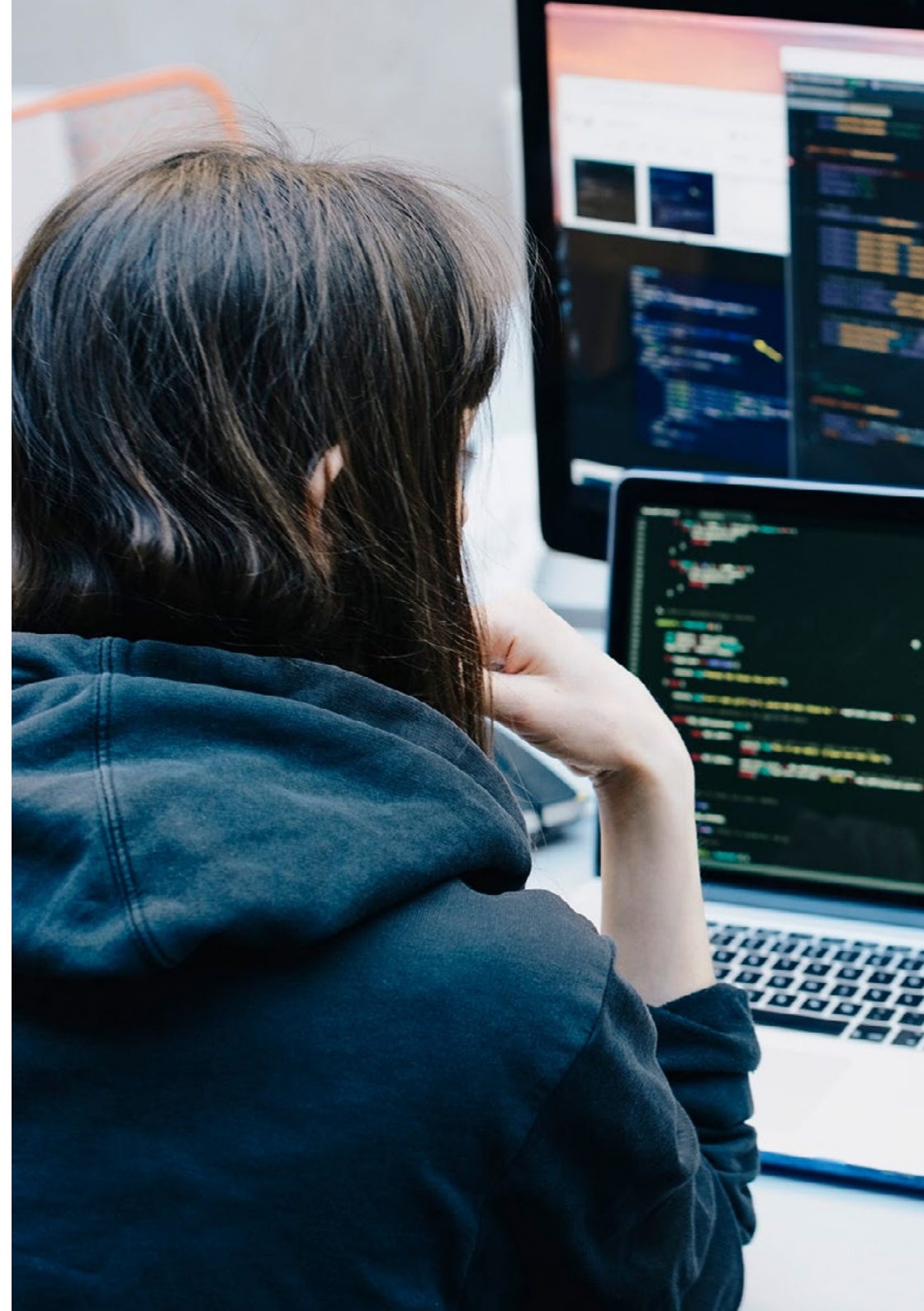
- ◆ Степень магистра в области анализа данных и бизнес-аналитики. Университет Овьедо
- ◆ MBA в области делового администрирования и менеджмента в Европейской бизнес-школе в Барселоне
- ◆ Магистр в области больших данных и бизнес-аналитики в Европейской бизнес-школе в Барселоне

Г-н Диас Диас-Чирон, Тобиас

- ◆ Научный сотрудник лаборатории ArCO в Университете Кастилии-Ла-Манчи, а также группы, занимающейся проектами, связанными с компьютерными архитектурами и сетями
- ◆ Консультант в компании Blue Telecom, занимающейся телекоммуникационным сектором
- ◆ Степень бакалавра в области вычислительной техники в Университете Кастилии-Ла-Манчи

Г-жа Мартинес Серрато, Йесика

- ◆ Технический специалист в области электронных средств безопасности в компании Securitas Seguridad España
- ◆ Аналитик в области бизнес-аналитики в компании Ricoria Technologies
- ◆ Ответственная за обучение новых сотрудников программному обеспечению для управления продажами (CRM, ERP, INTRANET), продуктам и процедурам в компании Ricoria Technologies (Алькала-де-Энарес)
- ◆ Ответственная за обучение новых стипендиатов, принятых в компьютерные классы в Университете Алькала
- ◆ Руководитель проекта в области интеграции ключевых клиентов в компании Correos y Telégrafos (Мадрид)
- ◆ Преподаватель информатики в Ассоциации ASALUMA





- ◆ IT-специалист, ответственная за работу в компьютерных классах OTEC в Университете Алкала
- ◆ Степень бакалавра в области инженерии электронных коммуникаций в Политехнической школе Университета Алькала
- ◆ Специализированная стипендия Университета Алькала для IT-специалиста в OTEC

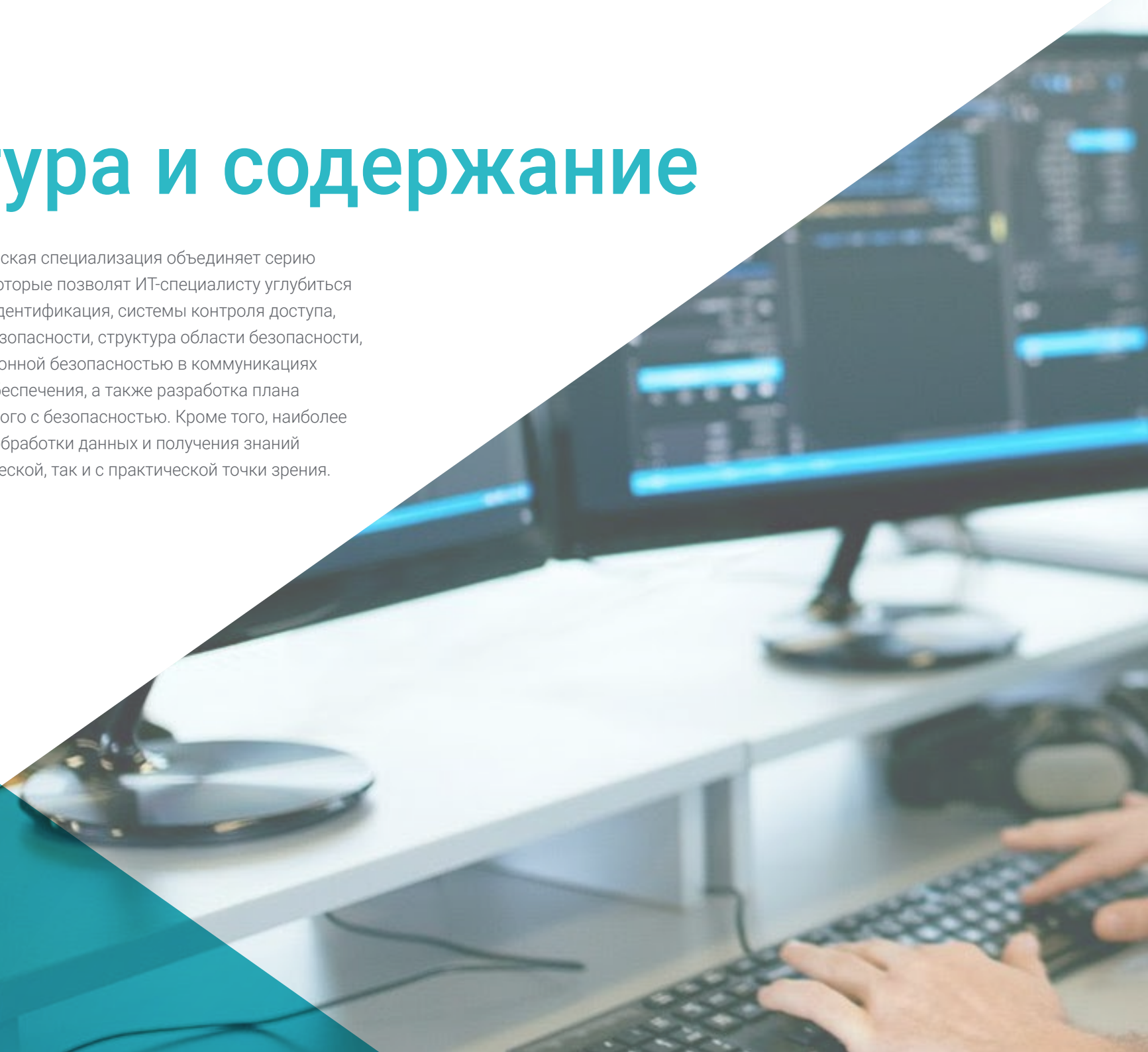
Г-н Тато Санчес, Рафаэль

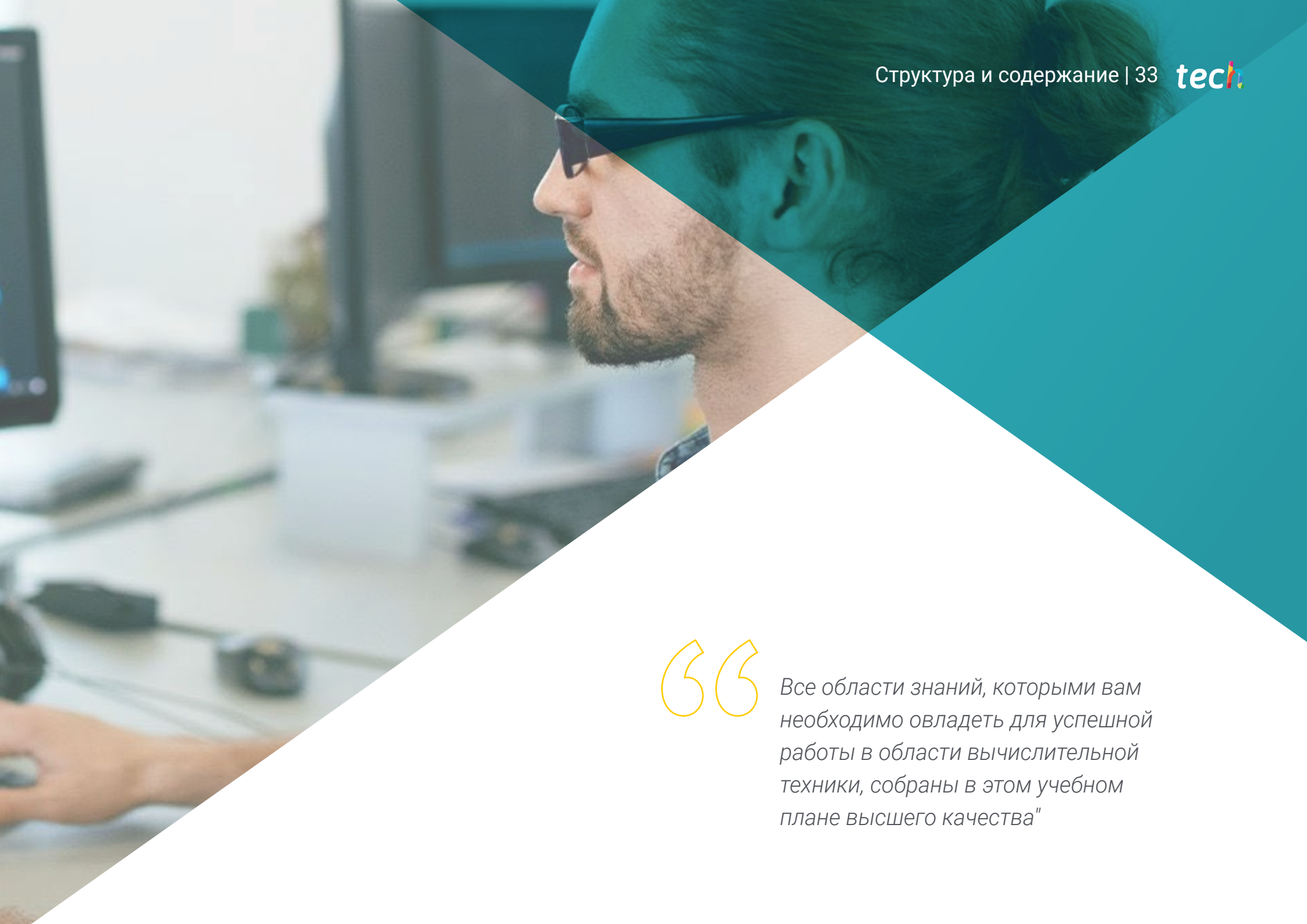
- ◆ Управление проектами. INDRA SISTEMAS S.A
- ◆ Технический директор. INDRA SISTEMAS S.A
- ◆ Системный инженер. ENA TRÁFICO S.A.U
- ◆ IFCD048PO: Управление проектами и методология разработки программного обеспечения с помощью SCRUM
- ◆ Coursera: Машинное обучение
- ◆ UdeMy: Глубокое обучение: от А до Я. Практические занятия по искусственным нейронным сетям
- ◆ Coursera: IBM: Основы масштабируемой науки о данных
- ◆ Coursera: IBM: Прикладной искусственный интеллект с глубоким обучением
- ◆ Coursera: IBM: Продвинутое машинное обучение и обработка сигналов
- ◆ Инженер в области промышленной электроники и автоматизации в Европейском университете Мадрида
- ◆ Степень магистра в области телекоммуникационной инженерии в Европейском университете Мадрида
- ◆ Степень магистра в области промышленности 4.0 в Международном университете Ла-Риоха
- ◆ Профессиональная сертификация. SSCE0110: Преподавание для профессионального обучения с целью трудоустройства

05

Структура и содержание

Эта Профессиональная магистерская специализация объединяет серию специализированных модулей, которые позволят ИТ-специалисту углубиться в такие аспекты, как цифровая идентификация, системы контроля доступа, архитектура информационной безопасности, структура области безопасности, системы управления информационной безопасностью в коммуникациях и эксплуатации программного обеспечения, а также разработка плана непрерывности бизнеса, связанного с безопасностью. Кроме того, наиболее полные и современные методы обработки данных и получения знаний рассматриваются как с теоретической, так и с практической точки зрения.





“

Все области знаний, которыми вам необходимо овладеть для успешной работы в области вычислительной техники, собраны в этом учебном плане высшего качества”

Модуль 1. Основы программирования

- 1.1. Введение в программирование
 - 1.1.1. Базовая структура компьютера
 - 1.1.2. Программное обеспечение
 - 1.1.3. Языки программирования
 - 1.1.4. Жизненный цикл программного приложения
- 1.2. Разработка алгоритмов
 - 1.2.1. Решение задач
 - 1.2.2. Описательные техники
 - 1.2.3. Элементы и структура алгоритма
- 1.3. Элементы программ
 - 1.3.1. Происхождение и особенности языка C++
 - 1.3.2. Среда разработки
 - 1.3.3. Концепция программы
 - 1.3.4. Фундаментальные типы данных
 - 1.3.5. Операторы
 - 1.3.6. Выражения
 - 1.3.7. Предложения
 - 1.3.8. Ввод и вывод данных
- 1.4. Операторы управления
 - 1.4.1. Предложения
 - 1.4.2. Бифуркации
 - 1.4.3. Петли
- 1.5. Абстракция и модульность: функции
 - 1.5.1. Модульное программирование
 - 1.5.2. Концепция функции и утилиты
 - 1.5.3. Определение функции
 - 1.5.4. Поток выполнения во время вызова функции
 - 1.5.5. Прототип функции
 - 1.5.6. Возвращение результатов
 - 1.5.7. Вызов функции: параметры
 - 1.5.8. Передача параметров по ссылке и по значению
 - 1.5.9. Область идентификатора
- 1.6. Статические структуры данных
 - 1.6.1. *Массивы*
 - 1.6.2. Матрицы. Полиэдры
 - 1.6.3. Поиск и сортировка
 - 1.6.4. Строки. Функции ввода/вывода для строк
 - 1.6.5. Структуры. Объединения
 - 1.6.6. Новые типы данных
- 1.7. Динамические структуры данных: указатели
 - 1.7.1. Концепция. Понятие указателя
 - 1.7.2. Операторы и операции с указателями
 - 1.7.3. *Массивы* указателей
 - 1.7.4. Указатели и *массивы*
 - 1.7.5. Указатели на строки
 - 1.7.6. Указатели на структуры
 - 1.7.7. Множественная косвенность
 - 1.7.8. Указатели на функции
 - 1.7.9. Передача функций, структур и *массивов* в качестве параметров функции
- 1.8. Файлы
 - 1.8.1. Основные понятия
 - 1.8.2. Операции с файлами
 - 1.8.3. Типы файлов
 - 1.8.4. Организация файлов
 - 1.8.5. Введение в файлы C++
 - 1.8.6. Работа с файлами
- 1.9. Рекурсия
 - 1.9.1. Определение рекурсии
 - 1.9.2. Виды рекурсии
 - 1.9.3. Преимущества и недостатки
 - 1.9.4. Квалификации
 - 1.9.5. Рекурсивно-итеративное преобразование
 - 1.9.6. Стек рекурсии

- 1.10. Тестирование и документация
 - 1.10.1. Тестирование программ
 - 1.10.2. Тестирование методом "белого ящика"
 - 1.10.3. Тестирование методом "черного ящика"
 - 1.10.4. Инструменты для тестирования
 - 1.10.5. Программная документация

Модуль 2. Структура данных

- 2.1. Введение в программирование на C++
 - 2.1.1. Классы, конструкторы, методы и атрибуты
 - 2.1.2. Переменные
 - 2.1.3. Условные выражения и циклы
 - 2.1.4. Объекты
- 2.2. Абстрактные типы данных (АТД)
 - 2.2.1. Типы данных
 - 2.2.2. Основные структуры и АТД
 - 2.2.3. Векторы и массивы
- 2.3. Линейные структуры данных
 - 2.3.1. Список АТД. Определение
 - 2.3.2. Связанные и дважды связанные списки
 - 2.3.3. Упорядоченные списки
 - 2.3.4. Списки в C++
 - 2.3.5. Стек АТД
 - 2.3.6. АТД очередь
 - 2.3.7. Стек и очередь в C++
- 2.4. Иерархические структуры данных
 - 2.4.1. АТД дерево
 - 2.4.2. Обходы
 - 2.4.3. N-арные деревья
 - 2.4.4. Бинарные деревья
 - 2.4.5. Бинарные деревья поиска
- 2.5. Иерархические структуры данных: сложные деревья
 - 2.5.1. Идеально сбалансированные деревья, или деревья минимальной высоты
 - 2.5.2. Многопутевые деревья
 - 2.5.3. Библиографические ссылки
- 2.6. Куча и очередь с приоритетом
 - 2.6.1. АТД куча
 - 2.6.2. АТД очередь с приоритетом
- 2.7. Что такое *хеш-таблицы*
 - 2.7.1. АТД *хеш-таблицы*
 - 2.7.2. Что такое *хеш-функции*
 - 2.7.3. Как применяет *хеш-функция* в *хеш-таблицах*
 - 2.7.4. Редисперсия
 - 2.7.5. Открытые *хеш-таблицы*
- 2.8. Графы
 - 2.8.1 АТД графы
 - 2.8.2 Типы графов
 - 2.8.3 Графическое представление и основные операции
 - 2.8.4 Проектирование графов
- 2.9. Продвинутое алгоритмы и концепции графов
 - 2.9.1. Задачи на графы
 - 2.9.2. Алгоритмы пути
 - 2.9.3. Алгоритмы поиска или обхода
 - 2.9.4. Другие виды алгоритмов
- 2.10. Другие виды структур данных
 - 2.10.1. Множества
 - 2.10.2. Массивы параллельные
 - 2.10.3. Таблица символов
 - 2.10.4. Префиксное дерево

Модуль 3. Алгоритм и вычислительная сложность

- 3.1. Введение в шаблоны разработки алгоритмов
 - 3.1.1. Рекурсия
 - 3.1.2. "Разделяй и властвуй"
 - 3.1.3. Другие шаблоны
- 3.2. Эффективность и анализ работы алгоритмов
 - 3.2.1. Меры эффективности
 - 3.2.2. Измерение объема данных на входе
 - 3.2.3. Измерение времени выполнения
 - 3.2.4. Случаи: худший, лучший и средний
 - 3.2.5. Асимптотическая нотация
 - 3.2.6. Критерии математического анализа нерекурсивных алгоритмов
 - 3.2.7. Критерии математического анализа рекурсивных алгоритмов
 - 3.2.8. Эмпирический анализ алгоритмов
- 3.3. Алгоритмы сортировки
 - 3.3.1. Концепция сортировки
 - 3.3.2. Пузырьковая сортировка
 - 3.3.3. Сортировка выбором
 - 3.3.4. Сортировка вставками
 - 3.3.5. Сортировка слиянием (*Merge Sort*)
 - 3.3.6. Быстрая сортировка (*Quicksort*)
- 3.4. Алгоритмы с применением деревьев
 - 3.4.1. Концепция дерева
 - 3.4.2. Бинарные деревья
 - 3.4.3. Обходы деревьев
 - 3.4.4. Представление выражений
 - 3.4.5. Упорядоченные бинарные деревья
 - 3.4.6. Сбалансированные бинарные деревья
- 3.5. Алгоритмы с применением куч
 - 3.5.1. Что такое кучи
 - 3.5.2. Алгоритм сортировки кучей
 - 3.5.3. Очереди с приоритетом



- 3.6. Алгоритмы на графах
 - 3.6.1. Представление
 - 3.6.2. Обход в ширину
 - 3.6.3. Обход в глубину
 - 3.6.4. Топологическая сортировка
- 3.7. Жадные алгоритмы
 - 3.7.1. Жадная стратегия
 - 3.7.2. Элементы жадной стратегии
 - 3.7.3. Обмен монет
 - 3.7.4. Задача коммивояжера
 - 3.7.5. Задача о рюкзаке
- 3.8. Поиск кратчайших путей
 - 3.8.1. Задача о кратчайшем пути
 - 3.8.2. Отрицательные дуги и циклы
 - 3.8.3. Алгоритм Дейкстры
- 3.9. Жадные алгоритмы на графах
 - 3.9.1. Минимальное остовное дерево
 - 3.9.2. Алгоритм Прима
 - 3.9.3. Алгоритм Краскала
 - 3.9.4. Анализ сложности
- 3.10. Техника *Backtracking*
 - 3.10.1. Техника *Backtracking*
 - 3.10.2. Альтернативные техники

Модуль 4. Продвинутое программирование алгоритмов

- 4.1. Анализ рекурсивных алгоритмов и алгоритмов "разделяй и властвуй">
 - 4.1.1. Постановка и решение однородных и неоднородных рекуррентных уравнений
 - 4.1.2. Обзор стратегии "разделяй и властвуй"
- 4.2. Амортизационный анализ
 - 4.2.1. Агрегатный анализ
 - 4.2.2. Метод учета
 - 4.2.3. Метод потенциалов
- 4.3. Динамическое программирование и алгоритмы для NP-задач
 - 4.3.1. Характеристики динамического программирования
 - 4.3.2. Отступление: Backtracking
 - 4.3.3. Разветвление и обрезка
- 4.4. Комбинаторная оптимизация
 - 4.4.1. Представление задач
 - 4.4.2. Одномерная оптимизация
- 4.5. Алгоритмы рандомизации
 - 4.5.1. Примеры алгоритмов рандомизации
 - 4.5.2. Задача Бюффона
 - 4.5.3. Алгоритмы с методом Монте-Карло
 - 4.5.4. Алгоритм Лас-Вегас
- 4.6. Локальный поиск и поиск с кандидатами
 - 4.6.1. *Градиентный подъем*
 - 4.6.2. *Поиск с восхождением к вершине*
 - 4.6.3. *Алгоритм имитации отжига*
 - 4.6.4. *Поиск с запретами*
 - 4.6.5. Поиск с кандидатами
- 4.7. Формальная проверка программ
 - 4.7.1. Спецификация функциональных абстракций
 - 4.7.2. Язык логики первого порядка
 - 4.7.3. Формальная система Хоара
- 4.8. Верификация итеративных программ
 - 4.8.1. Правила формальной системы Хоара

- 4.8.2. Концепция инвариантных итераций
- 4.9. Численные методы
 - 4.9.1. Метод бисекции
 - 4.9.2. Метод Ньютона — Рафсона
 - 4.9.3. Метод секущей
- 4.10. Параллельные алгоритмы
 - 4.10.1. Параллельные бинарные операции
 - 4.10.2. Параллельные операции на графах
 - 4.10.3. Параллелизм в "разделяй и властвуй"
 - 4.10.4. Параллелизм в динамическом программировании

Модуль 5. Продвинутое программирование

- 5.1. Введение в объектно-ориентированное программирование
 - 5.1.1. Введение в объектно-ориентированное программирование
 - 5.1.2. Разработка классов
 - 5.1.3. Введение в унифицированный язык моделирования (UML) для моделирования задач
- 5.2. Отношения между классами
 - 5.2.1. Абстракция и наследование
 - 5.2.2. Расширенные концепции наследования
 - 5.2.3. Полиморфизм
 - 5.2.4. Состав и агрегация
- 5.3. Введение в паттерны проектирования для объектно-ориентированных задач
 - 5.3.1. Что такое паттерны проектирования?
 - 5.3.2. Паттерн *Фабрика*
 - 5.3.4. Паттерн *Одиночка*
 - 5.3.5. Паттерн *Наблюдатель*
 - 5.3.6. Паттерн *Компоновщик*
- 5.4. Исключения
 - 5.4.1. Что такое исключения?
 - 5.4.2. Перехват и обработка исключений
 - 5.4.3. Запуск исключений
 - 5.4.4. Создание исключений

- 5.5. Пользовательские интерфейсы
 - 5.5.1. Введение во фреймворк Qt
 - 5.5.2. Позиционирование
 - 5.5.3. Что такое события?
 - 5.5.4. События: определение и захват
 - 5.5.5. Разработка пользовательского интерфейса
- 5.6. Введение в параллельное программирование
 - 5.6.1. Введение в параллельное программирование
 - 5.6.2. Концепция процесса и потока
 - 5.6.3. Взаимодействие между процессами или потоками
 - 5.6.4. Потоки в C++
 - 5.6.5. Преимущества и недостатки параллельного программирования
- 5.7. Управление потоками и синхронизация
 - 5.7.1. Жизненный цикл потока
 - 5.7.2. Класс *Thread*
 - 5.7.3. Планирование потоков
 - 5.7.4. Группы потоков
 - 5.7.5. Демонические потоки
 - 5.7.6. Синхронизация
 - 5.7.7. Механизмы блокировки
 - 5.7.8. Механизмы коммуникации
 - 5.7.9. Мониторы
- 5.8. Распространенные задачи в параллельном программировании
 - 5.8.1. Задача "производитель – потребитель"
 - 5.8.2. Задача о читателях – писателях
 - 5.8.3. Задача об обедающих философах
- 5.9. Документация и тестирование программного обеспечения
 - 5.9.1. Почему важно документировать программное обеспечение?
 - 5.9.2. Проектная документация
 - 5.9.3. Использование инструментов для документирования

- 5.10. Тестирование программного обеспечения
 - 5.10.1. Введение в тестирование программного обеспечения
 - 5.10.2. Виды тестирования
 - 5.10.3. Единичное тестирование
 - 5.10.4. Интеграционное тестирование
 - 5.10.5. Валидационное тестирование
 - 5.10.6. Тестирование системы

Модуль 6. Теоретическая информатика

- 6.1. Используемые математические понятия
 - 6.1.1. Введение в пропозициональную логику
 - 6.1.2. Теория отношений
 - 6.1.3. Нумеруемые и нумеруемые множества
- 6.2. Формальные языки и грамматики и введение в машины Тьюринга
 - 6.2.1. Формальные языки и грамматики
 - 6.2.2. Проблема принятия решения
 - 6.2.3. Машина Тьюринга
- 6.3. Расширения для машин Тьюринга, ограниченные машины Тьюринга и компьютеры
 - 6.3.1. Методы программирования для машин Тьюринга
 - 6.3.2. Расширения для машин Тьюринга
 - 6.3.3. Ограниченные машины Тьюринга
 - 6.3.4. Машины Тьюринга и компьютеры
- 6.4. Неразрешимость
 - 6.4.1. Нерекурсивно перечислимый язык
 - 6.4.2. Неразрешимая рекурсивно перечислимая задача
- 6.5. Другие неразрешимые задачи
 - 6.5.1. Неразрешимые задачи для машин Тьюринга
 - 6.5.2. Проблема почтовой корреспонденции (PCP)
- 6.6. Неразрешимые задачи
 - 6.6.1. Классы P и NP
 - 6.6.2. NP-полная задача
 - 6.6.3. Ограниченная задача удовлетворительности
 - 6.6.4. Другие NP-полные задачи

- 6.7. Задачи co-NP и PS
 - 6.7.1. Дополнение к языкам NP
 - 6.7.2. Решаемые задачи в полиномиальном пространстве
 - 6.7.3. PS-полные задачи
- 6.8. Классы языков, основанных на рандомизации
 - 6.8.1. Модель машины Тьюринга со случайностью
 - 6.8.2. Классы RP и ZPP
 - 6.8.3. Тест на первичность
 - 6.8.4. Сложность теста на первичность
- 6.9. Другие виды классов и грамматик
 - 6.9.1. Вероятностные конечные автоматы
 - 6.9.2. Клеточные автоматы
 - 6.9.3. Клетки МакКаллока и Питтса
 - 6.9.4. Грамматики Линденмайера
- 6.10. Продвинутое вычислительные системы
 - 6.10.1. Мембранные вычисления: P-системы
 - 6.10.2. ДНК-вычисления
 - 6.10.3. Квантовые вычисления

Модуль 7. Теория автоматов и формальных языков

- 7.1. Введение в теорию автоматов
 - 7.1.1. Зачем изучать теорию автоматов?
 - 7.1.2. Введение в формальные демонстрации
 - 7.1.3. Другие формы демонстрации
 - 7.1.4. Математическая индукция
 - 7.1.5. Алфавиты, строки и языки
- 7.2. Детерминированные конечные автоматы (ДКА)
 - 7.2.1. Введение в конечные автоматы
 - 7.2.2. Детерминированные конечные автоматы
- 7.3. Недетерминированные конечные автоматы (НДКА)
 - 7.3.1. Недетерминированные конечные автоматы
 - 7.3.2. Эквивалентность между ДКА и НДКА
 - 7.3.3. Конечные автоматы с переходами ϵ

- 7.4. Языки и регулярные выражения (I)
 - 7.4.1. Языки и регулярные выражения
 - 7.4.2. Конечные автоматы и регулярные выражения
- 7.5. Языки и регулярные выражения (II)
 - 7.5.1. Преобразование регулярных выражений в автоматы
 - 7.5.2. Применение регулярных выражений
 - 7.5.3. Алгебра регулярных выражений
- 7.6. Лемма о накачке и замкнутость регулярных языков
 - 7.6.1. Лемма о накачке
 - 7.6.2. Свойства замкнутости регулярных языков
- 7.7. Эквивалентность и минимизация автоматов
 - 7.7.1. Эквивалентность конечных автоматов
 - 7.7.2. Минимизация конечных автоматов
- 7.8. Контекстно-свободные грамматика
 - 7.8.1. Контекстно-свободные грамматика
 - 7.8.2. Деревья деривации
 - 7.8.3. Применение контекстно-свободных грамматик
 - 7.8.4. Неоднозначность в грамматиках и языках
- 7.9. Автоматы с магазинной памятью и контекстно-свободные грамматика
 - 7.9.1. Определение автоматов с магазинной памятью
 - 7.9.2. Языки, принимаемые автоматами с магазинной памятью
 - 7.9.3. Эквивалентность между автоматами с магазинной памятью и контекстно-свободными грамматиками
 - 7.9.4. Детерминированный автомат с магазинной памятью
- 7.10. Нормальные формы, лемма о накачке контекстно-свободных грамматик и свойства контекстно-свободных языков
 - 7.10.1. Нормальные формы контекстно-свободных грамматик
 - 7.10.2. Лемма о накачке
 - 7.10.3. Свойства замкнутости языков
 - 7.10.4. Свойства решений в контекстно-свободных языках

Модуль 8. Языковые процессоры

- 8.1. Введение в процесс компиляции
 - 8.1.1. Компиляция и интерпретация
 - 8.1.2. Среда выполнения компилятора
 - 8.1.3. Процесс анализа
 - 8.1.4. Процесс синтеза
- 8.2. Лексический анализатор
 - 8.2.1. Что такое лексический анализатор?
 - 8.2.2. Внедрение лексического анализатора
 - 8.2.3. Семантические действия
 - 8.2.4. Устранение ошибок
 - 8.2.5. Вопросы внедрения
- 8.3. Синтаксический анализ
 - 8.3.1. Что такое синтаксический анализатор?
 - 8.3.2. Предварительные концепции
 - 8.3.3. Нисходящие анализаторы
 - 8.3.4. Восходящие анализаторы
- 8.4. Синтаксический анализ: нисходящий и восходящий
 - 8.4.1. LL-анализатор (1)
 - 8.4.2. LR-анализатор (0)
 - 8.4.3. Пример анализатора
- 8.5. Продвинутый восходящий синтаксический анализ
 - 8.5.1. SLR-анализатор
 - 8.5.2. LR-анализатор (1)
 - 8.5.3. LR-анализатор (k)
 - 8.5.4. LALR-анализатор
- 8.6. Семантический анализ (I)
 - 8.6.1. Перевод на основе синтаксиса
 - 8.6.2. Таблица символов
- 8.7. Семантический анализ (II)
 - 8.7.1. Проверка типов
 - 8.7.2. Подсистема типов
 - 8.7.3. Эквивалентность типов и преобразований

- 8.8. Генерация кода и среда выполнения
 - 8.8.1. Аспекты разработки
 - 8.8.2. Среда выполнения
 - 8.8.3. Организация памяти
 - 8.8.4. Распределение памяти
- 8.9. Генерация промежуточного кода
 - 8.9.1. Перевод на основе синтеза
 - 8.9.2. Промежуточные представления
 - 8.9.3. Примеры переводов
- 8.10. Оптимизация кода
 - 8.10.1. Присвоение регистров
 - 8.10.2. Устранение "мертвых" распределений
 - 8.10.3. Выполнение во время компиляции
 - 8.10.4. Перестановка выражений
 - 8.10.5. Оптимизация петель

Модуль 9. Компьютерная графика и визуализация

- 9.1. Теория цвета
 - 9.1.1. Свойства света
 - 9.1.2. Цветовые модели
 - 9.1.3. Стандарт CIE
 - 9.1.4. Профайлинг
- 9.2. Примитивы вывода
 - 9.2.1. Видеоконтроллер
 - 9.2.2. Алгоритмы рисования линий
 - 9.2.3. Алгоритмы для рисования окружностей
 - 9.2.4. Алгоритмы заливки
- 9.3. 2D-преобразования, системы координат и 2D-обрезка
 - 9.3.1. Базовые геометрические преобразования
 - 9.3.2. Однородные координаты
 - 9.3.3. Обратное преобразование
 - 9.3.4. Композиция преобразований
 - 9.3.5. Другие виды преобразований

- 9.3.6. Изменение координат
- 9.3.7. Двумерные системы координат
- 9.3.8. Изменение координат
- 9.3.9. Нормализация
- 9.3.10. Алгоритмы обрезки
- 9.4. 3D-преобразования
 - 9.4.1. Транскрибирование
 - 9.4.2. Вращение
 - 9.4.3. Масштабирование
 - 9.4.4. Отражение
 - 9.4.5. Ножницы
- 9.5. Просмотр и изменение 3D-координат
 - 9.5.1. Трёхмерные системы координат
 - 9.5.2. Визуализация
 - 9.5.3. Изменение координат
 - 9.5.4. Проекция и нормализация
- 9.6. Проекция и 3D-обрезка
 - 9.6.1. Ортогональная проекция
 - 9.6.2. Косоугольная параллельная проекция
 - 9.6.3. Перспективная проекция
 - 9.6.4. Алгоритмы 3D-обрезки
- 9.7. Удаление скрытых поверхностей
 - 9.7.1. *Отбраковка задней поверхности*
 - 9.7.2. *Z-буферизация*
 - 9.7.3. Алгоритм художника
 - 9.7.4. Алгоритм Варнока
 - 9.7.5. Обнаружение скрытых линий
- 9.8. Интерполяция и параметрические кривые
 - 9.8.1. Интерполяция и полиномиальная аппроксимация
 - 9.8.2. Параметрическое представление
 - 9.8.3. Полином Лагранжа
 - 9.8.4. *Слайны*
 - 9.8.5. Базовые функции
 - 9.8.6. Матричное представление



- 9.9. Кривые Безье
 - 9.9.1. Алгебраическое построение
 - 9.9.2. Матричная форма
 - 9.9.3. Состав
 - 9.9.4. Геометрическое построение
 - 9.9.5. Алгоритм рисования
- 9.10. *В-сплайны*
 - 9.10.1. Проблема локального контроля
 - 9.10.2. Кубические однородные В-сплайны
 - 9.10.3. Базовые функции и контрольные точки
 - 9.10.4. Движение к происхождению и множественности
 - 9.10.5. Матричное представление
 - 9.10.6. Неоднородные В-сплайны

Модуль 10. Биоинспирированные алгоритмы

- 10.1. Введение в биоинспирированные алгоритмы
 - 10.1.1. Введение в биоинспирированные алгоритмы
- 10.2. Алгоритмы социальной адаптации
 - 10.2.1. Биоинспирированные алгоритмы, основанные на муравьиных колониях
 - 10.2.2. Разновидности алгоритмов муравьиных колоний
 - 10.2.3. Алгоритмы, основанные на облаках с частицами
- 10.3. Генетические алгоритмы
 - 10.3.1. Общая структура
 - 10.3.2. Внедрение основных операторов
- 10.4. Стратегии освоения и использования пространства для генетических алгоритмов
 - 10.4.1. Алгоритм СНС
 - 10.4.2. Мультимодальные задачи
- 10.5. Модели эволюционных вычислений (I)
 - 10.5.1. Эволюционные стратегии
 - 10.5.2. Эволюционное программирование
 - 10.5.3. Алгоритмы, основанные на дифференциальной эволюции
- 10.6. Модели эволюционных вычислений (II)
 - 10.6.1. Модели эволюции, основанные на оценке алгоритмов распределения (EDA)
 - 10.6.2. Генетическое программирование

- 10.7. Применение эволюционного программирования при нарушениях обучаемости
 - 10.7.1 Обучение на основе правил
 - 10.7.2 Эволюционные методы в задачах выбора решений
- 10.8. Многоцелевые задачи
 - 10.8.1. Концепция доминирования
 - 10.8.2. Применение эволюционных алгоритмов для решения многоцелевых задач
- 10.9. Нейронные сети (I)
 - 10.9.1. Введение в нейронные сети
 - 10.9.2. Практический пример с нейронными сетями
- 10.10. Нейронные сети (II)
 - 10.10.1. Примеры использования нейронных сетей в медицинских исследованиях
 - 10.10.2. Примеры использования нейронных сетей в экономике
 - 10.10.3. Примеры использования нейронных сетей в искусственном зрении

Модуль 11. Безопасность при проектировании и разработке систем

- 11.1. Информационные системы
 - 11.1.1. Домены информационной системы
 - 11.1.2. Компоненты информационных систем
 - 11.1.3. Виды деятельности информационной системы
 - 11.1.4. Жизненный цикл информационной системы
 - 11.1.5. Ресурсы информационной системы
- 11.2. Информационные системы. Типология
 - 11.2.1. Виды информационных систем
 - 11.2.1.1. Бизнес-системы
 - 11.2.1.2. Стратегические
 - 11.2.1.3. В зависимости от сферы применения
 - 11.2.1.4. Специфические
 - 11.2.2. Информационные системы. Реальные примеры
 - 11.2.3. Эволюция информационных систем: этапы
 - 11.2.4. Методологии информационных систем
- 11.3. Безопасность информационных систем. Правовые последствия
 - 11.3.1. Доступ к данным
 - 11.3.2. Угрозы безопасности: уязвимости

- 11.3.3. Правовые последствия: уголовные преступления
- 11.3.4. Процедуры по техническому обслуживанию информационной системы
- 11.4. Безопасность информационных систем. Протоколы безопасности
 - 11.4.1. Безопасность информационных систем
 - 11.4.1.1. Целостность
 - 11.4.1.2. Конфиденциальность
 - 11.4.1.3. Доступность
 - 11.4.1.4. Аутентификация
 - 11.4.2. Услуги по обеспечению безопасности
 - 11.4.3. Протоколы информационной безопасности. Типология
 - 11.4.4. Чувствительность информационных систем
- 11.5. Безопасность информационных систем. Меры и системы контроля доступа
 - 11.5.1. Меры по обеспечению безопасности
 - 11.5.2. Вид мер по обеспечению безопасности
 - 11.5.2.1. Профилактика
 - 11.5.2.2. Обнаружение
 - 11.5.2.3. Коррекция
 - 11.5.3. Системы контроля доступа. Типология
 - 11.5.4. Криптография
- 11.6. Безопасность сети и интернета
 - 11.6.1. *Файрволы*
 - 11.6.2. Цифровая идентификация
 - 11.6.3. Вирусы и черви
 - 11.6.4. *Взлом*
 - 11.6.5. Примеры и реальные кейсы
- 11.7. Компьютерные преступления
 - 11.7.1. Компьютерное преступление
 - 11.7.2. Компьютерные преступления. Типология
 - 11.7.3. Компьютерное преступление. Атака. Типологии
 - 11.7.4. Пример с виртуальной реальностью
 - 11.7.5. Профили правонарушителей и жертв. Типизация преступлений
 - 11.7.6. Компьютерные преступления. Примеры и реальные кейсы

- 11.8. План по обеспечению безопасности информационной системы
 - 11.8.1. План по обеспечению безопасности. Цели
 - 11.8.2. План по обеспечению безопасности. Планирование
 - 11.8.3. План по рискам. Анализ
 - 11.8.4. Политика безопасности. Внедрение в организацию
 - 11.8.5. План по обеспечению безопасности. Внедрение в организацию
 - 11.8.6. Процедуры по обеспечению безопасности. Виды
 - 11.8.7. План по обеспечению безопасности. Примеры
- 11.9. План действий в непредвиденных ситуациях
 - 11.9.1. План действий в непредвиденных ситуациях. Функции
 - 11.9.2. План действий в чрезвычайной ситуации: элементы и цели
 - 11.9.3. План непредвиденных в организации. Внедрение
 - 11.9.4. План действий в непредвиденных ситуациях. Примеры
- 11.10. Управление безопасностью информационных систем
 - 11.10.1. Правовые нормы
 - 11.10.2. Стандарты
 - 11.10.3. Сертификация
 - 11.10.4. Технологии

Модуль 12. Архитектуры и модели информационной безопасности

- 12.1. Архитектура информационной безопасности
 - 12.1.1. SGSI/PDS
 - 12.1.2. Стратегическая согласованность
 - 12.1.3. Управление рисками
 - 12.1.4. Измерение результативности
- 12.2. Модели информационной безопасности
 - 12.2.1. На основе политик безопасности
 - 12.2.2. На основе инструментов защиты
 - 12.2.3. На основе вовлеченных в работу команд
- 12.3. Модель безопасности. Ключевые компоненты
 - 12.3.1. Определение рисков
 - 12.3.2. Определение средств контроля
 - 12.3.3. Постоянная оценка уровня риска
 - 12.3.4. План по информированию сотрудников, поставщиков, партнеров и т. д.
- 12.4. Процесс управления рисками
 - 12.4.1. Определение активов
 - 12.4.2. Определение угроз
 - 12.4.3. Оценка рисков
 - 12.4.4. Определение приоритетов контроля
 - 12.4.5. Переоценка и остаточный риск
- 12.5. Бизнес-процессы и информационная безопасность
 - 12.5.1. Бизнес-процессы
 - 12.5.2. Оценка рисков на основе параметров бизнеса
 - 12.5.3. Анализ влияния на бизнес
 - 12.5.4. Деловые операции и информационная безопасность
- 12.6. Процесс непрерывного улучшения
 - 12.6.1. Цикл Деминга
 - 12.6.1.1. План
 - 12.6.1.2. Создание
 - 12.6.1.3. Верификация
 - 12.6.1.4. Действия
- 12.7. Архитектура безопасности
 - 12.7.1. Выбор и гомогенизация технологий
 - 12.7.2. Управление идентификацией. Аутентификация
 - 12.7.3. Управление доступом. Авторизация
 - 12.7.4. Безопасность сетевой инфраструктуры
 - 12.7.5. Технологии и решения в области шифрования
 - 12.7.6. Безопасность оконечного оборудования (EDR)
- 12.8. Нормативно-правовая база
 - 12.8.1. Отраслевые нормативные акты
 - 12.8.2. Сертификация
 - 12.8.3. Законодательство
- 12.9. Стандарт ISO 27001
 - 12.9.1. Внедрение
 - 12.9.2. Сертификация
 - 12.9.3. Аудиты и тесты на вторжение
 - 12.9.4. Непрерывное управление рисками
 - 12.9.5. Классификация информации
- 12.10. Законодательство о конфиденциальности. GDPR
 - 12.10.1. Сфера действия Общего регламента по защите данных (GDPR)
 - 12.10.2. Персональные данные

- 12.10.3. Роли, существующие в процессе обработки персональных данных
- 12.10.4. Права ARCO
- 12.10.5. Должностное лицо по защите данных (DPO). Функции

Модуль 13. Управление информационной безопасностью

- 13.1. Управление безопасностью
 - 13.1.1. Операции по обеспечению безопасности
 - 13.1.2. Правовые и нормативные аспекты
 - 13.1.3. Бизнес-квалификация
 - 13.1.4. Управление рисками
 - 13.1.5. Управление идентификацией и доступом
- 13.2. Структура зоны безопасности. Офис главного специалиста по информационной безопасности (CISO)
 - 13.2.1. Организационная структура. Место CISO в структуре
 - 13.2.2. Линии защиты
 - 13.2.3. Организационная схема офиса CISO
 - 13.2.4. Управление бюджетом
- 13.3. Управление в сфере безопасности
 - 13.3.1. Комитет по безопасности
 - 13.3.2. Комитет по мониторингу рисков
 - 13.3.3. Комитет по аудиту
 - 13.3.4. Кризисный комитет
- 13.4. Управление в сфере безопасности. Функции
 - 13.4.1. Политики и стандарты
 - 13.4.2. Генеральный план по обеспечению безопасности
 - 13.4.3. Система показателей
 - 13.4.4. Повышение осведомленности и обучение
 - 13.4.5. Безопасность цепи поставок
- 13.5. Операции по обеспечению безопасности
 - 13.5.1. Управление идентификацией и доступом
 - 13.5.2. Конфигурация правил сетевой безопасности. *Файрволы*
 - 13.5.3. Управление платформами IDS/IPS
 - 13.5.4. Анализ уязвимостей
- 13.6. Рамки кибербезопасности. NIST CSF
 - 13.6.1. Методология NIST
 - 13.6.1.1. Идентификация
 - 13.6.1.2. Защита
 - 13.6.1.3. Обнаружение
 - 13.6.1.4. Ответ
 - 13.6.1.5. Восстановление
- 13.7. Операционный центр безопасности (SOC). Функции
 - 13.7.1. Защита *Красная команда, испытание на вторжение, аналитика киберугроз*
 - 13.7.2. Выявление. SIEM, *аналитика поведения пользователей, предотвращение мошенничества*
 - 13.7.3. Ответ
- 13.8. Аудиты безопасности
 - 13.8.1. Тест на вторжение
 - 13.8.2. Задания *красной команды*
 - 13.8.3. Аудит исходного кода. Безопасная разработка
 - 13.8.4. Безопасность компонентов (*цепочка поставок программного обеспечения*)
 - 13.8.5. Криминалистическая экспертиза
- 13.9. Реагирование на инциденты
 - 13.9.1. Подготовка
 - 13.9.2. Выявление, анализ и отчетность
 - 13.9.3. Сдерживание, искоренение и восстановление
 - 13.9.4. Деятельность после инцидента
 - 13.9.4.1. Сохранение доказательств
 - 13.9.4.2. Криминалистическая экспертиза
 - 13.9.4.3. Управление разрывами
 - 13.9.5. Официальное руководство по управлению киберинцидентами
- 13.10. Управление уязвимостями
 - 13.10.1. Анализ уязвимостей
 - 13.10.2. Оценка уязвимости
 - 13.10.3. Системное базирование
 - 13.10.4. Уязвимость нулевого дня. *Нулевой день*

Модуль 14. Анализ рисков и среды информационной безопасности

- 14.1. Анализ среды
 - 14.1.1. Анализ экономического положения
 - 14.1.1.1. VUCA-среды
 - 14.1.1.1.1. Волатильность
 - 14.1.1.1.2. Неопределенность
 - 14.1.1.1.3. Сложность
 - 14.1.1.1.4. Неоднозначность
 - 14.1.1.2. BANI-среды
 - 14.1.1.2.1. Хрупкость
 - 14.1.1.2.2. Тревожность
 - 14.1.1.2.3. Нелинейность
 - 14.1.1.2.4. Непонятность
 - 14.1.2. Анализ общей среды. PESTEL
 - 14.1.2.1. Политический
 - 14.1.2.2. Экономический
 - 14.1.2.3. Социальный
 - 14.1.2.4. Технологичный
 - 14.1.2.5. Экологичный
 - 14.1.2.6. Юридический
 - 14.1.3. Анализ внутреннего положения. SWOT-анализ
 - 14.1.3.1. Цели
 - 14.1.3.2. Угрозы
 - 14.1.3.3. Возможности
 - 14.1.3.4. Преимущества
- 14.2. Риск и неопределенность
 - 14.2.1. Риск
 - 14.2.2. Управление рисками
 - 14.2.3. Стандарты управления рисками
- 14.3. Руководства по управлению рисками ISO 31.000:2018
 - 14.3.1. Цель
 - 14.3.2. Принципы
 - 14.3.3. Система отсчета
 - 14.3.4. Процесс
- 14.4. Методология анализа и управления рисками информационных систем (MAGERIT)
 - 14.4.1. Методология MAGERIT
 - 14.4.1.1. Цели
 - 14.4.1.2. Методика
 - 14.4.1.3. Элементы
 - 14.4.1.4. Техники
 - 14.4.1.5. Доступные инструменты (PILAR)
- 14.5. Передача киберрисков
 - 14.5.1. Передача рисков
 - 14.5.2. Киберриски. Типология
 - 14.5.3. Страхование от киберрисков
- 14.6. Agile-методологии для управления рисками
 - 14.6.1. Agile-методологии
 - 14.6.2. Scrum для управления рисками
 - 14.6.3. *Agile-управление рисками*
- 14.7. Технологии для управления рисками
 - 14.7.1. Применение искусственного интеллекта в управлении рисками
 - 14.7.2. *Блокчейн* и криптография. Методы сохранения стоимости
 - 14.7.3. Квантовые вычисления. Возможности или угрозы
- 14.8. Составление карт ИТ-рисков на основе Agile-методологий
 - 14.8.1. Представление вероятности и последствий в Agile-средах
 - 14.8.2. Риск как угроза стоимости
 - 14.8.3. Революция в управлении проектами и Agile-процессами на основе KRI
- 14.9. *Риск-ориентированное* управление рисками
 - 14.9.1. *Риск-ориентированное управление*
 - 14.9.2. *Риск-ориентированное управление*
 - 14.9.3. Разработка модели управления бизнесом с учетом рисков
- 14.10. Инновации и цифровая трансформация в управлении ИТ-рисками
 - 14.10.1. Agile-управление рисками как источник инноваций в бизнесе
 - 14.10.2. Преобразование данных в полезную для принятия решений информацию
 - 14.10.3. Целостный взгляд на предприятие через призму риска

Модуль 15. Криптография в ИТ

- 15.1. Криптография
 - 15.1.1. Криптография
 - 15.2.1. Математические основы
- 15.2. Криптология
 - 15.2.1. Криптология
 - 15.2.2. Криптоанализ
 - 15.2.3. Стеганография и стегоанализ
- 15.3. Криптографические протоколы
 - 15.3.1. Базовые блоки
 - 15.3.2. Базовые протоколы
 - 15.3.3. Промежуточные протоколы
 - 15.3.4. Расширенные протоколы
 - 15.3.5. Эзотерические протоколы
- 15.4. Криптографические методы
 - 15.4.1. Длина ключа
 - 15.4.2. Управление ключами
 - 15.4.3. Виды алгоритмов
 - 15.4.4. Агрегатные функции. *Хеш-функция*
 - 15.4.5. Генераторы псевдослучайных чисел
 - 15.4.6. Использование алгоритмов
- 15.5. Симметричная криптография
 - 15.5.1. Блочные шифры
 - 15.5.2. DES (*Data Encryption Standard*)
 - 15.5.3. Алгоритм RC4
 - 15.5.4. AES (*Advanced Encryption Standard*)
 - 15.5.5. Комбинация блочных шифров
 - 15.5.6. Получение ключей
- 15.6. Асимметричная криптография
 - 15.6.1. Протокол Диффи – Хеллмана
 - 15.6.2. DSA (*Digital Signature Algorithm*)
 - 15.6.3. RSA (Ривест, Шамир и Адлеман)
 - 15.6.4. Эллиптическая кривая
 - 15.6.5. Асимметричная криптография. Типология

- 15.7. Цифровые сертификаты
 - 15.7.1. Цифровая подпись
 - 15.7.2. Сертификаты X509
 - 15.7.3. Инфраструктура открытых ключей (PKI)
- 15.8. Способы реализации
 - 15.8.1. Kerberos
 - 15.8.2. IBM CCA
 - 15.8.3. *Pretty Good Privacy* (PGP)
 - 15.8.4. *ISO Authentication Framework*
 - 15.8.5. SSL и TLS
 - 15.8.6. Смарт-карты в платежных средствах (EMV)
 - 15.8.7. Протоколы мобильной связи
 - 15.8.8. *Блокчейн*
- 15.9. Стеганография
 - 15.9.1. Стеганография
 - 15.9.2. Стегоанализ
 - 15.9.3. Применение и использование
- 15.10. Квантовая криптография
 - 15.10.1. Квантовые алгоритмы
 - 15.10.2. Защита алгоритмов от квантовых вычислений
 - 15.10.3. Квантовое распределение ключей

Модуль 16. Управление идентификацией и доступом в ИТ-безопасности

- 16.1. Управление идентификацией и доступом (IAM)
 - 16.1.1. Цифровая идентификация
 - 16.1.2. Управление идентификацией
 - 16.1.3. Федеративные идентификации
- 16.2. Управление физическим доступом
 - 16.2.1. Системы защиты
 - 16.2.2. Безопасность территорий
 - 16.2.3. Восстановительные комплексы
- 16.3. Управление логическим доступом
 - 16.3.1. Аутентификация: типология

- 16.3.2. Протоколы аутентификации
- 16.3.3. Атаки на аутентификацию
- 16.4. Управление логическим доступом. Многофакторная аутентификация (MFA)
 - 16.4.1. Управление логическим доступом. Многофакторная аутентификация (MFA)
 - 16.4.2. Пароли. Важность
 - 16.4.3. Атаки на аутентификацию
- 16.5. Управление логическим доступом. Биометрическая аутентификация
 - 16.5.1. Управление логическим доступом. Биометрическая аутентификация
 - 16.5.1.1. Биометрическая аутентификация. Требования
 - 16.5.2. Операции
 - 16.5.3. Модели и методы
- 16.6. Системы управления аутентификацией
 - 16.6.1. *Технология единого входа (Single sign-on)*
 - 16.6.2. Kerberos
 - 16.6.3. Системы AAA
- 16.7. Системы управления аутентификацией: Системы AAA
 - 16.7.1. TACACS
 - 16.7.2. RADIUS
 - 16.7.3. DIAMETER
- 16.8. Службы по управлению доступом
 - 16.8.1. Файрволы — межсетевые экраны
 - 16.8.2. VPN — виртуальные частные сети
 - 16.8.3. IDS — система обнаружения вторжений
- 16.9. Системы управления доступом к сети
 - 16.9.1. NAC
 - 16.9.2. Архитектура и элементы
 - 16.9.3. Эксплуатация и стандартизация
- 16.10. Доступ к беспроводным сетям
 - 16.10.1. Виды беспроводных сетей
 - 16.10.2. Безопасность в беспроводных сетях
 - 16.10.3. Атаки на беспроводные сети

Модуль 17. Безопасность в сфере коммуникаций и эксплуатации программного обеспечения

- 17.1. Компьютерная безопасность в сфере коммуникаций и эксплуатации программного обеспечения
 - 17.1.1. Компьютерная безопасность
 - 17.1.2. Кибербезопасность
 - 17.1.3. Облачная безопасность
- 17.2. Компьютерная безопасность в сфере коммуникаций и эксплуатации программного обеспечения. Типология
 - 17.2.1. Физическая безопасность
 - 17.2.2. Логическая безопасность
- 17.3. Безопасность в сфере коммуникаций
 - 17.3.1. Основные элементы
 - 17.3.2. Сетевая безопасность
 - 17.3.3. Передовая практика
- 17.4. Киберразведка
 - 17.4.1. Социальная инженерия
 - 17.4.2. *Deer Web* — глубокая сеть
 - 17.4.3. *Фишинг*
 - 17.4.4. *Вредоносное программное обеспечение*
- 17.5. Безопасная разработка в сфере коммуникации и эксплуатации программного обеспечения
 - 17.5.1. Безопасная разработка. Протокол HTTP
 - 17.5.2. Безопасная разработка. Жизненный цикл
 - 17.5.3. Безопасная разработка. Безопасность PHP
 - 17.5.4. Безопасная разработка. Безопасность NET
 - 17.5.5. Безопасная разработка. Передовая практика
- 17.6. Системы управления информационной безопасностью в сфере коммуникаций и эксплуатации программного обеспечения
 - 17.6.1. GDPR
 - 17.6.2. ISO 27021
 - 17.6.3. ISO 27017/18

- 17.7. SIEM-технологии
 - 17.7.1. SIEM-технологии
 - 17.7.2. Деятельность SOC
 - 17.7.3. SIEM: поставщики
- 17.8. Роль в обеспечении безопасности в организациях
 - 17.8.1. Роли в организациях
 - 17.8.2. Роль специалистов в области IoT в компаниях
 - 17.8.3. Признанные на рынке сертификаты
- 17.9. Криминалистическая экспертиза
 - 17.9.1. Криминалистическая экспертиза
 - 17.9.2. Криминалистическая экспертиза. Методология
 - 17.9.3. Криминалистическая экспертиза. Инструменты и внедрение
- 17.10. Кибербезопасность сегодня
 - 17.10.1. Крупные кибернетические атаки
 - 17.10.2. Прогнозы по трудоустройству
 - 17.10.3. Задачи

Модуль 18. Безопасность в облачной среде

- 18.1. Безопасность в среде *облачных вычислений*
 - 18.1.1. Безопасность в среде *облачных вычислений*
 - 18.1.2. Безопасность в среде *облачных вычислений*. Угрозы и риски безопасности
 - 18.1.3. Безопасность в среде *облачных вычислений*. Ключевые аспекты безопасности
- 18.2. Виды *облачной инфраструктуры*
 - 18.2.1. Общедоступная
 - 18.2.2. Частная
 - 18.2.3. Гибридная
- 18.3. Модель совместного управления
 - 18.3.1. Элементы безопасности, управляемые поставщиком
 - 18.3.2. Элементы, управляемые клиентом
 - 18.3.3. Определение стратегии безопасности
- 18.4. Профилактические механизмы
 - 18.4.1. Системы управления аутентификацией
 - 18.4.2. Система управления авторизацией: политики доступа
 - 18.4.3. Системы управления ключами

- 18.5. Секьюритизация систем
 - 18.5.1. Секьюритизация систем хранения
 - 18.5.2. Защита систем управления базами данных
 - 18.5.3. Секьюритизация при передаче данных
- 18.6. Защита инфраструктуры
 - 18.6.1. Проектирование и внедрение безопасных сетей
 - 18.6.2. Безопасность вычислительных ресурсов
 - 18.6.3. Инструменты и ресурсы для защиты инфраструктуры
- 18.7. Обнаружение угроз и атак
 - 18.7.1. Системы аудита, *ведения журнала* и мониторинга
 - 18.7.2. Системы событий и сигнализации
 - 18.7.3. SIEM-системы
- 18.8. Реагирование на инциденты
 - 18.8.1. План по реагированию на инциденты
 - 18.8.2. Непрерывность бизнеса
 - 18.8.3. Криминалистический анализ и устранение последствий инцидентов аналогичного характера
- 18.9. Безопасность в публичных *облаках*
 - 18.9.1. AWS (Amazon Web Services)
 - 18.9.2. Microsoft Azure
 - 18.9.3. Google GCP
 - 18.9.4. Oracle *Cloud*
- 18.10. Регулирование и соблюдение
 - 18.10.1. Соблюдение норм безопасности
 - 18.10.2. Управление рисками
 - 18.10.3. Люди и процессы в организациях

Модуль 19. Безопасность в коммуникациях между устройствами интернета вещей (IoT)

- 19.1. От телеметрии к IoT
 - 19.1.1. Телеметрия
 - 19.1.2. Межмашинное взаимодействие (M2M)
 - 19.1.3. Демократизация телеметрии
- 19.2. Эталонные модели IoT
 - 19.2.1. Эталонные модели IoT
 - 19.2.2. Упрощенная архитектура IoT
- 19.3. Уязвимости безопасности IoT
 - 19.3.1. IoT-устройства
 - 19.3.2. IoT-устройства. Примеры использования
 - 19.3.3. IoT-устройства. Уязвимости
- 19.4. IoT-соединение
 - 19.4.1. Сети PAN, LAN, WAN
 - 19.4.2. Беспроводные технологии, не относящиеся к IoT
 - 19.4.3. Беспроводные технологии LPWAN
- 19.5. Технологии LPWAN
 - 19.5.1. "Железный треугольник" сетей LPWAN
 - 19.5.2. Свободные частотные диапазоны vs. Лицензированные диапазоны
 - 19.5.3. Возможности технологии LPWAN
- 19.6. Технология LoRaWAN
 - 19.6.1. Технология LoRaWAN
 - 19.6.2. Варианты использования LoRaWAN. Экосистема
 - 19.6.3. Безопасность LoRaWAN
- 19.7. Технология Sigfox
 - 19.7.1. Технология Sigfox
 - 19.7.2. Варианты использования Sigfox. Экосистема
 - 19.7.3. Безопасность Sigfox
- 19.8. Технология сотовой связи для IoT
 - 19.8.1. Технология сотовой связи для IoT (NB-IoT и LTE-M)
 - 19.8.2. Варианты использования технологии сотовой связи для IoT. Экосистема
 - 19.8.3. Безопасность технологии сотовой связи для IoT
- 19.9. Технология Wi-SUN
 - 19.9.1. Технология Wi-SUN

- 19.9.2. Варианты использования Wi-SUN. Экосистема
- 19.9.3. Безопасность Wi-SUN
- 19.10. Другие виды технологий IoT
 - 19.10.1. Другие виды технологий IoT
 - 19.10.2. Примеры использования и экосистема других технологий IoT
 - 19.10.3. Безопасность других технологий IoT

Модуль 20. План по обеспечению непрерывности бизнеса, связанный с безопасностью

- 20.1. План по обеспечению непрерывности бизнеса
 - 20.1.1. Планы по обеспечению непрерывности бизнеса (BCP)
 - 20.1.2. План по обеспечению непрерывности бизнеса (BCP). Основные вопросы
 - 20.1.3. План по обеспечению непрерывности бизнеса (BCP) для оценки стоимости бизнеса
- 20.2. Метрики в плане по обеспечению непрерывности бизнеса (BCP)
 - 20.2.1. *Целевое время восстановления (RTO) и Целевая точка восстановления (RPO)*
 - 20.2.2. Максимально допустимое время простоя (MTD)
 - 20.2.3. Минимальный уровень восстановления (ROL)
 - 20.2.4. Целевая точка восстановления (RPO)
- 20.3. Проекты непрерывного действия. Типология
 - 20.3.1. План по обеспечению непрерывности бизнеса (BCP)
 - 20.3.2. План по обеспечению непрерывности ИКТ
 - 20.3.3. План аварийного восстановления (DRP)
- 20.4. Управление рисками, связанными с BCP
 - 20.4.1. Анализ влияния на бизнес
 - 20.4.2. Преимущества внедрения BCP
 - 20.4.3. Менталитет, основанный на риске
- 20.5. Жизненный цикл плана по обеспечению непрерывности бизнеса
 - 20.5.1. Фаза 1: Анализ организации
 - 20.5.2. Фаза 2: Определение стратегии непрерывности
 - 20.5.3. Фаза 3: Реагирование в чрезвычайных ситуациях
 - 20.5.4. Фаза 4: Испытания, техническое обслуживание и ревизия

- 20.6. Фаза организационного анализа BCP
 - 20.6.1. Идентификация процессов, входящих в сферу действия BCP
 - 20.6.2. Определение критических областей бизнеса
 - 20.6.3. Выявление зависимостей между областями и процессами
 - 20.6.4. Определение адекватного MTD
 - 20.6.5. Результаты. Создание плана
- 20.7. Фаза определения стратегии непрерывности в рамках BCP
 - 20.7.1. Роли в фазе определения стратегии
 - 20.7.2. Задачи в фазе определения стратегии
 - 20.7.3. Результаты работы
- 20.8. Фаза реагирования на непредвиденные обстоятельства в рамках BCP
 - 20.8.1. Роли в фазе реагирования
 - 20.8.2. Задачи в этой фазе
 - 20.8.3. Результаты работы
- 20.9. Фаза тестирования, обслуживания и ревизии BCP
 - 20.9.1. Роли в фазе тестирования, обслуживания и ревизии
 - 20.9.2. Задачи в фазе тестирования, обслуживания и ревизии
 - 20.9.3. Результаты работы
- 20.10. Стандарты ISO, связанные с планами по обеспечению непрерывности бизнеса (BCP)
 - 20.10.1. ISO 22301, ISO 2019
 - 20.10.2. ISO 22313, ISO 2020
 - 20.10.3. Другие соответствующие стандарты ISO и международные стандарты

Модуль 21. Аналитика данных в организации бизнеса

- 21.1. Бизнес-анализ
 - 21.1.1. Бизнес-анализ
 - 21.1.2. Структура данных
 - 21.1.3. Этапы и элементы
- 21.2. Аналитика данных в компании
 - 21.2.1. Система показателей и KPI в различных отделах
 - 21.2.2. Оперативная, тактическая и стратегическая отчетность
- 21.2.3. Аналитика данных, применяемая в каждом отделе
 - 21.2.3.1. Маркетинг и коммуникации
 - 21.2.3.2. Коммерция
 - 21.2.3.3. Обслуживание клиентов
 - 21.2.3.4. Закупки
 - 21.2.3.5. Управление
 - 21.2.3.6. Управление персоналом
 - 21.2.3.7. Производство
 - 21.2.3.8. ИТ
- 21.3. Маркетинг и коммуникации
 - 21.3.1. KPI для измерения, применение и преимущества
 - 21.3.2. Маркетинговые системы и *хранилище данных*
 - 21.3.3. Внедрение структуры анализа данных в маркетинге
 - 21.3.4. План маркетинга и коммуникации
 - 21.3.5. Стратегии, прогнозирование и управление кампаниями
- 21.4. Коммерция и продажи
 - 21.4.1. Вклад аналитики данных в коммерческую сферу
 - 21.4.2. Потребности отдела продаж
 - 21.4.3. Изучение рынка
- 21.5. Обслуживание клиентов
 - 21.5.1. Лояльность
 - 21.5.2. Личные качества и эмоциональный интеллект
 - 21.5.3. Удовлетворенность клиентов
- 21.6. Закупки
 - 21.6.1. Аналитика данных для маркетинговых исследований
 - 21.6.2. Аналитика данных для конкурентных исследований
 - 21.6.3. Другие виды применения
- 21.7. Управление
 - 21.7.1. Потребности административного отдела
 - 21.7.2. *Хранилище данных* и анализ финансовых рисков
 - 21.7.3. *Хранилище данных* и анализ кредитных рисков
- 21.8. Человеческие ресурсы
 - 21.8.1. Управление человеческими ресурсами и преимущества аналитики данных



- 21.8.2. Инструменты анализа данных в отделе управления человеческими ресурсами
- 21.8.3. Применение аналитики данных в отделе управления человеческими ресурсами
- 21.9. Производство
 - 21.9.1. Анализ данных в производственном отделе
 - 21.9.2. Приложения
 - 21.9.3. Преимущества
- 21.10. ИТ
 - 21.10.1. Отдел ИТ
 - 21.10.2. Аналитика данных и цифровая трансформация
 - 21.10.3. Инновации и производительность

Модуль 22. Управление данными, обработка данных и информации согласно науке о данных

- 22.1. Статистика. Переменные, индексы и коэффициенты
 - 22.1.1. Статистика
 - 22.1.2. Статистические измерения
 - 22.1.3. Переменные, индексы и коэффициенты
- 22.2. Типология данных
 - 22.2.1. Качественные
 - 22.2.2. Количественные
 - 22.2.3. Характеристики и категории
- 22.3. Знание данных, полученных в результате измерений
 - 22.3.1. Измерения централизации
 - 22.3.2. Измерения дисперсии
 - 22.3.3. Корреляция
- 22.4. Знание данных, полученных в результате анализа графиков
 - 22.4.1. Визуализация в соответствии с видом данных
 - 22.4.2. Интерпретация графической информации
 - 22.4.3. Настройка графики с помощью R
- 22.5. Вероятность
 - 22.5.1. Вероятность

- 22.5.2. Функция вероятности
- 22.5.3. Распределения
- 22.6. Сбор данных
 - 22.6.1. Методология сбора
 - 22.6.2. Инструменты сбора
 - 22.6.3. Каналы сбора
- 22.7. Очистка данных
 - 22.7.1. Этапы очистки данных
 - 22.7.2. Качество данных
 - 22.7.3. Работа с данными (с помощью R)
- 22.8. Анализ данных, интерпретация и оценка результатов
 - 22.8.1. Статистические меры
 - 22.8.2. Индексы отношений
 - 22.8.3. Добыча данных
- 22.9. Хранилище информации (*хранилище данных*)
 - 22.9.1. Элементы
 - 22.9.2. Структура
- 22.10. Доступность данных
 - 22.10.1. Доступ
 - 22.10.2. Применение
 - 22.10.3. Безопасность

Модуль 23. IoT-устройства и платформы как основа для науки о данных

- 23.1. *Интернет вещей*
 - 23.1.1. Интернет будущего, *Интернет вещей*
 - 23.1.2. Консорциум промышленного интернета
- 23.2. Эталонная архитектура
 - 23.2.1. Эталонная архитектура
 - 23.2.2. Слои
 - 23.2.3. Компоненты
- 23.3. Датчики и устройства IoT
 - 23.3.1. Основные компоненты
 - 23.3.2. Датчики и исполнительные механизмы

- 23.4. Коммуникации и протоколы
 - 23.4.1. Протоколы. Модель OSI
 - 23.4.2. Коммуникационные технологии
- 23.5. Облачные платформы для IoT и IIoT
 - 23.5.1. Платформы общего назначения
 - 23.5.2. Промышленные платформы
 - 23.5.3. Платформы с открытым исходным кодом
- 23.6. Управление данными в IoT-платформах
 - 23.6.1. Механизмы управления данными. Открытые данные
 - 23.6.2. Обмен данными и визуализация
- 23.7. Безопасность в IoT
 - 23.7.1. Требования к безопасности и области безопасности
 - 23.7.2. Стратегии безопасности в IIoT
- 23.8. IoT-приложения
 - 23.8.1. Умные города
 - 23.8.2. Здоровье и фитнес
 - 23.8.3. Умный дом
 - 23.8.4. Другие виды применения
- 23.9. Приложения IIoT
 - 23.9.1. Производство
 - 23.9.2. Транспорт
 - 23.9.3. Энергия
 - 23.9.4. Сельское хозяйство и животноводство
 - 23.9.5. Другие сектора
- 23.10. Индустрия 4.0
 - 23.10.1. loRT (*Интернет роботизированных вещей*)
 - 23.10.2. Аддитивное 3D-производство
 - 23.10.3. *Аналитика больших данных*

Модуль 24. Графическое представление для анализа данных

- 24.1. Исследовательский анализ
 - 24.1.1. Представление для анализа информации
 - 24.1.2. Ценность графического представления
 - 24.1.3. Новые парадигмы графического представления
- 24.2. Оптимизация для науки о данных
 - 24.2.1. Цветовая гамма и дизайн
 - 24.2.2. Гештальт в графическом представлении
 - 24.2.3. Ошибки, которых следует избегать, и советы
- 24.3. Источники основных данных
 - 24.3.1. Для качественного представления
 - 24.3.2. Для количественного представления
 - 24.3.3. Для временного представления
- 24.4. Источники сложных данных
 - 24.4.1. Архивы, списки файлов и базы данных
 - 24.4.2. Открытые данные
 - 24.4.3. Непрерывно-генерируемые данные
- 24.5. Виды графиков
 - 24.5.1. Базовые виды представлений
 - 24.5.2. Блок-схемы
 - 24.5.3. Представление для дисперсионного анализа
 - 24.5.4. Круговые диаграммы
 - 24.5.5. Пузырьковая диаграмма
 - 24.5.6. Географические представления
- 24.6. Виды визуализации
 - 24.6.1. Сравнительная и реляционная
 - 24.6.2. Распределенная
 - 24.6.3. Иерархическая
- 24.7. Разработка отчетов с графическим представлением
 - 24.7.1. Применение графиков в маркетинговых отчетах
 - 24.7.2. Применение графиков в системах показателей и KPI
 - 24.7.3. Применение графиков в стратегических планах
 - 24.7.4. Другие виды использования: наука, здоровье, бизнес

- 24.8. Графический нарратив
 - 24.8.1. Графический нарратив
 - 24.8.2. Развитие
 - 24.8.3. Полезность
- 24.9. Инструменты, ориентированные на визуализацию
 - 24.9.1. Продвинутое инструменты
 - 24.9.2. Программное обеспечение в онлайн
 - 24.9.3. *Открытый код*
- 24.10. Новые технологии в визуализации данных
 - 24.10.1. Системы для виртуализации реальности
 - 24.10.2. Системы для расширения и улучшения реальности
 - 24.10.3. Интеллектуальные системы

Модуль 25. Инструменты науки о данных

- 25.1. Наука о данных
 - 25.1.1. Наука о данных
 - 25.1.2. Продвинутое инструменты для специалиста по анализу данных
- 25.2. Данные, информация и знания
 - 25.2.1. Данные, информация и знания
 - 25.2.2. Виды данных
 - 25.2.3. Источники данных
- 25.3. От данных к информации
 - 25.3.1. Анализ данных
 - 25.3.2. Виды анализа
 - 25.3.3. Извлечение информации из *набора данных*
- 25.4. Извлечение информации путем визуализации
 - 25.4.1. Визуализация как инструмент анализа
 - 25.4.2. Методы визуализации
 - 25.4.3. Визуализация набора данных
- 25.5. Качество данных
 - 25.5.1. Качество данных
 - 25.5.2. Очистка данных
 - 25.5.3. Базовая предварительная обработка данных

- 25.6. Набор данных
 - 25.6.1. Обогащение набора данных
 - 25.6.2. Проклятие размерности
 - 25.6.3. Модификация набора данных
- 25.7. Несбалансированность
 - 25.7.1. Несбалансированность классов
 - 25.7.2. Методы устранения несбалансированности
 - 25.7.3. Сбалансированность набора данных
- 25.8. Модели без отслеживания
 - 25.8.1. Модель без отслеживания
 - 25.8.2. Методы
 - 25.8.3. Классификация с помощью моделей без отслеживания
- 25.9. Модели с отслеживанием
 - 25.9.1. Модель с отслеживанием
 - 25.9.2. Методы
 - 25.9.3. Классификация с помощью моделей с отслеживанием
- 25.10. Инструменты и передовой опыт
 - 25.10.1. Передовые практики для специалиста по анализу данных
 - 25.10.2. Лучшая модель
 - 25.10.3. Полезные инструменты

Модуль 26. Добыча данных. Отбор, предварительная обработка и преобразование

- 26.1. Статистический вывод
 - 26.1.1. Описательная статистика vs. Статистический вывод
 - 26.1.2. Параметрические методы
 - 26.1.3. Непараметрические методы
- 26.2. Исследовательский анализ
 - 26.2.1. Описательный анализ
 - 26.2.2. Визуализация
 - 26.2.3. Подготовка данных
- 26.3. Подготовка данных
 - 26.3.1. Интеграция и очистка данных
 - 26.3.2. Нормализация данных
 - 26.3.3. Преобразование атрибутов
- 26.4. Отсутствующие данные
 - 26.4.1. Обработка отсутствующих данных
 - 26.4.2. Метод максимального правдоподобия
 - 26.4.3. Обработка отсутствующих данных в машинном обучении
- 26.5. Шум в данных
 - 26.5.1. Классы и признаки шума
 - 26.5.2. Фильтрация шумов
 - 26.5.3. Шумовой эффект
- 26.6. Проклятие размерности
 - 26.6.1. Передискретизация
 - 26.6.2. Неполная выборка
 - 26.6.3. Редукция многомерных данных
- 26.7. От непрерывных к дискретным признакам
 - 26.7.1. Непрерывные данные vs. Дискретные данные
 - 26.7.2. Процесс дискретизации
- 26.8. Данные
 - 26.8.1. Отбор данных
 - 26.8.2. Перспективы и критерии отбора
 - 26.8.3. Методы отбора
- 26.9. Выбор экземпляров
 - 26.9.1. Методы выбора экземпляров
 - 26.9.2. Выбор прототипов
 - 26.9.3. Расширенные методы выбора экземпляров
- 26.10. Предварительная обработка данных в среде больших данных
 - 26.10.1. Большие данные
 - 26.10.2. Классическая предварительная обработка vs. Массивная обработка
 - 26.10.3. Умные данные

Модуль 27. Предсказуемость и стохастический анализ

- 27.1. Временные ряды
 - 27.1.1. Временные ряды
 - 27.1.2. Полезность и применимость
 - 27.1.3. Соответствующие тематические исследования
- 27.2. Временная серия
 - 27.2.1. Сезонность
 - 27.2.2. Сезонная вариация
 - 27.2.3. Анализ остатков
- 27.3. Типологии
 - 27.3.1. Стационарная модель
 - 27.3.2. Нестационарная модель
 - 27.3.3. Преобразования и корректировки
- 27.4. Схемы для временных рядов
 - 27.4.1. Аддитивная модель
 - 27.4.2. Мультипликативная модель
 - 27.4.3. Процедуры определения типа модели
- 27.5. Основные методы *прогнозирования*
 - 27.5.1. Метод средних значений
 - 27.5.2. *"Наивный" подход*
 - 27.5.3. *"Наивный" сезонный подход*
 - 27.5.4. Сравнение методов
- 27.6. Анализ остатков
 - 27.6.1. Автокорреляция
 - 27.6.2. Автокорреляционная функция остатков
 - 27.6.3. Корреляционный анализ
- 27.7. Регрессия в контексте временных рядов
 - 27.7.1. Дисперсионный анализ
 - 27.7.2. Основы
 - 27.7.3. Практическое применение
- 27.8. Прогнозирующие модели временных рядов
 - 27.8.1. ARIMA
 - 27.8.2. Экспоненциальное сглаживание

- 27.9. Анализ временных рядов в R
 - 27.9.1. Подготовка данных
 - 27.9.2. Идентификация шаблонов
 - 27.9.3. Анализ модели
 - 27.9.4. Прогноз
- 27.10. Комбинированный графический анализ с помощью R
 - 27.10.1. Типичные ситуации
 - 27.10.2. Практическое применение для решения простых задач
 - 27.10.3. Практическое применение для решения продвинутых задач

Модуль 28. Проектирование и разработка интеллектуальных систем

- 28.1. Предварительная обработка данных
 - 28.1.1. Предварительная обработка данных
 - 28.1.2. Преобразование данных
 - 28.1.3. Добыча данных
- 28.2. Машинное обучение
 - 28.2.1. Контролируемое и неконтролируемое обучение
 - 28.2.2. Обучение с подкреплением
 - 28.2.3. Другие парадигмы обучения
- 28.3. Алгоритмы классификации
 - 28.3.1. Индуктивное машинное обучение
 - 28.3.2. Опорно-векторная машина (SVM) и метод k-ближайших соседей (KNN)
 - 28.3.3. Метрики и оценки для классификации
- 28.4. Алгоритмы регрессии
 - 28.4.1. Линейная регрессия, логистическая регрессия и нелинейные модели
 - 28.4.2. Временные серии
 - 28.4.3. Метрики и оценки для регрессии
- 28.5. Алгоритмы кластеризации
 - 28.5.1. Методы иерархической кластеризации
 - 28.5.2. Методы условной кластеризации
 - 28.5.3. Показатели и оценки *кластеризации*
- 28.6. Методы ассоциативных правил
 - 28.6.1. Методы извлечения правил
 - 28.6.2. Метрики и оценки для алгоритмов ассоциативных правил

- 28.7. Продвинутое методы классификации. Мультиклассовые алгоритмы
 - 28.7.1. Алгоритмы бэггинга
 - 28.7.2. Метод случайного леса
 - 28.7.3. "Бустинг" решающих деревьев
- 28.8. Графовая вероятностная модель
 - 28.8.1. Вероятностная модель
 - 28.8.2. Байесовские сети. Свойства, представление и параметризация
 - 28.8.3. Другие графовые вероятностные модели
- 28.9. Нейронные сети
 - 28.9.1. Машинное обучение с помощью искусственных нейронных сетей
 - 28.9.2. Нейронная сеть с *прямой связью*
- 28.10. Глубокое обучение
 - 28.10.1. Глубокие сети *прямой связи*
 - 28.10.2. Сверточные нейронные сети и модели последовательностей
 - 28.10.3. Инструменты для реализации глубоких нейронных сетей

Модуль 29. Архитектуры и системы с интенсивным использованием данных

- 29.1. Нефункциональные требования. Основные принципы применения больших данных
 - 29.1.1. Надежность
 - 29.1.2. Адаптивность
 - 29.1.3. Управляемость
- 29.2. Моделирование данных
 - 29.2.1. Реляционная модель
 - 29.2.2. Документальная модель
 - 29.2.3. Графовая модель данных
- 29.3. Базы данных. Управление хранением и поиском данных
 - 29.3.1. Что такое *хеш-индексы*
 - 29.3.2. Структурированное хранение в журнале
 - 29.3.3. В-дерево

- 29.4. Форматы кодирования данных
 - 29.4.1. Форматы, специфичные для конкретного языка
 - 29.4.2. Стандартизированные форматы
 - 29.4.3. Форматы двоичного кодирования
 - 29.4.4. Межпроцессный поток данных
- 29.5. Репликация
 - 29.5.1. Цели репликации
 - 29.5.2. Модели репликации
 - 29.5.3. Проблемы с репликацией
- 29.6. Распределенные транзакции
 - 29.6.1. Транзакция
 - 29.6.2. Протоколы для распределенных транзакций
 - 29.6.3. Сериализуемость транзакций
- 29.7. Секционирование
 - 29.7.1. Формы секционирования
 - 29.7.2. Взаимодействие вторичных индексов и секционирования
 - 29.7.3. Перебалансировка разделов
- 29.8. Обработка *данных в офлайн-режиме*
 - 29.8.1. Пакетная обработка
 - 29.8.2. Распределенные файловые системы
 - 29.8.3. MapReduce
- 29.9. Обработка данных в реальном времени
 - 29.9.1. Виды *брокеров сообщений*
 - 29.9.2. Представление баз данных в виде потоков данных
 - 29.9.3. Обработка потоков данных
- 29.10. Практическое применение в бизнесе
 - 29.10.1. Последовательность в чтении
 - 29.10.2. Комплексный подход к данным
 - 29.10.3. Масштабируемая распределенная система

Модуль 30. Практическое применение науки о данных в различных сферах бизнеса

- 30.1. Сфера здравоохранения
 - 30.1.1. Влияние ИИ и аналитики данных на сферу здравоохранения
 - 30.1.2. Возможности и проблемы
- 30.2. Риски и тенденции в здравоохранении
 - 30.2.1. Использование в сфере здравоохранения
 - 30.2.2. Потенциальные риски, связанные с использованием ИИ
- 30.3. Финансовые услуги
 - 30.3.1. Влияние ИИ и аналитики данных на сферу финансовых услуг
 - 30.3.2. Использование в сфере финансовых услуг
 - 30.3.3. Потенциальные риски, связанные с использованием ИИ
- 30.4. Розничная торговля
 - 30.4.1. Влияние ИИ и аналитики данных на сферу розничной торговли
 - 30.4.2. Использование в сфере розничной торговли
 - 30.4.3. Потенциальные риски, связанные с использованием ИИ
- 30.5. Индустрия 4.0
 - 30.5.1. Влияние ИИ и аналитики данных на Индустрию 4.0
 - 30.5.2. Использование в Индустрии 4.0
- 30.6. Риски и тенденции в Индустрии 4.0
 - 30.6.1. Потенциальные риски, связанные с использованием ИИ
- 30.7. Государственное управление
 - 30.7.1. Влияние ИИ и аналитики данных на сферу государственного управления
 - 30.7.2. Использование в сфере государственного управления
 - 30.7.3. Потенциальные риски, связанные с использованием ИИ
- 30.8. Образование
 - 30.8.1. Влияние ИИ и аналитики данных на сферу образования
 - 30.8.2. Потенциальные риски, связанные с использованием ИИ
- 30.9. Лесное и сельское хозяйство
 - 30.9.1. Влияние ИИ и аналитики данных на сферу лесного и сельского хозяйства
 - 30.9.2. Использование в сфере лесного и сельского хозяйства
 - 30.9.3. Потенциальные риски, связанные с использованием ИИ
- 30.10. Человеческие ресурсы
 - 30.10.1. Влияние ИИ и аналитики данных на сферу управления человеческими ресурсами
 - 30.10.2. Практическое применение в деловом мире
 - 30.10.3. Потенциальные риски, связанные с использованием ИИ

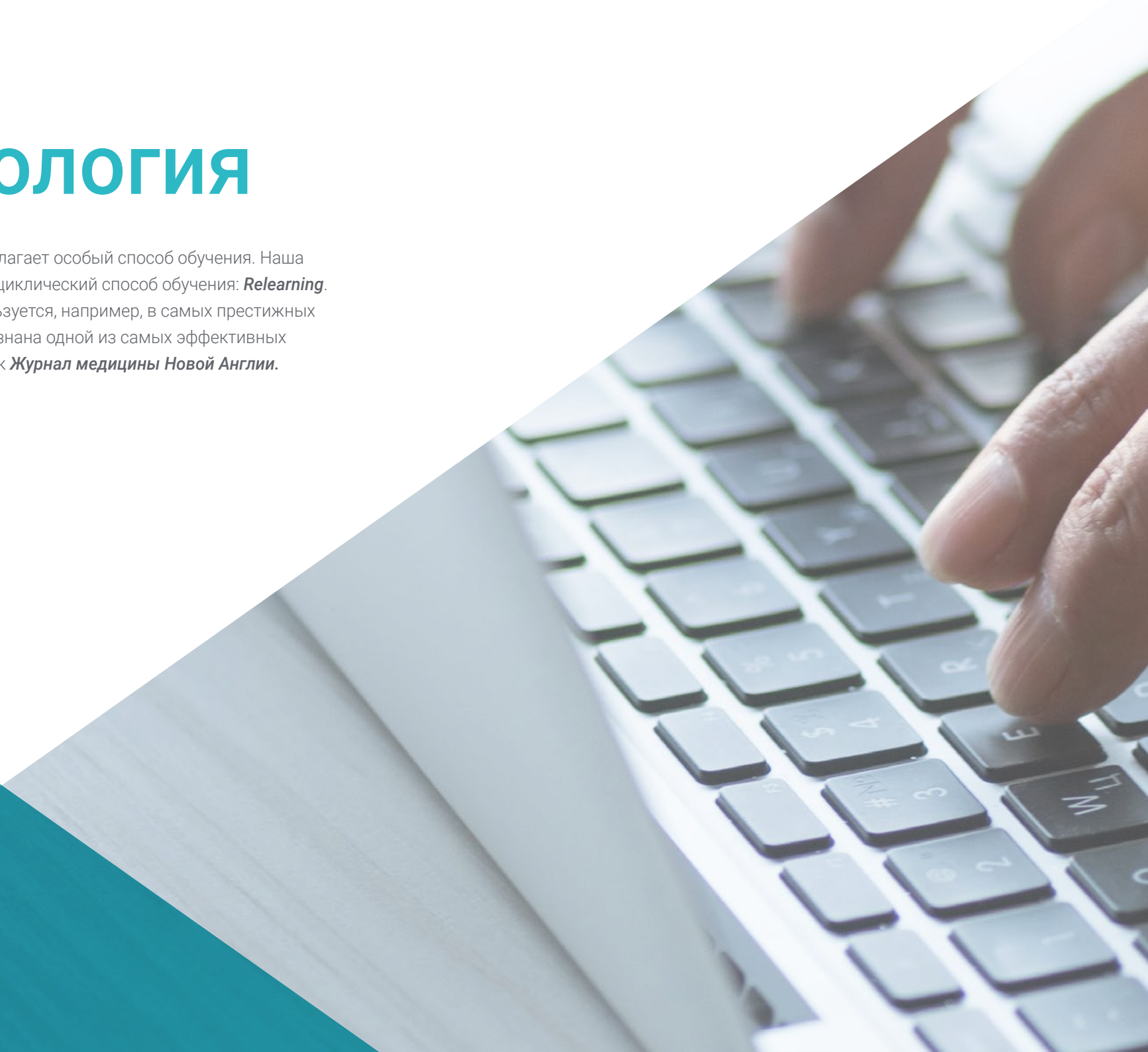


TECH предлагает лучшую программу для таких ИТ-специалистов, как вы, которые хотят изменить свою карьеру, чтобы ускорить свой профессиональный рост"

06

Методология

Данная учебная программа предлагает особый способ обучения. Наша методология развивается через циклический способ обучения: **Relearning**. Данная система обучения используется, например, в самых престижных медицинских школах мира и признана одной из самых эффективных ведущими изданиями, такими как *Журнал медицины Новой Англии*.



““

Откройте для себя методику Relearning, которая отвергает традиционное линейное обучение, чтобы показать вам циклический подход: способ, который доказал свою эффективность, особенно в предметах, требующих запоминания”

Метод кейс-стади предназначен для контекстуализации всего содержания

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

“

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



Вы получите доступ к системе обучения, основанной на повторении, с естественным и прогрессивным процессом обучения на протяжении всего учебного плана.



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

Инновационный и отличный от других метод обучения

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

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

Метод кейс-стади наиболее широко используется лучшими преподавателями в мире в качестве системы образования. Разработанный в 1912 году для того, чтобы студенты-юристы могли изучать право не только на основе теоретического содержания, метод кейс-стади заключается в том, что учащимся представляются реальные сложные ситуации для принятия обоснованных решений и ценностных суждений о том, как их разрешить. В 1924 году он был установлен в качестве стандартного метода обучения в Гарвардском университете.

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

Методология Relearning

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

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

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

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

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



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

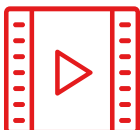
Методика Relearning позволит вам учиться с меньшими усилиями и большей эффективностью, все больше вовлекая вас в процесс обучения, развивая критическое мышление, отстаивая аргументы и противопоставляя мнения, что непосредственно приведет к успеху.

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

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



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



Учебный материал

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

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



Мастер-классы

Существуют научные данные о пользе экспертного наблюдения третьей стороны.

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



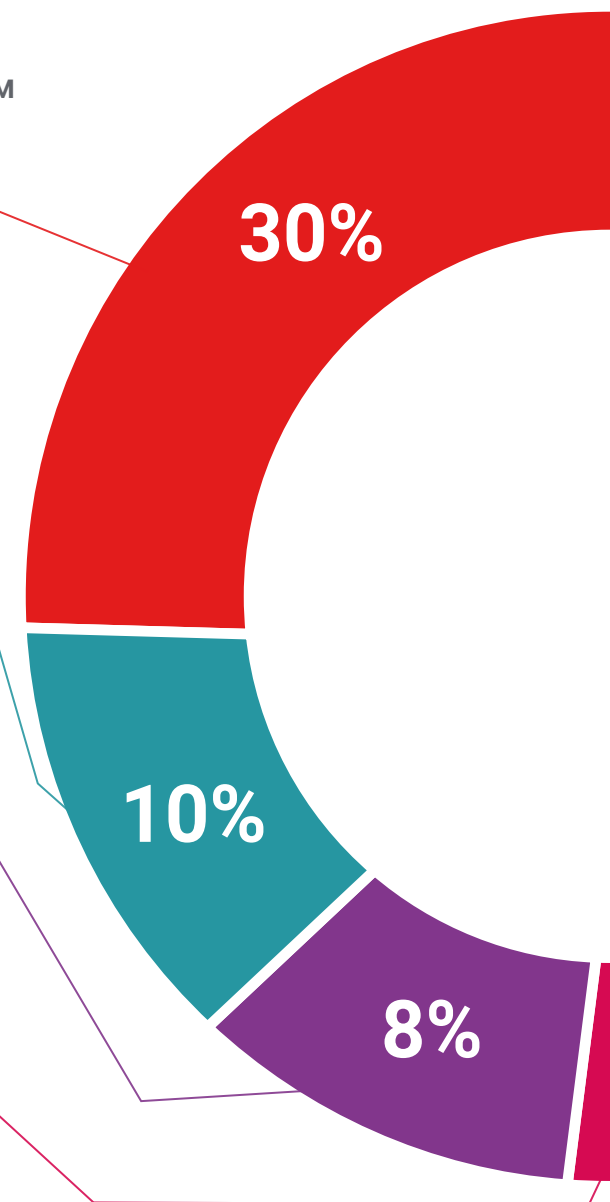
Практика навыков и компетенций

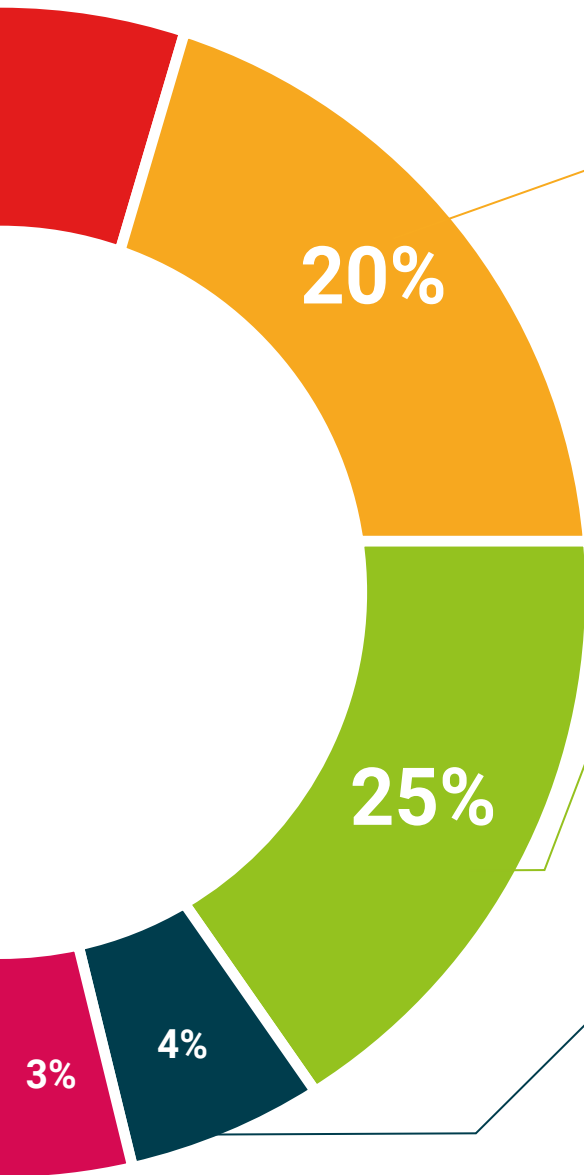
Студенты будут осуществлять деятельность по развитию конкретных компетенций и навыков в каждой предметной области. Практика и динамика приобретения и развития навыков и способностей, необходимых специалисту в рамках глобализации, в условиях которой мы живем.



Дополнительная литература

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





Метод кейс-стади

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



Интерактивные конспекты

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

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



Тестирование и повторное тестирование

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



07

Квалификация

Профессиональная магистерская специализация в области компьютерных наук, кибербезопасности и аналитики данных гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Профессиональной магистерской специализации, выдаваемого TESH Технологическим университетом.



““

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

Данная **Профессиональная магистерская специализация в области компьютерных наук, кибербезопасности и аналитики данных** содержит самую полную и современную программу на рынке.

После прохождения аттестации студент получит по почте* с подтверждением получения соответствующий диплом **Профессиональной магистерской специализации**, выданный **TECH Технологическим университетом**.

Диплом, выданный **TECH Технологическим университетом**, подтверждает квалификацию, полученную на Профессиональной магистерской специализации, и соответствует требованиям, обычно предъявляемым биржами труда, конкурсными экзаменами и комитетами по оценке карьеры.

Диплом: **Профессиональная магистерская специализация в области компьютерных наук, кибербезопасности и аналитики данных**

Количество учебных часов: **3000 часов**



*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.



Профессиональная магистерская специализация

Компьютерные науки,
кибербезопасность и
аналитика данных

- » Формат: онлайн
- » Продолжительность: 2 года
- » Учебное заведение: ТЕСН Технологический университет
- » Режим обучения: 16ч./неделя
- » Расписание: по своему усмотрению
- » Экзамены: онлайн

Профессиональная магистерская специализация

Компьютерные науки,
кибербезопасность и
аналитика данных