Профессиональная магистерская специализация

Управление информационной безопасностью

tech технологический университет

tech технологический университет

Профессиональная магистерская специализация

Управление информационной безопасностью

- Формат: **онлайн**
- Продолжительность: **2 года**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

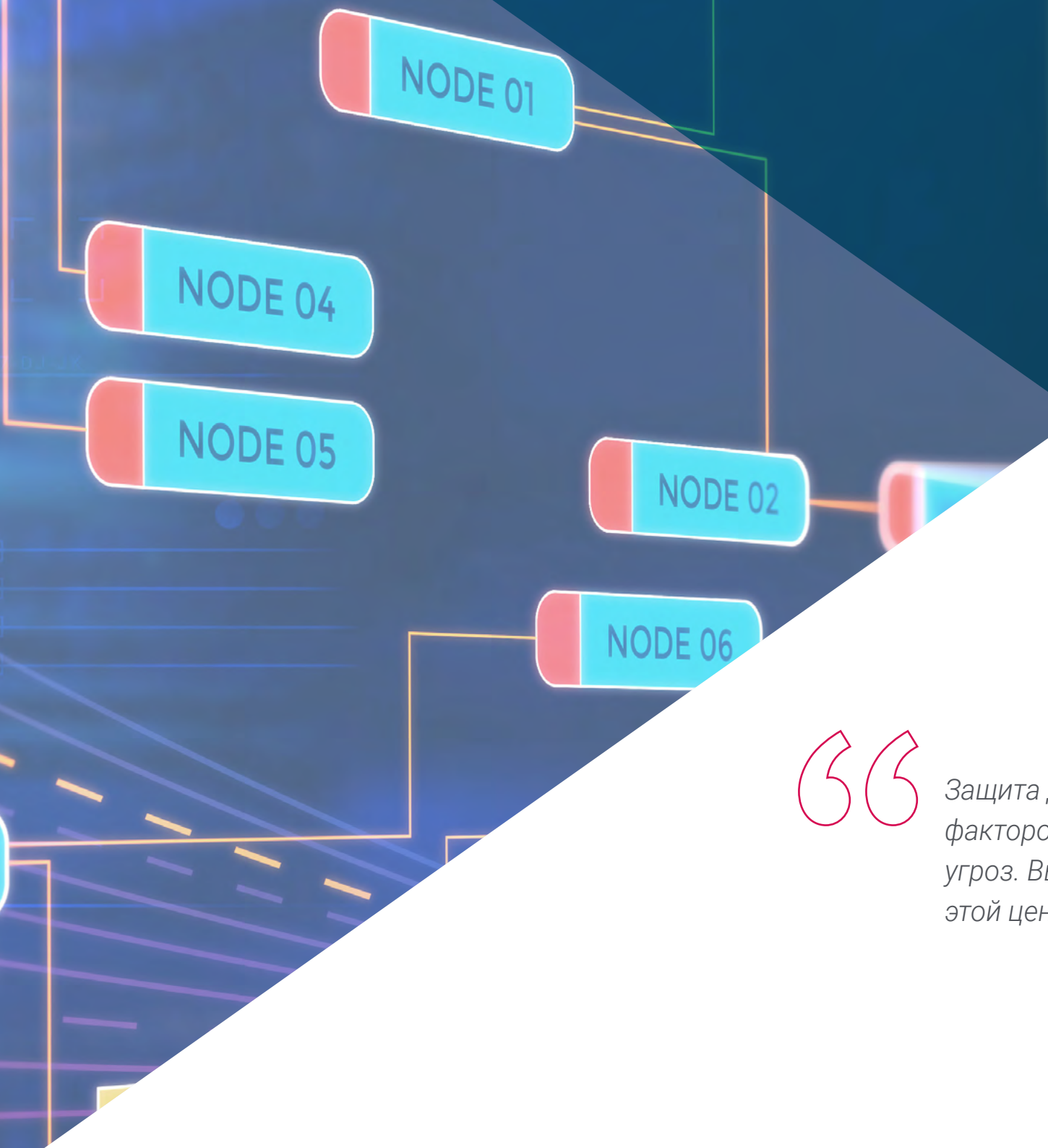
Веб-доступ: www.techtitute.com/ru/information-technology/advanced-master-degree/advanced-master-degree-secure-information-management

Оглавление

01

Презентация программы

В современную цифровую эпоху деятельность в различных сферах управляется комплексно через интернет. Развлечения, работа и общение с друзьями и семьей все больше зависят от онлайн-инструментов и ресурсов. Ежедневно передаются огромные объемы информации — от простых данных в разговорах в социальных сетях и мессенджерах до конфиденциальной личной и профессиональной информации, хранящейся на банковских или корпоративных платформах. В таких условиях необходимы специалисты, способные управлять и защищать информацию в разных контекстах, обеспечивая ее безопасность. Именно поэтому TECH разработал эту программу по программной инженерии, направленную на подготовку профессионалов, обладающих необходимыми навыками для эффективного управления и защиты данных, решения актуальных цифровых задач и создания более безопасных и надежных технологических сред.



Защита данных является ключевым фактором в условиях постоянных угроз. Вы можете стать хранителем этой ценной информации"

Каждую секунду в цифровой среде генерируются, передаются и хранятся тысячи данных. От онлайн-платежей и доступа к образовательным сервисам до координации бизнес-операций и защиты цифровых идентичностей — технологии стали неотъемлемой частью нашей жизни и работы, постоянно изменяя способы взаимодействия с информацией. Эти процессы генерируют и передают огромные объемы данных, включая как личную информацию, так и конфиденциальные корпоративные и институциональные файлы. Этот непрерывный поток данных подчеркивает необходимость их грамотного управления для обеспечения безопасности и конфиденциальности.

Управление и защита таких данных — сложная задача, требующая сочетания глубоких знаний в областях кибербезопасности и информационного менеджмента. Несмотря на различия, эти дисциплины должны быть интегрированы для эффективного решения современных цифровых задач. В этом контексте Профессиональная магистерская специализация в области управления информационной безопасностью представляет собой уникальную возможность для инженеров и IT-специалистов, стремящихся получить всестороннюю подготовку, позволяющую им освоить обе сферы и занять ведущие позиции в стремительно развивающейся отрасли.

Многие компании и организации сталкиваются с необходимостью защиты критически важных и конфиденциальных данных, но испытывают нехватку специалистов, способных эффективно управлять, хранить и контролировать цифровую информацию. Чтобы ответить на этот вызов, TECH разработал программу, объединяющую передовые учебные материалы и преподавательский состав с признанным профессиональным опытом. Такой подход гарантирует, что выпускники университета получат необходимые инструменты и знания, позволяющие им выделяться на рынке труда и занимать стратегические позиции в организациях, стремящихся усилить защиту своей информации.

Данная **Профессиональная магистерская специализация в области управления информационной безопасностью** содержит самую полную и актуальную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных специалистами в области управления информационной безопасностью
- Наглядное, схематичное и исключительно практическое содержание курса предоставляет научную и практическую информацию по тем дисциплинам, которые необходимы для осуществления профессиональной деятельности
- Практические упражнения для самопроверки, контроля и улучшения успеваемости
- Особое внимание уделяется инновационным методологиям в области управления информационной безопасностью
- 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

Приобретите навыки, необходимые для обеспечения безопасности и эффективного управления данными в конкурентной цифровой среде"

Закрепите свои теоретические знания с помощью многочисленных практических ресурсов, включенных в эту Профессиональную магистерскую специализацию по управлению информационной безопасностью”

Откройте для себя самую инновационную образовательную методику, разработанную TECH, чтобы гарантировать полное погружение и обучение в контексте.

Получите доступ к 100% онлайн-программе, которая позволит вам учиться в своем собственном темпе, в любое время и из любой точки мира.

В преподавательский состав входят профессионалы в области финансов, которые привносят в программу свой опыт своей работы, а также признанные специалисты из ведущих компаний и авторитетных университетов.

Мультимедийное содержание программы, разработанное с использованием новейших образовательных технологий, позволит специалисту пройти обучение с учетом ситуации и контекста, то есть в интерактивной среде, которая обеспечит погружение в учебный процесс, запрограммированный на обучение в реальных ситуациях.

В центре внимания этой программы — проблемно-ориентированное обучение, с помощью которого студент должен попытаться решить различные ситуации профессиональной практики, возникающие в течение учебного курса. Для этого специалисту будет помогать инновационная интерактивная видеосистема, созданная признанными и опытными специалистами.

02

Почему стоит учиться в TECH?

TECH – крупнейший в мире цифровой университет. Имея впечатляющий каталог из более чем 14 000 академических программ, доступных на 11 языках, он позиционируется как лидер по трудоустройству с показателем 99%. Кроме того, университет располагает огромным преподавательским составом, включающим более 6 000 преподавателей с высочайшим международным авторитетом.

Пройдите обучение в крупнейшем в мире цифровом университете и обеспечьте себе профессиональный успех. Будущее начинается в TECH”

Лучший онлайн-университет в мире по версии FORBES

Авторитетный журнал Forbes, специализирующийся на бизнесе и финансах, отметил TECH как "лучший онлайн-университет в мире" Об этом недавно сообщили в статье цифровой версии издания, где рассматривается успешный кейс этого учебного заведения, "благодаря его академическому предложению, отбору преподавательского состава и инновационному методу обучения, ориентированному на подготовку профессионалов будущего"

Лучший международный преподавательский состав

Преподавательский состав TECH включает более 6 000 специалистов с мировым признанием. Среди профессоров, исследователей и топ-менеджеров транснациональных корпораций — Исайя Ковингтон, тренер "Бостон Селтикс", Магда Романска, главный исследователь Harvard MetaLAB, Игнасио Вистумба, председатель отделения трансляционной молекулярной патологии в MD Anderson Cancer Center, Д.У. Пайн, креативный директор журнала TIME и другие.

Крупнейший цифровой университет в мире

TECH – крупнейший в мире цифровой университет. Мы — крупнейшее образовательное учреждение с самым обширным цифровым каталогом учебных программ, полностью онлайн, охватывающим большинство областей знаний. Мы предлагаем самое большое количество программ с выдачей дипломов собственного образца, а также официальных программ бакалавриата и программ последипломной подготовки в мире. В общей сложности более 14 000 университетских программ на десяти языках, что делает нас крупнейшим образовательным учреждением в мире.

Forbes
Mejor universidad online del mundo

Plan
de estudios
más completo

Profesorado
TOP
Internacional

La metodología
más eficaz

nº1
Mundial
Mayor universidad online del mundo

Самые полные учебные программы в университетской среде

TECH предлагает наиболее полные учебные программы, охватывающие как фундаментальные концепции, так и ключевые научные достижения в каждой конкретной области. Кроме того, эти программы постоянно обновляются, чтобы обеспечить студентам передовое академическое образование и наиболее востребованные профессиональные навыки. Таким образом, программы TECH дают студентам значительное преимущество для успешного карьерного роста.

Уникальный метод обучения

TECH — первый университет, использующий метод *Relearning* во всех своих учебных программах. Это лучшая методология онлайн-обучения, сертифицированная международными агентствами образовательного качества. Кроме того, эта инновационная академическая модель дополняется "Методом кейсов", формируя уникальную стратегию онлайн-обучения. В программу также включены передовые учебные ресурсы, среди которых подробные видеоматериалы, инфографики и интерактивные конспекты.

Официальный онлайн-университет NBA

TECH — официальный онлайн-университет NBA. Благодаря нашему партнерству с крупнейшей баскетбольной лигой мы предлагаем студентам эксклюзивные образовательные программы, а также широкий спектр учебных материалов, посвященных бизнесу лиги и другим аспектам спортивной индустрии. Каждая программа имеет уникальный учебный план и включает выдающихся приглашенных лекторов — профессионалов с выдающейся спортивной карьерой, которые поделятся своим опытом по самым актуальным темам.

Лидеры по трудоустройству

TECH удалось стать университетом-лидером по трудоустройству. 99% студентов получают работу по специальности в течение одного года после окончания любой из программ университета. Столько же студентов сразу же добиваются карьерного роста. Все это благодаря методологии обучения, эффективность которой основана на приобретении практических навыков, необходимых для профессионального развития.

Google Partner Premier

Американский технологический гигант присвоил TECH знак Google Partner Premier. Эта награда, доступная лишь 3% компаний мира, подчеркивает эффективный, гибкий и адаптированный подход, который этот университет предоставляет своим студентам. Признание не только подтверждает высокий уровень строгости, производительности и инвестиций в цифровую инфраструктуру TECH, но и ставит этот университет среди ведущих технологических компаний мира.

Университет, получивший самые высокие оценки от своих студентов

Ведущие сайты с отзывами признали TECH самым высоко оцененным университетом в мире по мнению его студентов. Данные платформы с отзывами, известные своей надежностью и престижем благодаря строгой проверке и валидации подлинности каждого мнения, присвоили TECH исключительно высокие оценки. Оценки, которые закрепляют за TECH статус абсолютного эталона среди университетов на международном уровне.

03

Учебный план

Учебные материалы, составляющие Профессиональную магистерскую специализацию в области управления информационной безопасностью, разработаны командой экспертов в области кибербезопасности и управления данными. Благодаря этому учебный план углубленно рассматривает основные цифровые угрозы и передовые методологии защиты и администрирования информации. Это позволит выпускникам университета выявлять конкретные риски и разрабатывать эффективные решения для обеспечения безопасности данных в различных профессиональных средах. Кроме того, программа охватывает самые инновационные инструменты отрасли, способствуя внедрению стратегий, направленных на защиту цифровых активов организаций.

Вы будете способствовать защите конфиденциальных данных и созданию безопасных систем, гарантирующих непрерывность работы компаний и учреждений"

Модуль 1. Аналитика данных в организации бизнеса

1.1. Бизнес-анализ
- 1.1.1. Бизнес-анализ
- 1.1.2. Структура данных
- 1.1.3. Этапы и элементы

1.2. Аналитика данных в компании
- 1.2.1. Показатели эффективности и KPI по отделам
- 1.2.2. Оперативная, тактическая и стратегическая отчетность
- 1.2.3. Аналитика данных, применяемая в каждом отделе
  - 1.2.3.1. Маркетинг и коммуникации
  - 1.2.3.2. Коммерция
  - 1.2.3.3. Обслуживание клиентов
  - 1.2.3.4. Закупки
  - 1.2.3.5. Администрация
  - 1.2.3.6. HR
  - 1.2.3.7. Производство
  - 1.2.3.8. Налог на транзакции

1.3. Маркетинг и коммуникации
- 1.3.1. Измеряемые Kpi, применение и преимущества
- 1.3.2. Маркетинговые системы и *хранилище данных*
- 1.3.3. Внедрение структуры анализа данных в маркетинге
- 1.3.4. План маркетинга и коммуникации
- 1.3.5. Стратегии, прогнозирование и управление кампаниями

1.4. Коммерция и продажи
- 1.4.1. Вклад аналитики данных в коммерческую сферу
- 1.4.2. Потребности отдела продаж
- 1.4.3. Изучение рынка

1.5. Обслуживание клиентов
- 1.5.1. Лояльность
- 1.5.2. Личные качества и эмоциональный интеллект
- 1.5.3. Удовлетворенность клиентов

1.6. Закупки
- 1.6.1. Аналитика данных для маркетинговых исследований
- 1.6.2. Аналитика данных для конкурентных исследований
- 1.6.3. Другое применение

1.7. Администрация
- 1.7.1. Потребности в административном отделе
- 1.7.2. *Хранилище данных* и анализ финансовых рисков
- 1.7.3. *Хранилище данных* и анализ кредитного риска

1.8. Человеческие ресурсы
- 1.8.1. HR и преимущества аналитики данных
- 1.8.2. Инструменты анализа данных в отделе кадров.
- 1.8.3. Применение аналитики данных в HR

1.9. Производство
- 1.9.1. Анализ данных в производственном отделе
- 1.9.2. Области применения
- 1.9.3. Преимущества

1.10. Налог на транзакции
- 1.10.1. Отдел ИТ
- 1.10.2. Аналитика данных и цифровая трансформация
- 1.10.3. Инновации и производительность

Модуль 2. Управление данными, обработка данных и составление отчетов по науке о данных

2.1. Статистика. Переменные, индексы и коэффициенты
- 2.1.1. Статистика
- 2.1.2. Статистические измерения
- 2.1.3. Переменные, индексы и коэффициенты

2.2. Типология данных
- 2.2.1. Качественные
- 2.2.2. Количественные
- 2.2.3. Характеристика и категории

2.3. Знание данных, полученных в результате измерений
- 2.3.1. Меры централизации
- 2.3.2. Меры дисперсии
- 2.3.3. Корреляция

2.4. Знание данных, полученных в результате графиков
- 2.4.1. Визуализация в соответствии с типом данных
- 2.4.2. Интерпретация графической информации
- 2.4.3. Настройка графики с помощью R

2.5. Вероятность
- 2.5.1. Вероятность
- 2.5.2. Функция вероятности
- 2.5.3. Распространения

2.6. Сбор данных
- 2.6.1. Методология сбора
- 2.6.2. Инструменты сбора
- 2.6.3. Каналы сбора

2.7. Очистка данных
- 2.7.1. Этапы очистки данных
- 2.7.2. Качество данных
- 2.7.3. Работа с данными (с помощью R)

2.8. Анализ данных, интерпретация и оценка результатов
- 2.8.1. Статистические меры
- 2.8.2. Индексы отношений
- 2.8.3. Добыча данных

2.9. Хранилище данных (*datawarehouse*)
- 2.9.1. Элементы
- 2.9.2. Дизайн

2.10. Доступность данных
- 2.10.1. Доступ
- 2.10.2. Полезность
- 2.10.3. Безопасность

Модуль 3. IoT-устройства и платформы как основа для науки о данных

3.1. *Интернет вещей*
- 3.1.1. Интернет будущего, *Интернет вещей*
- 3.1.2. Консорциум промышленного интернета

3.2. Эталонная архитектура
- 3.2.1. Эталонная архитектура
- 3.2.2. Слои
- 3.2.3. Компоненты

3.3. Датчики и устройства IoT
- 3.3.1. Основные компоненты
- 3.3.2. Датчики и исполнительные механизмы

3.4. Коммуникации и протоколы
- 3.4.1. Протоколы. Модель OSI
- 3.4.2. Коммуникационные технологии

3.5. *Облачные* платформы для IoT и IIoT
- 3.5.1. Платформы общего назначения
- 3.5.2. Промышленные платформы
- 3.5.3. Платформы с открытым исходным кодом

3.6. Управление данными в платформах IoT
- 3.6.1. Механизмы управления данными. Открытые данные
- 3.6.2. Обмен данными и визуализация

3.7. Безопасность в IoT
- 3.7.1. Требования к безопасности и области безопасности
- 3.7.2. Стратегии безопасности IIoT

3.8. IoT-приложения
- 3.8.1. Умные города
- 3.8.2. Здоровье и фитнес
- 3.8.3. Умный дом
- 3.8.4. Другое применение

3.9. Приложения IIoT
- 3.9.1. Создание
- 3.9.2. Транспортировка
- 3.9.3. Энергия
- 3.9.4. Сельское хозяйство и животноводство
- 3.9.5. Другие сектора

3.10. Индустрия 4.0
- 3.10.1. IoRT *(Интернет вещей робототехники)*
- 3.10.2. Аддитивное производство 3D
- 3.10.3. *Аналитика больших данных*

Модуль 4. Графическое представление для анализа данных

4.1. Исследовательский анализ
- 4.1.1. Представление для анализа информации
- 4.1.2. Ценность графического представления
- 4.1.3. Новые парадигмы графического представления

4.2. Оптимизация для науки о данных
- 4.2.1. Цветовая гамма и дизайн
- 4.2.2. Гештальт в графическом представлении
- 4.2.3. Ошибки, которых следует избегать, и советы

4.3. Источники основных данных
- 4.3.1. Для качественного представления
- 4.3.2. Для количественного представления
- 4.3.3. Для представления времени

4.4. Сложные источники данных
- 4.4.1. Файлы, список файлов и база данных
- 4.4.2. Открытые данные
- 4.4.3. Непрерывно генерируемые данные

4.5. Типы графиков
- 4.5.1. Базовые виды отображений
- 4.5.2. Блок-схема
- 4.5.3. Дисперсионный анализ
- 4.5.4. Круговые диаграммы
- 4.5.5. Пузырьковая диаграмма
- 4.5.6. Географическое представление

4.6. Виды визуализации
- 4.6.1. Сравнительная и реляционная
- 4.6.2. Распространение
- 4.6.3. Иерархическая

4.7. Разработка отчетов с графическим представлением
- 4.7.1. Применение графиков в маркетинговых отчетах
- 4.7.2. Применение графиков в приборных панелях и Kpi
- 4.7.3. Применение графиков в стратегических планах
- 4.7.4. Другие виды использования: наука, здоровье, бизнес

4.8. Графическое повествование
- 4.8.1. Графическое повествование
- 4.8.2. Развитие
- 4.8.3. Полезность

4.9. Инструменты, ориентированные на визуализацию
- 4.9.1. Расширенные инструменты
- 4.9.2. Онлайн программное обеспечение
- 4.9.3. *Open Source*

4.10. Новые технологии в визуализации данных
- 4.10.1. Системы для виртуализации реальности
- 4.10.2. Системы для расширения и улучшения реальности
- 4.10.3. Интеллектуальные системы

Модуль 5. Инструменты для науки о данных

5.1. Наука о данных
- 5.1.1. Наука о данных
- 5.1.2. Передовые инструменты для исследователя данных

5.2. Данные, информация и знания
- 5.2.1. Данные, информация и знания
- 5.2.2. Типы данных
- 5.2.3. Источники данных

5.3. От данных к информации
- 5.3.1. Анализ данных
- 5.3.2. Виды анализа
- 5.3.3. Извлечение информации из *набора данных*

5.4. Извлечение информации путем визуализации
- 5.4.1. Визуализация как инструмент анализа
- 5.4.2. Методы визуализации
- 5.4.3. Визуализация набора данных

5.5. Качество данных
- 5.5.1. Данные о качестве
- 5.5.2. Очистка данных
- 5.5.3. Основная предварительная обработка данных

5.6. *Набор данных*
- 5.6.1. Обогащение *набора данных*
- 5.6.2. Проклятие размерности
- 5.6.3. Модификация нашего набора данных

5.7. Выведение из равновесия
- 5.7.1. Дисбаланс классов
- 5.7.2. Методы устранения дисбаланса
- 5.7.3. Баланс *набора данных*

5.8. Модели без контроля
- 5.8.1. Модель без контроля
- 5.8.2. Методы
- 5.8.3. Классификация с помощью моделей без контроля

5.9. Модели под контролем
- 5.9.1. Модель под контролем
- 5.9.2. Методы
- 5.9.3. Классификация с помощью моделей под контролем

5.10. Инструменты и передовой опыт
- 5.10.1. Передовая практика для специалиста по исследованию данных
- 5.10.2. Лучшая модель
- 5.10.3. Полезные инструменты

Модуль 6. Добыча данных: выбор, предварительная обработка и преобразование

6.1. Статистический вывод
- 6.1.1. Описательная статистика vs. Статистическое заключение
- 6.1.2. Параметрические методы
- 6.1.3. Непараметрические методы

6.2. Исследовательский анализ
- 6.2.1. Описательный анализ
- 6.2.2. Визуализация
- 6.2.3. Подготовка данных

6.3. Подготовка данных
- 6.3.1. Интеграция и очистка данных
- 6.3.2. Нормализация данных
- 6.3.3. Преобразование данных

6.4. Отсутствующие значения
- 6.4.1. Обработка отсутствующих значений
- 6.4.2. Метод максимального правдоподобия
- 6.4.3. Обработка отсутствующих данных в машинном обучении

6.5. Шум в данных
- 6.5.1. Классы и признаки шума
- 6.5.2. Фильтрация шумов
- 6.5.3. Шумовой эффект

6.6. Проклятие размерности
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Редукция многомерных данных

6.7. От непрерывных к дискретным признакам
- 6.7.1. Непрерывные и дискретные данные
- 6.7.2. Процесс дискретизации

6.8. Данные
- 6.8.1. Выбор данных
- 6.8.2. Перспективы и критерии отбора
- 6.8.3. Методы отбора

6.9. Выбор экземпляров
- 6.9.1. Методы выбора экземпляра
- 6.9.2. Выбор прототипов
- 6.9.3. Расширенные методы выбора экземпляра

6.10. Предварительная обработка *больших данных*
- 6.10.1. *Большие данные*
- 6.10.2. Классическая модель vs массивная модель
- 6.10.3. *Умные данные*

Модуль 7. Предсказуемость и стохастический анализ

7.1. Временные ряды
- 7.1.1. Временные ряды
- 7.1.2. Полезность и применимость
- 7.1.3. Соответствующие тематические исследования

7.2. Временная серия
- 7.2.1. Сезонность (St)
- 7.2.2. Сезонная вариация
- 7.2.3. Остаточный анализ

7.3. Типологии
- 7.3.1. Стационарная модель
- 7.3.2. Нестационарная модель
- 7.3.3. Преобразования и корректировки

7.4. Схемы для временных рядов
- 7.4.1. Аддитивная модель
- 7.4.2. Мультипликативная модель
- 7.4.3. Процедуры определения типа модели

7.5. Основные методы *прогнозирования*
- 7.5.1. Средняя
- 7.5.2. *"Наивный" подход*
- 7.5.3. Сезонный *"наивный"* подход
- 7.5.4. Сравнение методов

7.6. Остаточный анализ
- 7.6.1. Автокорреляция
- 7.6.2. ACF остатков
- 7.6.3. Корреляционный анализ

7.7. Регрессия в контексте временных рядов
- 7.7.1. Дисперсионный анализ
- 7.7.2. Основы
- 7.7.3. Практическое применение

7.8. Прогнозирующие модели временных рядов
- 7.8.1. ARIMA
- 7.8.2. Экспоненциальное сглаживание

7.9. Анализ временных рядов в R
- 7.9.1. Подготовка данных
- 7.9.2. Идентификация шаблона
- 7.9.3. Анализ модели
- 7.9.4. Прогнозирование

7.10. Комбинированный графический анализ с помощью R
- 7.10.1. Типичные ситуации
- 7.10.2. Практическое применение для решения простых задач
- 7.10.3. Практическое применение для продвинутого решения проблем

Модуль 8. Проектирование и разработка интеллектуальных систем

8.1. Предварительная обработка данных
- 8.1.1. Предварительная обработка данных
- 8.1.2. Преобразование данных
- 8.1.3. Добыча данных

8.2. Машинное обучение
- 8.2.1. Контролируемое и неконтролируемое обучение
- 8.2.2. Обучение с подкреплением
- 8.2.3. Другие парадигмы обучения

8.3. Алгоритмы классификации
- 8.3.1. Индуктивное машинное обучение
- 8.3.2. SVM и KNN
- 8.3.3. Метрики и оценки для классификации

8.4. Алгоритмы регрессии
- 8.4.1. Линейная регрессия, логистическая регрессия и нелинейные модели
- 8.4.2. Временная серия
- 8.4.3. Метрики и оценки для регрессии

8.5. Алгоритмы кластеризации
- 8.5.1. Методы иерархической кластеризации
- 8.5.2. Методы условной кластеризации
- 8.5.3. Показатели и оценки *кластеризации*

8.6. Методы ассоциативных правил
- 8.6.1. Методы извлечения правил
- 8.6.2. Метрики и оценки для алгоритмов ассоциативных правил

8.7. Продвинутые методы классификации. Мультиклассовые алгоритмы
- 8.7.1. *Бэггинг*
- 8.7.2. Метод *случайного леса*
- 8.7.3. *Бустинг* деревьев решений

8.8. Графовая вероятностная модель
- 8.8.1. Вероятностная модель
- 8.8.2. Байесовские сети. Свойства, представление и параметризация
- 8.8.3. Другие графовые вероятностные модели

8.9. Нейронные сети
- 8.9.1. Машинное обучение с помощью искусственных нейронных сетей
- 8.9.2. Нейронная сеть с *прямой связью*

8.10. Глубокое обучение
- 8.10.1. Глубокие сети *прямой связи*
- 8.10.2. Конволюционные нейронные сети и модели последовательностей
- 8.10.3. Инструменты для реализации глубоких нейронных сетей

Модуль 9. Архитектуры и системы с интенсивным использованием данных

9.1. Нефункциональные требования. Основные принципы применения больших данных
- 9.1.1. Надежность
- 9.1.2. Адаптивность
- 9.1.3. Обслуживаемость

9.2. Моделирование данных
- 9.2.1. Реляционная модель
- 9.2.2. Документальная модель
- 9.2.3. Модель сетевых данных

9.3. Базы данных. Управление хранением и поиском данных
- 9.3.1. Хеш-индексы
- 9.3.2. Структурированное хранение журналов
- 9.3.3. B-деревья

9.4. Форматы кодирования данных
- 9.4.1. Форматы, специфичные для конкретного языка
- 9.4.2. Стандартизированные форматы
- 9.4.3. Форматы двоичного кодирования
- 9.4.4. Межпроцессный поток данных

9.5. Репликация
- 9.5.1. Цели репликации
- 9.5.2. Модели репликации
- 9.5.3. Проблемы с репликацией

9.6. Распределенные транзакции
- 9.6.1. Транзакция
- 9.6.2. Протоколы для распределенных транзакций
- 9.6.3. Сериализация транзакций

9.7. Секционирование
- 9.7.1. Формы разделения
- 9.7.2. Взаимодействие вторичного индекса и разделения
- 9.7.3. Перебалансировка разделов

9.8. Обработка данных в *offline*
- 9.8.1. Пакетная обработка
- 9.8.2. Распределенные файловые системы
- 9.8.3. *MapReduce*

9.9. Обработка данных в режиме реального времени
- 9.9.1. Типы *брокеров* сообщений
- 9.9.2. Представление баз данных в виде потоков данных
- 9.9.3. Обработка потоков данных

9.10. Практическое применение в бизнесе
- 9.10.1. Последовательность в чтении
- 9.10.2. Комплексный подход к данным
- 9.10.3. Масштабируемая распределенная система

Модуль 10. Практическое применение науки о данных в бизнес-секторах

10.1. Сфера здравоохранения
- 10.1.1. Последствия ИИ и аналитики данных в секторе здравоохранения
- 10.1.2. Возможности и проблемы

10.2. Риски и тенденции в здравоохранении
- 10.2.1. Использование в секторе здравоохранения
- 10.2.2. Потенциальные риски, связанные с использованием ИИ

10.3. Финансовые услуги
- 10.3.1. Влияние ИИ и аналитики данных для индустрии финансовых услуг
- 10.3.2. Использование в финансовых услугах
- 10.3.3. Потенциальные риски, связанные с использованием ИИ

10.4. Розничная торговля
- 10.4.1. Влияние ИИ и аналитики данных в розничной торговле
- 10.4.2. Розничное использование
- 10.4.3. Потенциальные риски, связанные с использованием ИИ

10.5. Индустрия 4.0
- 10.5.1. Влияние ИИ и аналитики данных на Индустрию 4.0.
- 10.5.2. Использование в Индустрии 4.0.

10.6. Риски и тенденции в Индустрии 4.0.
- 10.6.1. Потенциальные риски, связанные с использованием ИИ

10.7. Государственное управление
- 10.7.1. Влияние ИИ и аналитики данных на государственное управление
- 10.7.2. Использование в государственном управлении
- 10.7.3. Потенциальные риски, связанные с использованием ИИ

10.8. Образовательная сфера
- 10.8.1. Влияние ИИ и аналитики данных на образовательную сферу
- 10.8.2. Потенциальные риски, связанные с использованием ИИ

10.9. Лесное и сельское хозяйство
- 10.9.1. Влияние ИИ и аналитики данных на лесное и сельское хозяйство
- 10.9.2. Использование в лесном и сельском хозяйстве
- 10.9.3. Потенциальные риски, связанные с использованием ИИ

10.10. Человеческие ресурсы
- 10.10.1. Влияние ИИ и аналитики данных на управление персоналом
- 10.10.2. Практическое применение в деловом мире
- 10.10.3. Потенциальные риски, связанные с использованием ИИ

Модуль 11. Кибербезопасность и кибербезопасность

11.1. Кибербезопасность
- 11.1.1. Кибербезопасность
  - 11.1.1.1. Разведка
    - 11.1.1.1.1. Цикл разведки
  - 11.1.1.2. Кибербезопасность
  - 11.1.1.3. Кибербезопасность и кибербезопасность
- 11.1.2. Аналитик разведки
  - 11.1.2.1. Роль аналитика разведывательной службы
  - 11.1.2.2. Необъективность аналитика разведки в оценочной деятельности

11,2. Кибербезопасность
- 11.2.1. Уровни безопасности
- 11.2.2. Идентификация киберугроз
  - 11.2.2.1. Внешние угрозы
  - 11.2.2.2. Внутренние угрозы
- 11.2.3. Неблагоприятные действия
  - 11.2.3.1. Социальная инженерия
  - 11.2.3.2. Часто используемые методы

11.3. Инструменты и методы разведки
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Дистрибутивы и инструменты Linux
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Методология оценки
- 11.4.1. Анализ разведывательной информации
- 11.4.2. Методы организации полученной информации
- 11.4.3. Надежность и достоверность источников информации
- 11.4.4. Методологии анализа
- 11.4.5. Представление результатов разведки

11.5. Аудиты и документация
- 11.5.1. Аудит ИТ-безопасности
- 11.5.2. Документация и разрешения на проведение аудита
- 11.5.3. Виды аудита
- 11.5.4. Результаты
  - 11.5.4.1. Технический отчет
  - 11.5.4.2. Исполнительный отчет

11.6. Анонимность в интернете
- 11.6.1. Использование анонимизации
- 11.6.2. Методы анонимизации (Proxy, VPN)
- 11.6.3. Сети TOR, Freenet e IP2

11.7. Угрозы и виды безопасности
- 11.7.1. Виды угроз
- 11.7.2. Физическая безопасность
- 11.7.3. Безопасность в сетях
- 11.7.4. Логическая безопасность
- 11.7.5. Безопасность веб-приложений
- 11.7.6. Безопасность на мобильных устройствах

11.8. Регулирование и *комплаенс*
- 11.8.1. Общий регламент по защите данных
- 11.8.2. Семейство стандартов ISO 27000
- 11.8.3. Система кибербезопасности NIST
- 11.8.4. PIC
- 11.8.5. ISO 27032
- 11.8.6. Стандарты в сфере *облачной безопасности*
- 11.8.7. SOX
- 11.8.8. PCI

11.9. Анализ рисков и метрики
- 11.9.1. Масштабы рисков
- 11.9.2. Активы
- 11.9.3. Угрозы
- 11.9.4. Уязвимости
- 11.9.5. Оценка рисков
- 11.9.6. Обработка риска

11,10. Важные органы по вопросам кибербезопасности
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. OEA
- 11.10.4. UNASUR - PROSUR

Модуль 12. Безопасность хоста

12.1. Резервные копии
- 12.1.1. Стратегии резервного копирования
- 12.1.2. Инструменты для Windows
- 12.1.3. Инструменты для Linux
- 12.1.4. Инструменты для MacOS

12.2. Пользовательский антивирус
- 12.2.1. Виды антивирусов
- 12.2.2. Антивирус для Windows
- 12.2.3. Антивирус для Linux
- 12.2.4. Антивирус для MacOS
- 12.2.5. Антивирусы для смартфонов

12.3. Детекторы вторжения - HIDS
- 12.3.1. Методы обнаружения вторжений
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. Локальный *брандмауэр*
- 12.4.1. *Брандмауэры* для Windows
- 12.4.2. *Брандмауэры* для Linux
- 12.4.3. *Брандмауэры* для MacOS

12.5. Менеджеры паролей
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *StickyPassword*
- 12.5.5. *RoboForm*

12.6. Детекторы *фишинга*
- 12.6.1. Обнаружение *фишинга* вручную
- 12.6.2. *Антифишинговые* инструменты

12.7. *Шпионское программное обеспечение*
- 12.7.1. Механизмы предотвращения
- 12.7.2. *Антишпионские* инструменты

12.8. Трекеры
- 12.8.1. Меры по защите системы
- 12.8.2. Инструменты для борьбы с отслеживанием

12.9. EDR- *End Point Detection and Response*
- 12.9.1. Поведение системы EDR
- 12.9.2. Различия между EDR и антивирусом
- 12.9.3. Будущее систем EDR

12.10. Контроль над установкой программного обеспечения
- 12.10.1. Репозитории и магазины программного обеспечения
- 12.10.2. Списки разрешенного или запрещенного программного обеспечения
- 12.10.3. Критерии обновлений
- 12.10.4. Права на установку программного обеспечения

Модуль 13. Сетевая безопасность (периметр)

13.1. Системы обнаружения и предотвращения угроз
- 13.1.1. Общая нормативная база для инцидентов по безопасности
- 13.1.2. Современные системы защиты: *Глубокая защита* и SOC
- 13.1.3. Текущие сетевые архитектуры
- 13.1.4. Типы средств выявления и предотвращения инцидентов
  - 13.1.4.1. Сетевые системы
  - 13.1.4.2. Системы на базе хоста
  - 13.1.4.3. Централизованные системы
- 13.1.5. Связь и обнаружение экземпляров/*хостов*, контейнеров и *бессерверных систем*

13.2. *Брандмауэр*
- 13.2.1. Типы *брандмауэров*
- 13.2.2. Атаки и смягчение последствий
- 13.2.3. Лучший *брандмауэр* для Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables и iptables
  - 13.2.3.3. *Firewalld*
- 13.2.4. Системы обнаружения на основе системных журналов
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* и *DenyHosts*
  - 13.2.4.3. Fai2ban

13.3. Системы обнаружения и предотвращения вторжений (IDS/IPS)
- 13.3.1. Атаки на IDS/IPS
- 13.3.2. Системы IDS/IPS
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Брандмауэры* следующего поколения (NGFW)
- 13.4.1. Различия между NGFW и традиционными брандмауэрами
- 13.4.2. Основные возможности
- 13.4.3. Коммерческие решения
- 13.4.4. Брандмауэры для *облачных сервисов*
  - 13.4.4.1. *Облачная архитектура* VPC
  - 13.4.4.2. *Облачный сервис* ACLs
  - 13.4.4.3. *Security Group*

13.5. Прокси
- 13.5.1. Типы прокси
- 13.5.2. Использование прокси. Преимущества и недостатки

13.6. Антивирусные системы
- 13.6.1. Общий контекст *вредоносных программ* и индикатор компрометации (IOCs)
- 13.6.2. Проблемы с антивирусным движком

13.7. Системы защиты почтовых сервисов
- 13.7.1. Антиспам
  - 13.7.1.1. Черные и белые списки
  - 13.7.1.2. Байесовская фильтрация спама
- 13.7.2. *Почтовый шлюз* (MGW)

13.8. SIEM
- 13.8.1. Компоненты и архитектура
- 13.8.2. Правила корреляции и примеры использования
- 13.8.3. Актуальные проблемы систем SIEM

13.9. SOAR
- 13.9.1. SOAR и SIEM: враги или союзники
- 13.9.2. Будущее систем SOAR

13.10. Другие сетевые системы
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots и HoneyNets
- 13.10.4. CASB

Модуль 14. Безопасность смартфонов

14.1. Мир мобильных устройств
- 14.1.1. Виды мобильных платформ
- 14.1.2. iOS-устройства
- 14.1.3. Android-устройства

14.2. Управление мобильной безопасностью
- 14.2.1. Проект OWASP по мобильной безопасности
  - 14.2.1.1. Топ-10 уязвимостей
- 14.2.2. Коммуникации, сети и режимы подключения

14.3. Мобильное устройство в корпоративной среде
- 14.3.1. Риски
- 14.3.2. Политики безопасности
- 14.3.3. Мониторинг устройств
- 14.3.4. Управление мобильными устройствами (MDM)

14.4. Конфиденциальность пользователей и безопасность данных
- 14.4.1. Состояние информации
- 14.4.2. Защита данных и конфиденциальность
  - 14.4.2.1. Разрешения
  - 14.4.2.2. Шифрование
- 14.4.3. Безопасное хранение данных
  - 14.4.3.1. Безопасное хранение данных на iOS
  - 14.4.3.2. Безопасное хранение данных на Android
- 14.4.4. Передовые методы разработки приложений

14.5. Уязвимости и векторы атак
- 14.5.1. Уязвимости
- 14.5.2. Векторы атак
  - 14.5.2.1. *Вредоносное программное обеспечение*
  - 14.5.2.2. Эксфильтрация данных
  - 14.5.2.3. Манипуляции с данными

14.6. Основные угрозы
- 14.6.1. Непринужденный пользователь
- 14.6.2. *Вредоносное программное обеспечение*
  - 14.6.2.1. Типы *вредоносных программ*
- 14.6.3. Социальная инженерия
- 14.6.4. Утечка данных
- 14.6.5. Кража информации
- 14.6.6. Незащищенные сети *Wi-Fi*
- 14.6.7. Устаревшее программное обеспечение
- 14.6.8. Вредоносные приложения
- 14.6.9. Ненадежные пароли
- 14.6.10. Слабые или отсутствующие настройки безопасности
- 14.6.11. Физический доступ к информации
- 14.6.12. Потеря или кража устройства
- 14.6.13. Подмена личности (интеграция)
- 14.6.14. Слабая или неработающая криптография
- 14.6.15. Отказ в обслуживании (DoS)

14.7. Основные атаки
- 14.7.1. *Фишинговые* атаки
- 14.7.2. Атаки, связанные со способами коммуникации
- 14.7.3. *Смишинговые* атаки
- 14.7.4. Атаки *криптоджекинга*
- 14.7.5. *Человек посередине*

14.8. *Хакинг*
- 14.8.1. *Rooting и Jailbreaking*
- 14.8.2. Анатомия мобильной атаки
  - 14.8.2.1. Распространение угрозы
  - 14.8.2.2. Установка *вредоносных программ* на устройство
  - 14.8.2.3. Настойчивость
  - 14.8.2.4. Выполнение *полезной нагрузки* и извлечение информации
- 14.8.3. *Хакинг* устройств iOS: механизмы и средства
- 14.8.4. *Хакинг* устройств Android: механизмы и инструменты

14.9. Тестирование на проникновение
- 14.9.1. *iOS PenTesting*
- 14.9.2. *Android PenTesting*
- 14.9.3. Инструменты

14.10. Безопасность и защита
- 14.10.1. Настройки безопасности
  - 14.10.1.1. На устройствах IOS
  - 14.10.1.2. На устройствах Android
- 14.10.2. Меры по обеспечению безопасности
- 14.10.3. Защитные средства

Модуль 15. Безопасность в IoT

15.1. Приборы
- 15.1.1. Виды устройств
- 15.1.2. Стандартизированные архитектуры
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Протоколы внедрения
- 15.1.4. Технологии подключения

15.2. Устройства IoT. Области применения
- 15.2.1. *Умный дом*
- 15.2.2. *Умный город*
- 15.2.3. Транспорт
- 15.2.4. *Носимые приборы*
- 15.2.5. Сектор здравоохранения
- 15.2.6. IioT

15.3. Протоколы коммуникации
- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. *SmartHome*
- 15.4.1. Бытовая автоматизация
- 15.4.2. Сети
- 15.4.3. Бытовая техника
- 15.4.4. Наблюдение и охрана

15.5. *Умный город*
- 15.5.1. Освещение
- 15.5.2. Метеорология
- 15.5.3. Безопасность

15.6. Транспорт
- 15.6.1. Локализация
- 15.6.2. Осуществление платежей и получение услуг
- 15.6.3. Связь

15.7. *Носимые приборы*
- 15.7.1. Умная одежда
- 15.7.2. Умные ювелирные изделия
- 15.7.3. Умные часы

15.8. Сектор здравоохранения
- 15.8.1. Контроль физической нагрузки/частоты сердечных сокращений
- 15.8.2. Наблюдение за пациентами и пожилыми людьми
- 15.8.3. Импланты
- 15.8.4. Хирургические роботы

15.9. Связь
- 15.9.1. *Wi-Fi/сетевые шлюзы*
- 15.9.2. *Bluetooth*
- 15.9.3. Встроенные возможности подключения

15.10. Секьюритизация
- 15.10.1. Выделенные сети
- 15.10.2. Менеджер паролей
- 15.10.3. Использование зашифрованных протоколов
- 15.10.4. Советы по применению

Модуль 16. Этичный *хакинг*

16.1. Рабочая среда
- 16.1.1. Дистрибутивы Linux
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Системы виртуализации
- 16.1.3. *Sandbox*
- 16.1.4. Развертывание лабораторий

16,2. Методики
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. Разведка по открытым источникам (OSINT)
- 16.3.2. Поиск утечек данных и уязвимостей
- 16.3.3. Использование пассивных средств

16.4. Сканирование сети
- 16.4.1. Средства сканирования
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Другие средства сканирования
- 16.4.2. Методы сканирования
- 16.4.3. Методы обхода *брандмауэров* и IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Сетевые диаграммы

16.5. Перечисление
- 16.5.1. Перечисление SMTP
- 16.5.2. Перечисление DNS
- 16.5.3. Перечисление NetBIOS и Samba
- 16.5.4. Перечисление LDAP
- 16.5.5. Перечисление SNMP
- 16.5.6. Другие техники перечисления

16.6. Анализ уязвимостей
- 16.6.1. Решения для сканирования уязвимостей
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Системы оценки уязвимостей
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Атаки на *беспроводные сети*
- 16.7.1. Методология *взлома* беспроводных сетей
  - 16.7.1.1. Wi-Fi Discovery
  - 16.7.1.2. Анализ трафика
  - 16.7.1.3. Атаки *aircrack*
    - 16.7.1.3.1. Атаки WEP
    - 16.7.1.3.2. Атаки WPA/WPA2
  - 16.7.1.4. Атаки *Evil Twin*
  - 16.7.1.5. Атаки на WPS
  - 16.7.1.6. *Jamming*
- 16.7.2. Инструменты для обеспечения безопасности беспроводных сетей

16.8. Взлом веб-серверов
- 16.8.1. *Межсайтовый скриптинг*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQLinjection*

16.9. Эксплуатация уязвимостей
- 16.9.1. Использование известных *эксплойтов*
- 16.9.2. Использование *metasploit*
- 16.9.3. Использование *вредоносных программ*
  - 16.9.3.1. Определение и сфера применения
  - 16.9.3.2. Генерация *вредоносных программ*
  - 16.9.3.3. Обход антивирусных решений

16.10. Настойчивость
- 16.10.1. Установка руткитов
- 16.10.2. Использование ncat
- 16.10.3. Использование запланированных задач для создания бэкдоров
- 16.10.4. Создание пользователей
- 16.10.5. Система обнаружения вторжений на хосте

Модуль 17. Реверс-инжиниринг

17.1. Компиляторы
- 17.1.1. Виды кодов
- 17.1.2. Этапы работы компилятора
- 17.1.3. Таблица символов
- 17.1.4. Менеджер ошибок
- 17.1.5. Компилятор GCC

17.2. Виды анализа в компиляторах
- 17.2.1. Лексический анализ
  - 17.2.1.1. Терминология
  - 17.2.1.2. Лексические компоненты
  - 17.2.1.3. Лексический анализатор LEX
- 17.2.2. Синтаксический анализ
  - 17.2.2.1. Контекстно-свободная грамматика
  - 17.2.2.2. Виды синтаксического анализа
    - 17.2.2.2.1. Нисходящий анализ
    - 17.2.2.2.2. Восходящий анализ
  - 17.2.2.3. Синтаксические деревья и производные
  - 17.2.2.4. Виды синтаксических анализаторов
    - 17.2.2.4.1. LR-анализаторы (*Left To Right*)
    - 17.2.2.4.2. Анализаторы LALR
- 17.2.3. Семантический анализ
  - 17.2.3.1. Атрибутивная грамматика
  - 17.2.3.2. S-атрибутная грамматика
  - 17.2.3.3. L-атрибутная грамматика

17.3. Структуры данных ассемблера
- 17.3.1. Переменные
- 17.3.2. Массивы
- 17.3.3. Указатели
- 17.3.4. Конструкции
- 17.3.5. Предметы

17.4. Структуры кода ассемблера
- 17.4.1. Структуры отбора
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Структуры итераций
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Использование break
- 17.4.3. Функции

17.5. Архитектура аппаратного обеспечения x86
- 17.5.1. Архитектура процессоров в x86
- 17.5.2. Структуры данных в x86
- 17.5.3. Структуры кода в x86

17.6. Архитектура аппаратного обеспечения ARM
- 17.6.1. Архитектура процессоров ARM
- 17.6.2. Структуры данных в ARM
- 17.6.3. Структуры кода в ARM

17,7. Анализ статического кода
- 17.7.1. Дизассемблеры
- 17.7.2. IDA
- 17.7.3. Реконструкторы кода

17.8. Анализ динамического кода
- 17.8.1. Поведенческий анализ
  - 17.8.1.1. Коммуникация
  - 17.8.1.2. Мониторинг
- 17.8.2. Отладчики кода в Linux
- 17.8.3. Отладчики кода в Windows

17.9. *Sandbox*
- 17.9.1. Архитектура *песочницы*
- 17.9.2. Обход *песочницы*
- 17.9.3. Методы обнаружения
- 17.9.4. Методы избегания
- 17.9.5. Контрмеры
- 17.9.6. *Sandbox* в Linux
- 17.9.7. *Sandbox* в Windows
- 17.9.8. *Sandboxa* в MacOS
- 17.9.9. *Sandbox* в Android

17.10. Анализ вредоносного ПО
- 17.10.1. Методы анализа *вредоносного ПО*
- 17.10.2. Методы обфускации *вредоносного ПО*
  - 17.10.2.1. Обфускация исполняемых файлов
  - 17.10.2.2. Ограничение среды исполнения
- 17.10.3. Инструменты анализа *вредоносного ПО*

Модуль 18. Безопасная разработка

18.1. Безопасная разработка
- 18.1.1. Качество, функциональность и безопасность
- 18.1.2. Конфиденциальность, целостность и доступность
- 18.1.3. Жизненный цикл разработки программного обеспечения

18.2. Этап требований
- 18.2.1. Контроль аутентификации
- 18.2.2. Контроль ролей и привилегий
- 18.2.3. Риск-ориентированные требования
- 18.2.4. Утверждение привилегий

18.3. Этапы анализа и проектирования
- 18.3.1. Доступ к компонентам и системное администрирование
- 18.3.2. Контрольные журналы
- 18.3.3. Управление сессиями
- 18.3.4. Исторические данные
- 18.3.5. Правильная обработка ошибок
- 18.3.6. Разделение функций

18.4. Этап внедрения и кодирования
- 18.4.1. Обеспечение безопасности среды разработки
- 18.4.2. Подготовка технической документации
- 18.4.3. Безопасное кодирование
- 18.4.4. Безопасность коммуникаций

18.5. Надлежащая практика безопасного кодирования
- 18.5.1. Валидация входных данных
- 18.5.2. Кодирование выходных данных
- 18.5.3. Стиль программирования
- 18.5.4. Ведение журнала изменений
- 18.5.5. Криптографические практики
- 18.5.6. Управление ошибками и логами
- 18.5.7. Управление архивами
- 18.5.8. Управление памятью
- 18.5.9. Стандартизация и повторное использование функций безопасности

18.6. Подготовка сервера и *укрепление*
- 18.6.1. Управление пользователями, группами и ролями на сервере
- 18.6.2. Установка ПО
- 18.6.3. *Укрепление* сервера
- 18.6.4. Надежная конфигурация среды приложения

18.7. Подготовка БД и *укрепление сервера*
- 18.7.1. Оптимизация движка БД
- 18.7.2. Создание собственного пользователя для приложения
- 18.7.3. Назначение необходимых привилегий пользователю
- 18.7.4. *Укрепление* БД

18.8. Этап тестирования
- 18.8.1. Контроль качества в управлении безопасностью
- 18.8.2. Поэтапная проверка кода
- 18.8.3. Проверка управления конфигурации
- 18.8.4. Тестирование методом черного ящика

18.9. Подготовка к переходу на производство
- 18.9.1. Осуществлять контроль за изменениями
- 18.9.2. Осуществлять процедуры переналадки производства
- 18.9.3. Осуществлять процедуру *отката*
- 18.9.4. Предпроизводственное тестирование

18.10. Фаза технического обслуживания
- 18.10.1. Обеспечение на основе рисков
- 18.10.2. Тестирование обслуживания системы безопасности белого ящика
- 18.10.3. Тестирование обслуживания системы безопасности черного ящика

Модуль 19. Судебная экспертиза

19.1. Сбор и воспроизведение данных
- 19.1.1. Сбор волатильных данных
  - 19.1.1.1. Системная информация
  - 19.1.1.2. Сетевая информация
  - 19.1.1.3. Порядок волатильности
- 19.1.2. Сбор статистических данных
  - 19.1.2.1. Создание дублирующего изображения
  - 19.1.2.2. Подготовка документа о цепочке поставок
- 19.1.3. Методы валидации полученных данных
  - 19.1.3.1. Методы для Linux
  - 19.1.3.2. Методы для Windows

19.2. Оценка и преодоление антикриминалистических методов
- 19.2.1. Цели анктикриминалистических методов
- 19.2.2. Удаление данных
  - 19.2.2.1. Удаление данных и файлов
  - 19.2.2.2. Восстановление файлов
  - 19.2.2.3. Восстановление удаленных разделов
- 19.2.3. Защита с помощью пароля
- 19.2.4. Стеганография
- 19.2.5. Безопасное удаление данных с устройств
- 19.2.6. Шифрование

19.3. Криминалистика операционных систем
- 19.3.1. Судебная экспертиза Windows
- 19.3.2. Судебная экспертиза Linux
- 19.3.3. Судебная экспертиза Mac

19.4. Сетевая криминалистика
- 19.4.1. Анализ журнала
- 19.4.2. Корреляция данных
- 19.4.3. Расследование сети
- 19.4.4. Шаги, необходимые для проведения криминалистической экспертизы сети

19.5. Криминалистическая экспертиза Web
- 19.5.1. Расследование веб-атак
- 19.5.2. Обнаружение атак
- 19.5.3. Локализация IP-адресов

19.6. Судебная экспертиза баз данных
- 19.6.1. Судебная экспертиза MSSQL
- 19.6.2. Судебная экспертиза MySQL
- 19.6.3. Судебная экспертиза PostgreSQL
- 19.6.4. Судебная экспертиза MongoDB

19,7. Криминалистика в *облаке*
- 19.7.1. Виды преступлений в *облаке*
  - 19.7.1.1. *Облако* как предмет
  - 19.7.1.2. *Облако* как объект
  - 19.7.1.3. *Облако* как инструмент
- 19.7.2. Проблемы криминалистики в *облаке*
- 19.7.3. Исследование услуг по хранению данных в *облаке*
- 19.7.4. Инструменты криминалистического анализа для *облака*

19.8. Расследования преступлений, связанных с электронной почтой
- 19.8.1. Почтовые системы
  - 19.8.1.1. Почтовые клиенты
  - 19.8.1.2. Почтовые серверы
  - 19.8.1.3. Сервер SMTP
  - 19.8.1.4. Сервер POP3
  - 19.8.1.5. Сервер IMAP4
- 19.8.2. Преступления, связанные с электронной почтой
- 19.8.3. Сообщение на почте
  - 19.8.3.1. Стандартные заголовки
  - 19.8.3.2. Расширенные заголовки
- 19.8.4. Шаги по расследованию этих преступлений
- 19.8.5. Средства криминалистической экспертизы электронной почты

19.9. Судебная экспертиза мобильных устройств
- 19.9.1. Сотовые сети
  - 19.9.1.1. Виды сетей
  - 19.9.1.2. Содержимое хранилища CDR
- 19.9.2. *Модуль идентификации абонента* (SIM)
- 19.9.3. Логическое получение
- 19.9.4. Физическое получение
- 19.9.5. Получение файловой системы

19.10. Составление и предоставление отчетов о судебной экспертизе
- 19.10.1. Важные аспекты заключения судебной экспертизы
- 19.10.2. Классификация и виды отчетов
- 19.10.3. Руководство по написанию отчета
- 19.10.4. Презентация отчета
  - 19.10.4.1. Предварительная подготовка к даче показаний
  - 19.10.4.2. Изложение
  - 19.10.4.3. Общение с прессой

Модуль 20. Актуальные и будущие задачи в области кибербезопасности

20.1. Технология *блокчейн*
- 20.1.1. Области применения
- 20.1.2. Гарантия конфиденциальности
- 20.1.3. Гарантия отсутствия отказа от претензий

20.2. Цифровая валюта
- 20.2.1. Биткойны
- 20.2.2. Криптомонеты
- 20.2.3. Майнинг криптовалюты
- 20.2.4. Пирамидальные схемы
- 20.2.5. Другие потенциальные преступления и проблемы

20.3. *Дипфейк*
- 20.3.1. Влияние СМИ
- 20.3.2. Опасность для общества
- 20.3.3. Механизмы обнаружения

20.4. Будущее искусственного интеллекта
- 20.4.1. Искусственный интеллект и когнитивные вычисления
- 20.4.2. Применение в упрощении обслуживания клиентов

20.5. Цифровая конфиденциальность
- 20.5.1. Ценность данных в сети
- 20.5.2. Использование данных в сети
- 20.5.3. Конфиденциальность и управление цифровой идентичностью

20.6. Киберконфликты, киберпреступники и кибератаки
- 20.6.1. Влияние кибербезопасности на международные конфликты
- 20.6.2. Последствия кибератак для населения в целом
- 20.6.3. Виды киберпреступников. Защитные мероприятия

20.7. Удаленная работа
- 20.7.1. Революция дистанционной работы во время и после Covid19
- 20.7.2. Узкие места при доступе
- 20.7.3. Изменение площади атаки
- 20.7.4. Потребности работников

20.8. Новые *беспроводные технологии*
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Миллиметровые волны
- 20.8.4. Тенденция *Get Smart* вместо *Get more*

20.9. Будущая адресация в сетях
- 20.9.1. Актуальные проблемы IP-адресации
- 20.9.2. IPv6
- 20.9.3. IPv4+
- 20.9.4. Преимущества IPv4+ в сравнении с IPv4
- 20.9.5. Преимущества IPv6 в сравнении с IPv4

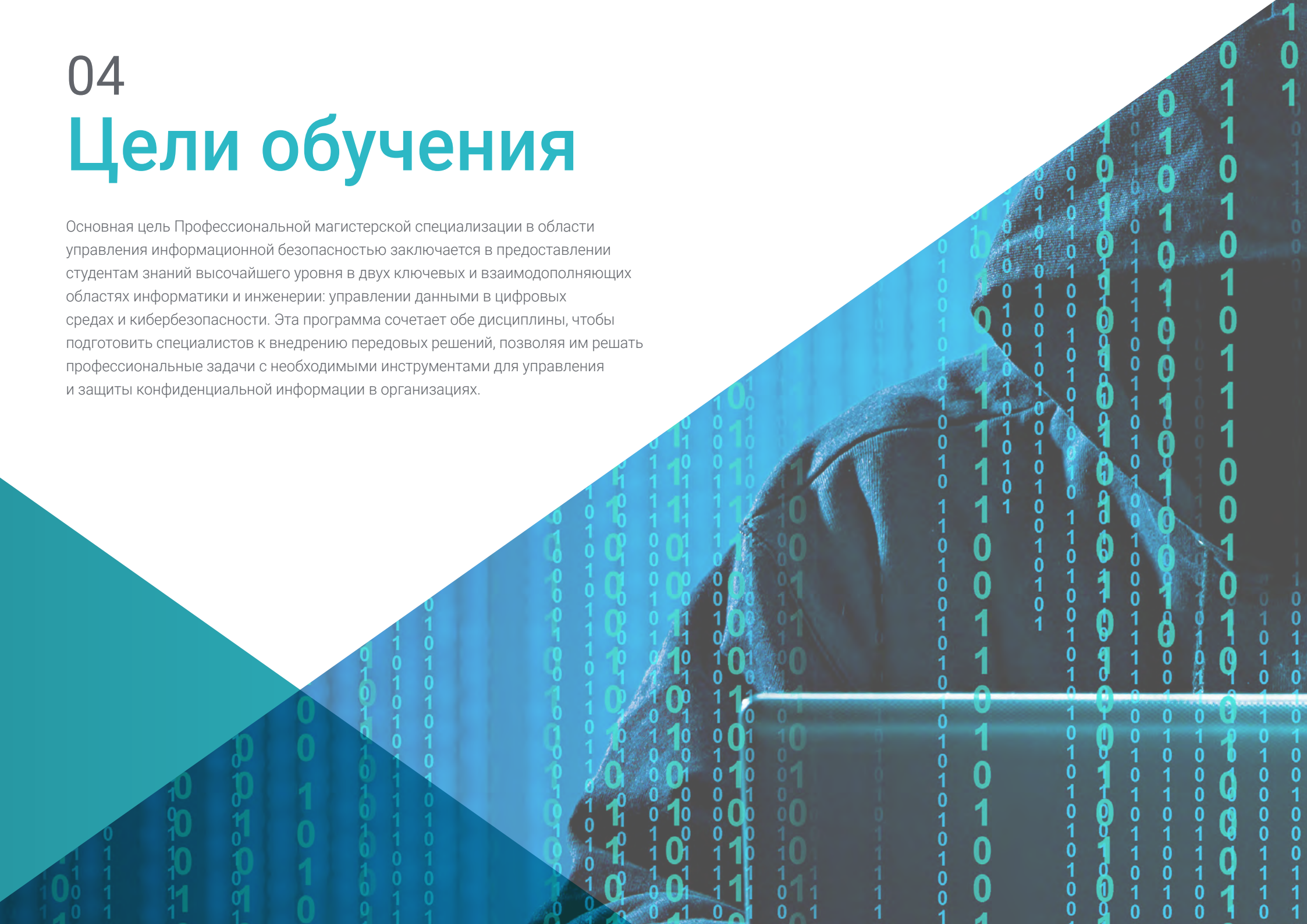
20.10. Задача повышения осведомленности населения о своевременном и непрерывном образовании
- 20.10.1. Текущие стратегии правительства
- 20.10.2. Сопротивляемость населения обучению
- 20.10.3. Планы обучения, которые должны быть внедрены компаниями

Вы будете учиться на реальных примерах, разработанных в смоделированных учебных средах, которые отражают современные проблемы в области управления данными и кибербезопасности”

04

Цели обучения

Основная цель Профессиональной магистерской специализации в области управления информационной безопасностью заключается в предоставлении студентам знаний высочайшего уровня в двух ключевых и взаимодополняющих областях информатики и инженерии: управлении данными в цифровых средах и кибербезопасности. Эта программа сочетает обе дисциплины, чтобы подготовить специалистов к внедрению передовых решений, позволяя им решать профессиональные задачи с необходимыми инструментами для управления и защиты конфиденциальной информации в организациях.



Преобразите свою профессиональную карьеру с этой инновационной программой Профессиональной магистерской специализации, которая станет важным этапом в вашей специализации в области управления данными и кибербезопасности”

Общие цели

- Развивать углубленные знания в аналитике данных и кибербезопасности для оптимизации бизнес-процессов с помощью инновационных инструментов и технологий
- Реализовывать эффективные стратегии безопасности для предотвращения цифровых угроз в системах, сетях и мобильных устройствах
- Решать задачи в области кибербезопасности с помощью аудитов, обратной инженерии и форензного анализа на основе доказательств
- Предсказывать технологические тенденции, применяя разрушительные решения, которые защищают цифровые активы и сложные системы

Лидировать в управлении данными и кибербезопасности в цифровой среде с этим программой специализации”

Конкретные цели

Модуль 1. Аналитика данных в организации бизнеса

- Развивать компетенции в использовании методов анализа данных
- Генерировать ценную информацию, которая будет способствовать принятию стратегических решений в бизнес-организациях, улучшая эффективность и конкурентоспособность

Модуль 2. Управление данными, обработка данных и составление отчетов по науке о данных

- Обучать эффективному управлению и обработке больших объемов данных
- Применять методологии и инструменты для структурирования, очистки и преобразования данных в полезную информацию для проектов в области науки о данных

Модуль 3. IoT-устройства и платформы как основа для науки о данных

- Предоставить необходимые знания о платформах и устройствах Интернета вещей и их интеграции в науку о данных
- Углубить знания в области захвата, обработки и анализа данных в реальном времени

Модуль 4. Графическое представление для анализа данных

- Представлять данные с помощью инструментов и передовых техник визуализации
- Облегчить понимание паттернов, тенденций и связей в больших объемах данных

Модуль 5. Инструменты науки о данных

- Обучать использованию инструментов и программного обеспечения, специфичных для науки о данных, таких как Python
- Углубляться в сбор, анализ и представление данных в различных профессиональных контекстах

Модуль 6. Добыча данных. Отбор, предварительная обработка и преобразование

- Предоставить знания и навыки, необходимые для применения методов добычи данных
- Анализировать выбор, предварительную обработку и преобразование данных для извлечения значимых паттернов и тенденций

Модуль 7. Предсказуемость и стохастический анализ

- Развивать компетенции в моделировании и анализе стохастических явлений
- Использовать продвинутые статистические методы для прогнозирования поведения и тенденций в неопределенных и динамичных средах

Модуль 8. Проектирование и разработка интеллектуальных систем

- Обучать проектированию и разработке интеллектуальных систем, интегрируя методы машинного обучения и искусственного интеллекта
- Создавать автоматизированные решения для эффективного решения сложных проблем

Модуль 9. Архитектуры и системы с интенсивным использованием данных

- Предоставить знания по созданию архитектур систем, способных эффективно обрабатывать большие объемы данных
- Использовать передовые технологии, такие как распределенные базы данных и параллельная обработка

Модуль 10. Практическое применение науки о данных в бизнес-секторах

- Развивать способность применять практики науки о данных в различных секторах бизнеса
- Интегрировать полученные знания для улучшения принятия решений, оптимизации процессов и инноваций в компании

Модуль 11. Кибербезопасность
- Предоставить знания и навыки, необходимые для применения методов кибербезопасности и кибербезопасности
- Защищать системы и сети компаний от киберугроз и обеспечивать целостность данных

Модуль 12. Безопасность хоста
- Обучать внедрению мер безопасности в хост-системы
- Обеспечивать защиту серверов и критических приложений с помощью инструментов и лучших практик информационной безопасности

Модуль 13. Сетевая безопасность (периметр)
- Предоставить знания о защите сетей и информационных систем на периферийном уровне
- Управлять межсетевыми экранами, VPN и другими инструментами для обеспечения безопасности инфраструктуры сети компании

Модуль 14. Безопасность смартфонов
- Развивать компетенции для обеспечения безопасности мобильных устройств
- Понимать общие уязвимости и применять превентивные меры для защиты информации и приложений на смартфонах

Модуль 15. Безопасность в IoT
- Предоставить необходимые знания для внедрения решений безопасности в устройства IoT
- Защищать сети и системы, которые соединяют устройства, гарантируя конфиденциальность и целостность данных, генерируемых ими

Модуль 16. Этичный хакинг
- Обучить практикам этичного хакинга, обучая проведению контролируемых тестов на проникновение
- Выявлять уязвимости в компьютерных системах для улучшения безопасности до того, как они будут использованы злоумышленниками

Модуль 17. Реверс-инжиниринг
- Предоставить знания о техниках инженерии обратного проектирования, позволяя анализировать и понимать работу программного обеспечения и аппаратного обеспечения
- Обнаруживать ошибки безопасности или улучшать функциональность существующих систем

Модуль 18. Безопасная разработка
- Обучать разработке безопасного программного обеспечения, обучая лучшим практикам кодирования и безопасности на протяжении всего жизненного цикла программного обеспечения
- Уметь предотвращать уязвимости и защищать компьютерные системы от атак

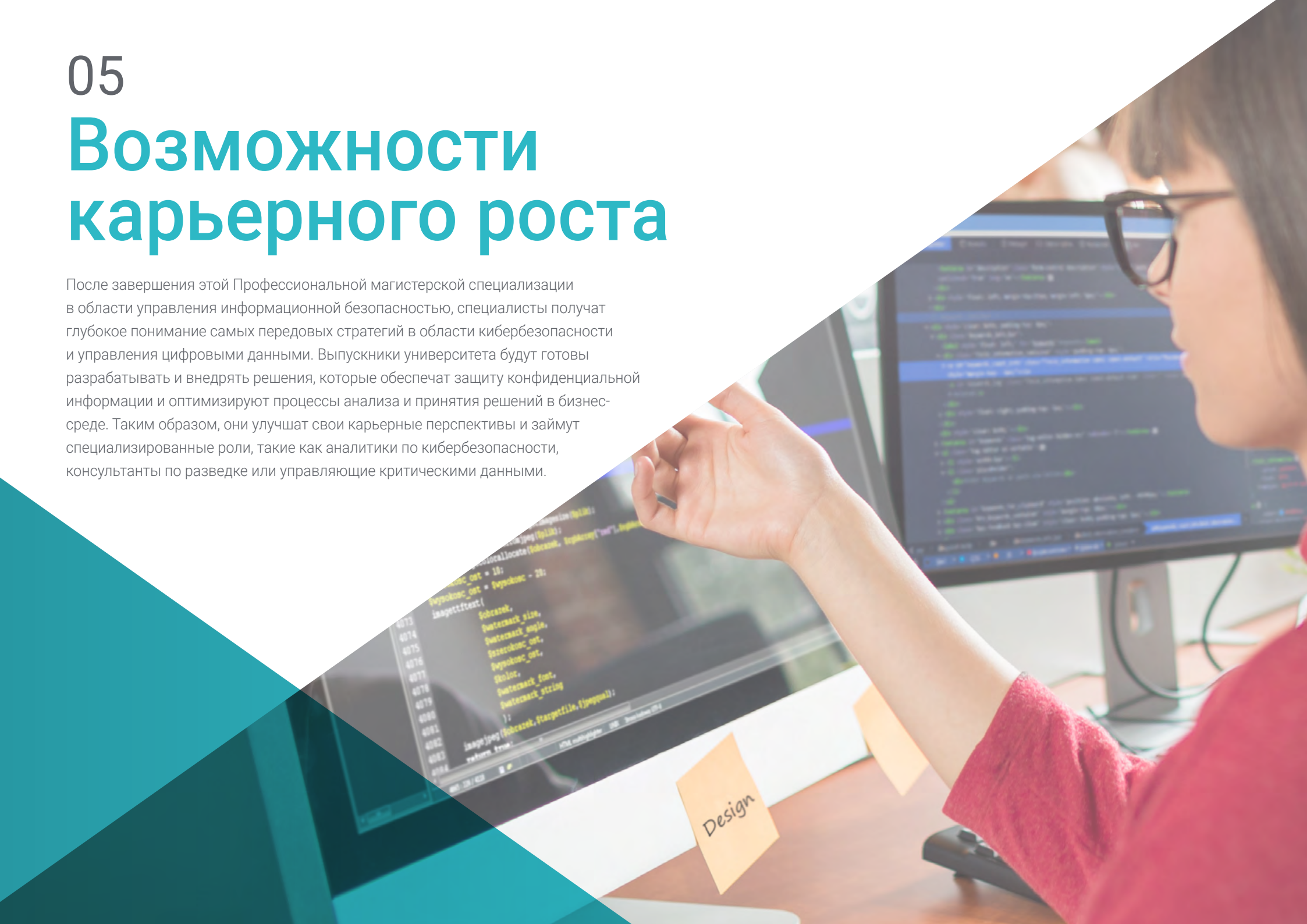
Модуль 19. Судебная экспертиза
- Развивать навыки, необходимые для проведения цифровых судебных расследований
- Использовать инструменты и передовые методы для восстановления, анализа и сохранения электронных доказательств при инцидентах информационной безопасности

Модуль 20. Актуальные и будущие задачи в области кибербезопасности
- Исследовать актуальные и будущие проблемы в области информационной безопасности, анализируя новые угрозы и новые технологии защиты
- Углубляться в стратегии минимизации рисков в постоянно меняющемся технологическом окружении

05

Возможности карьерного роста

После завершения этой Профессиональной магистерской специализации в области управления информационной безопасностью, специалисты получат глубокое понимание самых передовых стратегий в области кибербезопасности и управления цифровыми данными. Выпускники университета будут готовы разрабатывать и внедрять решения, которые обеспечат защиту конфиденциальной информации и оптимизируют процессы анализа и принятия решений в бизнес-среде. Таким образом, они улучшат свои карьерные перспективы и займут специализированные роли, такие как аналитики по кибербезопасности, консультанты по разведке или управляющие критическими данными.



Вы обеспечите безопасность цифровых активов и сыграете ключевую роль в цифровой трансформации организаций"

Профиль выпускника

Выпускник Профессиональной магистерской специализации в области управления информационной безопасностью станет высококвалифицированным специалистом по управлению и защите информации в цифровых средах. Он будет иметь углубленные знания в таких областях, как кибербезопасность, цифровая разведка и анализ данных, а также практические навыки в проектировании и внедрении стратегий защиты от угроз. Его профиль сочетает глубокое техническое понимание с стратегическими компетенциями, которые позволят ему возглавлять проекты в ключевых бизнес-секторах.

Вы станете лидером в области защиты данных и кибербезопасности, сотрудничая с компаниями для решения проблем цифровой среды.

- **Управление безопасностью:** Развивать способность выявлять риски, внедрять многоуровневые стратегии защиты и обеспечивать конфиденциальность, целостность и доступность данных
- **Критический анализ и решение проблем:** Использовать передовые методы для оценки систем, выявления уязвимостей и разработки решений, адаптированных к различным технологическим средам
- **Технические и цифровые компетенции:** Работать с передовыми инструментами анализа данных, кибербезопасности и систем разведки, что позволит вам возглавлять проекты технологических инноваций
- **Стратегическое мышление:** Проектировать политики безопасности и бизнес-стратегии, отвечающие текущим и будущим требованиям цифровой среды
- **Междисциплинарное сотрудничество:** Работать с многопрофильными командами для решения сложных задач и обеспечения безопасности сетей, платформ IoT и мобильных устройств

После завершения Профессиональной магистерской специализации вы сможете применять свои знания и навыки на следующих должностях:

1. **Директор по кибербезопасности:** Руководитель, отвечающий за координацию команд и разработку стратегий защиты цифровых активов в крупных организациях
2. **Аналитик данных:** Дизайнер предсказательных анализов и систем визуализации для оптимизации принятия решений
3. **Консультант по цифровой разведке:** Специалист, предлагающий продвинутые решения на основе разведки и анализа рисков
4. **Специалист по IoT и безопасности:** Разработчик мер защиты для подключенных устройств и промышленных сред
5. **Этичный хакер:** Оценщик уязвимостей, который исправляет ошибки в корпоративных системах для предотвращения кибератак
6. **Аудитор безопасности:** Инспектор, проводящий аудиты и судебные экспертизы для обеспечения соблюдения нормативных требований
7. **Менеджер корпоративных данных:** Администратор, отвечающий за разработку и управление системами хранения и анализа данных для повышения операционной эффективности

Пройдите эту программу и станьте специалистом в самых востребованных областях цифровой среды"

06

Методика обучения

TECH — первый в мире университет, объединивший метод ***кейс-стади*** с ***Relearning***, системой 100% онлайн-обучения, основанной на направленном повторении.

Эта инновационная педагогическая стратегия была разработана для того, чтобы предложить профессионалам возможность обновлять свои знания и развивать навыки интенсивным и эффективным способом. Модель обучения, которая ставит студента в центр учебного процесса и отводит ему ведущую роль, адаптируясь к его потребностям и оставляя в стороне более традиционные методологии.

TECH подготовит вас к решению новых задач в условиях неопределенности и достижению успеха в карьере”

Студент — приоритет всех программ TECH

В методике обучения TECH студент является абсолютным действующим лицом. Педагогические инструменты каждой программы были подобраны с учетом требований к времени, доступности и академической строгости, которые предъявляют современные студенты и наиболее конкурентоспособные рабочие места на рынке.

В асинхронной образовательной модели TECH студенты сами выбирают время, которое они выделяют на обучение, как они решат выстроить свой распорядок дня, и все это — с удобством на любом электронном устройстве, которое они предпочитают. Студентам не нужно посещать очные занятия, на которых они зачастую не могут присутствовать. Учебные занятия будут проходить в удобное для них время. Вы всегда можете решить, когда и где учиться.

“В TECH у вас НЕ будет занятий в реальном времени, на которых вы зачастую не можете присутствовать”

Самые обширные учебные планы на международном уровне

TECH характеризуется тем, что предлагает наиболее обширные академические планы в университетской среде. Эта комплексность достигается за счет создания учебных планов, которые охватывают не только основные знания, но и самые последние инновации в каждой области.

Благодаря постоянному обновлению эти программы позволяют студентам быть в курсе изменений на рынке и приобретать навыки, наиболее востребованные работодателями. Таким образом, те, кто проходит обучение в TECH, получают комплексную подготовку, которая дает им значительное конкурентное преимущество для продвижения по карьерной лестнице.

Более того, студенты могут учиться с любого устройства: компьютера, планшета или смартфона.

> *Модель TECH является асинхронной, поэтому вы можете изучать материал на своем компьютере, планшете или смартфоне в любом месте, в любое время и в удобном для вас темпе”*

Case studies или метод кейсов

Метод кейсов является наиболее распространенной системой обучения в лучших бизнес-школах мира. Разработанный в 1912 году для того, чтобы студенты юридических факультетов не просто изучали законы на основе теоретических материалов, он также имел цель представить им реальные сложные ситуации. Таким образом, они могли принимать взвешенные решения и выносить обоснованные суждения о том, как их разрешить. В 1924 году он был установлен в качестве стандартного метода обучения в Гарвардском университете.

При такой модели обучения студент сам формирует свою профессиональную компетенцию с помощью таких стратегий, как *обучение действием* (learning by doing) или *дизайн-мышление* (*design thinking*), используемых такими известными учебными заведениями, как Йель или Стэнфорд.

Этот метод, ориентированный на действия, будет применяться на протяжении всего академического курса, который студент проходит в TECH. Таким образом, они будут сталкиваться с множеством реальных ситуаций и должны будут интегрировать знания, проводить исследования, аргументировать и защищать свои идеи и решения. Все это делается для того, чтобы ответить на вопрос, как бы они поступили, столкнувшись с конкретными сложными событиями в своей повседневной работе.

Метод *Relearning*

В TECH *метод кейсов* дополняется лучшим методом онлайн-обучения — *Relearning*.

Этот метод отличается от традиционных методик обучения, ставя студента в центр обучения и предоставляя ему лучшее содержание в различных форматах. Таким образом, студент может пересматривать и повторять ключевые концепции каждого предмета и учиться применять их в реальной среде.

Кроме того, согласно многочисленным научным исследованиям, повторение является лучшим способом усвоения знаний. Поэтому в TECH каждое ключевое понятие повторяется от 8 до 16 раз в рамках одного занятия, представленного в разных форматах, чтобы гарантировать полное закрепление знаний в процессе обучения.

Метод Relearning позволит тебе учиться с меньшими усилиями и большей эффективностью, глубже вовлекаясь в свою специализацию, развивая критическое мышление, умение аргументировать и сопоставлять мнения — прямой путь к успеху.

Виртуальный кампус на 100% в онлайн-формате с лучшими учебными ресурсами

Для эффективного применения своей методики TECH предоставляет студентам учебные материалы в различных форматах: тексты, интерактивные видео, иллюстрации, карты знаний и др. Все они разработаны квалифицированными преподавателями, которые в своей работе уделяют особое внимание сочетанию реальных случаев с решением сложных ситуаций с помощью симуляции, изучению контекстов, применимых к каждой профессиональной сфере, и обучению на основе повторения, с помощью аудио, презентаций, анимации, изображений и т.д.

Последние научные данные в области нейронаук указывают на важность учета места и контекста, в котором происходит доступ к материалам, перед началом нового процесса обучения. Возможность индивидуальной настройки этих параметров помогает людям лучше запоминать и сохранять знания в гиппокампе для долгосрочного хранения. Речь идет о модели, называемой *нейрокогнитивным контекстно-зависимым электронным обучением*, которая сознательно применяется в данной университетской программе.

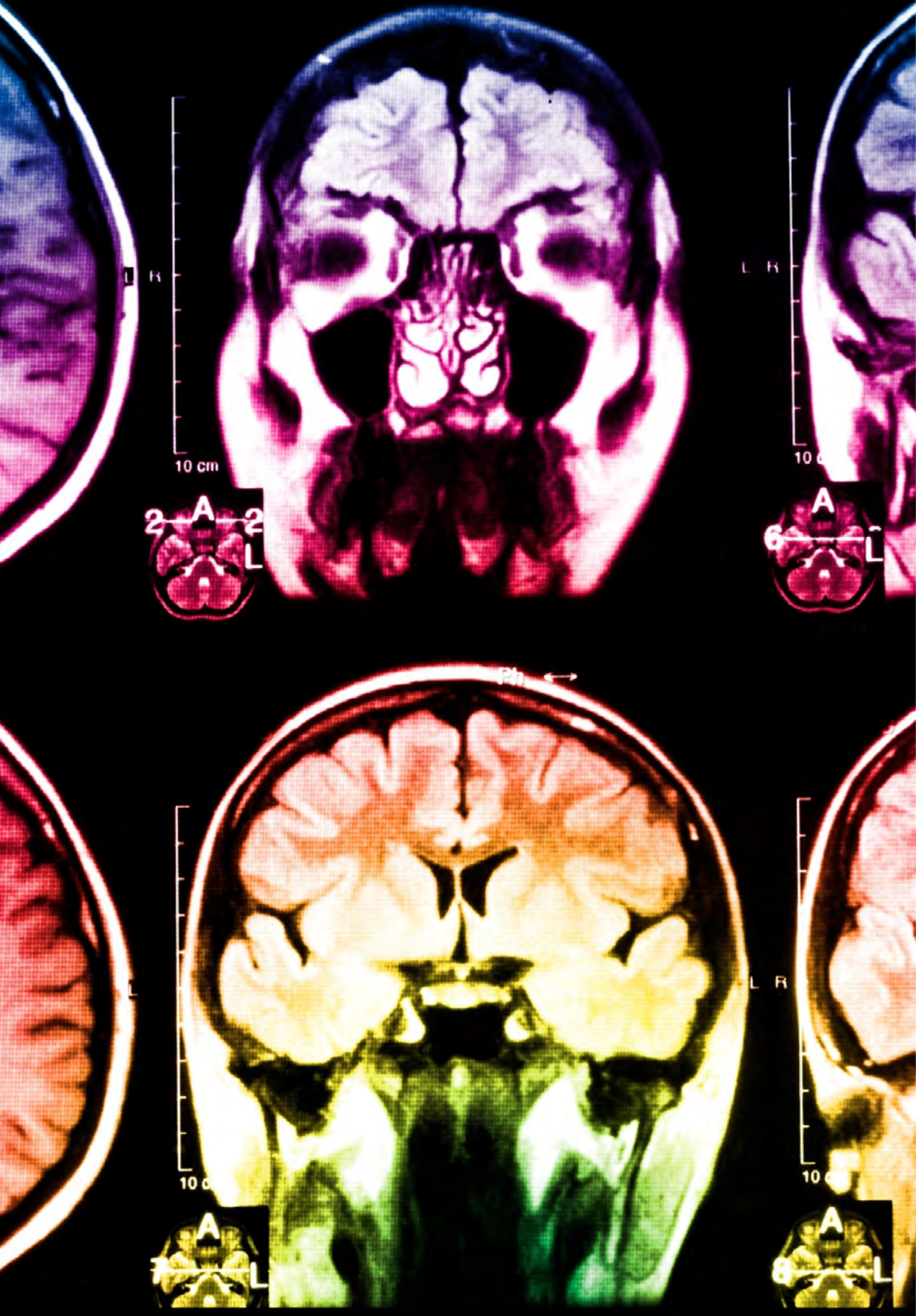
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи с техническим отделом, чат и видеоконференции).

Этот полноценный Виртуальный кампус также позволит студентам TECH организовывать свое учебное расписание в соответствии с личной доступностью или рабочими обязательствами. Таким образом, студенты смогут полностью контролировать академические материалы и учебные инструменты, необходимые для быстрого профессионального развития.

> *Онлайн-режим обучения на этой программе позволит вам организовать свое время и темп обучения, адаптировав его к своему расписанию”*

Эффективность метода обосновывается четырьмя ключевыми достижениями:

1. Студенты, которые следуют этому методу, не только добиваются усвоения знаний, но и развивают свои умственные способности с помощью упражнений по оценке реальных ситуаций и применению своих знаний.
2. Обучение прочно опирается на практические навыки, что позволяет студенту лучше интегрироваться в реальный мир.
3. Усвоение идей и концепций становится проще и эффективнее благодаря использованию ситуаций, возникших в реальности.
4. Ощущение эффективности затраченных усилий становится очень важным стимулом для студентов, что приводит к повышению интереса к учебе и увеличению времени, посвященному на работу над курсом.



Методика университета, получившая самую высокую оценку среди своих студентов

Результаты этой инновационной академической модели подтверждаются высокими уровнями общей удовлетворенности выпускников TECH.

Студенты оценивают качество преподавания, качество материалов, структуру и цели курса на отлично. Неудивительно, что учебное заведение стало лучшим университетом по оценке студентов на платформе отзывов Global Score получив 4,9 балла из 5.

Благодаря тому, что TECH идет в ногу с передовыми технологиями и педагогикой, вы можете получить доступ к учебным материалам с любого устройства с подключением к Интернету (компьютера, планшета или смартфона).

Вы сможете учиться, пользуясь преимуществами доступа к симулированным образовательным средам и модели обучения через наблюдение, то есть учиться у эксперта (learning from an expert).

Таким образом, в этой программе будут доступны лучшие учебные материалы, подготовленные с большой тщательностью:

Учебные материалы

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

Затем эти материалы переносятся в аудиовизуальный формат, на основе которого строится наш способ работы в интернете, с использованием новейших технологий, позволяющих нам предложить вам отличное качество каждого из источников, предоставленных к вашим услугам.

Практика навыков и компетенций

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

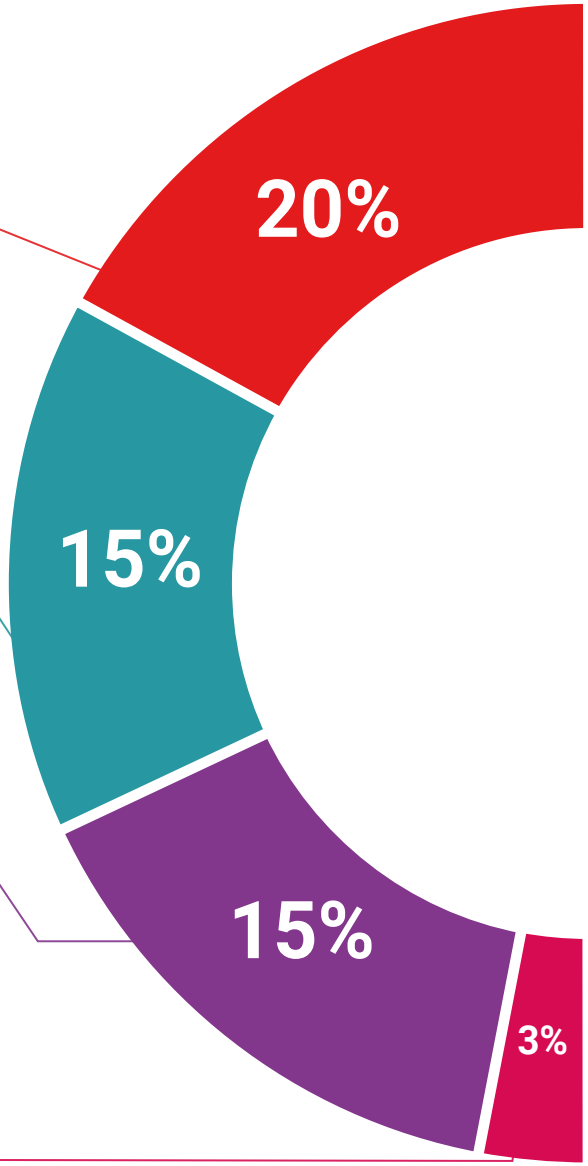
Интерактивные конспекты

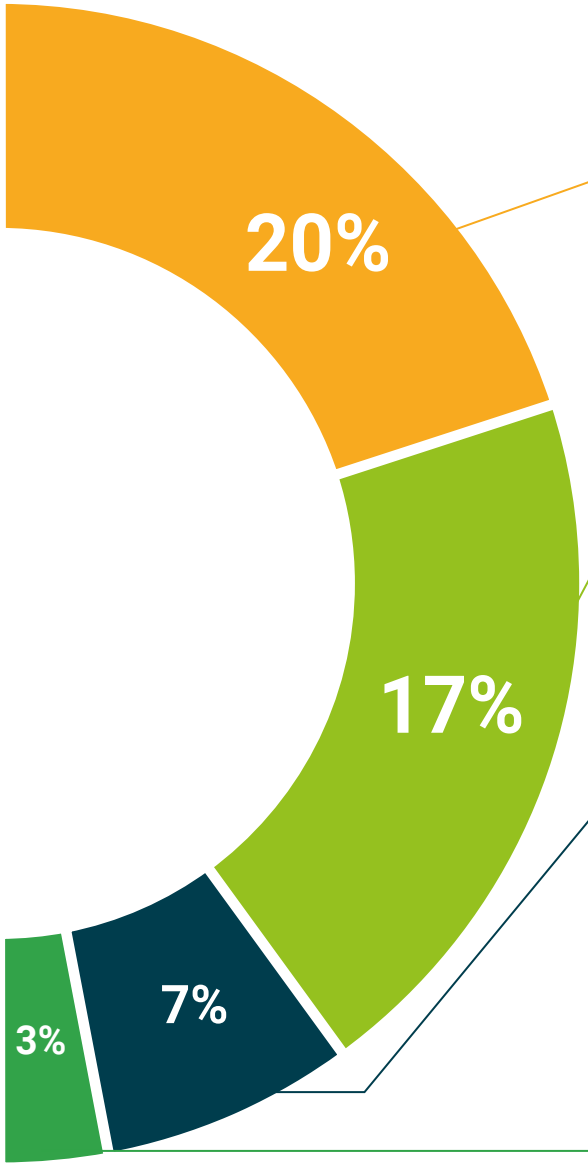
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

Эта эксклюзивная образовательная система для презентации мультимедийного содержания была награждена Microsoft как "Кейс успеха в Европе".

Дополнительная литература

Последние статьи, консенсусные документы, международные рекомендации... В нашей виртуальной библиотеке вы получите доступ ко всему, что необходимо для прохождения обучения.





Кейс-стади

Студенты завершат выборку лучших *кейс-стади* по предмету. Кейсы представлены, проанализированы и преподаются ведущими специалистами на международной арене.

Тестирование и повторное тестирование

Мы периодически оцениваем и переоцениваем ваши знания на протяжении всей программы. Мы делаем это на 3 из 4 уровней пирамиды Миллера.

Мастер-классы

Существуют научные данные о пользе экспертного наблюдения третьей стороны.

Так называемый метод *обучения у эксперта* (learning from an expert) укрепляет знания и память, а также формирует уверенность в ваших будущих сложных решениях.

Краткие справочные руководства

TECH предлагает наиболее актуальные материалы курса в виде карточек или кратких справочных руководств. Это сжатый, практичный и эффективный способ помочь студенту продвигаться в обучении.

07

Преподавательский состав

Эта программа преподается выдающимися профессионалами в области кибербезопасности и цифрового управления данными. Их опыт гарантирует, что студенты получат полные и актуальные знания, которые могут быть непосредственно применены в их карьере. Преподаватели этой Профессиональной магистерской специализации в области управления информационной безопасностью делятся своими знаниями, готовя высококвалифицированных специалистов, востребованных крупными компаниями на международном уровне.

Добивайтесь успеха с лучшими и приобретайте ключевые знания и навыки для лидерства в области управления данными и кибербезопасности в цифровой среде”

Приглашенный лектор международного уровня

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

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

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

Д-р Лемье, Фредерик

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

Благодаря TECH вы сможете учиться у лучших мировых профессионалов"

Руководство

Д-р Перальта Мартин-Паломино, Артуро

- CEO и CTO Prometeus Global Solutions
- CTO в Korporate Technologies
- CTO в AI Shephers GmbH
- Консультант и советник в области стратегического бизнеса в Alliance Medical
- Руководитель в области дизайна и разработки в компании DocPath
- Степень доктора в области компьютерной инженерии в Университете Кастилии-ла-Манча
- Степень доктора в области экономики, бизнеса и финансов Университета Камило Хосе Села
- Степень доктора в области психологии Университета Кастилии-ла-Манча
- Степень магистра Executive MBA Университета Изабель I
- Степень магистра в области управления коммерцией и маркетингом Университета Изабель I
- Степень магистра в области больших данных по программе Hadoop
- Степень магистра в области передовых информационных технологий Университета Кастилии-Ла-Манча
- Член исследовательской группы SMILE

Г-жа Фернандес Сапена, Соня

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

Преподаватели

Г-н Монторо Монтарросо, Андрес

- Исследователь в группе SMILe в Университете Кастилии-Ла-Манчи
- Клинический исследователь Университета Гранады
- Специалист по анализу данных в Prometeus Global Solutions
- Вице-президент и разработчик программного обеспечения в CireBits
- Степень доктора в области передовых информационных технологий Университета Кастилии-Ла-Манча
- Степень бакалавра 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 Сьюдаде-Реале, читает следующую лекцию: *"Приложения для обработки естественного языка: Нечеткая логика для анализа сообщений в социальных сетях"*
- Выступает на семинаре "Предотвращение коррупции в государственных органах и искусственный интеллект" на факультете права и социальных наук Толедо с лекцией: *Методы искусственного интеллекта*
- Докладчик на Первом международном семинаре по административному праву и искусственному интеллекту (DAIA). Организаторы: Центр европейских исследований Луиса Ортеги Альвареса и Исследовательский институт TransJus. Конференция *"Анализ настроений для предотвращения языка ненависти в социальных сетях"*

Г-н Перис Морильо, Луис Хавьер

- Старший технический руководитель и руководитель службы поддержки в HCL Technologies
- Технический редактор в Baeldung
- Agile-коуч и операционный менеджер в Mirai Advisory
- Разработчик, руководитель группы, Scrum-мастер, Agile-коуч и менеджер по продукту в DocPath
- Технолог в ARCO
- Степень бакалавра в области вычислительной техники в Университете Кастилии-Ла-Манчи
- Последипломное образование по управлению проектами от CEOE

Г-жа Фернандес Мелендес, Галина

- Специалист в области больших данных
- Аналитик данных в компании Aresi Gestión de Fincas
- Аналитик данных в ADN Mobile Solution
- Степень бакалавра в области делового администрирования в Университете Бисентенария-де-Арагуа. Каракас, Венесуэла
- Диплом в области планирования и государственных финансов Венесуэльской школы планирования
- Степень магистра в области анализа данных и бизнес-аналитики Университета Овьедо
- Степень магистра делового администрирования в области делового администрирования и менеджмента в Европейской школе бизнеса Барселоны
- Степень магистра в области больших данных и бизнес-аналитики, полученная в Европейской школе бизнеса в Барселоне

Г-жа Педрахас Параба, Мариа Елена

- Новые технологии и цифровая трансформация Консультант в области управленческих решений
- Научный сотрудник кафедры 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 Университета Кордоба
- Степень магистра в области науки о данных и компьютерной инженерии в Университете Гранады
- Степень магистра в области бизнес-консультирования, полученная в Папском университете Комильяс

Г-жа Мартинес Серрато, Йесика

- Менеджер по техническому обучению в Securitas Seguridad España
- Специалист в области образования, бизнеса и маркетинга
- *Менеджер продукции* в области электронной безопасности в Securitas Seguridad España
- Аналитик бизнес-аналитики в Ricopia Technologies
- Специалист по информатике и ответственная за компьютерные классы OTEC в Университете Алькала-де-Энарес
- Сотрудник Ассоциации ASALUMA
- Степень бакалавра в области инженерии электронных коммуникаций в Политехнической школе Университета Алькала-де-Энарес

Г-н Фондон Алькальде, Рубен

- Аналитик EMEA о Amazon Web Services
- Бизнес-аналитик в области управления потребительской ценностью в компании Vodafone España
- Руководитель отдела интеграции услуг в компании Entelgy для Telefónica Global Solutions
- Менеджер по работе с клиентами в области клонированных облачных серверов в компании EDM Electronics
- Менеджер по вопросам внедрения международных услуг в Vodafone Global Enterprise
- Консультант по разработке решений в Испании и Португалии, Telvent Global Services
- Бизнес-аналитик по Южной Европе в компании Vodafone Global Enterprise
- Инженер в области телекоммуникаций, Европейский университет в Мадриде
- Степень магистра в области больших данных и аналитики Международного университета Валенсии

Г-н Диас Диас-Чирон, Тобиас

- Научный сотрудник лаборатории ArCO Университета Кастилии-Ла-Манчи
- Консультант в компании Blue Telecom
- Фрилансер работающий в основном в телекоммуникационном секторе, специализирующийся на сетях 4G/5G
- OpenStack: развёртывание и администрирование
- Профессиональное образование в области инженерии со специализацией в инженерии в Университете Кастилии-Ла-Манчи
- Специализация в области компьютерной архитектуры и сетей
- Доцент Университета Кастилии-Ла-Манчи
- Докладчик на курсе Sepecam по сетевому администрированию

Г-н Тато Санчес, Рафаэль

- Технический директор в Indra Sistemas SA
- Системный инженер в ENA TRÁFICO SAU
- Степень магистра в области Индустрии 4.0. в онлайн-университете
- Степень магистра в области промышленной инженерии в Университете Европейского
- Степень в области промышленной электроники и автоматизации в Европейском университете Мадрида
- Промышленный инженер, Политехнический университет Мадрида

Г-жа Маркос Сбарбаро, Виктория Алисия

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

Г-н Катала Барба, Хосе Франсиско

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

Г-н Редондо, Хесус Серрано

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

Г-н Хименес Рамос, Альваро

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

Г-н Армеро Фернандес, Рафаэль

- Консультант по бизнес-аналитике в SDG Group
- Цифровой инженер в MI-GSO
- Инженер по логистике в компании Torrecid SA
- Специалист по качеству в INDRA
- Степень бакалавра в области аэрокосмической инженерии Политехнического университета Валенсии
- Степень магистра в области профессионального развития 4.0 Университета Алькалы

Г-н Перальта Алонсо, Йон

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

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

08

Квалификация

Профессиональная магистерская специализация в области управления информационной безопасностью гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Профессиональной магистерской специализации, выдаваемого TECH Технологическим университетом.

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

Данная **Профессиональной магистерской специализации в области управления информационной безопасностью** 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 в Профессиональной магистерской специализации, и соответствует требованиям, обычно предъявляемым биржами труда, конкурсными экзаменами и комитетами по оценке карьеры. Диплом:

Профессиональной магистерской специализации в области управления информационной безопасностью

Формат: **онлайн**

Продолжительность: **2 года**


tech технологический университет

Настоящий

ДИПЛОМ

свидетельствует о том, что

Г-н/Г-жа _____ с документом, удостоверяющий личность_____

Освоил(а) и успешно прошел(ла) аккредитацию программы

ПРОФЕССИОНАЛЬНАЯ МАГИСТЕРСКАЯ СПЕЦИАЛИЗАЦИЯ

в области

управления информационной безопасностью

Данный диплом специализированной программы, присуждаемый Университетом, соответствует 3000 учебным часам, с датой начала дд/мм/гггг и датой окончания дд/мм/гггг.

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

17 июня 2020 г.

Д-р Tere Guevara Navarro
Ректор

unique TECH code: AFWOR23S techtitute.com/certificates


Профессиональная магистерская специализация в области управления информационной безопасностью

Общее распределение учебного плана

Курс	Предмет	Часы	Характер
1º	Аналитика данных в организации бизнеса	150	Обязат
1º	Управление данными, обработка данных и составление отчетов по науке о данных	150	Обязат
1º	IoT-устройства и платформы как основа для науки о данных	150	Обязат
1º	Графическое представление для анализа данных	150	Обязат
1º	Инструменты науки о данных	150	Обязат
1º	Добыча данных. Отбор, предварительная обработка и преобразование	150	Обязат
1º	Предсказуемость и стохастический анализ	150	Обязат
1º	Проектирование и разработка интеллектуальных систем	150	Обязат
1º	Архитектуры и системы с интенсивным использованием данных	150	Обязат
1º	Практическое применение науки о данных в бизнес-секторах	150	Обязат

Курс	Предмет	Часы	Характер
2º	Кибеpразведка и кибербезопасность	150	Обязат
2º	Безопасность хоста	150	Обязат
2º	Сетевая безопасность (периметр)	150	Обязат
2º	Безопасность смартфонов	150	Обязат
2º	Безопасность в IoT	150	Обязат
2º	Этичный хакинг	150	Обязат
2º	Реверс-инжиниринг	150	Обязат
2º	Безопасная разработка	150	Обязат
2º	Судебная экспертиза	150	Обязат
2º	Актуальные и будущие задачи в области кибербезопасности	150	Обязат

Д-р Tere Guevara Navarro
Ректор

tech технологический университет

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

tech технологический университет

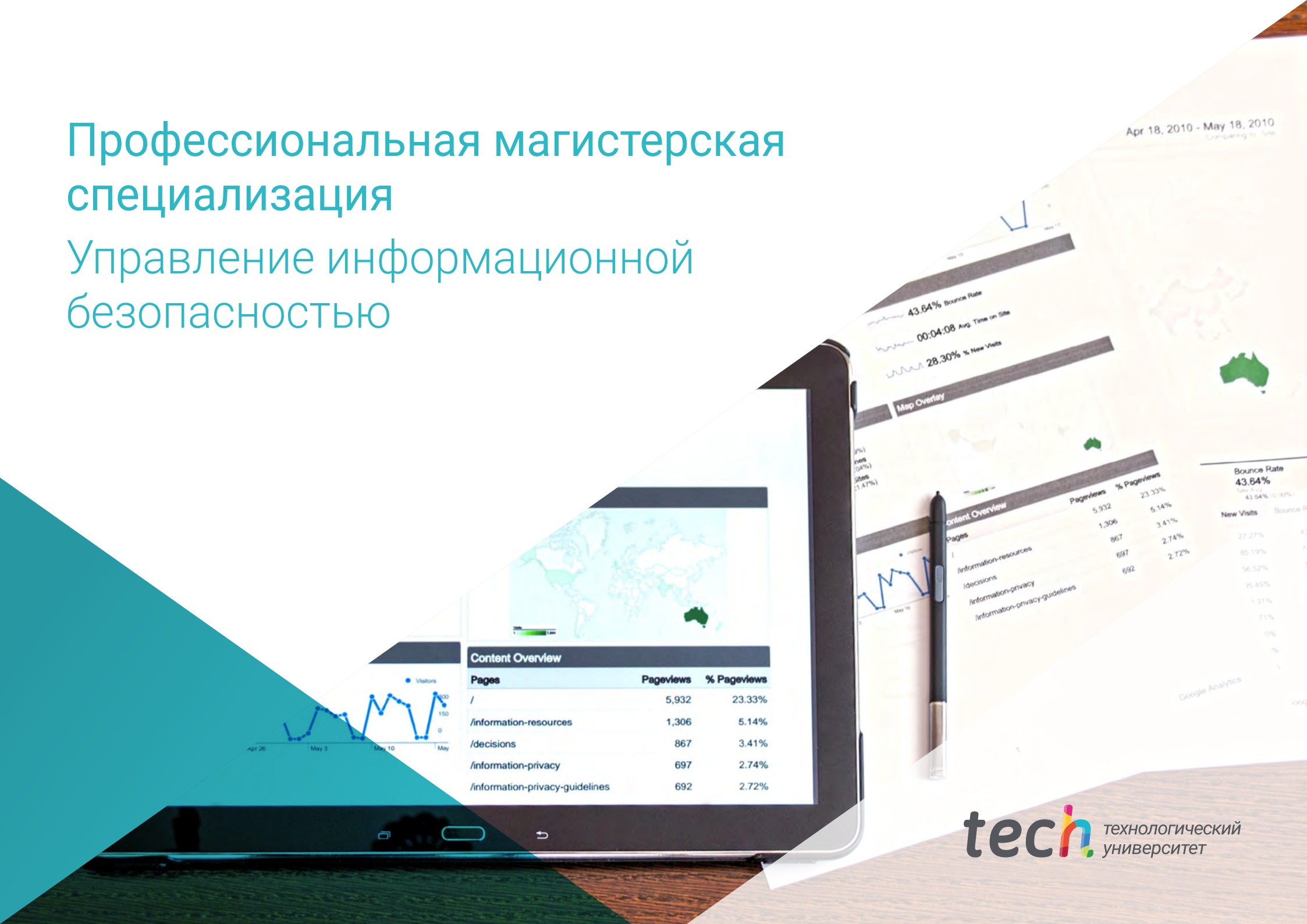
Профессиональная магистерская специализация

Управление информационной безопасностью

- Формат: **онлайн**
- Продолжительность: **2 года**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

Профессиональная магистерская специализация

Управление информационной безопасностью



tech технологический университет