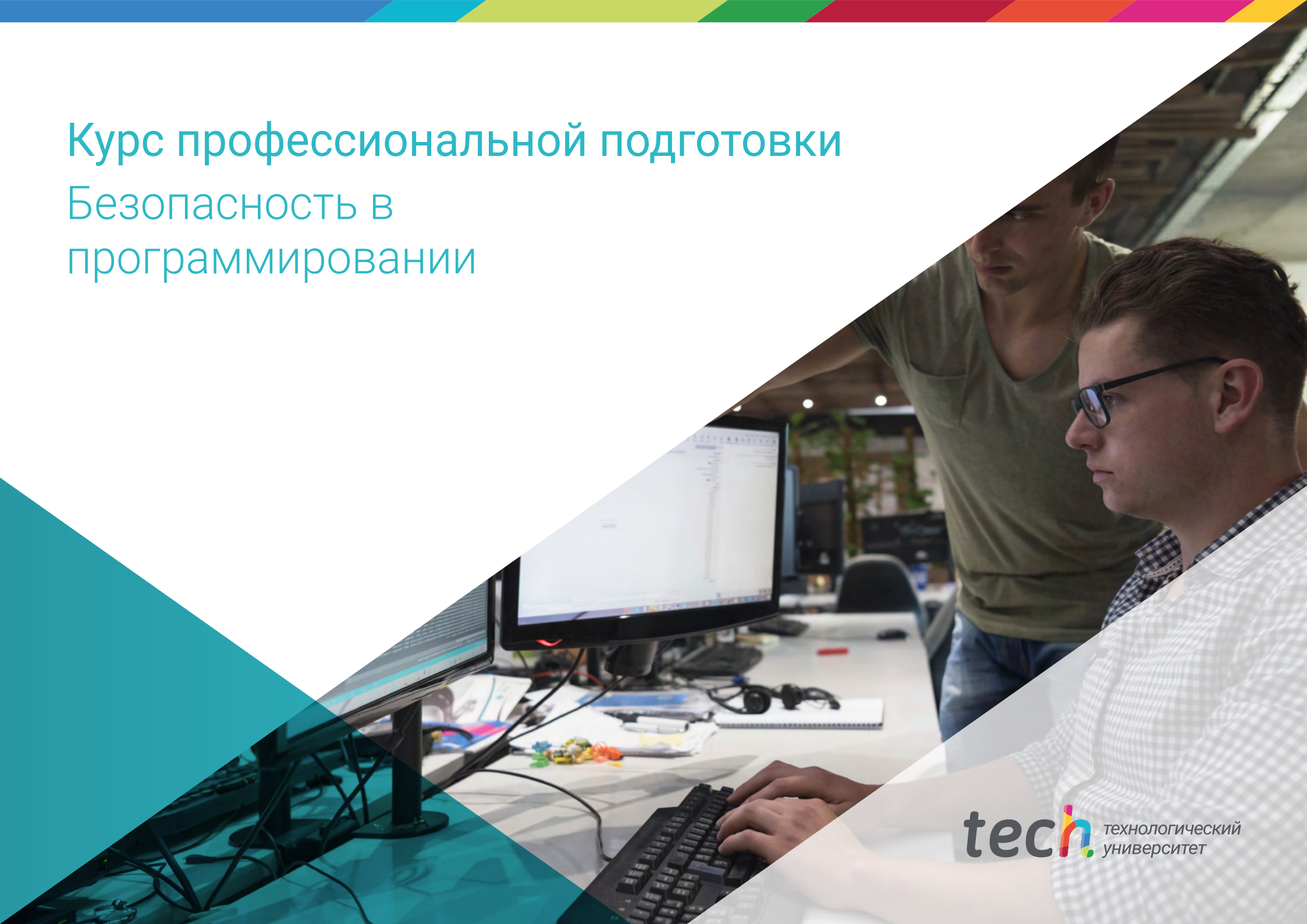
Курс профессиональной подготовки

Безопасность в программировании



tech технологический университет

технологический университет

Курс профессиональной подготовки

Безопасность в программировании

- Формат: **онлайн**
- Продолжительность: **6 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

Веб-доступ: www.techtitute.com/ru/information-technology/postgraduate-diploma/postgraduate-diploma-security-software-engineering

Оглавление

01

Презентация

Эта программа профессионального уровня позволит студентам узнать о процессе обеспечения информационной безопасности, его последствиях с точки зрения конфиденциальности, целостности, доступности и экономических затрат, а также понять проблемы, связанные с безопасностью программного обеспечения, его уязвимостями и классификацией.

Благодаря этой программе, отличающейся высокой научной строгостью, специалист получит знания, необходимые для внутреннего компьютерного контроля, а также для оценки и обнаружения уязвимостей в онлайн-приложениях.

Специализируйтесь на компьютерных системах у профессионалов с большим опытом работы в этом секторе”

Эта комплексная программа в области безопасности в программировании позволит ИТ-специалистам углубиться и обучиться процессам управления, проектирования, разработки и внедрения качественного и безопасного программного обеспечения, отвечающего поставленным целям.

Основная цель этого обучения заключается в том, чтобы студент достиг способности вносить существенные качественные улучшения, обеспечивая новые решения конкретных проблем, возникающих при разработке программного обеспечения. Программа также направлена на подготовку специалистов, способных использовать систематический и количественный подход к разработке и сопровождению программного обеспечения, чтобы они также получили глубокие знания в области программирования, внедрения и планирования компьютерных систем.

Благодаря этому курсу вы получите самые передовые дидактические ресурсы и сможете изучать программу обучения, которая объединяет самые глубокие знания по предмету, а группа преподавателей с высоким академическим уровнем и обширным международным опытом предоставляет наиболее полную и актуальную информацию о последних достижениях и методах в области разработки программного обеспечения и информационных систем.

Учебный план охватывает основные актуальные темы в области безопасности в программировании таким образом, что те, кто их освоит, будут подготовлены к работе в этой области. Поэтому это не просто очередная образовательная программа, а реальный инструмент обучения, позволяющий подходить к темам специальности современно, объективно и проницательно, опираясь на самую современную информацию.

Следует отметить, что поскольку это программа проводится на 100% онлайн, студенты не обусловлены фиксированным расписанием или необходимостью переезда в другое физическое место, а могут получить доступ к содержимому в любое время суток, уравновешивая свою работу или личную жизнь с учебой. Кроме того, студентам будет предоставлен доступ к эксклюзивному набору дополнительных *мастер-классов*, проводимых всемирно признанным экспертом в области программирования. Таким образом, студенты смогут улучшить свои навыки в этой области, пользуясь гарантированным качеством, характерным для TECH.

Данный **Курс профессиональной подготовки в области безопасности в программировании** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

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

Совершенствуйте свои навыки в области программирования вместе с TECH! Вы сможете получить доступ к уникальным мастер-классам под руководством всемирно признанного эксперта в этой востребованной области”

Данный Курс профессиональной подготовки — лучшее вложение средств при выборе программы повышения квалификации в области безопасности в программировании. *Мы предлагаем вам качественный и свободный доступ к материалам”*

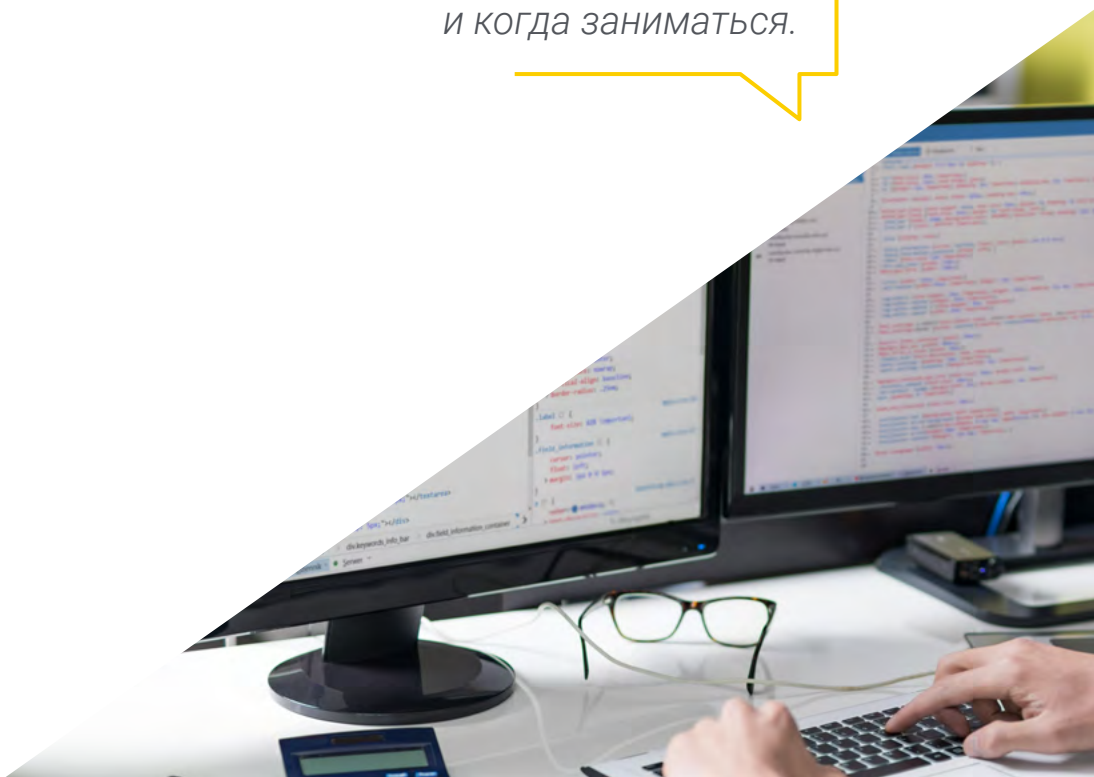
Данный курс позволит вам изучить лучший дидактический материал в более легкой и контекстной форме.

Этот Курс профессиональной подготовки в 100% онлайн-формате позволит вам совмещать учебу с профессиональной деятельностью. Вы сами выбираете, где и когда заниматься.

В преподавательский состав входят профессионалы из области безопасности в программировании, которые привносят в эту программу подготовки опыт своей работы, а также признанных специалистов из престижных сообществ и университетов.

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

Структура этой программы основана на проблемно-ориентированном обучении, с помощью которого специалист должен попытаться разрешать различные ситуации из профессиональной практики, возникающие в течение учебного курса. Для этого студенту будет помогать инновационная интерактивная видеосистема, созданная известными и опытными специалистами в области безопасности в программировании



02

Цели

Курс профессиональной подготовки в области безопасности в программировании призван помочь специалистам приобрести и изучить новые разработки в этой области и позволить им заниматься своей профессией качественно и профессионально.

Наша цель — чтобы вы стали лучшим специалистом в своей отрасли. И для этого у нас есть лучшая методология и содержание"

Общие цели

- Приобрести знания в области в области безопасности в программировании
- Освоить новые навыки в области современных технологий, последних разработок программного обеспечения
- Обрабатывать данные, полученные в ходе деятельности по разработке программного обеспечения

Совершенствуя свои навыки в области безопасности в программировании, вы сможете быть более конкурентоспособными. Продолжите обучаться и дайте толчок своей карьере"

Конкретные цели

Модуль 1. Управление безопасностью

- Научиться использовать передовые методы обеспечения безопасности при управлении услугами информационных технологий
- Приобрести знания для правильной сертификации процессов безопасности
- Понять механизмы и методы аутентификации для контроля доступа, а также процесс аудита доступа
- Освоить программы управления безопасностью, управление рисками и разработать политики безопасности
- Узнать о планах обеспечения непрерывности бизнеса, их этапах и процессе поддержания
- Знать процедуры правильной защиты компании с помощью сетей DMZ, использования систем обнаружения вторжений и других методологий

Модуль 2. Безопасность программного обеспечения

- Понимать проблемы безопасности программного обеспечения, уязвимости и способы их классификации
- Знать принципы проектирования, методологии и стандарты в области безопасности программного обеспечения
- Понять применение безопасности на различных этапах жизненного цикла программного обеспечения
- Приобрести необходимых знаний для безопасного кодирования программного обеспечения и методов проверки
- Освоить методологии и процессы обеспечения безопасности при разработке и предоставлении облачных услуг
- Понять основы криптологии и различные методы шифрования, доступные в настоящее время

Модуль 3. Аудит безопасности

- Приобрести знания, необходимые для правильного выполнения процесса внутреннего аудита и контроля ИТ
- Понять процессы, которые необходимо выполнить для аудита безопасности систем и сетей
- Освоить различные вспомогательные инструменты, методологии и последующий анализ в ходе аудита безопасности интернета и мобильных устройств
- Изучить свойства и факторы влияния, обуславливающие бизнес-риски, и определить правильность внедрения соответствующего управления рисками
- Знать меры по снижению рисков, а также методологии внедрения системы управления информационной безопасностью и нормативные акты и стандарты, которые необходимо использовать
- Понимать процедуры проведения аудита безопасности, его отслеживания и представления результатов

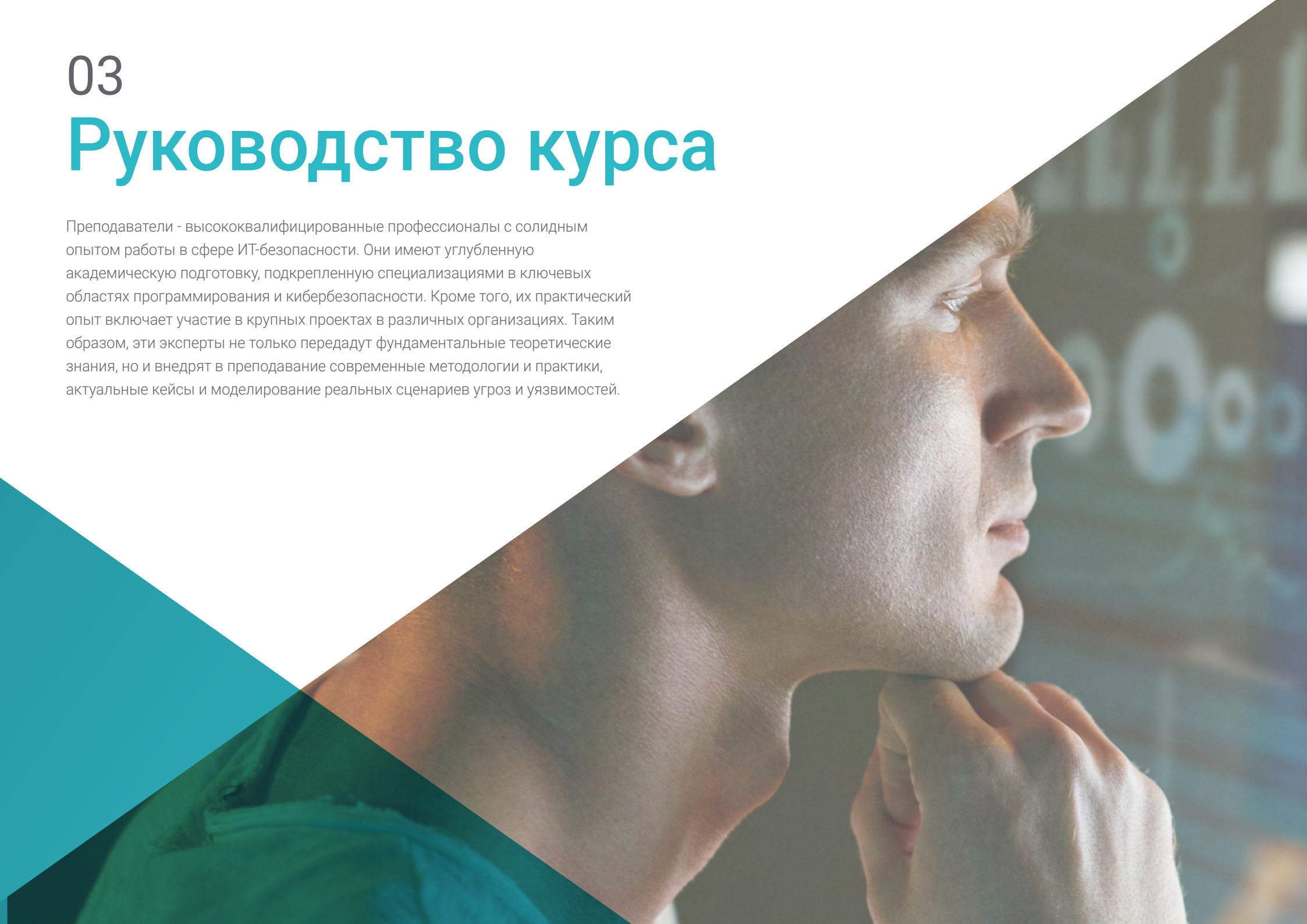
Модуль 4. Безопасность в онлайн-приложениях

- Приобрести необходимые знания для оценки и обнаружения уязвимостей в онлайн-приложениях
- Изучить процедуры, которые необходимо использовать при разработке веб-приложений и их последующей проверке с помощью анализа и тестов безопасности
- Узнать о мерах безопасности при развертывании и производстве веб-приложений
- Понять концепции, функции и технологии, применяемые для обеспечения безопасности веб-сервисов, а также тесты безопасности и защитные меры
- Освоить процедуры этического взлома, анализа вредоносных программ и криминалистики
- Изучить меры по смягчению и локализации инцидентов на веб-сервисах
- Получить знания по внедрению передовых методов разработки и создания онлайн-приложений, а также по наиболее распространенным ошибкам

03

Руководство курса

Преподаватели - высококвалифицированные профессионалы с солидным опытом работы в сфере ИТ-безопасности. Они имеют углубленную академическую подготовку, подкрепленную специализациями в ключевых областях программирования и кибербезопасности. Кроме того, их практический опыт включает участие в крупных проектах в различных организациях. Таким образом, эти эксперты не только передадут фундаментальные теоретические знания, но и внедрят в преподавание современные методологии и практики, актуальные кейсы и моделирование реальных сценариев угроз и уязвимостей.



Приверженность преподавателей к академическому совершенству и их ориентация на практическое применение обеспечат приобретение вами критически важных навыков для решения задач в области ИТ-безопасности”

Приглашенный руководитель международного уровня

Даррен Палсифер — опытный **архитектор программного обеспечения**, новатор с выдающимся международным послужным списком в области **разработки программного обеспечения и** микропрограмм. Кроме того, он обладает высокоразвитыми навыками **общения**, **управления проектами** и ведения **бизнеса**, что позволило ему возглавить крупные глобальные инициативы.

На протяжении своей карьеры он также занимал ответственные должности, такие как **главный архитектор решений для государственного** сектора в корпорации **Intel**, где он продвигал современный бизнес-**процессы и технологии** для клиентов, партнеров и пользователей в государственном секторе. Кроме того, он основал компанию **Yoly Inc.**, где также занимал пост **генерального директора**, занимаясь созданием **инструментов для агрегации и диагностики социальных сетей** на основе **программного обеспечения как услуга** (SaaS), использующее технологии ***больших данных*** и **Веб** 2.0.

Кроме того, он работал в других компаниях, в том числе **генеральным директором по инженерным** вопросам в **Dell Technologies**, где возглавлял подразделение ***больших данных* в облаке**, руководил командами в **США** и **Китае** по управлению крупными проектами и реструктуризации бизнес-подразделений для успешной интеграции. Он также занимал должность директора по информационным технологиям (***Chief Information Officer*** в компании XanGo, где руководил такими проектами, как поддержка справочной службы, **поддержка производства** и **разработка решений**.

Среди множества специализаций, в которых он является экспертом, выделяется технология ***Edge to Cloud***, **кибербезопасность**, **генеративный искусственный интеллект**, ***разработка программного обеспечения***, **сетевые технологии**, **облачная нативная разработка** и **контейнерная экосистема**. Он делится своими знаниями в еженедельном **подкасте** и **информационном бюллетене "Embracing Digital Transformation"**, который он создал и представил, помогая организациям успешно пройти через **цифровую трансформацию,** используя персонал, **процессы** и **технологии**.

Г-н Палсифер, Даррен

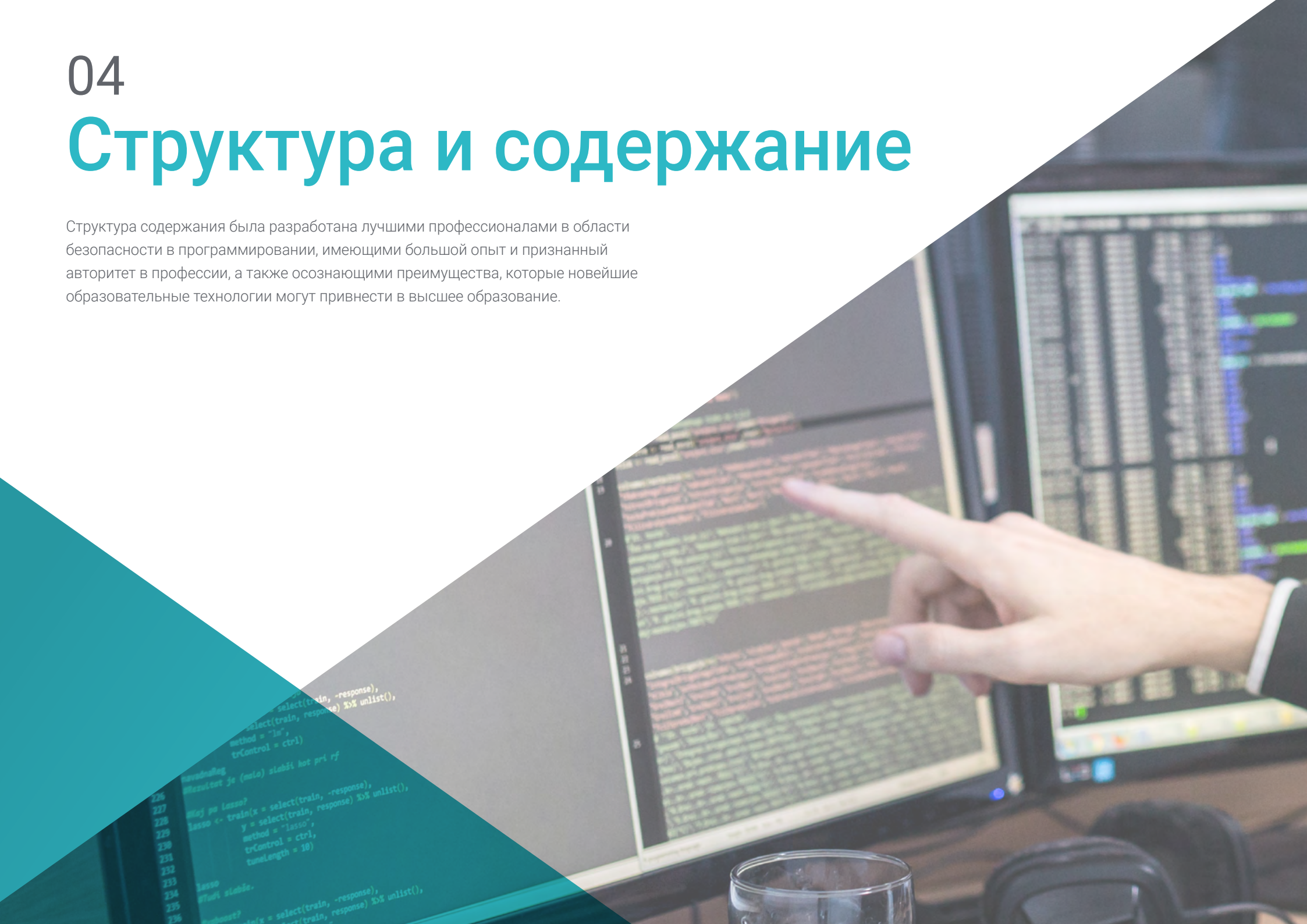
- Главный архитектор решений для государственного сектора, Intel, Калифорния, США
- Ведущий и автор проекта *"Воплощение цифровой трансформации"*, Калифорния, США
- Основатель и генеральный директор компании Yoly Inc., Арканзас
- Генеральный директор по инженерным вопросам в компании Dell Technologies, Арканзас
- Директор по информационным технологиям (*Chief Information Officer*) компании XanGo, Юта
- Старший архитектор в Cadence Design Systems, Калифорния
- Старший менеджер по проектным процессам в Lucent Technologies, Калифорния
- Инженер-программист в компании Cemax-Icon, Калифорния
- Инженер-программист в компании ISG Technologies, Канада
- MBA в области управления технологиями в Университете Феникса, Калифорния
- Степень бакалавра в области информатики и электротехники в Университете Бригама Янга

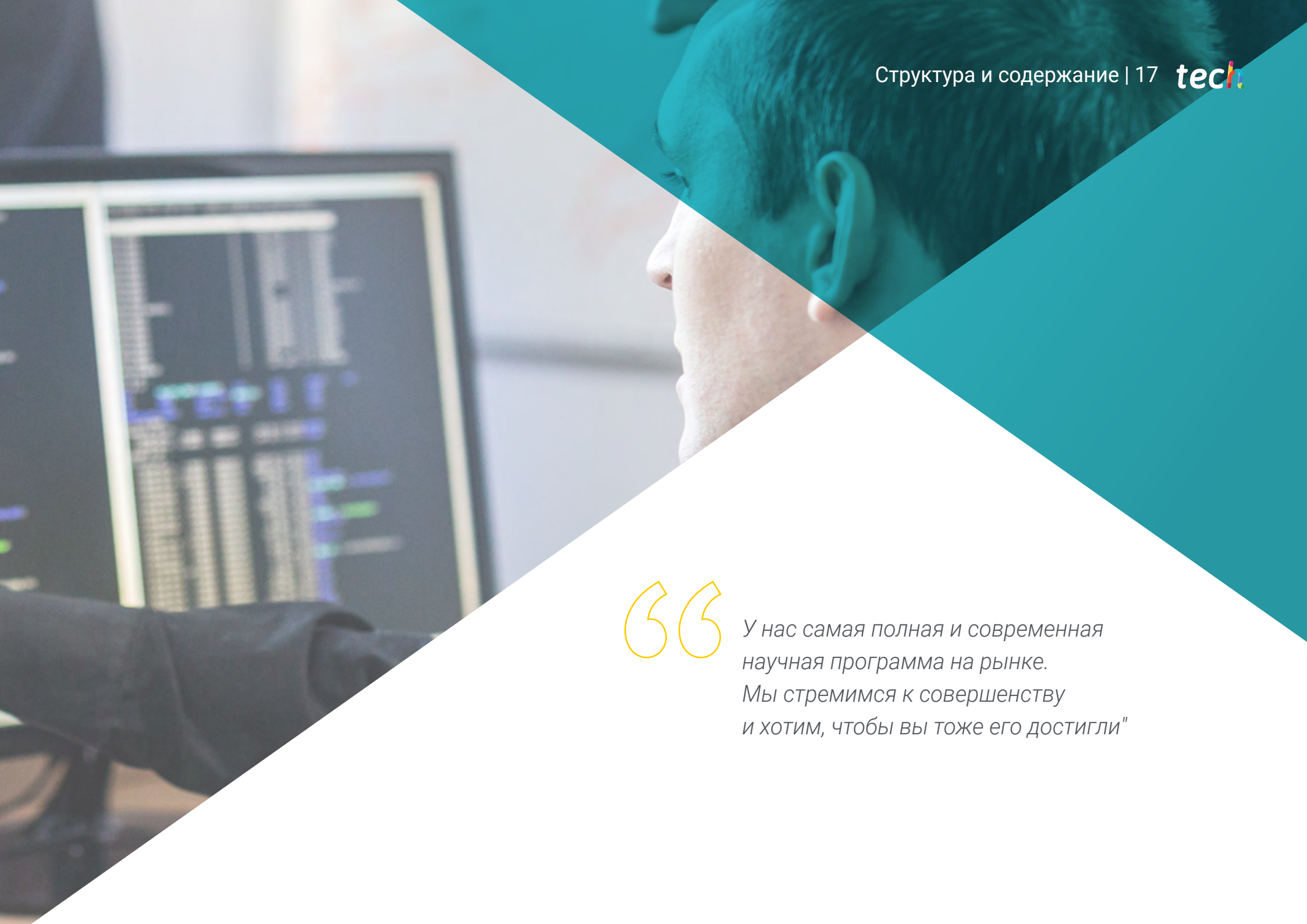
Благодаря TECH вы сможете учиться у лучших мировых профессионалов"

04

Структура и содержание

Структура содержания была разработана лучшими профессионалами в области безопасности в программировании, имеющими большой опыт и признанный авторитет в профессии, а также осознающими преимущества, которые новейшие образовательные технологии могут привнести в высшее образование.





У нас самая полная и современная научная программа на рынке. Мы стремимся к совершенству и хотим, чтобы вы тоже его достигли"

Модуль 1. Управление безопасностью

1.1. Визуализация информации
- 1.1.1. Введение
- 1.1.2. Информационная безопасность подразумевает конфиденциальность, целостность и доступность.
- 1.1.3. Безопасность - это экономический вопрос
- 1.1.4. Безопасность - это процесс
- 1.1.5. Классификация информации
- 1.1.6. Информационная безопасность включает в себя управление рисками
- 1.1.7. Безопасность связана с элементами управления безопасностью
- 1.1.8. Безопасность является как физической, так и логической
- 1.1.9. Безопасность включает в себя людей

1.2. Специалист по информационной безопасности
- 1.2.1. Введение
- 1.2.2. Информационная безопасность как профессия
- 1.2.3. Сертификация (ISC) 2
- 1.2.4. Стандарт ISO 27001
- 1.2.5. Эффективные методы обеспечения безопасности при управлении ИТ-услугами
- 1.2.6. Модели зрелости для информационной безопасности
- 1.2.7. Другие сертификаты, стандарты и профессиональные ресурсы

1.3. Контроль доступа
- 1.3.1. Введение
- 1.3.2. Требования по контролю доступа
- 1.3.3. Механизмы аутентификации
- 1.3.4. Методы авторизации
- 1.3.5. Учет доступа и аудит
- 1.3.6. Технологии тройного А

1.4. Программы, процессы и политики информационной безопасности
- 1.4.1. Введение
- 1.4.2. Программы управления безопасностью
- 1.4.3. Управление рисками
- 1.4.4. Разработка политики безопасности

1.5. Планы обеспечения непрерывности бизнеса
- 1.5.1. Введение в BCP
- 1.5.2. Стадии I и II
- 1.5.3. Стадии III и IV
- 1.5.4. Обслуживание BCP

1.6. Процедуры для надлежащей защиты компании
- 1.6.1. Сети DMZ
- 1.6.2. Системы обнаружения вторжений
- 1.6.3. Требования по контролю доступа
- 1.6.4. Обучение у нападающего: *Honeypot*

1.7. Архитектура безопасности. Профилактика
- 1.7.1. Обзор. Деятельность и многоуровневая модель
- 1.7.2. Защита периметра (*брандмауэры*, WAF, IPS и т.д...)
- 1.7.3. Защита конечных точек (оборудование, серверы и услуги)

1.8. Архитектура безопасности. Обнаружение
- 1.8.1. Обнаружение и мониторинг обзора
- 1.8.2. *Журналы*, зашифрованное разбиение трафика, запись и *Siems*
- 1.8.3. Оповещения и разведка

1.9. Архитектура безопасности. Реакция
- 1.9.1. Реакция Продукты, услуги и ресурсы
- 1.9.2. Управление инцидентами
- 1.9.3. CERTS и CSIRT

1.10. Архитектура безопасности. Восстановление
- 1.10.1. Устойчивость, концепции, бизнес-требования и стандарты
- 1.10.2. Устойчивость ИТ-решений
- 1.10.3. Антикризисное управление и руководство

Модуль 2. Безопасность программного обеспечения

2.1. Вопросы безопасности программного обеспечения
- 2.1.1. Введение в проблему безопасности программного обеспечения
- 2.1.2. Уязвимости и их классификация
- 2.1.3. Защищенные свойства программного обеспечения
- 2.1.4. Референсы

2.2. Принципы проектирования безопасности программного обеспечения
- 2.2.1. Введение
- 2.2.2. Принципы проектирования безопасности программного обеспечения
- 2.2.3. Типы S-SDLC
- 2.2.4. Безопасность программного обеспечения на этапах S-SDLC
- 2.2.5. Методологии и стандарты
- 2.2.6. Референсы

2.3. Безопасность жизненного цикла программного обеспечения на этапах разработки требований и проектирования
- 2.3.1. Введение
- 2.3.2. Моделирование атак
- 2.3.3. Случаи жестокого обращения
- 2.3.4. Разработка требований безопасности
- 2.3.5. Анализ риска. Архитектура
- 2.3.6. Модели проектирования
- 2.3.7. Референсы

2.4. Безопасность жизненного цикла программного обеспечения на этапах кодирования, тестирования и эксплуатации
- 2.4.1. Введение
- 2.4.2. Тестирование безопасности с учетом рисков
- 2.4.3. Обзор кода
- 2.4.4. Тест на проникновение
- 2.4.5. Операции по обеспечению безопасности
- 2.4.6. Внешний обзор
- 2.4.7. Референсы

2.5. Приложения для безопасного кодирования I
- 2.5.1. Введение
- 2.5.2. Практика безопасного кодирования
- 2.5.3. Обработка и проверка записей
- 2.5.4. Переполнение памяти
- 2.5.5. Референсы

2.6. Приложения для безопасного кодирования II
- 2.6.1. Введение
- 2.6.2. *Переполнения целых чисел*, ошибки усечения и проблемы с преобразованием типов между целыми числами
- 2.6.3. Ошибки и исключения
- 2.6.4. Приватность и конфиденциальность
- 2.6.5. Привилегированные программы
- 2.6.6. Референсы

2.7. Безопасность в разработке и в облаке
- 2.7.1. Безопасность в развитии; методология и практика
- 2.7.2. Модели PaaS, IaaS, CaaS и SaaS
- 2.7.3. Безопасность в облаке и для облачных услуг

2.8. Шифрование
- 2.8.1. Основы криптологии
- 2.8.2. Симметричное и асимметричное шифрование
- 2.8.3. Шифрование в состоянии покоя и при транспортировке

2.9. Оркестровка и автоматизация безопасности (SOAR)
- 2.9.1. Сложность ручной обработки; необходимость автоматизации задач
- 2.9.2. Продукты и услуги
- 2.9.3. Архитектура SOAR

2.10. Безопасность при телеработе
- 2.10.1. Потребность и сценарии
- 2.10.2. Продукты и услуги
- 2.10.3. Безопасность при телеработе

Модуль 3. Аудит безопасности

3.1. Введение в информационные системы и их аудит
- 3.1.1. Введение в информационные системы и роль компьютерного аудита
- 3.1.2. Определения понятий "ИТ-аудит" и "внутренний ИТ-контроль"
- 3.1.3. Функции и цели ИТ-аудита
- 3.1.4. Различия между внутренним контролем и ИТ-аудитом

3.2. Внутренний контроль информационных систем
- 3.2.1. Функциональная блок-схема центра обработки данных
- 3.2.2. Классификация средств контроля информационных систем
- 3.2.3. Золотое правило

3.3. Процесс и этапы аудита информационных систем
- 3.3.1. Оценка рисков (EDR) и другие методологии ИТ-аудита
- 3.3.2. Проведение аудита информационных систем. Этапы аудита
- 3.3.3. Ключевые навыки аудитора информационных систем

3.4. Технический аудит безопасности систем и сетей
- 3.4.1. Технические аудиты безопасности. Проверка на вторжение. Предварительные концепции
- 3.4.2. Аудит безопасности в системах. Инструменты поддержки
- 3.4.3. Аудит безопасности в сети. Инструменты поддержки

3.5. Технический аудит безопасности интернета и мобильных устройств
- 3.5.1. Аудит безопасности интернета. Инструменты поддержки
- 3.5.2. Аудит безопасности мобильных устройств. Инструменты поддержки
- 3.5.3. Приложение 1. Структура исполнительного отчета и технического отчета
- 3.5.4. Приложение 2. Инвентаризация инструментов
- 3.5.5. Приложение 3. Методики

3.6. Система управления информационной безопасностью
- 3.6.1. Безопасность ИС: свойства и факторы влияния
- 3.6.2. Общеорганизационный риск и управление рисками: внедрение механизмов контроля
- 3.6.3. Система управления информационной безопасностью (СУИБ): концепция и критические факторы успеха
- 3.6.4. СУИБ - модель PDCA
- 3.6.5. ISMS ISO-IEC 27001: организационный контекст
- 3.6.6. Параграф 4. Организационная трансформация
- 3.6.7. Параграф 5. Лидерство
- 3.6.8. Параграф 6. Планирование
- 3.6.9. Параграф 7. Поддержка
- 3.6.10. Параграф 8. Операция
- 3.6.11. Параграф 9. Оценка эффективности
- 3.6.12. Параграф 10. Улучшение
- 3.6.13. Приложение к ISO 27001/ISO-IEC 27002: цели и средства контроля
- 3.6.14. Аудит СУИБ

3.7. Проведение аудита
- 3.7.1. Процедуры
- 3.7.2. Техники

3.8. Прослеживаемость
- 3.8.1. Методики
- 3.8.2. Анализ

3.9. Хранение
- 3.9.1. Техники
- 3.9.2. Результаты

3.10. Отчетность и представление доказательств
- 3.10.1. Типы отчетов
- 3.10.2. Анализ данных
- 3.10.3. Представление доказательств

Модуль 4. Безопасность в онлайн-приложениях

4.1. Уязвимости и проблемы безопасности в онлайн-приложениях
- 4.1.1. Введение в безопасность в онлайн-приложениях
- 4.1.2. Уязвимости безопасности при разработке веб-приложений
- 4.1.3. Уязвимости безопасности пути внедрения веб-приложений
- 4.1.4. Уязвимости безопасности при развертывания веб-приложений
- 4.1.5. Официальные списки уязвимостей безопасности

4.2. Политики и стандарты для обеспечения безопасности онлайн-приложений
- 4.2.1. Основные принципы обеспечения безопасности онлайн-приложений
- 4.2.2. Политика безопасности
- 4.2.3. Система управления информационной безопасностью
- 4.2.4. Жизненный цикл разработки безопасного программного обеспечения
- 4.2.5. Стандарты безопасности приложений

4.3. Безопасность при разработке веб-приложений
- 4.3.1. Введение в безопасность веб-приложений
- 4.3.2. Безопасность при разработке веб-приложений

4.4. Тестирование онлайн-безопасности веб-приложений
- 4.4.1. Анализ и тестирование безопасности веб-приложений
- 4.4.2. Безопасность при развертывании и производстве веб-приложений

4.5. Безопасность веб-сервисов
- 4.5.1. Введение в безопасность веб-сервисов
- 4.5.2. Функции и технологии обеспечения безопасности веб-сервисов

4.6. Тестирование онлайн безопасности веб-приложений
- 4.6.1. Оценка безопасности веб-сервисов
- 4.6.2. Онлайн-защита. *Брандмауэры и шлюзы* XML

4.7. Этический *хакинг*, *вредоносное ПО и криминалистика*
- 4.7.1. Этичный *хакинг*
- 4.7.2. Анализ *вредоносных программ*
- 4.7.3. Криминалистический анализ

4.8. Разрешение инцидентов для веб-сервисов
- 4.8.1. Мониторинг
- 4.8.2. Инструменты измерения эффективности
- 4.8.3. Меры сдерживания
- 4.8.4. Анализ коренных причин
- 4.8.5. Проактивное управление проблемами

4.9. Эффективные методы обеспечения безопасности приложений
- 4.9.1. Руководство по надлежащей практике разработки онлайн-приложений
- 4.9.2. Руководство по передовой практике внедрения онлайн-приложений

4.10. Распространенные ошибки, подрывающие безопасность приложений
- 4.10.1. Распространенные ошибки при разработке
- 4.10.2. Распространенные ошибки в хостинге
- 4.10.3. Распространенные ошибки в производстве

Комплексная и многопрофильная формате программа, которая позволит вам добиться успехов в карьере, следуя последним достижениям в области фундаментов на скальном и почвенном грунте”

05

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.

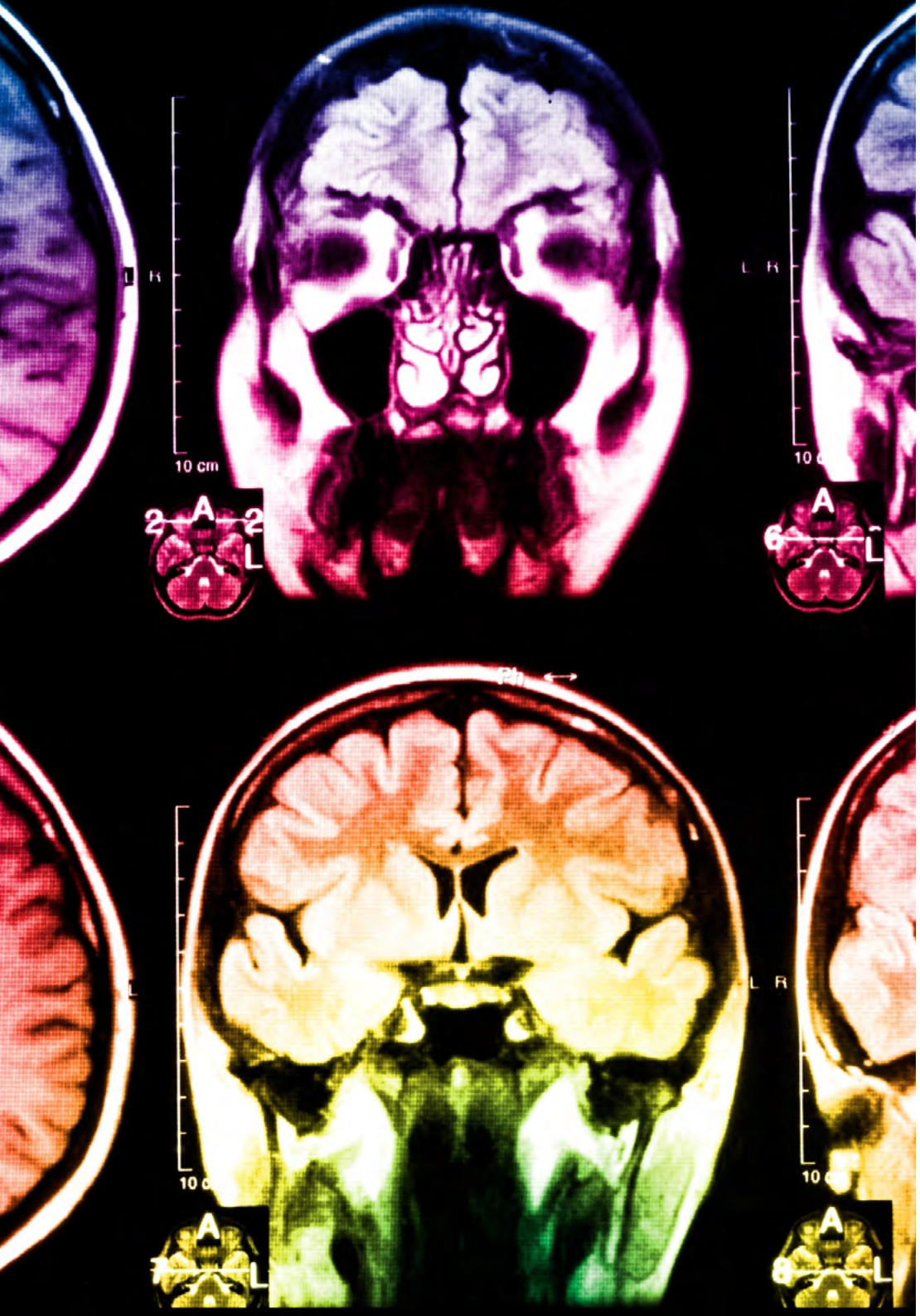
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи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

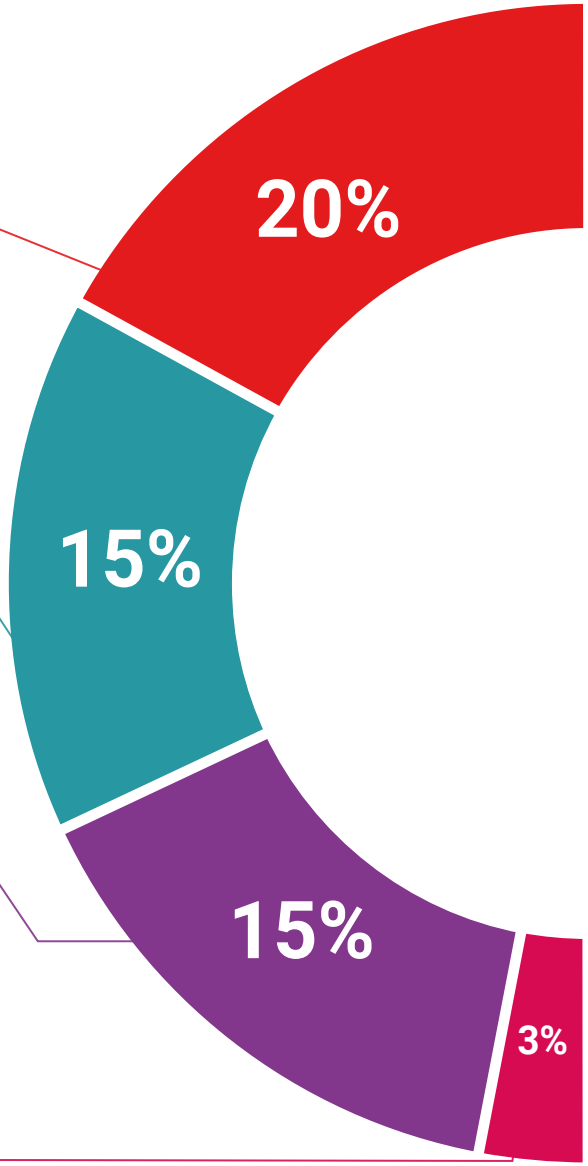
Студенты будут осуществлять деятельность по развитию конкретных компетенций и навыков в каждой предметной области. Практика и динамика приобретения и развития навыков и способностей, необходимых специалисту в рамках глобализации, в которой мы живем.

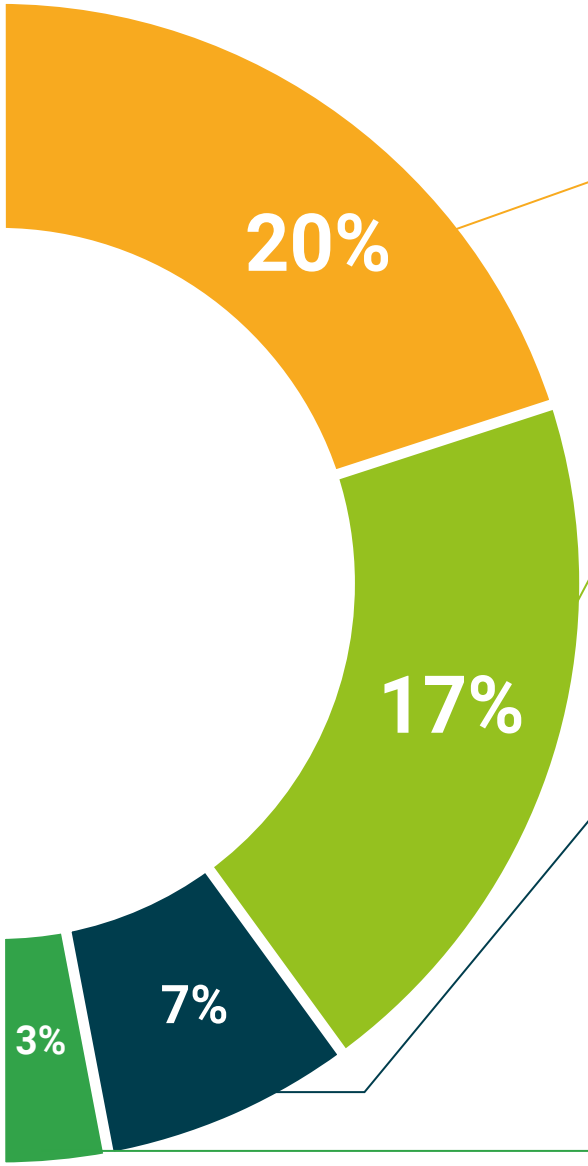
Интерактивные конспекты

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.

06

Квалификация

Курс профессиональной подготовки в области безопасности в программировании гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Курса профессиональной подготовки, выдаваемого TECH Технологическим университетом.

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

Данный **Курс профессиональной подготовки в области безопасности в программировании** содержит самую полную и современную программу на рынке.

После прохождения аттестации студент получит по почте* с подтверждением получения соответствующий диплом о прохождении **Курса профессиональной подготовки**, выданный **TECH Технологическим университетом.**

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

Диплом: **Курс профессиональной подготовки в области безопасности в программировании**

Формат: **онлайн**

Продолжительность: **6 месяцев**


tech технологический университет

Настоящий

ДИПЛОМ

свидетельствует о том, что

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

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

КУРС ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

в области

безопасности в программировании

Данный диплом специализированной программы, присуждаемый Университетом, соответствует 600 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

*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

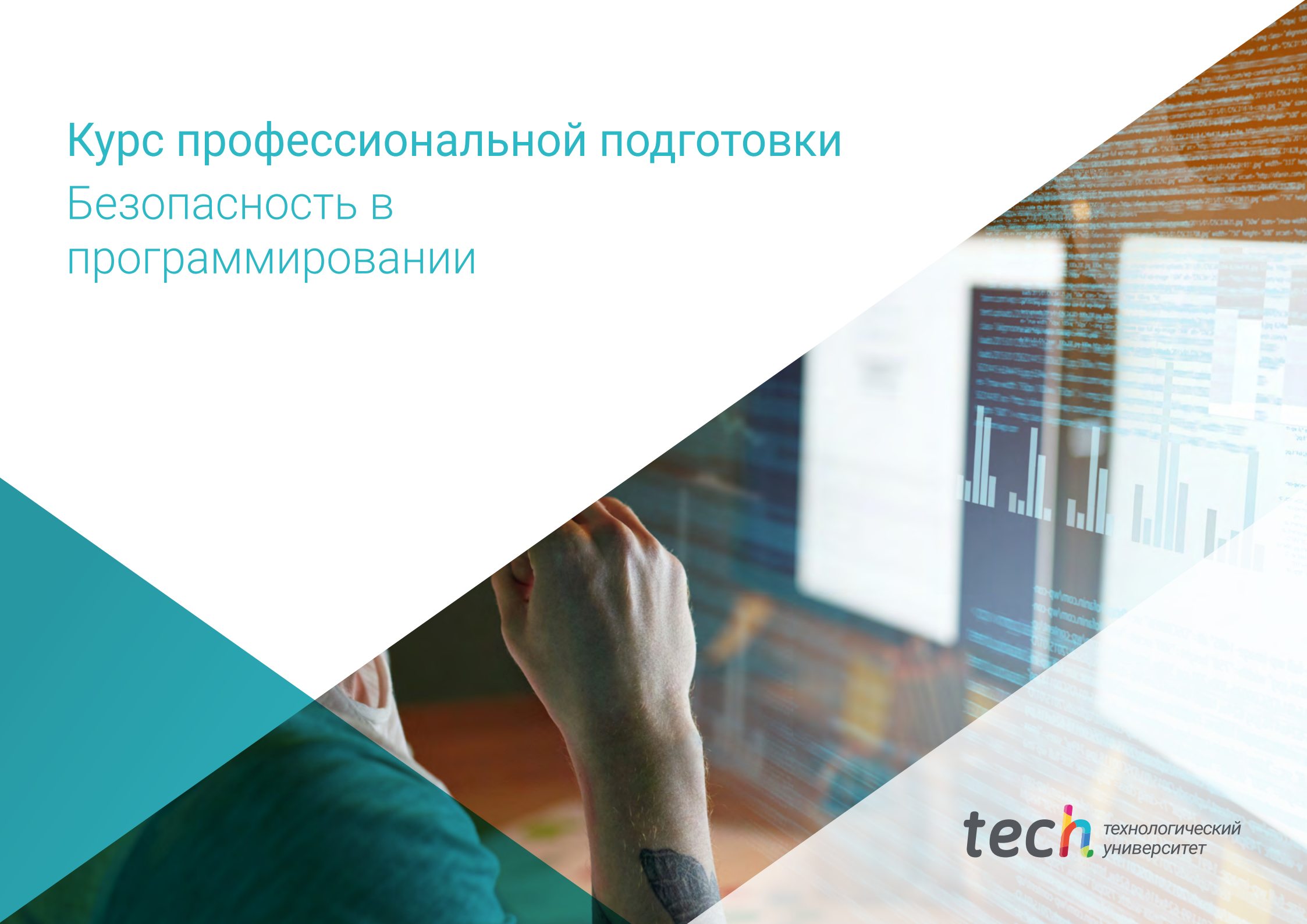
Курс профессиональной подготовки

Безопасность в программировании

- Формат: **онлайн**
- Продолжительность: **6 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**

Курс профессиональной подготовки

Безопасность в программировании



tech технологический университет