Бизнес-магистратура

Управление политикой кибербезопасности в компании

tech технологический университет

технологический университет

Бизнес-магистратура

Управление политикой кибербезопасности в компании

- Формат: **онлайн**
- Продолжительность: **12 месяцев**
- Учебное заведение: **TECH Технологический университет**
- Расписание: **по своему усмотрению**
- Экзамены: **онлайн**
- Программа предназначена для: **выпускников университетов и дипломированных специалистов, ранее окончивших любую из специальностей в области социальных, юридических, административных и бизнес-наук**

Веб-доступ: www.techtitute.com/ru/school-of-business/executive-master-degree/master-corporate-cybersecurity-policy-management

Оглавление

01

Добро пожаловать

Сегодня убытки от кибератак исчисляются миллионами и далеко не единицами. Подверженность кибератакам такова, что даже государства могут стать мишенью киберинцидентов. Это подчеркивает важность наличия специализированных менеджеров по управлению политикой кибербезопасности, обладающих необходимыми инструментами организации, внедрения и мониторинга для координации всех усилий по обеспечению кибербезопасности. Данная программа готовит менеджеров к работе в неопределенных сценариях с учетом требований безопасности и передовых знаний, обеспечивая качественные решения в области информационной безопасности. Благодаря исчерпывающему теоретическому материалу, основанному на реальных примерах, вы получите современное и комплексное представление обо всех функциях, которые должен выполнять менеджер по кибербезопасности. И все это — в 100% онлайн-формате, без очных занятий и заранее установленного расписания, с полной гибкостью.

Бизнес-магистратура в области управления политикой кибербезопасности в компании TECH Технологического университета

Данная программа приносит неисчислимую пользу вашей политике кибербезопасности, зная все ее нюансы, начиная от самих систем безопасности и заканчивая практикой анализа угроз, которая даст вам ключи к позиционированию себя как преимущества в вашей организации"

02

Почему стоит учиться в TECH?

TECH — это крупнейшая бизнес-школа 100% онлайн-формата в мире. Мы являемся элитной бизнес-школой с образовательной моделью с самыми высокими академическими стандартами. Международный высокопроизводительный центр интенсивного обучения управленческим навыкам.

TECH — это передовой технологический университет, который предоставляет все свои ресурсы в распоряжение студентов, чтобы помочь им достичь успеха в бизнесе"

В TECH Технологического университета

Инновации

Мы предлагаем вам модель онлайн-обучения, сочетающую в себе новейшие образовательные технологии и максимальную педагогическую строгость. Уникальный метод с высочайшим международным признанием, который даст вам возможность развиваться в мире постоянных перемен, где инновации играют ключевую роль в деятельности каждого предпринимателя.

"История успеха Microsoft Europe" за включение в программы инновационной интерактивной мультивидеосистемы.

Высокие требования

Чтобы поступить в TECH, не потребуется большие затраты. Чтобы учиться у нас, вам не нужно делать большие инвестиции. Однако для того, чтобы получить диплом в TECH, необходимо проверить уровень знаний и возможностей студента. Наши академические стандарты очень высоки...

95% | **студентов TECH успешно завершают обучение**

Нетворкинг

Профессионалы со всего мира принимают участие в TECH, чтобы вы смогли создать большую сеть контактов, полезных для вашего будущего.

100 000+

менеджеров, прошедших ежегодную подготовку

200+

разных национальностей

Расширение прав и возможностей

Развивайтесь наряду с лучшими компаниями и профессионалами, обладающими большим авторитетом и влиянием. Мы создали стратегические альянсы и ценную сеть контактов с основными экономическими субъектами на 7 континентах.

+500+ | **соглашений о сотрудничестве с лучшими компаниями**

Талант

Наша программа - это уникальное предложение для раскрытия вашего таланта в мире бизнеса. Возможность, с помощью которой вы сможете заявить о своих интересах и видении своего бизнеса.

TECH помогает студентам показать миру свой талант при прохождении этой программы.

Мультикультурный контекст

Обучаясь в TECH, студенты могут получить уникальный опыт. Вы будете учиться в многокультурном контексте. В данной программе мы применяем глобальный подход, благодаря которому вы сможете узнать о том, как работают в разных частях света, собрать самую свежую информацию, которая наилучшим образом соответствует вашей бизнес-идее.

Наши студенты представляют более 200 национальностей.

Учитесь у лучших

Наши преподаватели объясняют в аудиториях, что привело их к успеху в их компаниях, работая в реальном, живом и динамичном контексте. Преподаватели, которые полностью посвящают себя тому, чтобы предложить вам качественную специализацию, которая позволит вам продвинуться по карьерной лестнице и выделиться в мире бизнеса.

Преподаватели представляют 20 различных национальностей.

В TECH у вас будет доступ к самому строгому и современному методу кейсов в академической среде"

TECH стремится к совершенству и для этого обладает рядом характеристик, которые делают его уникальным университетом:

Анализ

TECH исследует критическую сторону студента, его способность задавать вопросы, навыки решения проблем и навыки межличностного общения.

Академическое превосходство

TECH предлагает студентам лучшую методику онлайн-обучения. Университет сочетает метод *Relearning* (наиболее признанная во всем мире методология последипломного обучения) с «методом кейсов» Гарвардской школы бизнеса. Традиции и современность в сложном балансе и в контексте самого требовательного академического маршрута.

Экономия за счет масштаба

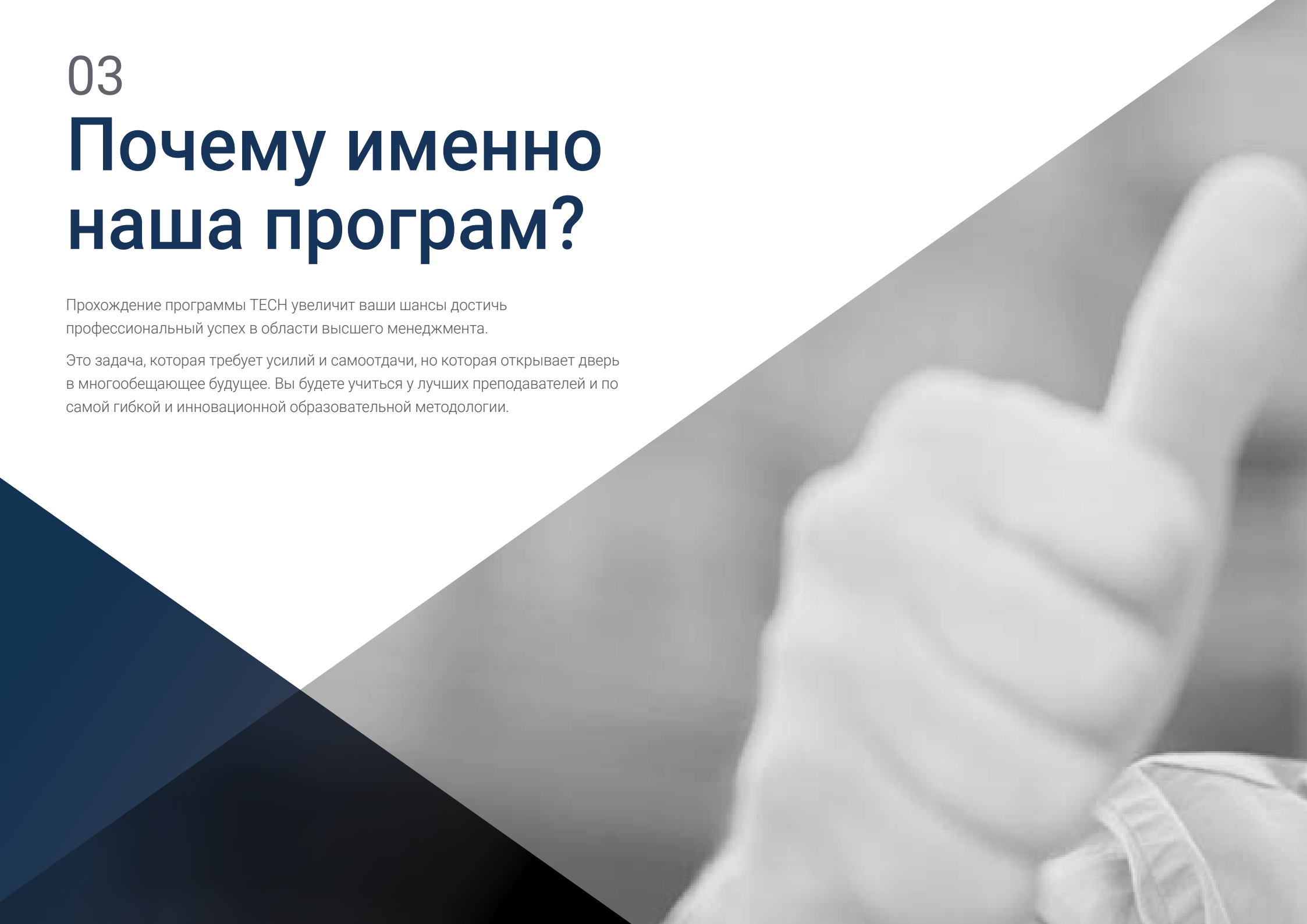
TECH — крупнейший в мире онлайн-университет. В его портфолио насчитывается более 10 000 университетских последипломных программ. А в новой экономике **объем + технология = разорительная цена**. Таким образом, мы заботимся о том, чтобы учеба для вас была не такой дорогой, как в другом университете.

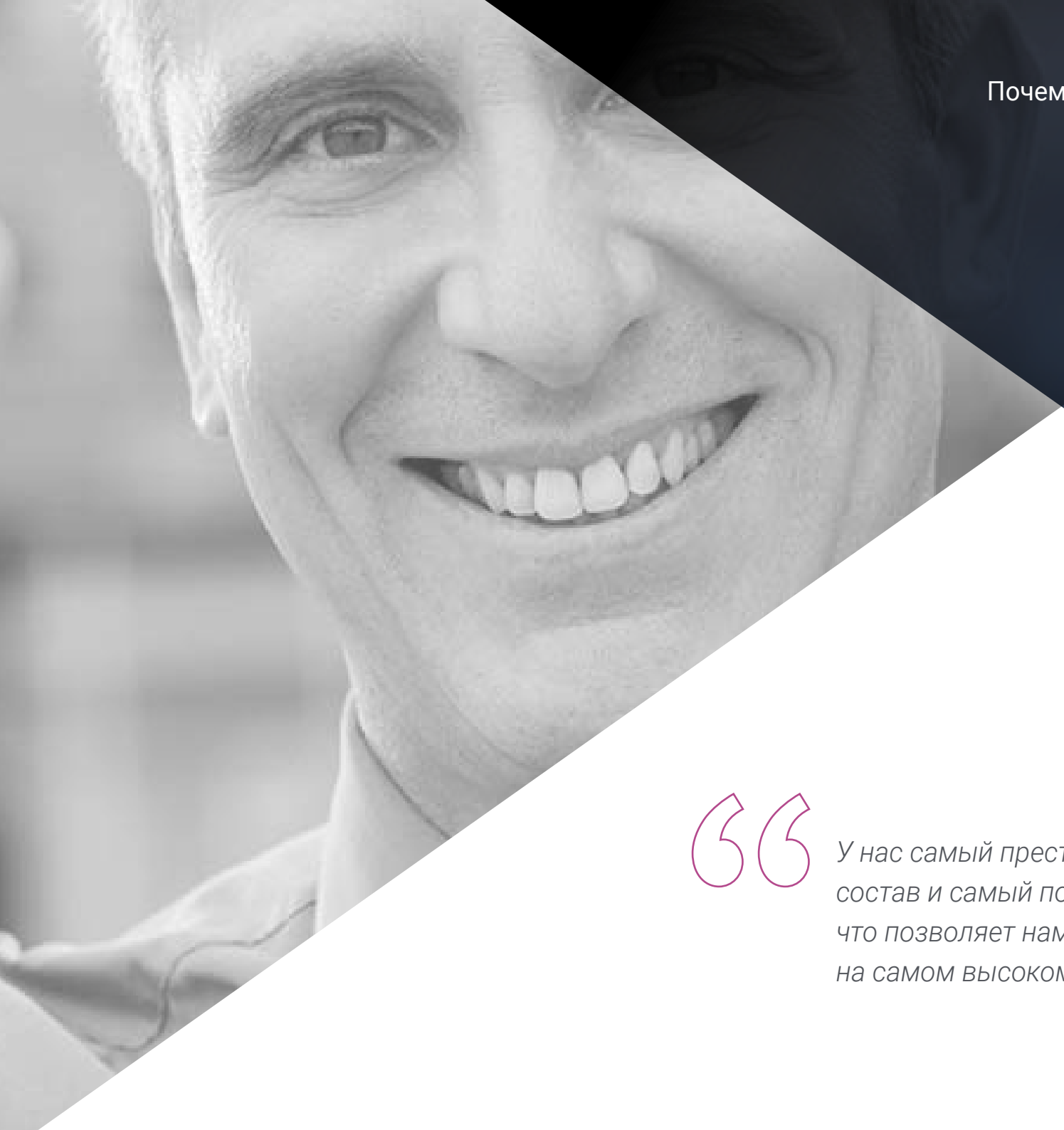
03

Почему именно наша програм?

Прохождение программы TECH увеличит ваши шансы достичь профессиональный успех в области высшего менеджмента.

Это задача, которая требует усилий и самоотдачи, но которая открывает дверь в многообещающее будущее. Вы будете учиться у лучших преподавателей и по самой гибкой и инновационной образовательной методологии.





У нас самый престижный преподавательский состав и самый полный учебный план на рынке, что позволяет нам предложить вам обучение на самом высоком академическом уровне"

Эта программа обеспечит вам множество преимуществ в трудоустройстве и вопросах личностного развития, включая следующие:

01

Дать решающий толчок карьере студента

Мы даем вам возможность взять под контроль свое будущее и полностью раскрыть свой потенциал. Пройдя нашу программу, вы приобретете необходимые навыки, чтобы за короткий срок добиться положительных изменений в своей карьере.

70% студентов этой специализации добиваются успешных изменений в своей карьере менее чем за 2 года.

02

Разрабатывать стратегическое и глобальное видение компании

Мы предлагаем вам глубокое понимание общего менеджмента, чтобы вы узнали, как каждое решение влияет на различные функциональные области компании.

Наше глобальное видение компании улучшит ваше стратегическое мышление.

03

Закрепиться в высшем руководстве предприятия

Обучение в TECH открывает двери в профессиональную среду, в которой студенты смогут позиционировать себя в качестве руководителей высокого уровня, обладающих широким видением международной среды.

Вы будете работать над более чем 100 реальными кейсами из области высшего менеджмента.

04

Брать на себя новые обязанности

Мы покажем вам последние тенденции, разработки и стратегии для осуществления вашей профессиональной деятельности в меняющихся условиях.

45% наших студентов получают повышение внутри компании.

05

Получить доступ к мощной сети контактов

TECH формирует своих студентов, чтобы максимально расширить их возможности. Студенты с теми же интересами и желанием развиваться. Таким образом, можно будет обмениваться контактами партнеров, клиентов или поставщиков.

Вы найдете сеть контактов, необходимых для вашего профессионального развития.

06

Разрабатывать свой бизнес-проект в строгой последовательности

Вы получите глубокое стратегическое видение, которое поможет вам разработать собственный проект, принимая во внимание различные направления деятельности компании.

20% наших студентов разрабатывают собственную бизнес-идею.

07

Совершенствовать свои *софт-скиллы* и управленческие умения

Мы помогаем вам применять и развивать полученные знания и совершенствовать навыки межличностного общения, чтобы стать лидером, который меняет мир к лучшему.

Улучшите свои коммуникативные и лидерские навыки и продвигайтесь по карьерной лестнице.

08

Стать частью эксклюзивного сообщества

Мы предлагаем вам возможность стать частью сообщества элитных менеджеров, крупных компаний, известных институтов и квалифицированных преподавателей из самых престижных университетов мира: сообщества TECH Технологического университета.

Мы даем вам возможность специализироваться с командой признанных преподавателей на международной сцене.

04

Цели

Поскольку кибербезопасность является одним из важнейших аспектов развития любой современной компании, цель данной программы не может быть иной, как предложить наилучшую подготовку в области управления политикой кибербезопасности. Для этого группа экспертов в области информационных технологий подготовила комплексный учебный материал, полностью ориентированный на совершенствование навыков, компетенций и умений менеджеров.

Руководите кибербезопасностью своей организации, изучив все тонкости наиболее эффективных политик кибербезопасности"

TECH делает цели своих студентов своими собственными
Мы работаем вместе для достижения этих целей

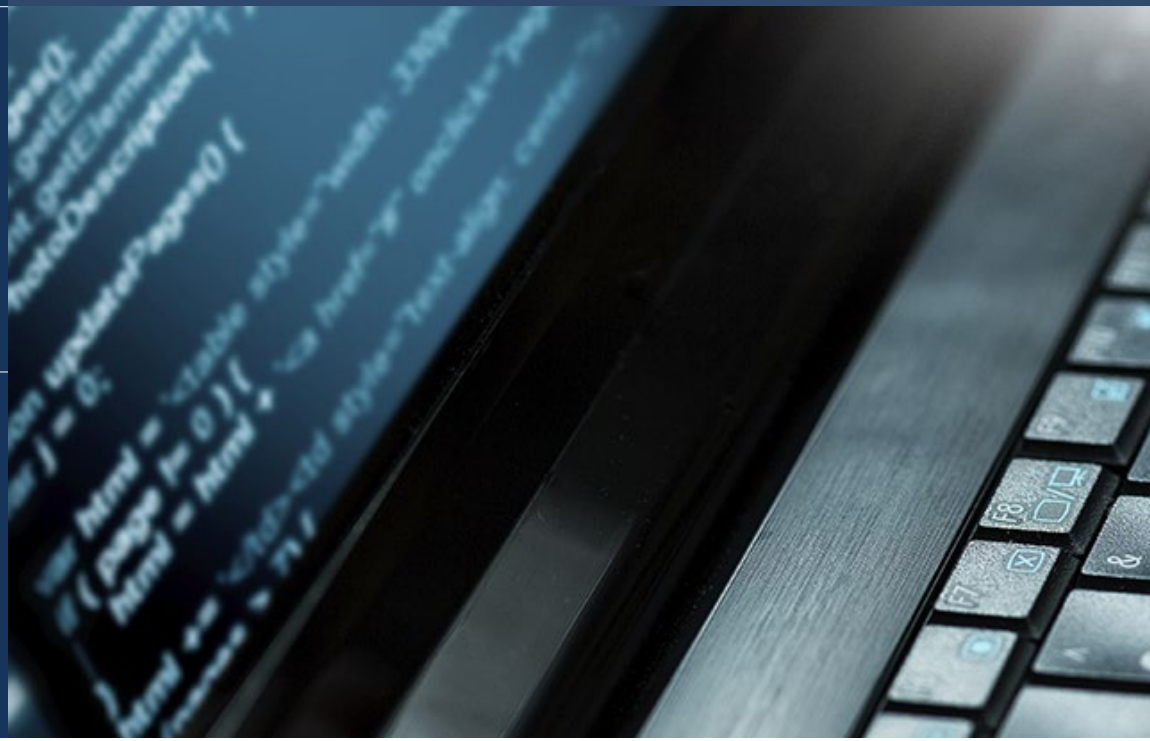
Бизнес-магистратура в области управления политикой кибербезопасности в компании научит студентов:

01 Расширить понимание основных концепций информационной безопасности

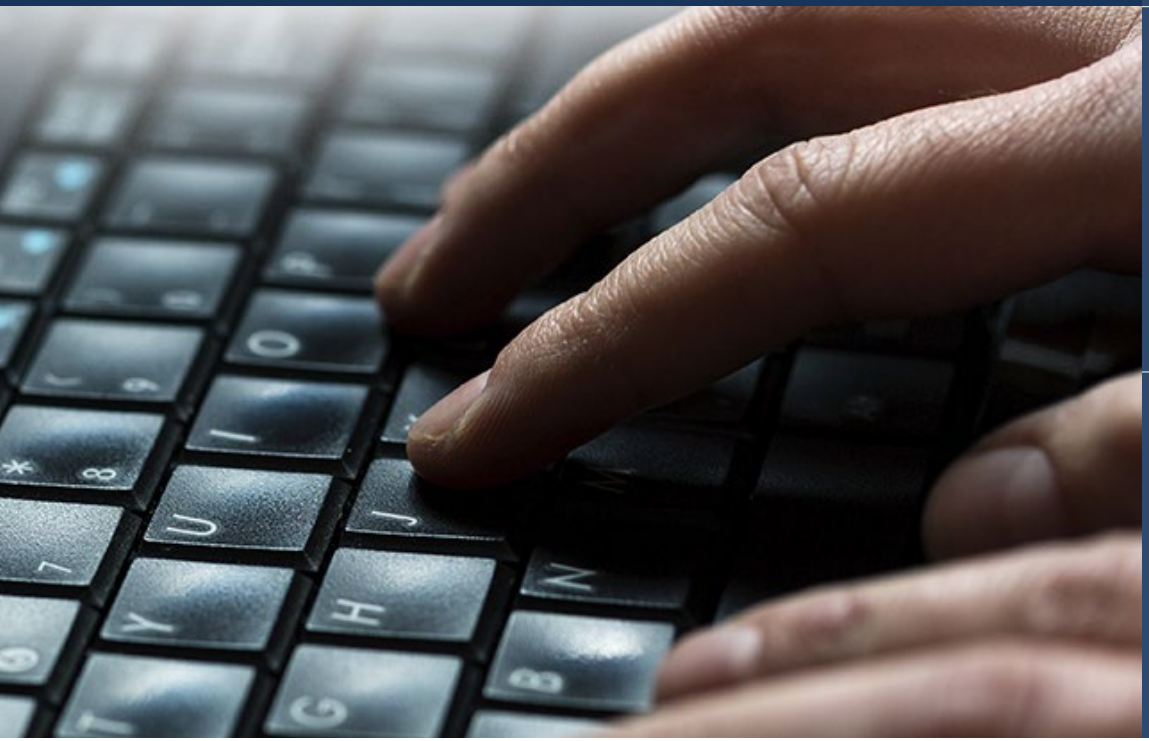
02 Проанализировать нормы и стандарты, применимые в настоящее время к СУИБ

03 Внедрить СУИБ в компании

04 Определить, какие департаменты должно охватывать внедрение системы управления безопасностью



05 Разработать необходимые меры для обеспечения эффективной практики в области информационной безопасности



06 Определить, что такое аутентификация и идентификация

07 Проанализировать различные доступные методы аутентификации и их практическую реализацию

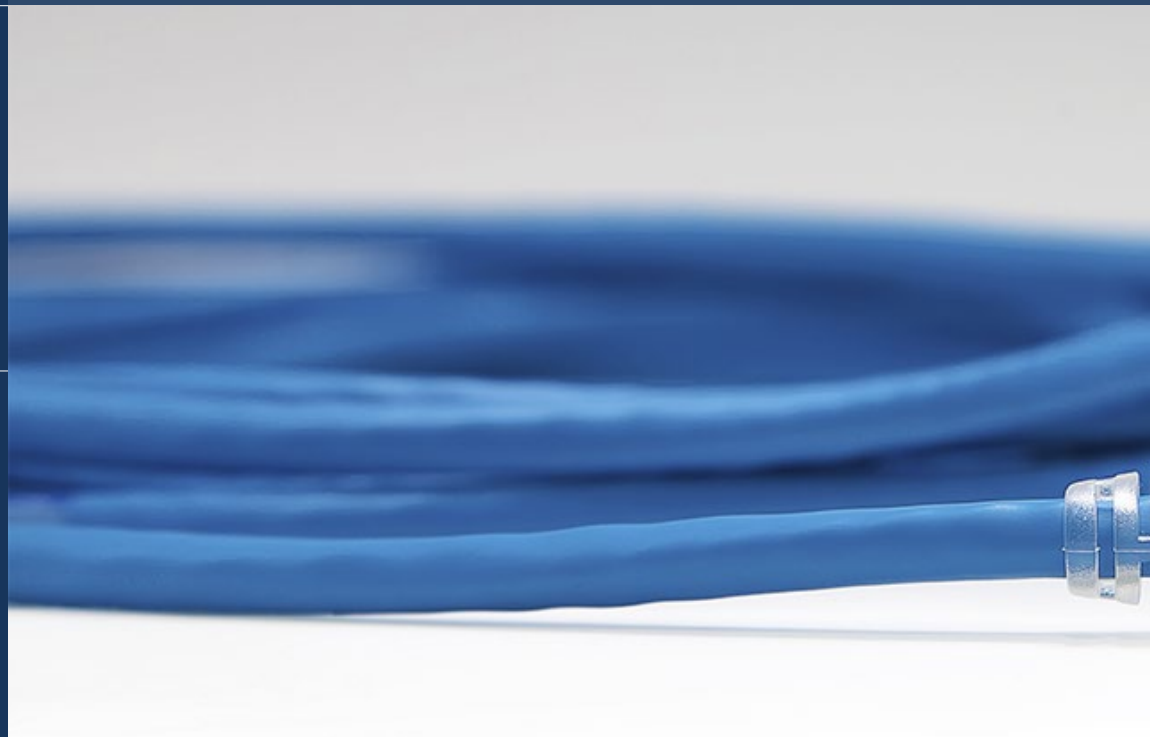
08 Реализовать правильную политику контроля доступа к программному обеспечению и системам

09 Развивать знания о том, как управлять инцидентами, вызванными событиями в области IT-безопасности

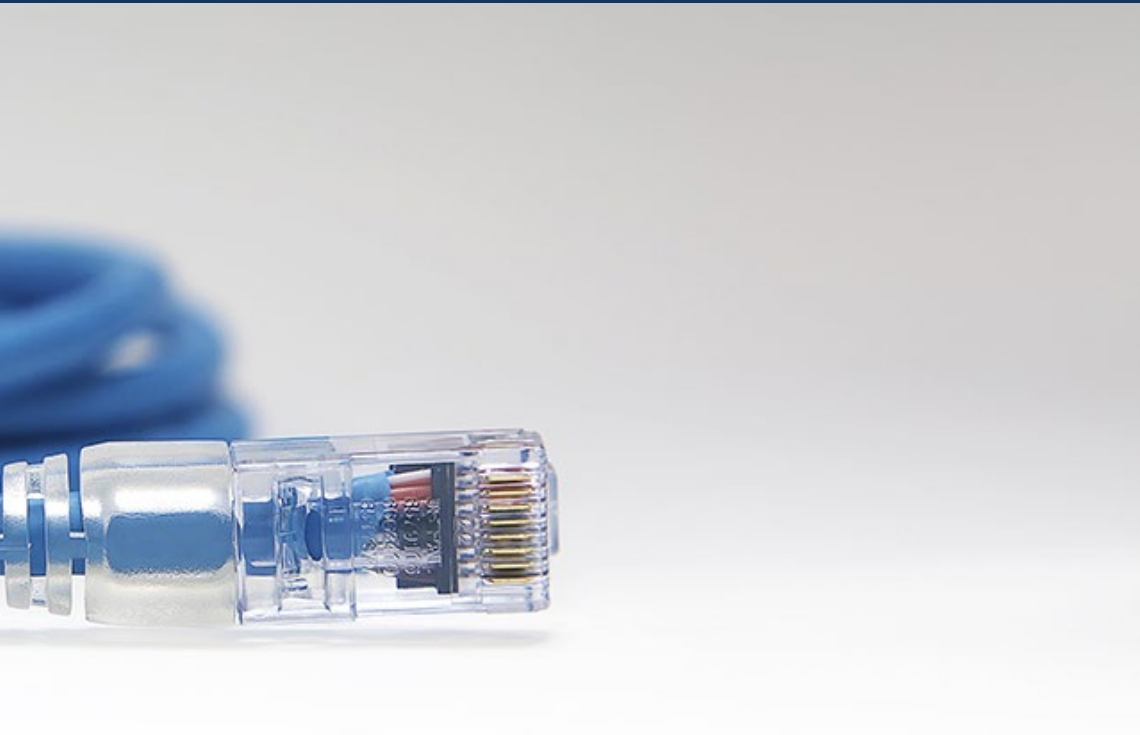
10 Проанализировать понятия "безопасная зона" и "безопасный периметр"

11 Проанализировать различные алгоритмы шифрования, используемые в сетях связи

12 Определить различные реальные атаки на нашу информационную систему



13 Оценить различные политики безопасности для смягчения последствий атак



14 Разработать концепцию мониторинга и внедрения метрик

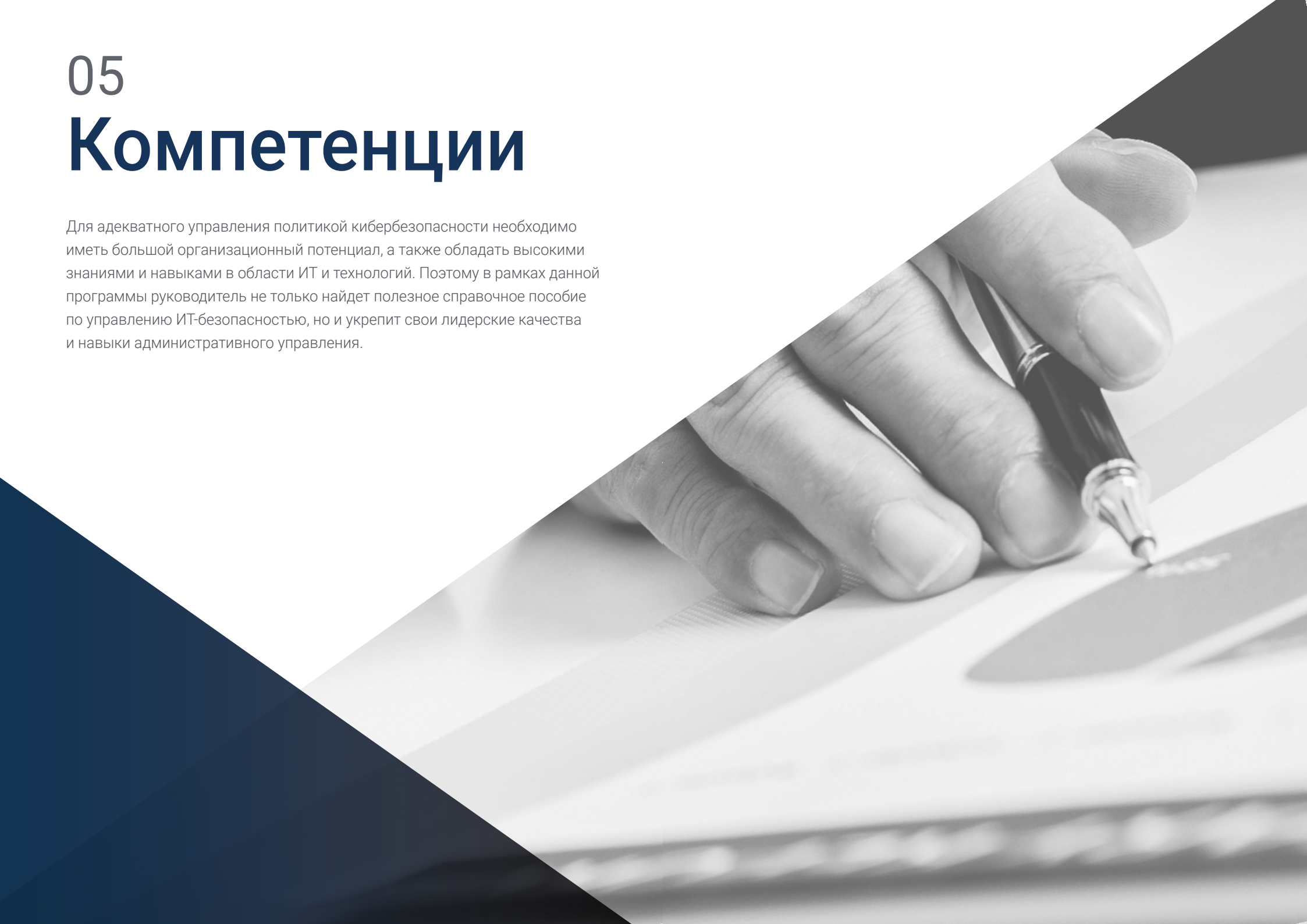
15 Сформировать экспертизу концепции непрерывности информационной безопасности

16 Определить, что такое криптография, и виды криптографии

05

Компетенции

Для адекватного управления политикой кибербезопасности необходимо иметь большой организационный потенциал, а также обладать высокими знаниями и навыками в области ИТ и технологий. Поэтому в рамках данной программы руководитель не только найдет полезное справочное пособие по управлению ИТ-безопасностью, но и укрепит свои лидерские качества и навыки административного управления.



Вы отточите навыки, необходимые для успешной работы в качестве эксперта-менеджера в области политики кибербезопасности, что даст вам преимущество при занятии руководящих должностей"

01 Определить вовлеченность СУИБ во внутреннюю организацию, а также его статус

02 Внедрить политику безопасности в компании

03 Определить, какие меры нам необходимо осуществить в отношении поставщиков и обслуживания информационных систем

04 Сформировать специализированные знания по контролю угроз

05 Определить этапы превентивного управления угрозами

06 Разработать методологии для анализа киберугроз

07 Классифицировать угрозы по степени воздействия и серьезности

08 Разработать собственную методику анализа и превентивного контроля угроз

09 Внедрить правильную политику контроля доступа к сетям и службам

10 Проанализировать важность правильной обработки инцидентов безопасности

11 Составьте подборку различных существующих биометрических систем

12 Изучить биометрию и биометрические системы

13 Внедрить правильные политики физической безопасности и системы контроля физического доступа в центрах обработки данных

14 Создать безопасную сеть

15 Изучить уязвимости в мобильных и IoT платформах и как их избежать

16 Определить виды социальной инженерии и узнать, как их смягчить

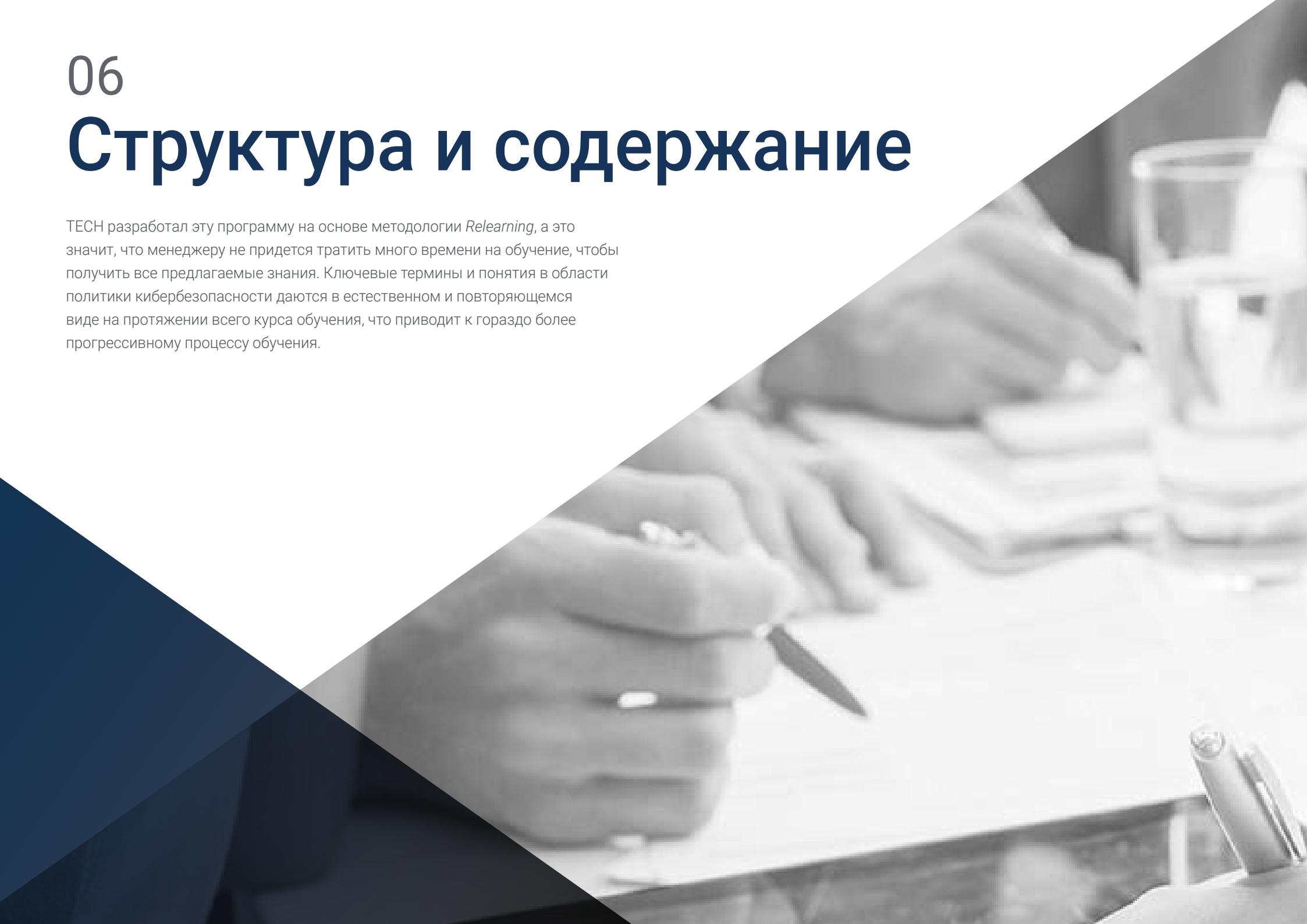
17 Проанализировать концепцию мониторинга и внедрения метрики

18 Определить необходимость обеспечения непрерывности информационной безопасности

06

Структура и содержание

TECH разработал эту программу на основе методологии *Relearning*, а это значит, что менеджеру не придется тратить много времени на обучение, чтобы получить все предлагаемые знания. Ключевые термины и понятия в области политики кибербезопасности даются в естественном и повторяющемся виде на протяжении всего курса обучения, что приводит к гораздо более прогрессивному процессу обучения.



Вы сможете свободно входить в виртуальный класс 24 часа в сутки, выбирая и подстраивая темп обучения под свои интересы"

Учебный план

Бизнес-магистратура в области управления политикой кибербезопасности в компании от TECH Технологического университета — это интенсивная программа, которая готовит студентов к работе в наиболее сложных областях кибербезопасности бизнеса.

Содержание Бизнес-магистратура в области управления политикой кибербезопасности в компании призвано способствовать развитию управленческих навыков, позволяющих принимать более взвешенные решения в условиях неопределенности.

Данная Бизнес-магистратура углубленно рассматривает цифровой мир, безопасность в этой среде и становление электронной коммерции в компаниях и предназначена для подготовки специалистов, понимающих управление политикой кибербезопасности в компании со стратегической, международной и инновационной точек зрения.

Данная Бизнес-магистратура рассчитана на 12 месяцев и состоит из 10 модулей:

Модуль 1	Система управления информационной безопасностью (СУИБ)
Модуль 2	Организационные аспекты политики информационной безопасности
Модуль 3	Политика безопасности для анализа угроз компьютерных систем
Модуль 4	Практическая реализация политик безопасности в software и hardware
Модуль 5	Политика управления инцидентами безопасности
Модуль 6	Внедрение политики физической и экологической безопасности в компании
Модуль 7	Политика безопасной коммуникации в компаниях
Модуль 8	Практическая реализация политики безопасности перед угрозой атак
Модуль 9	Инструменты мониторинга в политике безопасности информационных систем
Модуль 10	Практическая политика аварийного восстановления системы безопасности

Где, когда и как учиться?

TECH предлагает возможность освоения данной Бизнес-магистратура в области управления политикой кибербезопасности в компании в полностью онлайн-режиме. В течение 12 месяцев обучения вы сможете в любое время получить доступ ко всему содержанию данной программы, что позволит вам самостоятельно управлять учебным временем.

Уникальный, ключевой и решающий опыт обучения для повышения вашего профессионального роста"

Модуль 1. Система управления информационной безопасностью (СУИБ)

1.1. Информационная безопасность. Основные вопросы
1.1.1. Информационная безопасность
1.1.1.1. Конфиденциальность
1.1.1.2. Целостность
1.1.1.3. Доступность
1.1.1.4. Меры информационной безопасности

1.2. Система управления информационной безопасностью
1.2.1. Модели управления информационной безопасностью
1.2.2. Документы для внедрения СУИБ
1.2.3. Уровни и средства контроля СУИБ

1.3. Международные нормы и стандарты
1.3.1. Международные стандарты в области информационной безопасности
1.3.2. Происхождение и эволюция стандарта
1.3.3. Международные стандарты управления информационной безопасностью
1.3.4. Другие справочные нормы

1.4. Нормы ISO/IEC 27.000
1.4.1. Предмет и область применения
1.4.2. Структура нормы
1.4.3. Сертификация
1.4.4. Этапы аккредитации
1.4.5. Преимущества норм ISO/IEC 27.000

1.5. Разработка и внедрение общей системы информационной безопасности
1.5.1. Этапы внедрения системы общей информационной безопасности
1.5.2. План по обеспечению непрерывности бизнеса

1.6. Фаза I: диагностика
1.6.1. Предварительная диагностика
1.6.2. Определение уровня стратификации
1.6.3. Уровень соответствия стандартам/нормам

1.7. Фаза II: подготовка
1.7.1. Организационная трансформация
1.7.2. Анализ применимых правил техники безопасности
1.7.3. Сфера применения общей системы информационной безопасности
1.7.4. Политика общей системы информационной безопасности
1.7.5. Цели общей системы информационной безопасности

1.8. Фаза III: планирование
1.8.1. Классификация активов
1.8.2. Оценка рисков
1.8.3. Выявление угроз и рисков

1.9. Фаза IV: реализация и мониторинг
1.9.1. Анализ результатов
1.9.2. Распределение обязанностей
1.9.3. Сроки выполнения плана действий
1.9.4. Мониторинг и аудит

1.10. Политика безопасности в управлении инцидентами
1.10.1. Стадии
1.10.2. Категоризация инцидентов
1.10.3. Управление и процедуры в случае инцидентов

Модуль 2. Организационные аспекты политики информационной безопасности

2.1. Внутренняя организация
2.1.1. Распределение обязанностей
2.1.2. Разделение обязанностей
2.1.3. Контакты с органами власти
2.1.4. Информационная безопасность в управлении проектами

2.2. Управление активами
2.2.1. Ответственность за активы
2.2.2. Классификация информации
2.2.3. Обращение с носителями информации

2.3. Политики безопасности в бизнес-процессах
2.3.1. Анализ уязвимых бизнес-процессов
2.3.2. Анализ влияния на бизнес
2.3.3. Классификация процессов по степени влияния на бизнес

2.4. Политики безопасности, связанные с человеческими ресурсами
2.4.1. До приема на работу
2.4.2. Во время приема на работу
2.4.3. Увольнение или изменение должности

2.5. Политика безопасности управления
2.5.1. Руководство по управлению информационной безопасностью
2.5.2. BIA — анализ воздействия
2.5.3. План восстановления как политика безопасности

2.6. Приобретение и обслуживание информационных систем
2.6.1. Требования к безопасности информационных систем
2.6.2. Безопасность данных разработки и поддержки
2.6.3. Данные тестирования

2.7. Безопасность в отношениях с поставщиками
2.7.1. IT-безопасность с поставщиками
2.7.2. Управление предоставлением услуг с гарантией
2.7.3. Безопасность цепи поставок

2.8. Эксплуатационная безопасность
2.8.1. Обязанности в процессе эксплуатации
2.8.2. Защита от вредоносного кода
2.8.3. Резервные копии
2.8.4. Записи о деятельности и мониторинге

2.9. Управление безопасностью и нормативно-правовым регулированием
2.9.1. Соблюдение требований законодательства
2.9.2. Проверки информационной безопасности

2.10. Безопасность в обеспечении непрерывности бизнеса
2.10.1. Непрерывность информационной безопасности
2.10.2. Резервирование

Модуль 3. Политика безопасности для анализа угроз компьютерных систем

3.1. Управление угрозами в политике безопасности
3.1.1. Управление рисками
3.1.2. Риск безопасности
3.1.3. Методологии в управлении угрозами
3.1.4. Внедрение методологий

3.2. Этапы управления угрозами
3.2.1. Идентификация
3.2.2. Анализ
3.2.3. Локализация
3.2.4. Защитные меры

3.3. Аудит систем на предмет обнаружения угроз
3.3.1. Классификация и информационный поток
3.3.2. Анализ уязвимых процессов

3.4. Классификация рисков
3.4.1. Виды рисков
3.4.2. Расчет вероятности возникновения угрозы
3.4.3. Остаточный риск

3.5. Обработка риска
3.5.1. Осуществление мер по обеспечению безопасности
3.5.2. Передача или поглощение

3.6. Контроль рисков
3.6.1. Непрерывный процесс управления рисками
3.6.2. Внедрение метрики безопасности
3.6.3. Стратегическая модель метрики информационной безопасности

3.7. Практические методологии анализа и контроля угроз
3.7.1. Список угроз
3.7.2. Список контрольных мероприятий
3.7.3. Список мер обеспечения безопасности

3.8. Стандарт ISO 27005
3.8.1. Идентификация рисков
3.8.2. Анализ риска
3.8.3. Оценка рисков

3.9. Матрица рисков, воздействий и угроз
3.9.1. Данные, системы и персонал
3.9.2. Вероятность возникновения угрозы
3.9.3. Размер ущерба

3.10. Разработка этапов и процессов анализа угроз
3.10.1. Выявление критических элементов организации
3.10.2. Определение угроз и последствий
3.10.3. Анализ последствий и рисков
3.10.4. Методики

Модуль 4. Практическая реализация политик безопасности в software и hardware

4.1. Практическая реализация политик безопасности в software и hardware
4.1.1. Осуществление идентификации и авторизации
4.1.2. Внедрение методов идентификации
4.1.3. Средства технической авторизации

4.2. Технологии идентификации и авторизации
4.2.1. Идентификатор и OTP
4.2.2. USB-токен или смарт-карта PKI
4.2.3. Ключ "Конфиденциальная защита"
4.2.4. Активная RFID метка

4.3. Политики безопасности в отношении доступа к программному обеспечению и системам
4.3.1. Реализация политик контроля доступа
4.3.2. Внедрение политики доступа к коммуникациям
4.3.3. Типы инструментов безопасности для контроля доступа

4.4. Управление доступом к пользователям
4.4.1. Управление правами доступа
4.4.2. Разделение ролей и функций доступа
4.4.3. Реализация прав доступа в системах

4.5. Контроль доступа к системам и приложениям
4.5.1. Норма минимального доступа
4.5.2. Технологии безопасного входа в систему
4.5.3. Политики безопасности паролей

4.6. Технологии систем идентификации
4.6.1. Активный каталог
4.6.2. OTP
4.6.3. PAP, CHAP
4.6.4. KERBEROS, DIAMETER, NTLM

4.7. CIS Controls для укрепления системы
4.7.1. Базовые CIS Controls
4.7.2. Основные CIS Controls
4.7.3. Организационные CIS Controls

4.8. Эксплуатационная безопасность
4.8.1. Защита от вредоносного кода
4.8.2. Резервные копии
4.8.3. Записи о деятельности и мониторинге

4.9. Управление техническими уязвимостями
4.9.1. Технические уязвимости
4.9.2. Управление техническими уязвимостями
4.9.3. Ограничения на установку software

4.10. Внедрение практик политики безопасности
4.10.1. Логические уязвимости
4.10.2. Осуществление оборонной политики

Модуль 5. Политика управления инцидентами безопасности

5.1. Политики и усовершенствования в области управления инцидентами информационной безопасности
5.1.1. Управление инцидентами
5.1.2. Ответственность и процедуры
5.1.3. Оповещение о событиях

5.2. Системы обнаружения и предотвращения вторжений (IDS/IPS)
5.2.1. Рабочие данные системы
5.2.2. Типы систем обнаружения вторжений
5.2.3. Критерии для размещения IDS/IPS

5.3. Реагирование на инциденты безопасности
5.3.1. Процедура сбора данных
5.3.2. Процесс проверки вторжения
5.3.3. Органы CERT

5.4. Процесс уведомления и управления попытками вторжения
5.4.1. Обязанности в процессе уведомления
5.4.2. Классификация инцидентов
5.4.3. Процесс разрешения и восстановления

5.5. Криминалистический анализ как политика безопасности
5.5.1. Цифровые доказательства: нестабильные данные и энергонезависимые данные
5.5.2. Анализ и сбор электронных доказательств
5.5.2.1. Анализ электронных доказательств
5.5.2.2. Сбор электронных доказательств

5.6. Инструменты систем обнаружения и предотвращения вторжений (IDS/IPS)
5.6.1. Snort
5.6.2. Suricata
5.6.3. Solar-Winds

5.7. Инструменты централизации событий
5.7.1. SIM
5.7.2. SEM
5.7.3. Управление информацией и событиями в области безопасности (SIEM)

5.8. Руководство по безопасности CCN-STIC 817
5.8.1. Руководство по безопасности CCN-STIC 817
5.8.2. Управление киберинцидентами
5.8.3. Метрики и индикаторы

5.9. NIST SP800-61
5.9.1. Возможности реагирования на инциденты информационной безопасности
5.9.2. Обработка инцидента
5.9.3. Координация и обмен информацией

5.10. Стандарт ISO 27035
5.10.1. Норма ISO 27035. Принципы управления инцидентами
5.10.2. Руководство по разработке плана управления инцидентами
5.10.3. Руководство по операциям реагирования на инциденты

Модуль 6. Внедрение политики физической и экологической безопасности в компании

6.1. Зона безопасности
6.1.1. Периметр физической безопасности
6.1.2. Работа в безопасных зонах
6.1.3. Безопасность офисов, служебных помещений и ресурсов

6.2. Физические элементы управления вводом
6.2.1. Политики контроля физического доступа
6.2.2. Системы контроля физического ввода

6.3. Уязвимости физического доступа
6.3.1. Основные физические уязвимости
6.3.2. Реализация мер по обеспечению безопасности

6.4. Физиологические биометрические системы
6.4.1. Отпечаток пальца
6.4.2. Система распознавания лиц
6.4.3. Распознавание радужной оболочки глаза и сетчатки глаза
6.4.4. Другие физиологические биометрические системы

6.5. Биометрические поведенческие системы
6.5.1. Распознавание подписи
6.5.2. Распознание личности
6.5.3. Распознание голоса
6.5.4. Другие биометрические поведенческие системы

6.6. Управление рисками в биометрии
6.6.1. Внедрение биометрических систем
6.6.2. Уязвимости биометрических систем

6.7. Осуществление политики в *хостах*
6.7.1. Прокладка питающей и защитной кабельной сети
6.7.2. Расположение оборудования
6.7.3. Вывод оборудования за пределы помещения
6.7.4. IT-оборудование без присмотра и политика свободного места

6.8. Защита окружающей среды
6.8.1. Системы пожарной безопасности
6.8.2. Системы защиты от сейсмических воздействий
6.8.3. Системы защиты от землетрясений

6.9. Безопасность в центре обработки данных
6.9.1. Двери безопасности
6.9.2. Системы видеонаблюдения (CCTV)
6.9.3. Контроль безопасности

6.10. Международные правила физической безопасности
6.10.1. IEC 62443-2-1 (Европа)
6.10.2. NERC CIP-005-5 (США)
6.10.3. NERC CIP-014-2 (США)

Модуль 7. Политика безопасной коммуникации в компаниях

7.1. Управление безопасностью в сети
7.1.1. Контроль и мониторинг сети
7.1.2. Разделение сетей
7.1.3. Системы безопасности в сети

7.2. Протоколы безопасной связи
7.2.1. Модель TCP/IP
7.2.2. Протокол IPSEC
7.2.3. Протокол TLS

7.3. Протокол TLS 1.3
7.3.1. Фазы процесса TLS 1.3
7.3.2. Протокол *Handshake*
7.3.3. Протокол о регистрации
7.3.4. Отличия от TLS 1.2

7.4. Криптографические алгоритмы
7.4.1. Криптографические алгоритмы, используемые в коммуникациях
7.4.2. *Cipher-suites*
7.4.3. Криптографические алгоритмы, разрешенные для TLS 1.3

7.5. Функции дайджеста
7.5.1. Функции дайджеста
7.5.2. MD6
7.5.3. SHA

7.6. PKI. Инфраструктура открытых ключей
7.6.1. PKI и ее подразделения
7.6.2. Электронный сертификат
7.6.3. Типы цифровых сертификатов

7.7. Туннельный и транспортный режимы коммуникации
7.7.1. Туннельный режим
7.7.2. Транспортный режим
7.7.3. Реализация зашифрованного туннеля

7.8. SSH. *Secure Shell*
7.8.1. SSH. Безопасная капсула
7.8.2. Как работает SSH
7.8.3. SSH-средства

7.9. Аудит криптографических систем
7.9.1. Проверка целостности
7.9.2. Тестирование криптографических систем

7.10. Криптографические системы
7.10.1. Уязвимости криптографических систем
7.10.2. Защитные меры в криптографии

Модуль 8. Практическая реализация политики безопасности перед угрозой атак

8.1. *System Hacking*
8.1.1. Риски и уязвимости
8.1.2. Контрмеры

8.2. DoS в сервисах
8.2.1. Риски и уязвимости
8.2.2. Контрмеры

8.3. *Session Hijacking*
8.3.1. Процесс *Hijacking*
8.3.2. Меры противодействия *Hijacking*

8.4. Обход IDS, *Firewalls and Honeypots*
8.4.1. Методы избегания
8.4.2. Осуществление контрмер

8.5. *Hacking Web Servers*
8.5.1. Атаки на веб-серверы
8.5.2. Реализация мер по обеспечению безопасности

8.6. *Hacking Web Applications*
8.6.1. Атаки на веб-приложения
8.6.2. Реализация мер по обеспечению безопасности

8.7. *Hacking Wireless Networks*
8.7.1. Уязвимости в сетях wifi
8.7.2. Реализация мер по обеспечению безопасности

8.8. *Hacking Mobile Platforms*
8.8.1. Уязвимости мобильных платформ
8.8.2. Осуществление контрмер

8.9. *Ramsonware*
8.9.1. Уязвимости, связанные с *Ramsonware*
8.9.2. Осуществление контрмер

8.10. Социальная инженерия
8.10.1. Типы социальной инженерии
8.10.2. Меры противодействия социальной инженерии

Модуль 9. Инструменты мониторинга в политике безопасности информационных систем

9.1. Политики мониторинга информационных систем
9.1.1. Мониторинг системы
9.1.2. Метрические данные
9.1.3. Типы метрики

9.2. Аудит и регистрация систем
9.2.1. Аудит и регистрация систем
9.2.2. Аудит и регистрация Windows
9.2.3. Аудит и регистрация Linux

9.3. Протокол SNMP. *Simple Network Management Protocol*
9.3.1. Протокол SNMP
9.3.2. Как работает SNMP
9.3.3. SNMP-средства

9.4. Мониторинг сети
9.4.1. Сетевой мониторинг в системах управления
9.4.2. Инструменты мониторинга для систем управления

9.5. Nagios. Система мониторинга сети
9.5.1. Nagios
9.5.2. Как работает Nagios
9.5.3. Установка Nagios

9.6. Zabbix. Система мониторинга сети
9.6.1. Zabbix
9.6.2. Как работает Zabbix
9.6.3. Установка Zabbix

9.7. Cacti. Система мониторинга сети
9.7.1. Cacti
9.7.2. Как работает Cacti
9.7.3. Установка Cacti

9.8. Pandora. Система мониторинга сети
9.8.1. Pandora
9.8.2. Как работает Pandora
9.8.3. Установка Pandora

9.9. SolarWinds. Система мониторинга сети
9.9.1. SolarWinds
9.9.2. Как работает SolarWinds
9.9.3. Установка SolarWinds

9.10. Правила мониторинга
9.10.1. CIS Controls по аудиту и регистрации
9.10.2. NIST 800-123 (США)

Модуль 10. Практическая политика аварийного восстановления системы безопасности

10.1. DRP. План аварийного восстановления
10.1.1. Цель DRP
10.1.2. Преимущества DRP
10.1.3. Последствия отсутствия DRP и его неактуальности

10.2. Руководство по определению DRP (плана аварийного восстановления)
10.2.1. Сфера применения и цели
10.2.2. Разработка стратегии восстановления
10.2.3. Распределение ролей и обязанностей
10.2.4. Проведение инвентаризации аппаратного, программного обеспечения и услуг
10.2.5. Устойчивость к простоям и потере данных
10.2.6. Установление конкретных типов DRP, которые необходимы
10.2.7. Реализация плана обучения, повышения осведомленности и коммуникации

10.3. Сфера применения и цели DRP (плана аварийного восстановления)
10.3.1. Ответная гарантия
10.3.2. Технологические компоненты
10.3.3. Сфера применения политики непрерывности

10.4. Разработка стратегии DRP (аварийного восстановления)
10.4.1. Стратегия аварийного восстановления
10.4.2. Бюджет
10.4.3. Человеческие и физические ресурсы
10.4.4. Руководящие должности в зоне риска
10.4.5. Технология
10.4.6. Данные

10.5. Непрерывность информационных процессов
10.5.1. Планирование непрерывности деятельности
10.5.2. Осуществление непрерывности
10.5.3. Проверка оценки непрерывности

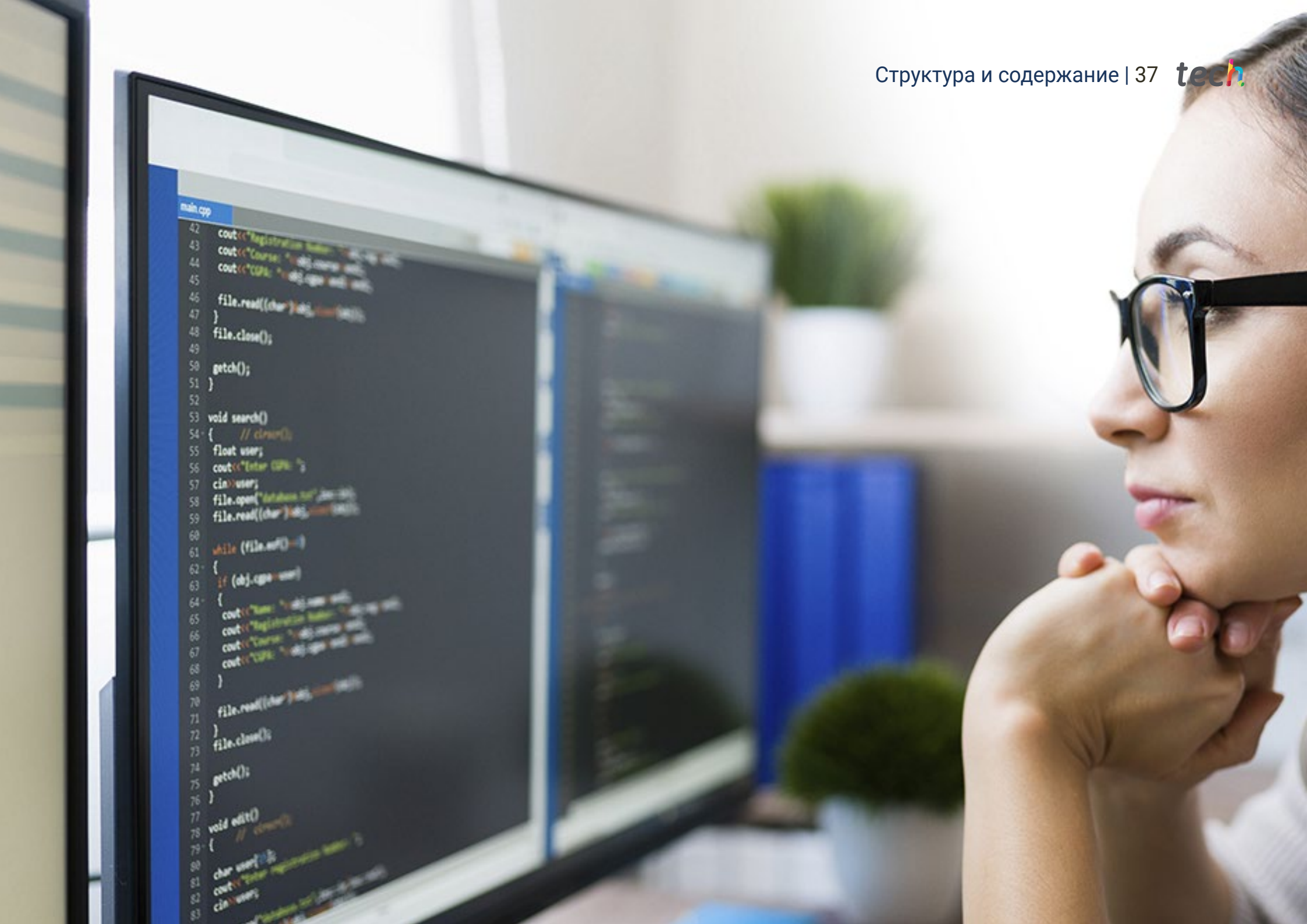
10.6. Сфера применения BCP (плана обеспечения непрерывности бизнеса)
10.6.1. Определение наиболее критических процессов
10.6.2. Подход на основе активов
10.6.3. Подход на основе процессов

10.7. Внедрение защищенных бизнес-процессов
10.7.1. Приоритетные направления деятельности
10.7.2. Идеальные сроки восстановления
10.7.3. Стратегии выживания

10.8. Анализ организации
10.8.1. Получение информации
10.8.2. Анализ воздействия на бизнес (BIA)
10.8.3. Анализ рисков в организации

10.9. Ответ на непредвиденные ситуации
10.9.1. План действий в кризисной ситуации
10.9.2. Планы восстановления операционной среды
10.9.3. Технические рабочие процедуры или процедуры, связанные с инцидентами

10.10. Международная норма ISO 27031 BCP
10.10.1. Цели
10.10.2. Термины и определения
10.10.3. Операция


main.cpp
void search()
float user;
while (file.eof())
if (obj.cgpa
void edit()
char user[20];

07

Методология

Данная учебная программа предлагает особый способ обучения. Наша методология разработана в режиме циклического обучения: ***Relearning***.

Данная система обучения используется, например, в самых престижных медицинских школах мира и признана одной из самых эффективных ведущими изданиями, такими как ***Журнал медицины Новой Англии.***

Откройте для себя методику Relearning, которая отвергает традиционное линейное обучение, чтобы показать вам циклические системы обучения: способ, который доказал свою огромную эффективность, особенно в предметах, требующих запоминания"

Бизнес-школа TECH использует метод кейсов для контекстуализации всего содержания

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

С TECH вы сможете познакомиться со способом обучения, который опровергает основы традиционных методов образования в университетах по всему миру"

Эта программа подготовит вас к решению бизнес-задач в условиях неопределенности и достижению успеха в бизнесе.

Наша программа подготовит вас к решению новых задач в условиях неопределенности и достижению успеха в карьере.

Инновационный и отличный от других метод обучения

Эта программа TECH - интенсивная программа обучения, созданная с нуля для того, чтобы предложить менеджерам задачи и бизнес-решения на самом высоком уровне, на международной арене. Благодаря этой методологии ускоряется личностный и профессиональный рост, делая решающий шаг на пути к успеху. Метод кейсов, составляющий основу данного содержания, обеспечивает следование самым современным экономическим, социальным и деловым реалиям.

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

Метод кейсов является наиболее широко используемой системой обучения в лучших бизнес-школах мира на протяжении всего времени их существования. Разработанный в 1912 году для того, чтобы студенты-юристы могли изучать право не только на основе теоретического содержания, метод кейсов заключается в том, что им представляются реальные сложные ситуации для принятия обоснованных решений и ценностных суждений о том, как их разрешить. В 1924 году он был установлен в качестве стандартного метода обучения в Гарвардском университете.

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

Методология *Relearning*

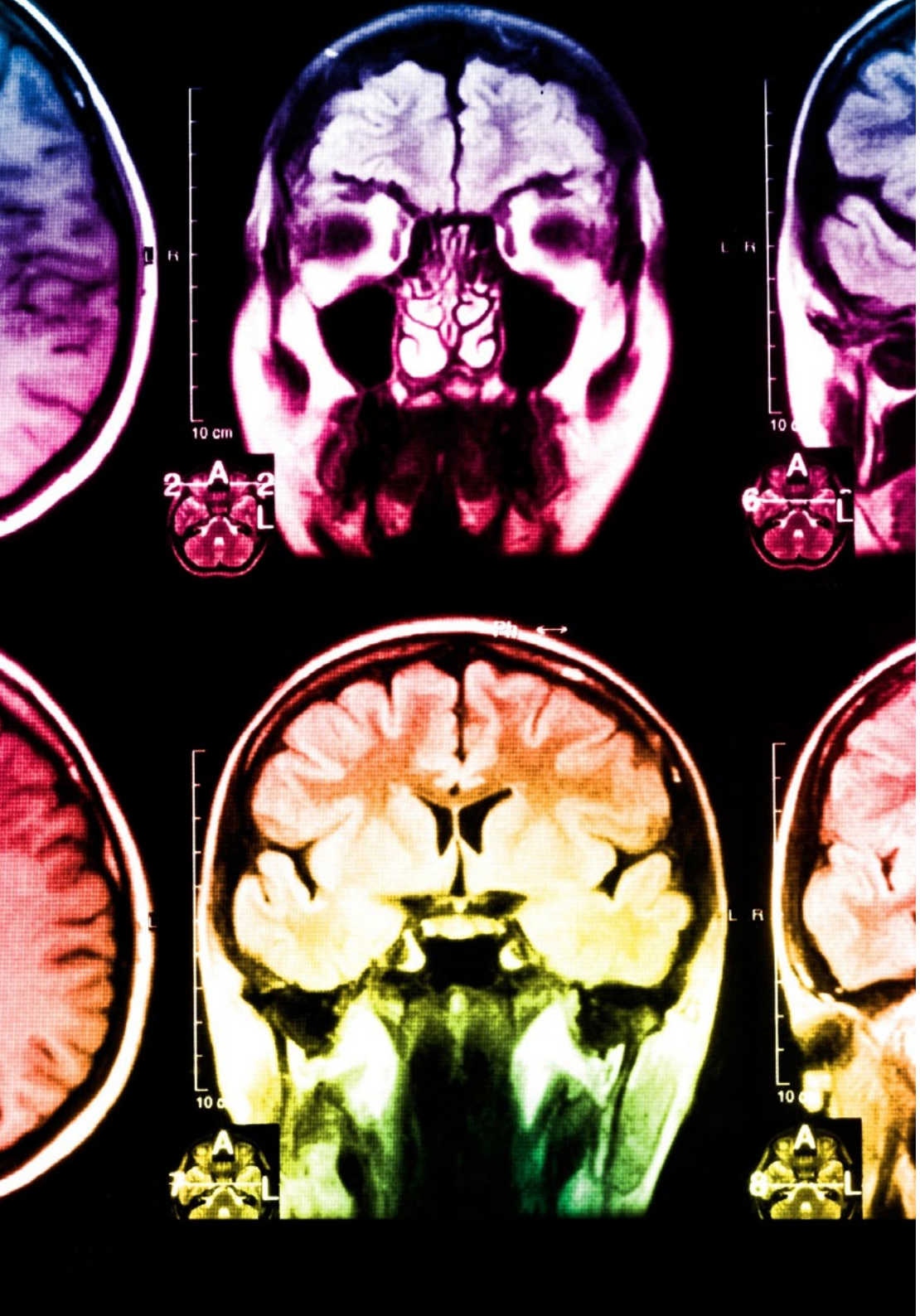
TECH эффективно объединяет метод кейсов с системой 100% онлайн-обучения, основанной на повторении, которая сочетает различные дидактические элементы в каждом уроке.

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

> *Наша онлайн-система позволит вам организовать свое время и темп обучения, адаптируя его к вашему графику. Вы сможете получить доступ к содержанию с любого стационарного или мобильного устройства с выходом в интернет.*

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

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



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

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

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

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

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

Учебный материал

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

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

Мастер-классы

Существуют научные данные о пользе экспертного наблюдения третьей стороны.

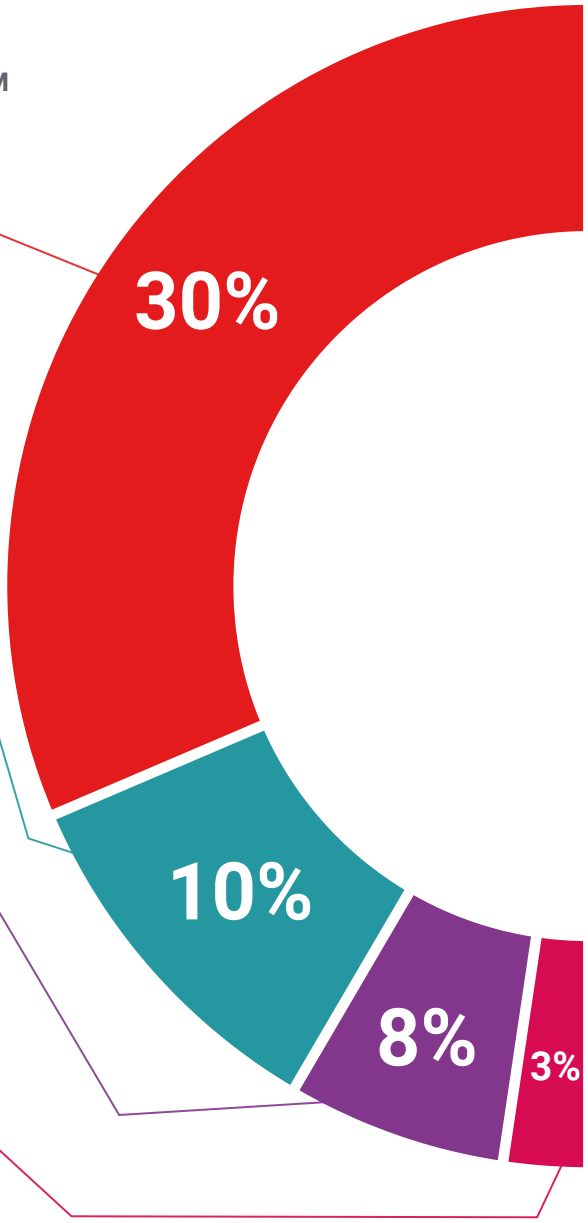
Так называемый метод обучения у эксперта укрепляет знания и память, а также формирует уверенность в наших будущих сложных решениях.

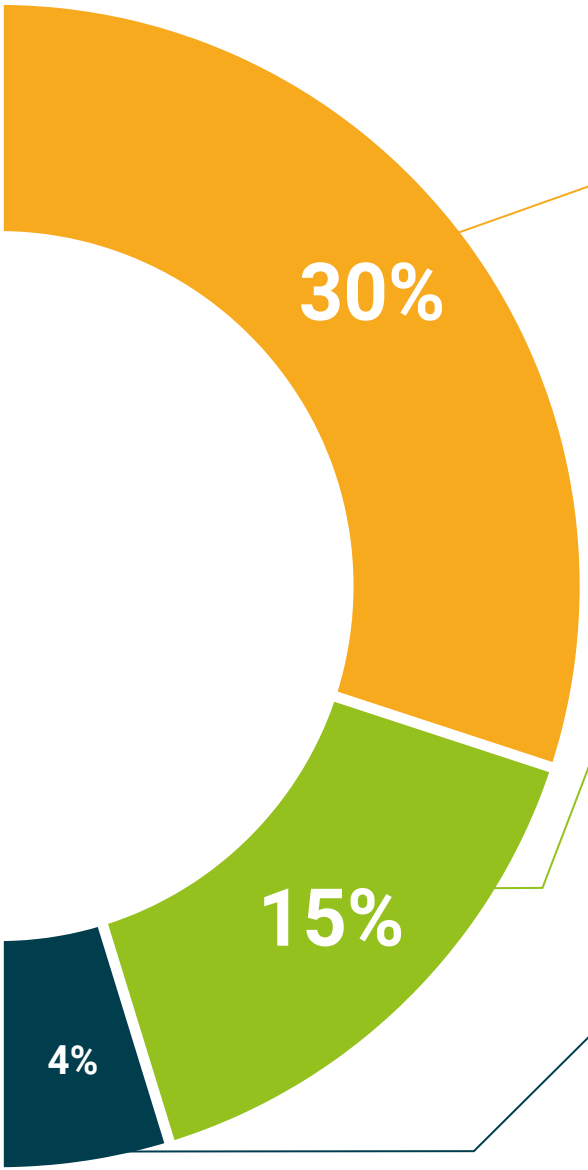
Практика управленческих навыков

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

Дополнительная литература

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





Метод кейсов

Метод дополнится подборкой лучших кейсов, выбранных специально для этой квалификации. Кейсы представляются, анализируются и преподаются лучшими специалистами в области высшего менеджмента на международной арене.

Интерактивные конспекты

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

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

Тестирование и повторное тестирование

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

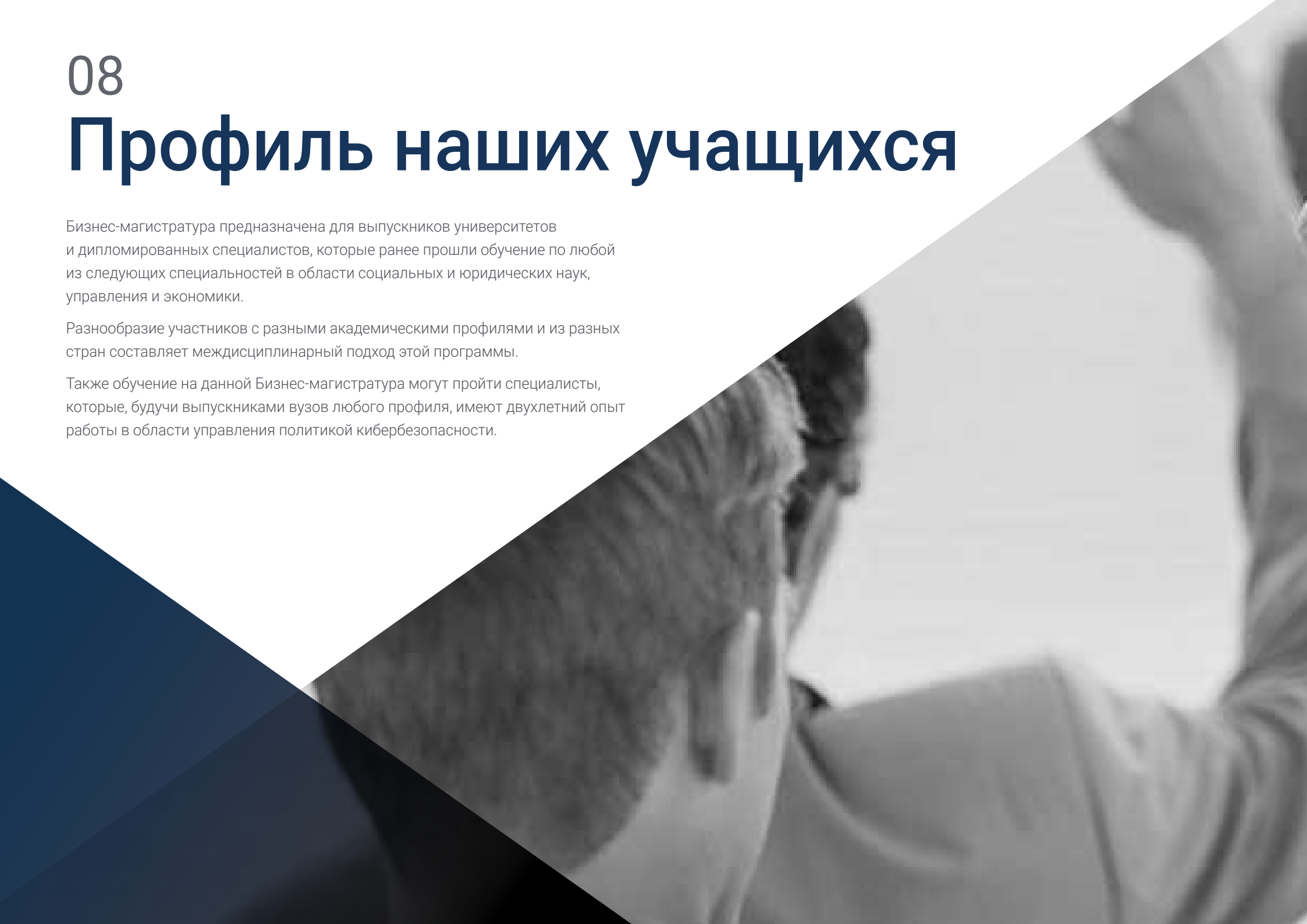
08

Профиль наших учащихся

Бизнес-магистратура предназначена для выпускников университетов и дипломированных специалистов, которые ранее прошли обучение по любой из следующих специальностей в области социальных и юридических наук, управления и экономики.

Разнообразие участников с разными академическими профилями и из разных стран составляет междисциплинарный подход этой программы.

Также обучение на данной Бизнес-магистратура могут пройти специалисты, которые, будучи выпускниками вузов любого профиля, имеют двухлетний опыт работы в области управления политикой кибербезопасности.

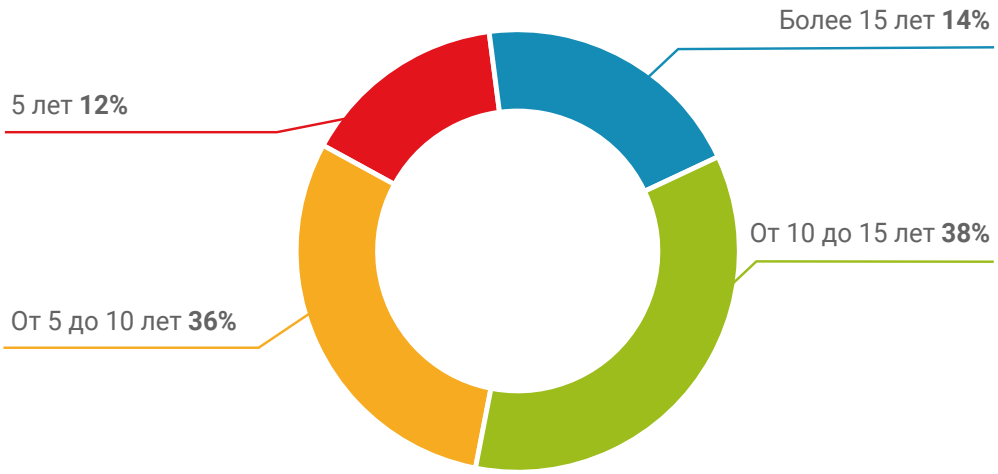


Если вы хотите повысить свой профессиональный уровень, получив качественные знания, основанные на самых современных реалиях в области кибербезопасности, регистрируйтесь на эту программу"

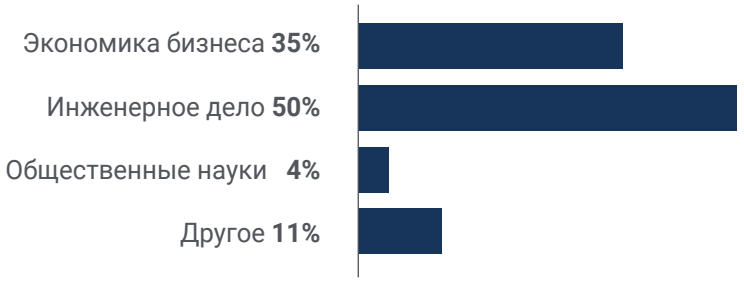
Средний возраст

В возрасте от **35** до **45** лет

Годы практики

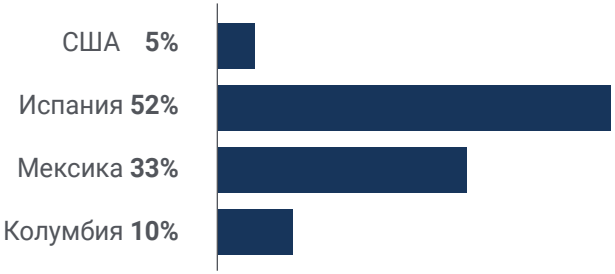


Образование



Академический профиль

Географическое распределение



Габриэль Гутьеррес Гомес

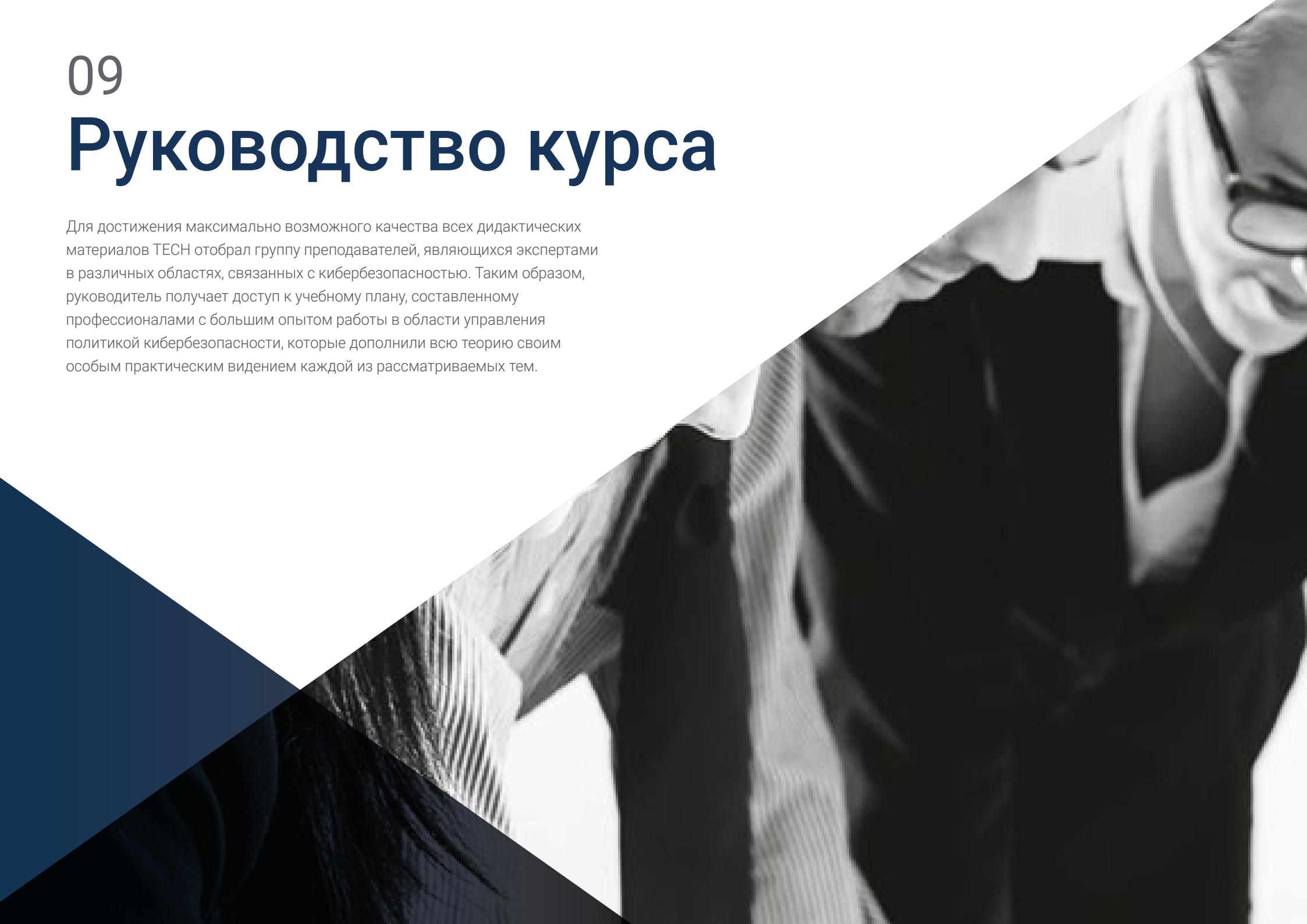
Руководитель отдела кибербезопасности

"После того как наша организация подверглась серьезной компьютерной атаке, мы стали уделять больше внимания защите наших баз данных и выделили для этого небольшой отдел. Благодаря этой программе мне удалось возглавить эту работу, разработать и внедрить политику кибербезопасности, которую мы используем до сих пор"

09

Руководство курса

Для достижения максимально возможного качества всех дидактических материалов TECH отобрал группу преподавателей, являющихся экспертами в различных областях, связанных с кибербезопасностью. Таким образом, руководитель получает доступ к учебному плану, составленному профессионалами с большим опытом работы в области управления политикой кибербезопасности, которые дополнили всю теорию своим особым практическим видением каждой из рассматриваемых тем.



Вас ждет преподавательский состав, имеющий опыт работы в сфере высшего менеджмента и управления комплексной ИТ-безопасностью, а также темы, посвященные обслуживанию информационных систем, криминалистическому анализу и хакерскому взлому”

Руководство

Г-жа Фернандес Сапена, Соня

- Преподаватель по компьютерной безопасности и этическому взлому в Национальном справочном центре информационных технологий и телекоммуникаций Getafe 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
- Компьютерный инженер 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 Солана Вильяриас, Фабиан

- Консультант в области информационных технологий
- Разработчик и администратор опросных услуг в компании Investigación, Planificación y Desarrollo, S.A.
- Специалист по обслуживанию финансовых рынков и IT-систем в компании Iberia Financial Software
- Веб-разработчик и специалист по доступности в компании Indra
- Степень бакалавра в области высшей системной инженерии в Университете Уэльса/CESINE
- Диплом в области технической инженерии по специальности "Инженерия компьютерных систем" Университета Уэльса / CESINE

Г-жа Лопес Гарсия, Роза Мария

- Специалист в области управления информацией
- Преподаватель Профессионального института Linux
- Участник в академии Hacker Incibe
- Менеджер по работе с талантами в области кибербезопасности в Teamciberhack
- Административный, бухгалтерский и финансовый менеджер в компании Integra2Transportes
- Административный помощник по закупкам ресурсов в Образовательном центре Cardenal Marcelo Espínola
- Старший технический сотрудник в области кибербезопасности и этического взлома
- Член Киберпатруля

Г-н Оропесиано Карризоса, Франсиско

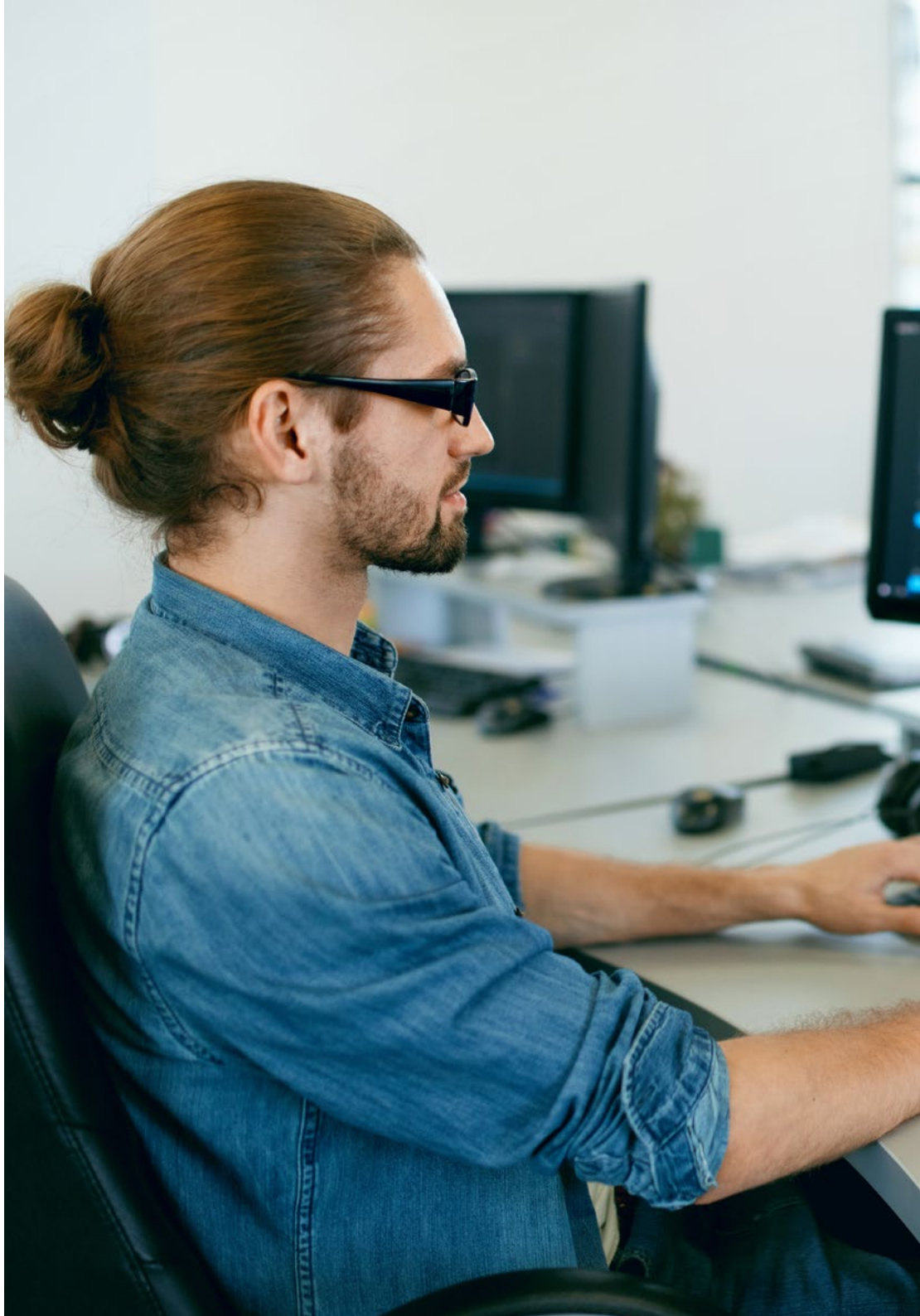
- Компьютерный инженер
- Специалист по микрокомпьютерам, сетевым технологиям и безопасности в Cas-Training
- Разработчик веб-сервисов, CMS, e-Commerce, UI и UX в Fersa Reparaciones
- Менеджер веб-сервисов, контента, почты и DNS в компании Oropesia Web & Network
- Графический дизайнер и дизайнер веб-приложений в компании Xarxa Sakai Projectes
- Диплом в области системных вычислений Университета Алькала де Энарес
- Степень магистра в DevOps: Docker and Kubernetes от Cyber Business Center
- Специалист по сетевой и компьютерной безопасности Университета Балеарских островов
- Курс профессиональной подготовки в области графического дизайна Политехнического университета в Мадриде

Г-н Ортега Лопес, Флоренсио

- Консультант по безопасности (управление идентификационными данными) в SIA Group
- Консультант по ICTs и безопасности в качестве независимого сотрудника
- Преподаватель в сфере IT
- Степень бакалавра в области технической промышленной инженерии Университета Алькала-де-Энарес
- Степень магистра в области преподавания в UNIR
- MBA в области делового администрирования и менеджмента в IDE-CESEM
- Степень магистра в области управления и менеджмента информационных технологий в IDE-CESEM
- Сертификат управления информационной безопасностью (CISM) в ISACA

Г-н Перальта Алонсо, Джон

- Старший консультант - защита данных и кибербезопасность. Altia
- Юрист / Юридический консультант. Юридический и экономический консалтинг Arriaga Associates, S.L.
- Юридический консультант / Стажер. Профессиональное бюро: Оскар Падура
- Степень бакалавра в области юриспруденции. Государственный университет Страны Басков
- Степень магистра по специальности «Сотрудник по защите данных» Инновационная школа EIS
- Степень магистра в области права. Государственный университет Страны Басков
- Степень магистра в области практики гражданского судопроизводства Международный университет Изабель I Кастильской
- Преподаватель в магистратуре по защите персональных данных, кибербезопасности и праву ICTs

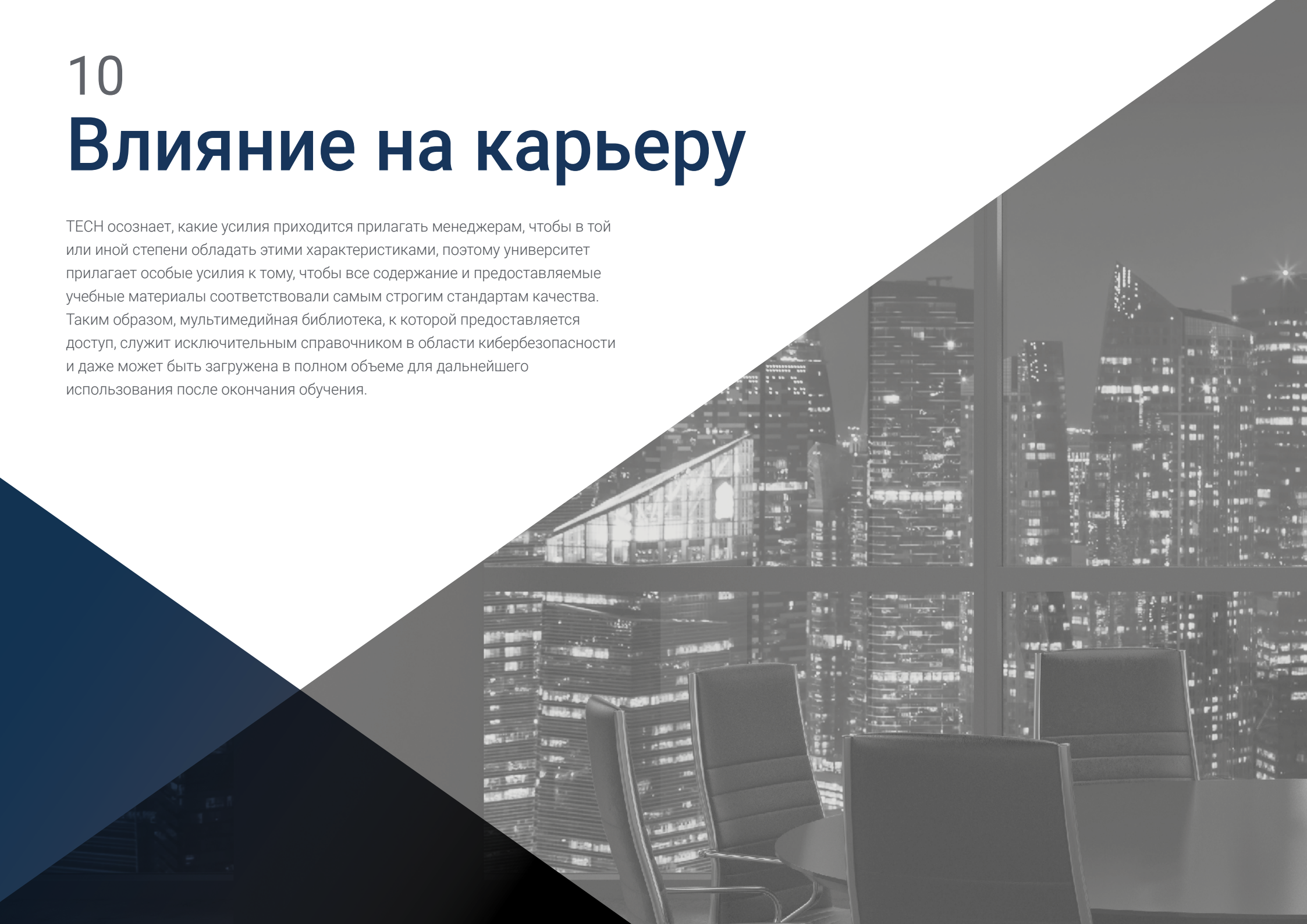


TECH тщательно подобрал команду преподавателей для этой программы, чтобы вы могли учиться у лучших специалистов современности"

10

Влияние на карьеру

TECH осознает, какие усилия приходится прилагать менеджерам, чтобы в той или иной степени обладать этими характеристиками, поэтому университет прилагает особые усилия к тому, чтобы все содержание и предоставляемые учебные материалы соответствовали самым строгим стандартам качества. Таким образом, мультимедийная библиотека, к которой предоставляется доступ, служит исключительным справочником в области кибербезопасности и даже может быть загружена в полном объеме для дальнейшего использования после окончания обучения.



Вы добьетесь экономического и профессионального роста, к которому стремитесь, благодаря постоянной поддержке преподавательского и технического коллектива, стремящегося привести вас к вершине менеджмента в области политики кибербезопасности"

Поступите в Специализированную магистратуру прямо сейчас и добивайтесь позитивных изменений в своем окружении.

Готовы ли вы решиться на перемены? Вас ждет отличный профессиональный рост

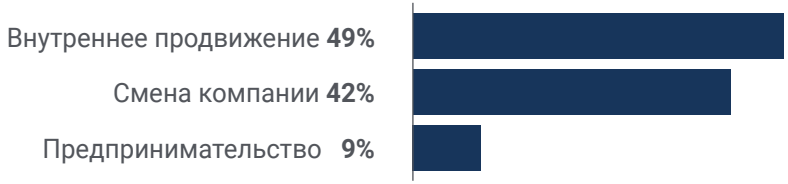
Бизнес-магистратура в области управления политикой кибербезопасности в компании от TECH — это интенсивная программа, которая готовит студентов к решению задач и принятию бизнес-решений в области кибербезопасности. Главная цель данной программы — поддержать ваш личностный и профессиональный рост и помочь вам добиться успеха.

Если вы хотите самосовершенствоваться, добиться позитивных изменений на профессиональном уровне и общаться с лучшими, то это место для вас.

Благодаря педагогической методике от TECH вы достигнете желаемых результатов в работе за меньшее время, чем вы думаете.

Время перемен

Что изменится



Повышение заработной платы

Прохождение этой программы означает для наших студентов повышение заработной платы более чем на **25,22%**

Предыдущая заработная плата	Повышение заработной платы	Последующая заработная плата
57 900 €	**25,22%**	**72 500€**

11

Преимущества для вашей компании

Бизнес-магистратура в области управления политикой кибербезопасности в компании способствует раскрытию максимального потенциала талантов организации через обучение руководителей высокого уровня.

Прохождение этой образовательной программы — это уникальная возможность получить доступ к мощной сети контактов, в которой можно найти будущих профессиональных партнеров, клиентов или поставщиков.

Киберугрозы — одна из самых серьезных уязвимостей, которой подвергаются компании всех типов и размеров. Специализируйтесь в той области, которая имеет наибольший прогноз на будущее"

Развитие и удержание талантов в компаниях – лучшая долгосрочная инвестиция.

01

Рост талантов и интеллектуального капитала

Профессионал привносит в компанию новые концепции, стратегии и перспективы, которые могут привести к соответствующим изменениям в организации.

02

Удержание руководителей с высоким потенциалом и избежание "утечки мозгов"

Эта программа укрепляет связь между компанией и специалистом и открывает новые возможности для профессионального роста внутри компании.

03

Создание агентов изменений

Вы сможете принимать решения в периоды неопределенности и кризиса, помогая организации преодолеть их.

04

Расширение возможностей для международной экспансии

Эта программа позволит компании установить контакт с основными рынками мировой экономики.

05

Разработка собственных проектов

Профессионал может работать над реальным проектом или разрабатывать новые проекты в области НИОКР или развития бизнеса своей компании.

06

Повышение конкурентоспособности

Данная программа предоставит специалистам необходимые навыки, чтобы они могли решать новые задачи и тем самым двигать организацию вперед.

12

Квалификация

Бизнес-магистратура в области управления политикой кибербезопасности в компании гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Бизнес-магистратура, выдаваемого TECH Технологическим университетом.

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

Данная **Бизнес-магистратура в области управления политикой кибербезопасности в компании** содержит самую полную и современную программу на рынке.

После прохождения аттестации студент получит по почте* с подтверждением получения соответствующий диплом **Бизнес-магистратура** выданный **TECH Технологическим университетом.**

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

Диплом: **Бизнес-магистратура в области управления политикой кибербезопасности в компаниях**

Формат: **онлайн**

Продолжительность: **12 месяцев**


tech технологический университет

Настоящий

ДИПЛОМ

свидетельствует о том, что

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

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

БИЗНЕС-МАГИСТРАТУРА

в области

управления политикой кибербезопасности в компаниях

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

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

17 июня 2020 г.

Д-р Tere Guevara Navarro
Ректор

unique TECH code: AFWOR23S techtitute.com/certificates


Бизнес-магистратура в области управления политикой кибербезопасности в компаниях

Общее распределение учебного плана

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

Общее распределение учебного плана

Курс	Предмет	Часы	Характер
1°	Система управления информационной безопасностью (СУИБ)	150	Обязат
1°	Организационные аспекты политики информационной безопасности	150	Обязат
1°	Политика безопасности для анализа угроз компьютерных систем	150	Обязат
1°	Практическая реализация политик безопасности в software и hardware	150	Обязат
1°	Политика управления инцидентами безопасности	150	Обязат
1°	Внедрение политики физической и экологической безопасности в компании	150	Обязат
1°	Политика безопасной коммуникации в компаниях	150	Обязат
1°	Практическая реализация политики безопасности перед угрозой атак	150	Обязат
1°	Инструменты мониторинга в политике безопасности информационных систем	150	Обязат
1°	Практическая политика аварийного восстановления системы безопасности	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

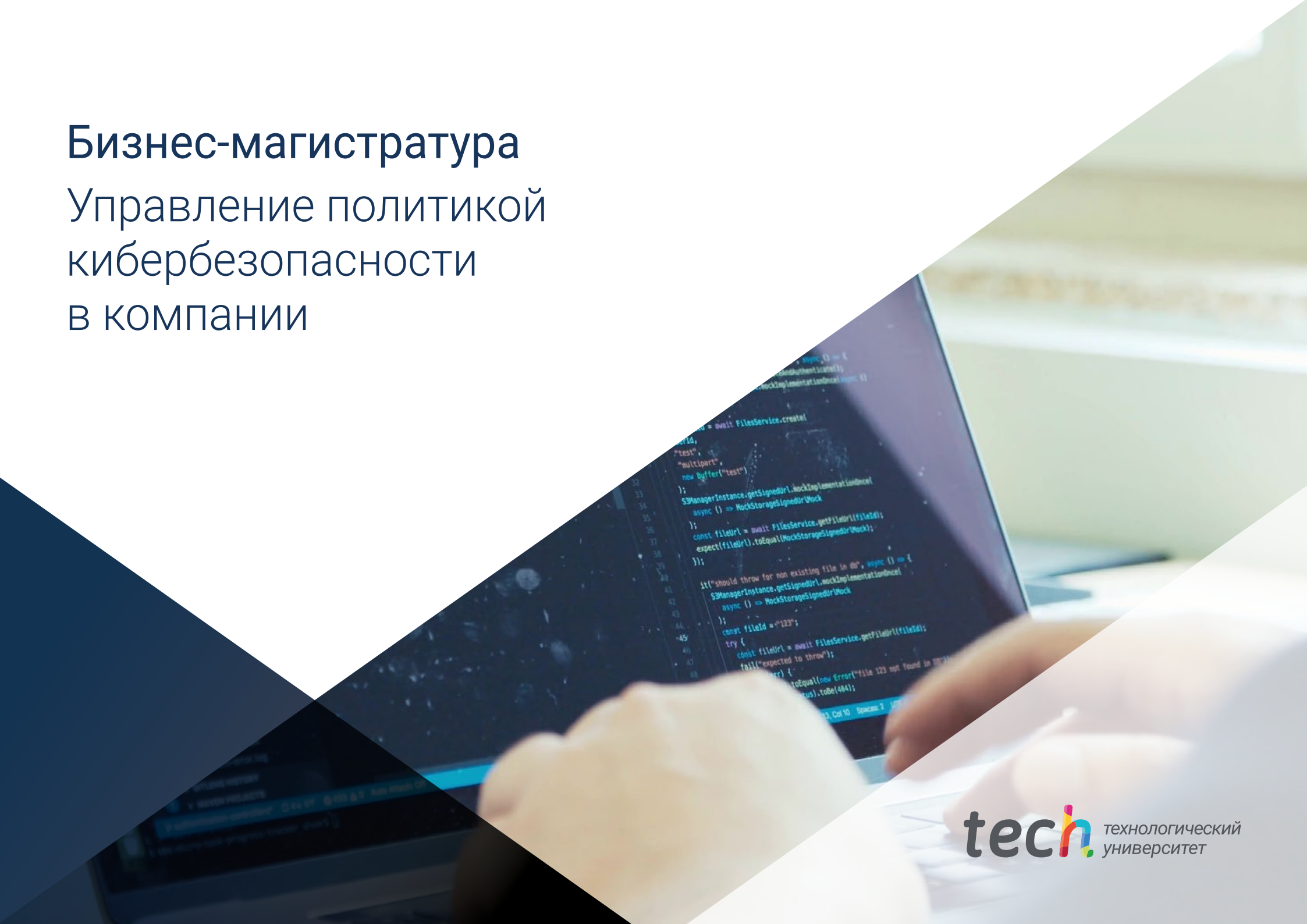
Бизнес-магистратура

Управление политикой кибербезопасности в компании

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

Бизнес-магистратура

Управление политикой кибербезопасности в компании



tech технологический университет