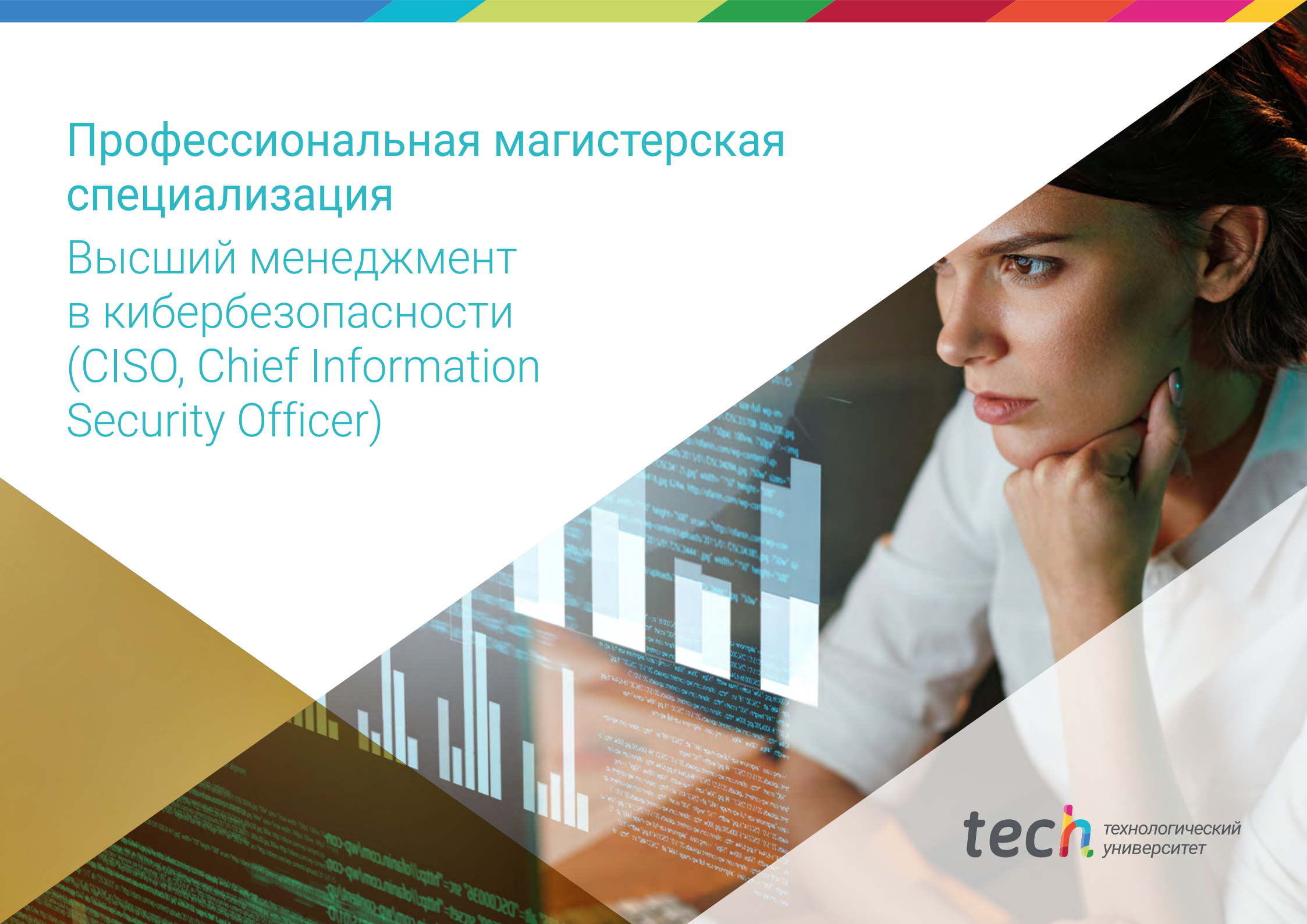
Профессиональная магистерская специализация

Высший менеджмент в кибербезопасности (CISO, Chief Information Security Officer)



tech технологический университет

tech технологический университет

Профессиональная магистерская специализация

Высший менеджмент в кибербезопасности (CISO, Chief Information Security Officer)

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

Веб-доступ: www.techtitute.com/ru/information-technology/advanced-master-degree/advanced-master-degree-senior-cybersecurity-management-ciso-chief-information-security-officer

Оглавление

01

Презентация программы

В настоящее время кибербезопасность стала основным столпом защиты как отдельных лиц, так и компаний от растущего количества цифровых угроз. Эта дисциплина направлена не только на сохранение технологических систем и критической информации организаций, но и на руководство планированием, внедрением и контролем стратегий безопасности. Таким образом, ее основная цель — снизить риски и эффективно реагировать на кибератаки и инциденты. Среди основных обязанностей директора по кибербезопасности выделяются разработка политик безопасности, управление технологическими рисками и руководство специализированными командами. В условиях вызовов, вытекающих из технологического прогресса и цифровизации, появилась эта программа, разработанная специально для решения данных проблем. TECH направлен не только на обеспечение эффективности защиты информации, но и на выявление и управление новыми уязвимостями. Это позиционирует CISO как самый важный элемент для устойчивости любой организации.

Получите специализацию в TECH и станьте лидером в одной из самых важных областей ИТ”

Высший менеджмент в области кибербезопасности оказался ключевым для обеспечения стабильности и непрерывности работы организаций в условиях цифрового и высокосвязного мира. С помощью внедрения надежных стратегий безопасности и применения передовых технологий были снижены риски и предотвращены атаки с катастрофическими последствиями. В таких критически важных секторах, как банковское дело, здравоохранение и государственная инфраструктура, безопасность была усилена благодаря эффективному управлению и соблюдению норм, осуществляемым лидерами, специализирующимися в этой области.

Эта дисциплина позволила организациям создать более безопасные цифровые рабочие среды, что, в свою очередь, укрепило доверие клиентов, партнеров и пользователей. Успешные результаты позволили сэкономить значительные суммы — миллионы долларов, предотвращая потенциальные экономические потери, а также способствовали формированию организационной культуры, в которой безопасность является общей приоритетной задачей. Кроме того, эта дисциплина оказалась незаменимой для защиты инноваций, репутации и устойчивости организаций в условиях постоянно меняющейся среды.

Профессиональная магистерская специализация в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer) от TECH разработана для специализации профессионалов в области лидерства в разработке эффективных стратегий безопасности. В течение программы студент будет учиться в собственном темпе, сосредотачиваясь на развитии управленческих навыков и стратегического бизнес-видения. Кроме того, он получит доступ к передовой специализации, которая готовит его к успешной карьере в области, крайне востребованной на мировом рынке. Благодаря полностью онлайн-формату студенты смогут совмещать обучение с рабочими обязанностями, что позволит им продвигаться вперед, не жертвуя своей профессиональной деятельностью.

Данная программа **Профессиональная магистерская специализация в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer)** содержит самую полную и современную образовательную программу на рынке. Основными особенностями обучения являются:

- Разбор практических кейсов, представленных экспертами в области информатики
- Наглядное, схематичное и исключительно практическое содержание курса предоставляет научную и практическую информацию по тем дисциплинам, которые необходимы для осуществления профессиональной деятельности
- Практические упражнения для самопроверки, контроля и улучшения успеваемости
- Особое внимание уделяется инновационным методологиям в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer)
- 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

Профессиональная магистерская специализация выведет вас на передовые позиции в отрасли и откроет безграничные возможности для карьерного роста"

Развивайте навыки, необходимые для решения задач будущего, не пренебрегая текущей деятельностью"

Станьте защитником технологических инфраструктур с помощью метода Relearning, который адаптируется к вашему темпу обучения.

Станьте частью крупнейшего в мире цифрового университета и обучайтесь из любой точки мира.

В преподавательский состав входят профессионалы в области дизайна, которые привносят в эту программу опыт своей работы, а также признанные специалисты из ведущих сообществ и престижных университетов.

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

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

02

Почему стоит учиться в TECH?

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

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

Лучший онлайн-университет в мире по версии FORBES

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

Лучший международный преподавательский состав

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

Крупнейший цифровой университет в мире

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

Forbes
Mejor universidad online del mundo

Plan
de estudios
más completo

Profesorado
TOP
Internacional

La metodología
más eficaz

nº1
Mundial
Mayor universidad online del mundo

Самые полные учебные программы в университетской среде

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

Уникальный метод обучения

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

Официальный онлайн-университет NBA

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

Лидеры по трудоустройству

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

Google Partner Premier

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

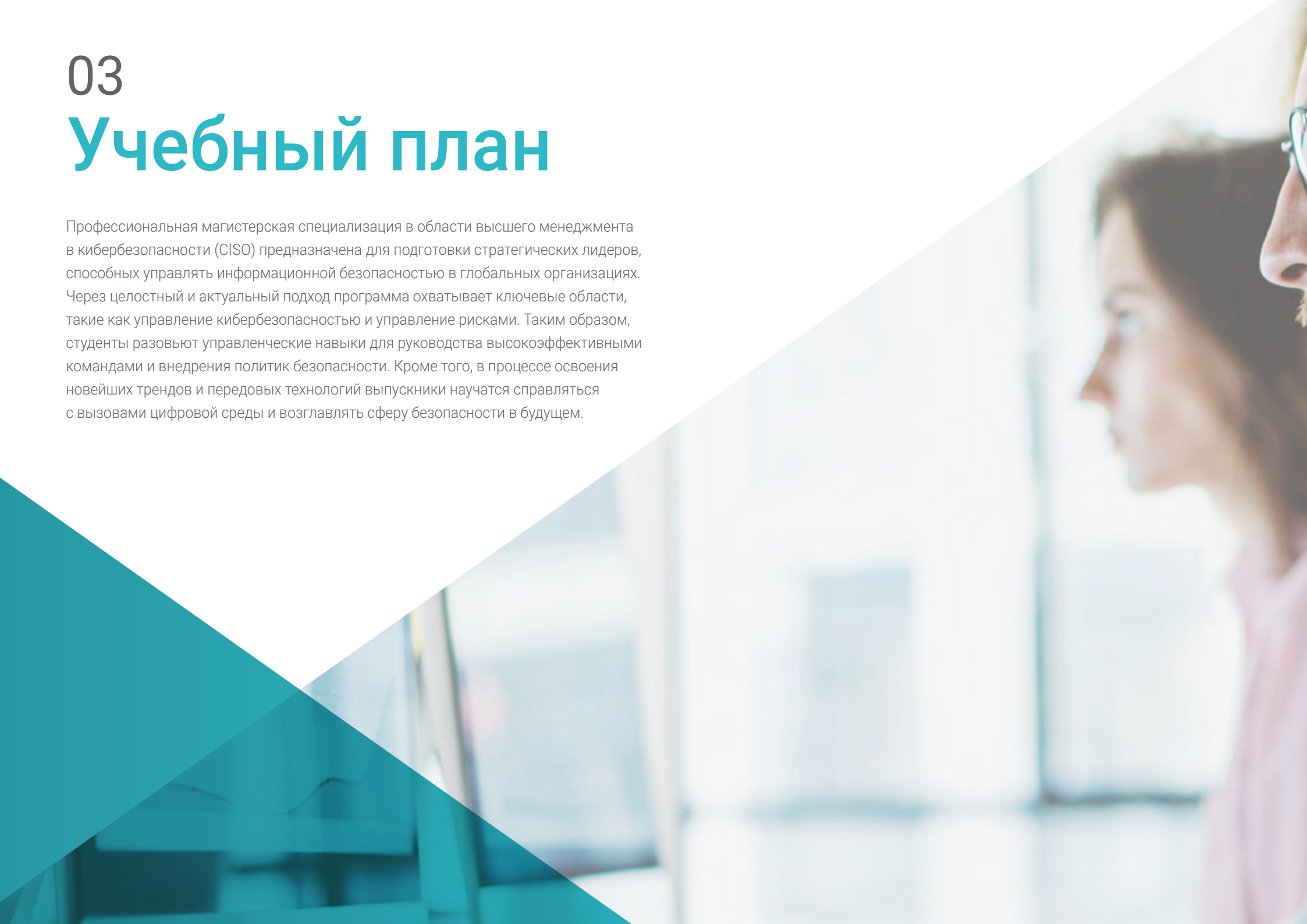
Университет, получивший самые высокие оценки от своих студентов

Студенты признали TECH самым высоко оцененным университетом в мире на ведущих платформах с отзывами, отметив его высший рейтинг — 4,9 из 5, основанный на более чем 1 000 рецензиях. Эти результаты укрепляют позиции TECH как ведущего международного университета, отражая его превосходство и положительное влияние образовательной модели.

03

Учебный план

Профессиональная магистерская специализация в области высшего менеджмента в кибербезопасности (CISO) предназначена для подготовки стратегических лидеров, способных управлять информационной безопасностью в глобальных организациях. Через целостный и актуальный подход программа охватывает ключевые области, такие как управление кибербезопасностью и управление рисками. Таким образом, студенты разовьют управленческие навыки для руководства высокоэффективными командами и внедрения политик безопасности. Кроме того, в процессе освоения новейших трендов и передовых технологий выпускники научатся справляться с вызовами цифровой среды и возглавлять сферу безопасности в будущем.



TECH готовит вас к роли стратега, который предотвращает, обнаруживает и смягчает киберугрозы в глобальной бизнес-среде"

Модуль 1. Кибербезопасность

1.1. Кибербезопасность
- 1.1.1. Кибербезопасность
  - 1.1.1.1. Разведка
    - 1.1.1.1.1. Цикл разведки
  - 1.1.1.2. Кибербезопасность
  - 1.1.1.3. Кибербезопасность и кибербезопасность
- 1.1.2. Аналитик разведывательной службы
  - 1.1.2.1. Роль аналитика разведывательной службы
  - 1.1.2.2. Необъективность аналитика разведки в оценочной деятельности

1.2. Кибербезопасность
- 1.2.1. Уровни безопасности
- 1.2.2. Идентификация киберугроз
  - 1.2.2.1. Внешние угрозы
  - 1.2.2.2. Внутренние угрозы
- 1.2.3. Неблагоприятные действия
  - 1.2.3.1. Социальная инженерия
  - 1.2.3.2. Часто используемые методы

1.3. Инструменты и методы разведки
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Дистрибутивы и инструменты Linux
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. Методология оценки
- 1.4.1. Анализ разведывательной информации
- 1.4.2. Методы организации полученной информации
- 1.4.3. Надежность и достоверность источников информации
- 1.4.4. Методологии анализа
- 1.4.5. Представление результатов разведки

1.5. Аудиты и документация
- 1.5.1. Аудит ИТ-безопасности
- 1.5.2. Документация и разрешения на проведение аудита
- 1.5.3. Виды аудита
- 1.5.4. Результаты
  - 1.5.4.1. Технический отчет
  - 1.5.4.2. Исполнительный отчет

1.6. Анонимность в интернете
- 1.6.1. Использование анонимизации
- 1.6.2. Методы анонимизации (Proxy, VPN)
- 1.6.3. Сети TOR, Freenet e IP2

1.7. Угрозы и виды безопасности
- 1.7.1. Виды угроз
- 1.7.2. Физическая безопасность
- 1.7.3. Безопасность в сетях
- 1.7.4. Логическая безопасность
- 1.7.5. Безопасность веб-приложений
- 1.7.6. Безопасность на мобильных устройствах

1.8. Регулирование и *комплаенс*
- 1.8.1. Общий регламент по защите данных
- 1.8.2. Семейство стандартов ISO 27000
- 1.8.3. Система кибербезопасности NIST
- 1.8.4. PIC
- 1.8.5. ISO 27032
- 1.8.6. Стандарты в сфере *облачной безопасности*
- 1.8.7. SOX
- 1.8.8. PCI

1.9. Анализ рисков и метрики
- 1.9.1. Масштабы рисков
- 1.9.2. Активы
- 1.9.3. Угрозы
- 1.9.4. Уязвимости
- 1.9.5. Оценка рисков
- 1.9.6. Обработка риска

1.10. Важные органы по вопросам кибербезопасности
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. OEA
- 1.10.4. UNASUR - PROSUR

Модуль 2. Безопасность хоста

2.1. Резервные копии
- 2.1.1. Стратегии резервного копирования
- 2.1.2. Инструменты для Windows
- 2.1.3. Инструменты для Linux
- 2.1.4. Инструменты для MacOS

2.2. Пользовательский антивирус
- 2.2.1. Виды антивирусов
- 2.2.2. Антивирус для Windows
- 2.2.3. Антивирус для Linux
- 2.2.4. Антивирус для MacOS
- 2.2.5. Антивирусы для смартфонов

2.3. Детекторы вторжения - HIDS
- 2.3.1. Методы обнаружения вторжений
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Локальный брандмауэр
- 2.4.1. Брандмауэры для Windows
- 2.4.2. Брандмауэры для Linux
- 2.4.3. Брандмауэры для MacOS

2.5. Менеджеры паролей
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Детекторы *фишинга*
- 2.6.1. Обнаружение *фишинга* вручную
- 2.6.2. *Антифишинговые* инструменты

2.7. Шпионское программное обеспечение
- 2.7.1. Механизмы предотвращения
- 2.7.2. *Антишпионские* инструменты

2.8. Трекеры
- 2.8.1. Меры по защите системы
- 2.8.2. Инструменты для борьбы с трекингом

2.9. EDR- *End Point Detection and Response*
- 2.9.1. Поведение системы EDR
- 2.9.2. Различия между EDR и антивирусом
- 2.9.3. Будущее систем EDR

2.10. Контроль над установкой программного обеспечения
- 2.10.1. Репозитории и магазины программного обеспечения
- 2.10.2. Списки разрешенного или запрещенного программного обеспечения
- 2.10.3. Критерии обновлений
- 2.10.4. Права на установку программного обеспечения

Модуль 3. Сетевая безопасность (периметр)

3.1. Системы обнаружения и предотвращения угроз
- 3.1.1. Общая нормативная база для инцидентов по безопасности
- 3.1.2. Современные системы защиты: *Defense in Depth* и SOC
- 3.1.3. Текущие сетевые архитектуры
- 3.1.4. Типы средств выявления и предотвращения инцидентов
  - 3.1.4.1. Сетевые системы
  - 3.1.4.2. Системы на базе хоста
  - 3.1.4.3. Централизованные системы
- 3.1.5. Связь и обнаружение экземпляров/хостов, контейнеров и бессерверных систем

3.2. Брандмауэр
- 3.2.1. Типы файерволов
- 3.2.2. Атаки и смягчение последствий
- 3.2.3. Лучший *брандмауэр* для Linux
  - 3.2.3.1. UFW
  - 3.2.3.2. *Nftables и iptables*
  - 3.2.3.3. Firewalld
- 3.2.4. Системы обнаружения на основе системных журналов
  - 3.2.4.1. TCP Wrappers
  - 3.2.4.2. BlockHosts и DenyHosts
  - 3.2.4.3. Fai2ban

3.3. Системы обнаружения и предотвращения вторжений (IDS/IPS)
- 3.3.1. Атаки на IDS/IPS
- 3.3.2. Системы IDS/IPS
  - 3.3.2.1. Snort
  - 3.3.2.2. Suricata

3.4. Брандмауэры следующего поколения (NGFW)
- 3.4.1. Различия между NGFW и традиционными брандмауэрами
- 3.4.2. Основные возможности
- 3.4.3. Коммерческие решения
- 3.4.4. Брандмауэры для облачных сервисов
  - 3.4.4.1. Архитектура Cloud VPC
  - 3.4.4.2. Cloud ACLs
  - 3.4.4.3. Security Group

3.5. *Прокси*
- 3.5.1. Типы *прокси*
- 3.5.2. Использование *прокси*. Преимущества и недостатки

3.6. Антивирусные системы
- 3.6.1. Общий контекст *вредоносных программ* и IOCs
- 3.6.2. Проблемы с антивирусным движком

3.7. Системы защиты почтовых сервисов
- 3.7.1. Антиспам
  - 3.7.1.1. Черные и белые списки
  - 3.7.1.2. Байесовская фильтрация спама
- 3.7.2. Mail Gateway (MGW)

3.8. SIEM
- 3.8.1. Компоненты и архитектура
- 3.8.2. Правила корреляции и примеры использования
- 3.8.3. Актуальные проблемы систем SIEM

3.9. SOAR
- 3.9.1. SOAR и SIEM: враги или союзники
- 3.9.2. Будущее систем SOAR

3.10. Другие сетевые системы
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. HoneyPots и HoneyNets
- 3.10.4. CASB

Модуль 4. Безопасность смартфонов

4.1. Мир мобильных устройств
- 4.1.1. Виды мобильных платформ
- 4.1.2. iOS-устройства
- 4.1.3. Android-устройства

4.2. Управление безопасностью мобильных устройств
- 4.2.1. Проект по мобильной безопасности OWASP
  - 4.2.1.1. Топ-10 уязвимостей
- 4.2.2. Коммуникации, сети и режимы подключения

4.3. Мобильное устройство в корпоративной среде
- 4.3.1. Риски
- 4.3.2. Мониторинг устройств
- 4.3.3. Управление мобильными устройствами (MDM)

4.4. Конфиденциальность пользователей и безопасность данных
- 4.4.1. Состояние информации
- 4.4.2. Безопасное хранение данных
  - 4.4.2.1. Безопасное хранение данных на iOS
  - 4.4.2.2. Безопасное хранение данных на Android
- 4.4.3. Передовые методы разработки приложений

4.5. Уязвимости и векторы атак
- 4.5.1. Уязвимости
- 4.5.2. Векторы атак
  - 4.5.2.1. Вредоносное программное обеспечение
  - 4.5.2.2. Эксфильтрация данных
  - 4.5.2.3. Манипуляции с данными

4.6. Основные угрозы
- 4.6.1. Непринужденный пользователь
- 4.6.2. *Вредоносное программное обеспечение*
  - 4.6.2.1. Виды вредоносного ПО
- 4.6.3. Социальная инженерия
- 4.6.4. Утечка данных
- 4.6.5. Кража информации
- 4.6.6. Незащищенные сети Wi-Fi
- 4.6.7. Устаревшее программное обеспечение
- 4.6.8. Вредоносные приложения
- 4.6.9. Ненадежные пароли
- 4.6.10. Слабые или отсутствующие настройки безопасности
- 4.6.11. Физический доступ к информации
- 4.6.12. Потеря или кража устройства
- 4.6.13. Подмена личности (целостность)
- 4.6.14. Слабая или неработающая криптография
- 4.6.15. Отказ в обслуживании (DoS)

4.7. Основные атаки
- 4.7.1. *Фишинговые* атаки
- 4.7.2. Атаки, связанные со способами коммуникации
- 4.7.3. *Смишинг*-атаки
- 4.7.4. Атаки *криптоджекинга*
- 4.7.5. *Человек посередине*

4.8. Хакинг
- 4.8.1. *Рутинг* и *джейлбрейк*
- 4.8.2. Анатомия мобильной атаки
  - 4.8.2.1. Распространение угрозы
  - 4.8.2.2. Установка *вредоносных программ* на устройство
  - 4.8.2.3. Настойчивость
  - 4.8.2.4. Выполнение *полезной нагрузки* и извлечение информации
- 4.8.3. *Хакинг* устройств iOS: механизмы и средства
- 4.8.4. *Хакинг* устройств Android: механизмы и инструменты

4.9. Тестирование на проникновение
- 4.9.1. iOS *пентесты*
- 4.9.2. Android *пентесты*
- 4.9.3. Инструменты

4.10. Безопасность и защита
- 4.10.1. Настройки безопасности
  - 4.10.1.1. На устройствах IOS
  - 4.10.1.2. На устройствах Android
- 4.10.2. Меры по обеспечению безопасности
- 4.10.3. Защитные средства

Модуль 5. Безопасность в IoT

5.1. Приборы
- 5.1.1. Виды устройств
- 5.1.2. Стандартизированные архитектуры
  - 5.1.2.1. ONEM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Протоколы внедрения
- 5.1.4. Технологии подключения

5.2. Устройства IoT. Области применения
- 5.2.1. *Умный дом*
- 5.2.2. *Умный город*
- 5.2.3. Транспорт
- 5.2.4. *Носимые приборы*
- 5.2.5. Сектор здравоохранения
- 5.2.6. IioT

5.3. Протоколы коммуникации
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*
- 5.4.1. Бытовая автоматизация
- 5.4.2. Сети
- 5.4.3. Бытовая техника
- 5.4.4. Наблюдение и охрана

5.5. *Умный город*
- 5.5.1. Освещение
- 5.5.2. Метеорология
- 5.5.3. Безопасность

5.6. Транспорт
- 5.6.1. Локализация
- 5.6.2. Осуществление платежей и получение услуг
- 5.6.3. Связь

5.7. *Носимые приборы*
- 5.7.1. Умная одежда
- 5.7.2. Умные ювелирные изделия
- 5.7.3. Умные часы

5.8. Сектор здравоохранения
- 5.8.1. Контроль физической нагрузки/частоты сердечных сокращений
- 5.8.2. Наблюдение за пациентами и пожилыми людьми
- 5.8.3. Имплантируемые
- 5.8.4. Хирургические роботы

5.9. Связь
- 5.9.1. Wi-Fi/сетевые шлюзы
- 5.9.2. Bluetooth
- 5.9.3. Встроенные возможности подключения

5.10. Секьюритизация
- 5.10.1. Выделенные сети
- 5.10.2. Менеджер паролей
- 5.10.3. Использование зашифрованных протоколов
- 5.10.4. Советы по применению

Модуль 6. Этичный хакинг

6.1. Рабочая среда
- 6.1.1. Дистрибутивы Linux
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Системы виртуализации
- 6.1.3. *Sandbox*
- 6.1.4. Развертывание лабораторий

6.2. Методики
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. *Footprinting*
- 6.3.1. Разведка по открытым источникам (OSINT)
- 6.3.2. Поиск утечек данных и уязвимостей
- 6.3.3. Использование пассивных средств

6.4. Сканирование сети
- 6.4.1. Средства сканирования
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Другие средства сканирования
- 6.4.2. Методы сканирования
- 6.4.3. Методы обхода брандмауэров и IDS
- 6.4.4. *Banner Grabbing*
- 6.4.5. Сетевые диаграммы

6.5. Перечисление
- 6.5.1. Перечисление SMTP
- 6.5.2. Перечисление DNS
- 6.5.3. Перечисление NetBIOS и Samba
- 6.5.4. Перечисление LDAP
- 6.5.5. Перечисление SNMP
- 6.5.6. Другие техники перечисления

6.6. Анализ уязвимостей
- 6.6.1. Решения для сканирования уязвимостей
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Системы оценки уязвимостей
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Атаки на беспроводные сети
- 6.7.1. Методология взлома беспроводных сетей
  - 6.7.1.1. Wi-Fi *Discovery*
  - 6.7.1.2. Анализ трафика
  - 6.7.1.3. Атаки *aircrack*
    - 6.7.1.3.1. Атаки WEP
    - 6.7.1.3.2. Атаки WPA/WPA2
  - 6.7.1.4. Атаки *Evil Twin*
  - 6.7.1.5. Атаки на WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Инструменты для обеспечения безопасности беспроводных сетей

6.8. Взлом веб-серверов
- 6.8.1. *Cross Site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQLinjection*

6.9. Эксплуатация уязвимостей
- 6.9.1. Использование известных *эксплойтов*
- 6.9.2. Использование *metasploit*
- 6.9.3. Использование *вредоносных программ*
  - 6.9.3.1. Определение и сфера применения
  - 6.9.3.2. Генерация *вредоносных программ*
  - 6.9.3.3. Обход антивирусных решений

6.10. Настойчивость
- 6.10.1. Установка *руткитов*
- 6.10.2. Использование ncat
- 6.10.3. Использование запланированных задач для создания бэкдоров
- 6.10.4. Создание пользователей
- 6.10.5. Система обнаружения вторжений на хосте

Модуль 7. Реверс-инжиниринг

7.1. Компиляторы
- 7.1.1. Виды кодов
- 7.1.2. Этапы работы компилятора
- 7.1.3. Таблица символов
- 7.1.4. Менеджер ошибок
- 7.1.5. Компилятор GCC

7.2. Виды анализа в компиляторах
- 7.2.1. Лексический анализ
  - 7.2.1.1. Терминология
  - 7.2.1.2. Лексические компоненты
  - 7.2.1.3. Лексический анализатор LEX
- 7.2.2. Синтаксический анализ
  - 7.2.2.1. Контекстно-свободная грамматика
  - 7.2.2.2. Виды синтаксического анализа
    - 7.2.2.2.1. Нисходящий анализ
    - 7.2.2.2.2. Восходящий анализ
  - 7.2.2.3. Синтаксические деревья и производные
  - 7.2.2.4. Виды синтаксических анализаторов
    - 7.2.2.4.1. LR-анализаторы (*Left To Right*)
    - 7.2.2.4.2. Анализаторы LALR
- 7.2.3. Семантический анализ
  - 7.2.3.1. Атрибутивная грамматика
  - 7.2.3.2. S-атрибутная грамматика
  - 7.2.3.3. L-атрибутная грамматика

7.3. Структуры данных ассемблера
- 7.3.1. Переменные
- 7.3.2. Массивы
- 7.3.3. Указатели
- 7.3.4. Конструкции
- 7.3.5. Предметы

7.4. Структуры кода ассемблера
- 7.4.1. Структуры отбора
  - 7.4.1.1. *If, else if, Else*
  - 7.4.1.2. *Switch*
- 7.4.2. Структуры итераций
  - 7.4.2.1. *For*
  - 7.4.2.2. *While*
  - 7.4.2.3. Использование *break*
- 7.4.3. Функции

7.5. Архитектура аппаратного обеспечения x86
- 7.5.1. Архитектура процессоров в x86
- 7.5.2. Структуры данных в x86
- 7.5.3. Структуры кода в x86
- 7.5.3. Структуры кода в x86

7.6. Архитектура аппаратного обеспечения ARM
- 7.6.1. Архитектура процессоров ARM
- 7.6.2. Структуры данных в ARM
- 7.6.3. Структуры кода в ARM

7.7. Анализ статического кода
- 7.7.1. Дизассемблеры
- 7.7.2. IDA
- 7.7.3. Реконструкторы кода

7.8. Анализ динамического кода
- 7.8.1. Поведенческий анализ
  - 7.8.1.1. Коммуникация
  - 7.8.1.2. Мониторинг
- 7.8.2. Отладчики кода в Linux
- 7.8.3. Отладчики кода в Windows

7.9. Sandbox
- 7.9.1. Архитектура *Sandbox*
- 7.9.2. Обход *Sandbox*
- 7.9.3. Методы обнаружения
- 7.9.4. Методы избегания
- 7.9.5. Контрмеры
- 7.9.6. Sandbox в Linux
- 7.9.7. Sandbox в Windows
- 7.9.8. Sandbox в MacOS
- 7.9.9. Sandbox в Android

7.10. Анализ *вредоносного программного обеспечения*
- 7.10.1. Методы анализа *вредоносного ПО*
- 7.10.2. Методы обфускации *вредоносного ПО*
  - 7.10.2.1. Обфускация исполняемых файлов
  - 7.10.2.2. Ограничение среды исполнения
- 7.10.3. Инструменты анализа *вредоносного ПО*

Модуль 8. Безопасная разработка

8.1. Безопасная разработка
- 8.1.1. Качество, функциональность и безопасность
- 8.1.2. Конфиденциальность, целостность и доступность
- 8.1.3. Жизненный цикл разработки *программного обеспечения*

8.2. Этап требований
- 8.2.1. Контроль аутентификации
- 8.2.2. Контроль ролей и привилегий
- 8.2.3. Риск-ориентированные требования
- 8.2.4. Утверждение привилегий

8.3. Этапы анализа и проектирования
- 8.3.1. Доступ к компонентам и системное администрирование
- 8.3.2. Контрольные журналы
- 8.3.3. Управление сессиями
- 8.3.4. Исторические данные
- 8.3.5. Правильная обработка ошибок
- 8.3.6. Разделение функций

8.4. Этап внедрения и кодификации
- 8.4.1. Обеспечение безопасности среды разработки
- 8.4.2. Подготовка технической документации
- 8.4.3. Безопасное кодирование
- 8.4.4. Безопасность коммуникаций

8.5. Надлежащая практика безопасного кодирования
- 8.5.1. Валидация входных данных
- 8.5.2. Кодирование выходных данных
- 8.5.3. Стиль программирования
- 8.5.4. Ведение журнала изменений
- 8.5.5. Криптографические практики
- 8.5.6. Управление ошибками и логами
- 8.5.7. Управление архивами
- 8.5.8. Управление памятью
- 8.5.9. Стандартизация и повторное использование функций безопасности

8.6. Подготовка сервера и *укрепление*
- 8.6.1. Управление пользователями, группами и ролями на сервере
- 8.6.2. Установка ПО
- 8.6.3. *Укрепление* сервера
- 8.6.4. Надежная конфигурация среды приложения

8.7. Подготовка БД и *укрепление*
- 8.7.1. Оптимизация движка БД
- 8.7.2. Создание собственного пользователя для приложения
- 8.7.3. Назначение необходимых привилегий пользователю
- 8.7.4. *Укрепление* БД

8.8. Этап тестирования
- 8.8.1. Контроль качества в управлении безопасностью
- 8.8.2. Поэтапная проверка кода
- 8.8.3. Проверка управления конфигурации
- 8.8.4. Тестирование методом черного ящика

8.9. Подготовка к переходу на производство
- 8.9.1. Осуществлять контроль за изменениями
- 8.9.2. Осуществлять процедуры переналадки производства
- 8.9.3. Осуществлять процедуру *отката*
- 8.9.4. Предпроизводственное тестирование

8.10. Фаза технического обслуживания
- 8.10.1. Обеспечение на основе рисков
- 8.10.2. Тестирование обслуживания системы безопасности белого ящика
- 8.10.3. Тестирование обслуживания системы безопасности черного ящика

Модуль 9. Практическое внедрение политик безопасности в программном и аппаратном обеспечении

9.1. Практическое внедрение политик безопасности в программном и аппаратном обеспечении
- 9.1.1. Осуществление идентификации и авторизации
- 9.1.2. Внедрение методов идентификации
- 9.1.3. Средства технической авторизации

9.2. Технологии идентификации и авторизации
- 9.2.1. Идентификатор и OTP
- 9.2.2. USB-токен или смарт-карта PKI
- 9.2.3. Ключ "Конфиденциальная защита"
- 9.2.4. Активная RFID-метка

9.3. Политики безопасности в отношении доступа к программному обеспечению и системам
- 9.3.1. Внедрение политик контроля доступа
- 9.3.2. Внедрение политики доступа к коммуникациям
- 9.3.3. Типы инструментов безопасности для контроля доступа

9.4. Управление доступом к пользователям
- 9.4.1. Управление правами доступа
- 9.4.2. Разделение ролей и функций доступа
- 9.4.3. Реализация прав доступа в системах

9.5. Контроль доступа к системам и приложениям
- 9.5.1. Норма минимального доступа
- 9.5.2. Технологии безопасного входа в систему
- 9.5.3. Политики безопасности паролей

9.6. Технологии систем идентификации
- 9.6.1. Активный каталог
- 9.6.2. OTP
- 9.6.3. PAP, CHAP
- 9.6.4. KERBEROS, DIAMETER, NTLM

9.7. CIS Controls для укрепления системы
- 9.7.1. Базовые CIS Controls
- 9.7.2. Основные CIS Controls
- 9.7.3. Организационные CIS Controls

9.8. Эксплуатационная безопасность
- 9.8.1. Защита от вредоносного кода
- 9.8.2. Резервные копии
- 9.8.3. Записи о деятельности и мониторинге

9.9. Управление техническими уязвимостями
- 9.9.1. Технические уязвимости
- 9.9.2. Управление техническими уязвимостями
- 9.9.3. Ограничения на установку программного обеспечения

9.10. Внедрение практик политики безопасности
- 9.10.1. Логические уязвимости
- 9.10.2. Осуществление политики защиты

Модуль 10. Судебная экспертиза

10.1. Сбор и воспроизведение данных
- 10.1.1. Сбор волатильных данных
  - 10.1.1.1. Системная информация
  - 10.1.1.2. Сетевая информация
  - 10.1.1.3. Порядок волатильности
- 10.1.2. Сбор статистических данных
  - 10.1.2.1. Создание дублирующего изображения
  - 10.1.2.2. Подготовка документа о цепочке поставок
- 10.1.3. Методы валидации полученных данных
  - 10.1.3.1. Методы для Linux
  - 10.1.3.2. Методы для Windows

10.2. Оценка и преодоление антикриминалистических методов
- 10.2.1. Цели анктикриминалистических методов
- 10.2.2. Удаление данных
  - 10.2.2.1. Удаление данных и файлов
  - 10.2.2.2. Восстановление файлов
  - 10.2.2.3. Восстановление удаленных разделов
- 10.2.3. Защита с помощью пароля
- 10.2.4. Стеганография
- 10.2.5. Безопасное удаление данных с устройств
- 10.2.6. Шифрование

10.3. Судебная экспертиза операционных систем
- 10.3.1. Судебная экспертиза Windows
- 10.3.2. Судебная экспертиза Linux
- 10.3.3. Судебная экспертиза Mac

10.4. Судебная экспертиза сети
- 10.4.1. Анализ журнала
- 10.4.2. Корреляция данных
- 10.4.3. Расследование сети
- 10.4.4. Шаги, необходимые для проведения криминалистической экспертизы сети

10.5. Судебная экспертиза Web
- 10.5.1. Расследование веб-атак
- 10.5.2. Обнаружение атак
- 10.5.3. Локализация IP-адресов

10.6. Криминалистическая экспертиза баз данных
- 10.6.1. Судебная экспертиза MSSQL
- 10.6.2. Судебная экспертиза MySQL
- 10.6.3. Судебная экспертиза PostgreSQL
- 10.6.4. Судебная экспертиза MongoDB

10.7. Судебная экспертиза облачного сервиса
- 10.7.1. Виды преступлений в облаке
  - 10.7.1.1. Облако как субъект
  - 10.7.1.2. Облако как объект
  - 10.7.1.3. Облако как средство
- 10.7.2. Трудности судебной экспертизы в облаке
- 10.7.3. Исследование услуг по хранению данных в облаке
- 10.7.4. Средства проведения криминалистической экспертизы в облаке

10.8. Расследования преступлений, связанных с электронной почтой
- 10.8.1. Почтовые системы
  - 10.8.1.1. Почтовые клиенты
  - 10.8.1.2. Почтовые серверы
  - 10.8.1.3. Сервер SMTP
  - 10.8.1.4. Сервер POP3
  - 10.8.1.5. Сервер IMAP4
- 10.8.2. Преступления, связанные с электронной почтой
- 10.8.3. Сообщение на почте
  - 10.8.3.1. Стандартные заголовки
  - 10.8.3.2. Расширенные заголовки
- 10.8.4. Шаги по расследованию этих преступлений
- 10.8.5. Средства криминалистической экспертизы электронной почты

10.9. Судебная экспертиза мобильных устройств
- 10.9.1. Сотовые сети
  - 10.9.1.1. Виды сетей
  - 10.9.1.2. Содержимое хранилища CDR
- 10.9.2. *Модуль идентификации абонента* (SIM)
- 10.9.3. Логическое получение
- 10.9.4. Физическое получение
- 10.9.5. Получение файловой системы

10.10. Составление и представление отчетов о судебной экспертизе
- 10.10.1. Важные аспекты заключения судебной экспертизы
- 10.10.2. Классификация и виды отчетов
- 10.10.3. Руководство по написанию отчета
- 10.10.4. Презентация отчета
  - 10.10.4.1. Предварительная подготовка к даче показаний
  - 10.10.4.2. Изложение
  - 10.10.4.3. Общение с прессой

Модуль 11. Безопасность при проектировании и разработке систем

11.1. Информационные системы
- 11.1.1. Домены информационной системы
- 11.1.2. Компоненты информационных систем
- 11.1.3. Виды деятельности информационной системы
- 11.1.4. Жизненный цикл информационной системы
- 11.1.5. Ресурсы информационной системы

11.2. Информационные системы. Типология
- 11.2.1. Виды информационных систем
  - 11.2.1.1. Бизнес-системы
  - 11.2.1.2. Стратегические
  - 11.2.1.3. В зависимости от сферы применения
  - 11.2.1.4. Специфические
- 11.2.2. Информационные системы. Реальные примеры
- 11.2.3. Эволюция: информационных систем: Этапы
- 11.2.4. Методологии информационных систем

11.3. Безопасность информационных систем. Правовые последствия
- 11.3.1. Доступ к данным
- 11.3.2. Угрозы безопасности: Уязвимости
- 11.3.3. Правовые последствия: Преступление
- 11.3.4. Процедуры по техническому обслуживанию информационной системы

11.4. Безопасность информационных систем. Протоколы безопасности
- 11.4.1. Безопасность информационных систем
  - 11.4.1.1. Целостность
  - 11.4.1.2. Конфиденциальность
  - 11.4.1.3. Доступность
  - 11.4.1.4. Аутентификация
- 11.4.2. Услуги по обеспечению безопасности
- 11.4.3. Протоколы информационной безопасности. Типология
- 11.4.4. Чувствительность информационных систем

11.5. Безопасность информационных систем. Меры и системы контроля доступа
- 11.5.1. Меры по обеспечению безопасности
- 11.5.2. Вид мер по обеспечению безопасности
  - 11.5.2.1. Профилактика
  - 11.5.2.2. Обнаружение
  - 11.5.2.3. Правильность
- 11.5.3. Системы контроля доступа. Типология
- 11.5.4. Криптография

11.6. Безопасность сети и интернета
- 11.6.1. Брандмауэры
- 11.6.2. Цифровая идентификация
- 11.6.3. Вирусы и черви
- 11.6.4. Хакинг
- 11.6.5. Примеры и реальные кейсы

11.7. Компьютерные преступления
- 11.7.1. Компьютерное преступление
- 11.7.2. Компьютерные преступления. Типология
- 11.7.3. Компьютерное преступление. Атака. Типологии
- 11.7.4. Кейс в виртуальной реальности
- 11.7.5. Профили правонарушителей и жертв. Типизация преступлений
- 11.7.6. Компьютерные преступления. Примеры и реальные кейсы

11.8. План по обеспечению безопасности информационной системы
- 11.8.1. План по обеспечению безопасности. Цели
- 11.8.2. План по обеспечению безопасности. Планирование
- 11.8.3. План по рискам. Анализ
- 11.8.4. Политика безопасности. Внедрение в организацию
- 11.8.5. План по обеспечению безопасности. Внедрение в организацию
- 11.8.6. Процедуры по обеспечению безопасности. Типы
- 11.8.7. План по обеспечению безопасности. Примеры

11.9. План действий в чрезвычайных ситуациях
- 11.9.1. План действий в непредвиденных ситуациях. Функции
- 11.9.2. План действий в чрезвычайных ситуациях: Элементы и цели
- 11.9.3. План непредвиденных в организации. Внедрение
- 11.9.4. План действий в непредвиденных ситуациях. Примеры

11.10. Управление безопасностью информационных систем
- 11.10.1. Правовые нормы
- 11.10.2. Стандарты
- 11.10.3. Сертификация
- 11.10.4. Технологии

Модуль 12. Архитектуры и модели информационной безопасности

12.1. Архитектура информационной безопасности
- 12.1.1. SGSI / PDS
- 12.1.2. Стратегическая согласованность
- 12.1.3. Управление рисками
- 12.1.4. Измерение результативности

12.2. Модели информационной безопасности
- 12.2.1. На основе политик безопасности
- 12.2.2. На основе инструментов защиты
- 12.2.3. На основе вовлеченных в работу команд

12.3. Модель безопасности. Ключевые компоненты
- 12.3.1. Определение рисков
- 12.3.2. Определение средств контроля
- 12.3.3. Постоянная оценка уровня риска
- 12.3.4. План по информированию сотрудников, поставщиков, партнеров и т. д.

12.4. Процесс управления рисками
- 12.4.1. Определение активов
- 12.4.2. Определение угроз
- 12.4.3. Оценка рисков
- 12.4.4. Определение приоритетов контроля
- 12.4.5. Переоценка и остаточный риск

12.5. Бизнес-процессы и информационная безопасность
- 12.5.1. Бизнес-процессы
- 12.5.2. Оценка рисков на основе параметров бизнеса
- 12.5.3. Анализ влияния на бизнес
- 12.5.4. Деловые операции и информационная безопасность

12.6. Процесс непрерывного улучшения
- 12.6.1. Цикл Деминга
  - 12.6.1.1. Планировать
  - 12.6.1.2. Создавать
  - 12.6.1.3. Верифицировать
  - 12.6.1.4. Действовать

12.7. Архитектура безопасности
- 12.7.1. Выбор и гомогенизация технологий
- 12.7.2. Управление идентификацией. Аутентификация
- 12.7.3. Управление доступом. Полномочия
- 12.7.4. Безопасность сетевой инфраструктуры
- 12.7.5. Технологии и решения в области шифрования
- 12.7.6. Безопасность оконечного оборудования (EDR)

12.8. Нормативно-правовая база
- 12.8.1. Отраслевые нормативные акты
- 12.8.2. Сертификация
- 12.8.3. Законодательство

12.9. Стандарт ISO 27001
- 12.9.1. Внедрение
- 12.9.2. Сертификация
- 12.9.3. Аудиты и тесты на вторжение
- 12.9.4. Непрерывное управление рисками
- 12.9.5. Классификация информации

12.10. Законодательство о конфиденциальности. GDPR
- 12.10.1. Сфера действия Общего регламента по защите данных (GDPR)
- 12.10.2. Персональные данные
- 12.10.3. Роли в обработке персональных данных
- 12.10.4. Права ARCO
- 12.10.5. Должностное лицо по защите данных (DPO). Функции

Модуль 13. Система управления информационной безопасностью (СУИБ)

13.1. Информационная безопасность. Основные вопросы
- 13.1.1. Информационная безопасность
  - 13.1.1.1. Конфиденциальность
  - 13.1.1.2. Целостность
  - 13.1.1.3. Доступность
  - 13.1.1.4. Меры информационной безопасности

13.2. Система управления информационной безопасностью
- 13.2.1. Модели управления информационной безопасностью
- 13.2.2. Документы для внедрения СУИБ
- 13.2.3. Уровни и средства контроля СУИБ

13.3. Международные нормы и стандарты
- 13.3.1. Международные стандарты в области информационной безопасности
- 13.3.2. Происхождение и эволюция стандарта
- 13.3.3. Международные стандарты управления информационной безопасностью
- 13.3.4. Другие справочные нормы

13.4. Нормы ISO/IEC 27.000
- 13.4.1. Предмет и область применения
- 13.4.2. Структура нормы
- 13.4.3. Сертификация
- 13.4.4. Этапы аккредитации
- 13.4.5. Преимущества норм ISO/IEC 27.000

13.5. Разработка и внедрение общей системы информационной безопасности
- 13.5.1. Этапы внедрения системы общей информационной безопасности
- 13.5.2. План по обеспечению непрерывности бизнеса

13.6. Фаза I: диагностика
- 13.6.1. Предварительная диагностика
- 13.6.2. Определение уровня стратификации
- 13.6.3. Уровень соответствия стандартам/нормам

13.7. Фаза II: подготовка
- 13.7.1. Организационная трансформация
- 13.7.2. Анализ применимых правил техники безопасности
- 13.7.3. Сфера применения общей системы информационной безопасности
- 13.7.4. Политика общей системы информационной безопасности
- 13.7.5. Цели общей системы информационной безопасности

13.8. Фаза III: планирование
- 13.8.1. Классификация активов
- 13.8.2. Оценка рисков
- 13.8.3. Выявление угроз и рисков

13.9. Фаза IV: реализация и мониторинг
- 13.9.1. Анализ результатов
- 13.9.2. Распределение обязанностей
- 13.9.3. Сроки выполнения плана действий
- 13.9.4. Мониторинг и аудиты

13.10. Политика безопасности в управлении инцидентами
- 13.10.1. Стадии
- 13.10.2. Категоризация инцидентов
- 13.10.3. Управление и процедуры в случае инцидентов

Модуль 14. Управление ИТ-безопасностью

14.1. Управление безопасностью
- 14.1.1. Операции по обеспечению безопасности
- 14.1.2. Правовые и нормативные аспекты
- 14.1.3. Расширение возможностей бизнеса
- 14.1.4. Управление рисками
- 14.1.5. Управление идентификацией и доступом

14.2. Структура зоны безопасности. Офис CISO
- 14.2.1. Организационная структура. Место CISO в структуре
- 14.2.2. Линии защиты
- 14.2.3. Организационная схема офиса CISO
- 14.2.4. Управление бюджетом

14.3. Управление в сфере безопасности
- 14.3.1. Комитет по безопасности
- 14.3.2. Комитет по мониторингу рисков
- 14.3.3. Комитет по аудиту
- 14.3.4. Кризисный комитет

14.4. Управление в сфере безопасности. Функции
- 14.4.1. Политики и стандарты
- 14.4.2. Генеральный план по обеспечению безопасности
- 14.4.3. Приборные панели
- 14.4.4. Повышение осведомленности и обучение
- 14.4.5. Безопасность цепи поставок

14.5. Операции по обеспечению безопасности
- 14.5.1. Управление идентификацией и доступом
- 14.5.2. Конфигурация правил сетевой безопасности. Файрволы
- 14.5.3. Управление платформами IDS/IPS
- 14.5.4. Анализ уязвимостей

14.6. Рамки кибербезопасности. NIST CSF
- 14.6.1. Методология NIST
  - 14.6.1.1. Идентифицировать
  - 14.6.1.2. Защитить
  - 14.6.1.3. Обнаружить
  - 14.6.1.4. Ответить
  - 14.6.1.5. Восстановить

14.7. Операционный центр безопасности (SOC). Функции
- 14.7.1. Защита. *Red Team, пентестинг, разведка угроз*
- 14.7.2. Выявление. SIEM, *аналитика поведения пользователей, предотвращение мошенничества*
- 14.7.3. Ответ

14.8. Аудиты безопасности
- 14.8.1. Тест на вторжение
- 14.8.2. Упражнения по *red team*
- 14.8.3. Аудит исходного кода. Безопасная разработка
- 14.8.4. Безопасность компонентов (*цепочка поставок программного обеспечения*)
- 14.8.5. Судебная экспертиза

14.9. Реагирование на инциденты
- 14.9.1. Подготовка
- 14.9.2. Выявление, анализ и отчетность
- 14.9.3. Сдерживание, искоренение и восстановление
- 14.9.4. Деятельность после инцидента
  - 14.9.4.1. Сохранение доказательств
  - 14.9.4.2. Судебная экспертиза
  - 14.9.4.3. Управление разрывами
- 14.9.5. Официальное руководство по управлению киберинцидентами

14.10. Управление уязвимостями
- 14.10.1. Анализ уязвимостей
- 14.10.2. Оценка уязвимости
- 14.10.3. Системное базирование
- 14.10.4. Уязвимость нулевого дня. Zero-day

Модуль 15. Политика управления инцидентами безопасности

15.1. Политики и усовершенствования в области управления инцидентами информационной безопасности
- 15.1.1. Управление инцидентами
- 15.1.2. Ответственность и процедуры
- 15.1.3. Оповещение о событиях

15.2. Системы обнаружения и предотвращения вторжений (IDS/IPS)
- 15.2.1. Рабочие данные системы
- 15.2.2. Типы систем обнаружения вторжений
- 15.2.3. Критерии для размещения IDS/IPS

15.3. Реагирование на инциденты безопасности
- 15.3.1. Процедура сбора данных
- 15.3.2. Процесс проверки вторжения
- 15.3.3. Органы CERT

15.4. Процесс уведомления и управления попытками вторжения
- 15.4.1. Обязанности в процессе уведомления
- 15.4.2. Классификация инцидентов
- 15.4.3. Процесс разрешения и восстановления

15.5. Криминалистический анализ как политика безопасности
- 15.5.1. Цифровые доказательства: нестабильные данные и энергонезависимые данные
- 15.5.2. Анализ и сбор электронных доказательств
  - 15.5.2.1. Анализ электронных доказательств
  - 15.5.2.2. Сбор электронных доказательств

15.6. Инструменты систем обнаружения и предотвращения вторжений (IDS/IPS)
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. Инструменты централизации событий
- 15.7.1. SIM
- 15.7.2. SEM
- 15.7.3. SIEM

15.8. Руководство по безопасности CCN-STIC 817
- 15.8.1. Управление киберинцидентами
- 15.8.2. Метрики и индикаторы

15.9. NIST SP800-61
- 15.9.1. Возможности реагирования на инциденты информационной безопасности
- 15.9.2. Обработка инцидента
- 15.9.3. Координация и обмен информацией

15.10. Стандарт ISO 27035
- 15.10.1. Норма ISO 27035. Принципы управления инцидентами
- 15.10.2. Руководство по разработке плана управления инцидентами
- 15.10.3. Руководство по операциям реагирования на инциденты

Модуль 16. Анализ рисков и среды ИТ-безопасности

16.1. Анализ среды
- 16.1.1. Анализ экономического положения
  - 16.1.1.1. VUCA-среды
    - 16.1.1.1.1. Волатильность
    - 16.1.1.1.2. Неопределенность
    - 16.1.1.1.3. Сложность
    - 16.1.1.1.4. Неоднозначность
  - 16.1.1.2. BANI-среды
    - 16.1.1.2.1. Хрупкость
    - 16.1.1.2.2. Тревожность
    - 16.1.1.2.3. Нелинейность
    - 16.1.1.2.4. Непонятность
- 16.1.2. Анализ общей среды. PESTEL
  - 16.1.2.1. Политический
  - 16.1.2.2. Экономический
  - 16.1.2.3. Социальный
  - 16.1.2.4. Технологичный
  - 16.1.2.5. Экологичный
  - 16.1.2.6. Юридический
- 16.1.3. Анализ внутреннего положения. SWOT-анализ
  - 16.1.3.1. Цели
  - 16.1.3.2. Угрозы
  - 16.1.3.3. Возможности
  - 16.1.3.4. Преимущества

16.2. Риск и неопределенность
- 16.2.1. Риск
- 16.2.2. Управление рисками
- 16.2.3. Стандарты управления рисками

16.3. Руководства по управлению рисками ISO 31.000:2018
- 16.3.1. Цель
- 16.3.2. Принципы
- 16.3.3. Система координат
- 16.3.4. Процесс

16.4. Методология анализа и управления рисками информационных систем (MAGERIT)
- 16.4.1. Методология MAGERIT
  - 16.4.1.1. Цели
  - 16.4.1.2. Методика
  - 16.4.1.3. Элементы
  - 16.4.1.4. Техники
  - 16.4.1.5. Доступные инструменты (PILAR)

16.5. Передача киберрисков
- 16.5.1. Передача рисков
- 16.5.2. Киберриски. Типология
- 16.5.3. Страхование от киберрисков

16.6. Agile-методологии для управления рисками
- 16.6.1. Методологии Agile
- 16.6.2. Scrum для управления рисками
- 16.6.3. *Управление рисками в Agile*

16.7. Технологии для управления рисками
- 16.7.1. Применение искусственного интеллекта в управлении рисками
- 16.7.2. *Блокчейн* и криптография. Методы сохранения стоимости
- 16.7.3. Квантовые вычисления. Возможности или угрозы

16.8. Составление карт ИТ-рисков на основе Agile-методологий
- 16.8.1. Представление вероятности и последствий в Agile-средах
- 16.8.2. Риск как угроза стоимости
- 16.8.3. Революция в управлении проектами и Agile-процессами на основе KRI

16.9. *Риск-ориентированное* управление
- 16.9.1. *Ориентирование на риск*
- 16.9.2. *Риск-ориентированное* управление
- 16.9.3. Разработка модели управления бизнесом с учетом рисков

16.10. Инновации и цифровая трансформация в управлении ИТ-рисками
- 16.10.1. Agile-управление рисками как источник инноваций в бизнесе
- 16.10.2. Преобразование данных в полезную для принятия решений информацию
- 16.10.3. Целостный взгляд на предприятие через призму риска

Модуль 17. Политики безопасности для анализа угроз в информационных системах

17.1. Управление угрозами в политике безопасности
- 17.1.1. Управление рисками
- 17.1.2. Риск безопасности
- 17.1.3. Методологии в управлении угрозами
- 17.1.4. Внедрение методологий

17.2. Этапы управления угрозами
- 17.2.1. Идентификация
- 17.2.2. Анализ
- 17.2.3. Локализация
- 17.2.4. Защитные меры

17.3. Аудит систем на предмет обнаружения угроз
- 17.3.1. Классификация и информационный поток
- 17.3.2. Анализ уязвимых процессов

17.4. Классификация рисков
- 17.4.1. Виды рисков
- 17.4.2. Расчет вероятности возникновения угрозы
- 17.4.3. Остаточный риск

17.5. Обработка риска
- 17.5.1. Осуществление мер по обеспечению безопасности
- 17.5.2. Передача или поглощение

17.6. Контроль рисков
- 17.6.1. Непрерывный процесс управления рисками
- 17.6.2. Внедрение метрики безопасности
- 17.6.3. Стратегическая модель метрики информационной безопасности

17.7. Практические методологии анализа и контроля угроз
- 17.7.1. Список угроз
- 17.7.2. Список контрольных мероприятий
- 17.7.3. Список мер обеспечения безопасности

17.8. Стандарт ISO 27005
- 17.8.1. Идентификация рисков
- 17.8.2. Анализ риска
- 17.8.3. Оценка рисков

17.9. Матрица рисков, воздействий и угроз
- 17.9.1. Данные, системы и персонал
- 17.9.2. Вероятность возникновения угрозы
- 17.9.3. Размер ущерба

17.10. Разработка этапов и процессов анализа угроз
- 17.10.1. Выявление критических элементов организации
- 17.10.2. Определение угроз и последствий
- 17.10.3. Анализ последствий и рисков
- 17.10.4. Методики

Модуль 18. Практическая реализация политики безопасности перед угрозой атак

18.1. *System Hacking*
- 18.1.1. Риски и уязвимости
- 18.1.2. Контрмеры

18.2. DoS в сервисах
- 18.2.1. Риски и уязвимости
- 18.2.2. Контрмеры

18.3. *Session Hijacking*
- 18.3.1. Процесс *Hijacking*
- 18.3.2. Меры противодействия *Hijacking*

18.4. Обход IDS, *Firewalls and Honeypots*
- 18.4.1. Методы избегания
- 18.4.2. Осуществление контрмер

18.5. *Hacking Web Servers*
- 18.5.1. Атаки на веб-серверы
- 18.5.2. Реализация мер по обеспечению безопасности

18.6. *Hacking Web Applications*
- 18.6.1. Атаки на веб-приложения
- 18.6.2. Реализация мер по обеспечению безопасности

18.7. *Hacking Wireless Networks*
- 18.7.1. Уязвимости в сетях wifi
- 18.7.2. Реализация мер по обеспечению безопасности

18.8. *Hacking Mobile Platforms*
- 18.8.1. Уязвимости мобильных платформ
- 18.8.2. Осуществление контрмер

18.9. *Программы-вымогатели (Ransomware)*
- 18.9.1. Уязвимости, связанные с программой-вымогателем
- 18.9.2. Осуществление контрмер

18.10. Социальная инженерия
- 18.10.1. Типы социальной инженерии
- 18.10.2. Меры противодействия социальной инженерии

Модуль 19. Криптография в ИТ

19.1. Криптография
- 19.1.1. Криптография
- 19.1.2. Математические основы

19.2. Криптология
- 19.2.1. Криптология
- 19.2.2. Криптоанализ
- 19.2.3. Стеганография и стегоанализ

19.3. Криптографические протоколы
- 19.3.1. Базовые блоки
- 19.3.2. Базовые протоколы
- 19.3.3. Промежуточные протоколы
- 19.3.4. Расширенные протоколы
- 19.3.5. Экзотерические протоколы

19.4. Криптографические методы
- 19.4.1. Длина ключа
- 19.4.2. Управление ключами
- 19.4.3. Типы алгоритмов
- 19.4.4. Агрегатные функции. *Хеш-функция*
- 19.4.5. Генераторы псевдослучайных чисел
- 19.4.6. Использование алгоритмов

19.5. Симметричная криптография
- 19.5.1. Блочные шифры
- 19.5.2. DES (*Data Encryption Standard*)
- 19.5.3. Алгоритм RC4
- 19.5.4. AES (*Advanced Encryption Standard*)
- 19.5.5. Комбинация блочных шифров
- 19.5.6. Получение ключей

19.6. Асимметричная криптография
- 19.6.1. Протокол Диффи — Хеллмана
- 19.6.2. DSA (*Digital Signature Algorithm*)
- 19.6.3. RSA (Ривест, Шамир и Адлеман)
- 19.6.4. Эллиптическая кривая
- 19.6.5. Асимметричная криптография. Типология

19.7. Цифровые сертификаты
- 19.7.1. Цифровая подпись
- 19.7.2. Сертификаты X509
- 19.7.3. Инфраструктура открытых ключей (PKI)

19.8. Способы реализации
- 19.8.1. Kerberos
- 19.8.2. IBM CCA
- 19.8.3. *Pretty Good Privacy* (PGP)
- 19.8.4. ISO *Authentication Framework*
- 19.8.5. SSL и TLS
- 19.8.6. Смарт-карты в платежных средствах (EMV)
- 19.8.7. Протоколы мобильной связи
- 19.8.8. *Блокчейн*

19.9. Стеганография
- 19.9.1. Стеганография
- 19.9.2. Стегоанализ
- 19.9.3. Применение и использование

19.10. Квантовая криптография
- 19.10.1. Квантовые алгоритмы
- 19.10.2. Защита алгоритмов от квантовых вычислений
- 19.10.3. Квантовое распределение ключей

Модуль 20. Управление идентификацией и доступом в ИТ-безопасности

20.1. Управление идентификацией и доступом (IAM)
- 20.1.1. Цифровая идентичность
- 20.1.2. Управление идентификацией
- 20.1.3. Федеративные удостоверения

20.2. Управление физическим доступом
- 20.2.1. Системы защиты
- 20.2.2. Безопасность территорий
- 20.2.3. Восстановительные комплексы

20.3. Управление логическим доступом
- 20.1.1. Аутентификация: Типология
- 20.1.2. Протоколы аутентификации
- 20.1.3. Атаки на аутентификацию

20.4. Управление логическим доступом. Многофакторная аутентификация (MFA)
- 20.4.1. Управление логическим доступом. Многофакторная аутентификация (MFA)
- 20.4.2. Пароли. Важность
- 20.4.3. Атаки на аутентификацию

20.5. Управление логическим доступом. Биометрическая аутентификация
- 20.5.1. Контроль логического доступа. Биометрическая аутентификация
  - 20.5.1.1. Биометрическая аутентификация. Требования
- 20.5.2. Функционирование
- 20.5.3. Модели и методы

20.6. Системы управления аутентификацией
- 20.6.1. *Единая регистрация*
- 20.6.2. Kerberos
- 20.6.3. Системы AAA

20.7. Системы управления аутентификацией: Системы AAA
- 20.7.1. TACACS
- 20.7.2. RADIUS
- 20.7.3. DIAMETER

20.8. Службы по управлению доступом
- 20.8.1. FW — межсетевые экраны
- 20.8.2. VPN — виртуальные частные сети
- 20.8.3. IDS — система обнаружения вторжений

20.9. Системы управления доступом к сети
- 20.9.1. NAC
- 20.9.2. Архитектура и элементы
- 20.9.3. Эксплуатация и стандартизация

20.10. Доступ к беспроводным сетям
- 20.10.1. Виды беспроводных сетей
- 20.10.2. Безопасность в беспроводных сетях
- 20.10.3. Атаки на беспроводные сети

Модуль 21. Безопасность в коммуникациях и работе программного обеспечения

21.1. Информационная безопасность в сфере коммуникаций и эксплуатации программного обеспечения
- 21.1.1. Информационная безопасность
- 21.1.2. Кибербезопасность
- 21.1.3. Облачная безопасность

21.2. Информационная безопасность в сфере коммуникаций и эксплуатации программного обеспечения. Типология
- 21.2.1. Физическая безопасность
- 21.2.2. Логическая безопасность

21.3. Безопасность в сфере коммуникаций
- 21.3.1. Основные элементы
- 21.3.2. Сетевая безопасность
- 21.3.3. Передовая практика

21.4. Кибербезопасность
- 21.4.1. Социальная инженерия
- 21.4.2. *Глубокая сеть*
- 21.4.3. *Фишинг*
- 21.4.4. *Вредоносное программное обеспечение*

21.5. Безопасная разработка в сфере коммуникации и эксплуатации программного обеспечения
- 21.1.1. Безопасная разработка. Протокол HTTP
- 21.1.2. Безопасная разработка. Жизненный цикл
- 21.1.3. Безопасная разработка. PHP-безопасность
- 21.1.4. Безопасная разработка. NET-безопасность
- 21.1.5. Безопасная разработка. Передовая практика

21.6. Системы управления информационной безопасностью в сфере коммуникации и эксплуатации программного обеспечения
- 21.6.1. GDPR
- 21.6.2. ISO 27021
- 21.6.3. ISO 27017/18

21.7. SIEM-технологии
- 21.7.1. SIEM-технологии
- 21.7.2. Деятельность SOC
- 21.7.3. SIEM: *поставщики*

21.8. Роль в обеспечении безопасности в организациях
- 21.8.1. Роли в организациях
- 21.8.2. Роль специалистов в области IoT в компаниях
- 21.8.3. Признанные на рынке сертификаты

21.9. Судебная экспертиза
- 21.9.1. Судебная экспертиза
- 21.9.2. Криминалистическая экспертиза. Методология
- 21.9.3. Криминалистическая экспертиза. Инструменты и внедрение

21.10. Кибербезопасность сегодня
- 21.10.1. Крупные кибернетические атаки
- 21.10.2. Прогнозы по трудоустройству
- 21.10.3. Задачи

Модуль 22. Безопасность в облачных *средах*

22.1. Безопасность в среде *облачных вычислений*
- 22.1.1. Безопасность в среде *облачных вычислений*
- 22.1.2. Безопасность в среде *облачных вычислений.* Угрозы и риски безопасности
- 22.1.3. Безопасность в среде *облачных вычислений.* Ключевые аспекты безопасности

22.2. Виды *облачной* инфраструктуры
- 22.2.1. Публичная
- 22.2.2. Частная
- 22.2.3. Гибридная

22.3. Модель совместного управления
- 22.3.1. Элементы безопасности, управляемые поставщиком
- 22.3.2. Элементы, управляемые клиентом
- 22.3.3. Определение стратегии безопасности

22.4. Профилактические механизмы
- 22.4.1. Системы управления аутентификацией
- 22.4.2. Система управления авторизацией: Политики доступа
- 22.4.3. Системы управления ключами

22.5. Секьюритизация систем
- 22.5.1. Секьюритизация систем хранения
- 22.5.2. Защита систем баз данных
- 22.5.3. Секьюритизация данных при передаче

22.6. Защита инфраструктуры
- 22.6.1. Проектирование и внедрение безопасных сетей
- 22.6.2. Безопасность вычислительных ресурсов
- 22.6.3. Инструменты и ресурсы для защиты инфраструктуры

22.7. Обнаружение угроз и атак
- 22.7.1. Системы аудита, *ведения журнала* и мониторинга
- 22.7.2. Системы событий и сигнализации
- 22.7.3. Системы SIEM

22.8. Реагирование на инциденты
- 22.8.1. План по реагированию на инциденты
- 22.8.2. Непрерывность бизнеса
- 22.8.3. Криминалистический анализ и устранение последствий инцидентов аналогичного характера

22.9. Безопасность в публичных *облаках*
- 22.9.1. AWS (Amazon Web Services)
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle Cloud

22.10. Регулирование и соблюдение
- 22.10.1. Соблюдение норм безопасности
- 22.10.2. Управление рисками
- 22.10.3. Люди и процессы в организациях

Модуль 23. Инструменты мониторинга в политике безопасности информационных систем

23.1. Политики мониторинга информационных систем
- 23.1.1. Мониторинг системы
- 23.1.2. Метрические данные
- 23.1.3. Типы метрики

23.2. Аудит и регистрация систем
- 23.2.1. Аудит и регистрация Windows
- 23.2.2. Аудит и регистрация Linux

23.3. Протокол SNMP. *Simple Network Management Protocol*
- 23.3.1. Протокол SNMP
- 23.3.2. Как работает SNMP
- 23.3.3. SNMP-инструменты

23.4. Мониторинг сети
- 23.4.1. Сетевой мониторинг в системах управления
- 23.4.2. Инструменты мониторинга для систем управления

23.5. Nagios. Система мониторинга сети
- 23.5.1. Nagios
- 23.5.2. Как работает Nagios
- 23.5.3. Установка Nagios

23.6. Zabbix. Система мониторинга сети
- 23.6.1. Zabbix
- 23.6.2. Как работает Zabbix
- 23.6.3. Установка Zabbix

23.7. Cacti. Система мониторинга сети
- 23.7.1. Cacti
- 23.7.2. Как работает Cacti
- 23.7.3. Установка Cacti

23.8. Pandora. Система мониторинга сети
- 23.8.1. Pandora
- 23.8.2. Как работает Pandora
- 23.8.3. Установка Pandora

23.9. SolarWinds. Система мониторинга сети
- 23.9.1. SolarWinds
- 23.9.2. Как работает SolarWinds
- 23.9.3. Установка SolarWinds

23.10. Правила мониторинга
- 23.10.1. CIS Controls по аудиту и регистрации
- 23.10.2. NIST 800-123 (США)

Модуль 24. Безопасность в коммуникациях между устройствами интернета вещей (IoT)

24.1. От телеметрии к IoT
- 24.1.1. Телеметрия
- 24.1.2. Межмашинное взаимодействие (M2M)
- 24.1.3. Демократизация телеметрии

24.2. Эталонные модели IoT
- 24.2.1. Эталонные модели IoT
- 24.2.2. Упрощенная архитектура IoT

24.3. Уязвимости безопасности IoT
- 24.3.1. IoT-устройства
- 24.3.2. Устройства IoT. Примеры использования
- 24.3.3. Устройства IoT. Уязвимости

24.4. IoT-соединение
- 24.4.1. Сети PAN, LAN, WAN
- 24.4.2. Беспроводные технологии, не относящиеся к IoT
- 24.4.3. Беспроводные технологии LPWAN

24.5. LPWAN-технологии
- 24.5.1. "Железный треугольник" сетей LPWAN
- 24.5.2. Свободные частотные диапазоны vs. Лицензированные диапазоны
- 24.5.3. Возможности технологии LPWAN

24.6. Технология LoRaWAN
- 24.6.1. Технология LoRaWAN
- 24.6.2. Варианты использования LoRaWAN. Экосистема
- 24.6.3. Безопасность LoRaWAN

24.7. Технология Sigfox
- 24.7.1. Технология Sigfox
- 24.7.2. Варианты использования Sigfox. Экосистема
- 24.7.3. Безопасность Sigfox

24.8. Сотовая технология IoT
- 24.8.1. Сотовая технология IoT (NB-IoT и LTE-M)
- 24.8.2. Случаи использования сотового IoT. Экосистема
- 24.8.3. Безопасность сотовой технологии IoT

24.9. Технология WiSUN
- 24.9.1. Технология WiSUN
- 24.9.2. Случаи использования WiSUN. Экосистема
- 24.9.3. Безопасность WiSUN

24.10. Другие виды технологий IoT
- 24.10.1. Другие виды технологий IoT
- 24.10.2. Примеры использования и экосистема других технологий IoT
- 24.10.3. Безопасность других технологий IoT

Модуль 25. План по обеспечению непрерывности бизнеса, связанный с безопасностью

25.1. План по обеспечению непрерывности бизнеса
- 25.1.1. Планы по обеспечению непрерывности бизнеса (BCP)
- 25.1.2. План по обеспечению непрерывности бизнеса (BCP). Основные вопросы
- 25.1.3. План по обеспечению непрерывности бизнеса (BCP) для оценки стоимости бизнеса

25.2. Метрики в плане по обеспечению непрерывности бизнеса (BCP)
- 25.2.1. *Recovery time objective* (RTO) и *recovery point objective* (RPO)
- 25.2.2. Максимально допустимое время простоя (MTD)
- 25.2.3. Минимальный уровень восстановления (ROL)
- 25.2.4. Целевая точка восстановления (RPO)

25.3. Проекты непрерывного действия. Типология
- 25.3.1. План по обеспечению непрерывности бизнеса (BCP)
- 25.3.2. План по обеспечению непрерывности ИКТ
- 25.3.3. План аварийного восстановления (DRP)

25.4. Управление рисками, связанными с BCP
- 25.4.1. Анализ влияния на бизнес
- 25.4.2. Преимущества внедрения BCP
- 25.4.3. Менталитет, основанный на риске

25.5. Жизненный цикл плана по обеспечению непрерывности бизнеса
- 25.5.1. Фаза 1: Анализ организации
- 25.5.2. Фаза 2: Определение стратегии обеспечения непрерывности
- 25.5.3. Фаза 3: Ответ на непредвиденные ситуации
- 25.5.4. Фаза 4: Испытание, обслуживание и осмотр

25.6. Фаза организационного анализа BCP
- 25.6.1. Идентификация процессов, входящих в сферу действия BCP
- 25.6.2. Определение критических областей бизнеса
- 25.6.3. Выявление зависимостей между областями и процессами
- 25.6.4. Определение адекватного MTD
- 25.6.5. Результаты. Создание плана

25.7. Фаза определения стратегии непрерывности в рамках BCP
- 25.7.1. Роли в фазе определения стратегии
- 25.7.2. Задачи в фазе определения стратегии
- 25.7.3. Результаты

25.8. Фаза реагирования на непредвиденные обстоятельства в рамках BCP
- 25.8.1. Роли в фазе реагирования
- 25.8.2. Задачи в этой фазе
- 25.8.3. Результаты

25.9. Фаза тестирования, обслуживания и ревизии BCP
- 25.9.1. Роли в фазе тестирования, обслуживания и ревизии
- 25.9.2. Задачи в фазе тестирования, обслуживания и ревизии
- 25.9.3. Результаты

25.10. Стандарты ISO, связанные с планами по обеспечению непрерывности бизнеса (BCP)
- 25.10.1. ISO 22301:2019
- 25.10.2. ISO 22313:2020
- 25.10.3. Другие соответствующие стандарты ISO и международные стандарты

Модуль 26. Практическая политика аварийного восстановления системы безопасности

26.1. DRP. План аварийного восстановления
- 26.1.1. Цель DRP
- 26.1.2. Преимущества DRP
- 26.1.3. Последствия отсутствия DRP и его неактуальности

26.2. Руководство по определению DRP (плана аварийного восстановления)
- 26.2.1. Сфера применения и цели
- 26.2.2. Разработка стратегии восстановления
- 26.2.3. Распределение ролей и обязанностей
- 26.2.4. Проведение инвентаризации оборудования, программного обеспечения и услуг
- 26.2.5. Устойчивость к простоям и потере данных
- 26.2.6. Установление конкретных типов DRP's, которые необходимы
- 26.2.7. Реализация плана обучения, повышения осведомленности и коммуникации

26.3. Сфера применения и цели DRP (плана аварийного восстановления)
- 26.3.1. Ответная гарантия
- 26.3.2. Технологические компоненты
- 26.3.3. Сфера применения политики непрерывности

26.4. Разработка стратегии DRP (аварийного восстановления)
- 26.4.1. Стратегия аварийного восстановления
- 26.4.2. Бюджет
- 26.4.3. Человеческие и физические ресурсы
- 26.4.4. Руководящие должности в зоне риска
- 26.4.5. Технология
- 26.4.6. Данные

26.5. Непрерывность информационных процессов
- 26.5.1. Планирование непрерывности деятельности
- 26.5.2. Осуществление непрерывности
- 26.5.3. Проверка оценки непрерывности

26.6. Сфера применения BCP (плана обеспечения непрерывности бизнеса)
- 26.6.1. Определение наиболее критических процессов
- 26.6.2. Подход на основе активов
- 26.6.3. Подход на основе процессов

26.7. Внедрение защищенных бизнес-процессов
- 26.7.1. Приоритетные направления деятельности
- 26.7.2. Идеальные сроки восстановления
- 26.7.3. Стратегии выживания

26.8. Анализ организации
- 26.8.1. Получение информации
- 26.8.2. Анализ воздействия на бизнес (BIA)
- 26.8.3. Анализ рисков в организации

26.9. Ответ на непредвиденные ситуации
- 26.9.1. План действий в кризисной ситуации
- 26.9.2. Планы восстановления операционной среды
- 26.9.3. Технические рабочие процедуры или процедуры, связанные с инцидентами

26.10. Международная норма ISO 27031 BCP
- 26.10.1. Цели
- 26.10.2. Термины и определения
- 26.10.3. Операция

Модуль 27. Внедрение политики физической и экологической безопасности в компании

27.1. Зона безопасности
- 27.1.1. Периметр физической безопасности
- 27.1.2. Работа в безопасных зонах
- 27.1.3. Безопасность офисов, служебных помещений и ресурсов

27.2. Физические элементы управления вводом
- 27.2.1. Политики контроля физического доступа
- 27.2.2. Системы контроля физического ввода

27.3. Уязвимости физического доступа
- 27.3.1. Основные физические уязвимости
- 27.3.2. Реализация мер по обеспечению безопасности

27.4. Физиологические биометрические системы
- 27.4.1. Отпечаток пальца
- 27.4.2. Система распознавания лиц
- 27.4.3. Распознавание радужной оболочки глаза и сетчатки глаза
- 27.4.4. Другие физиологические биометрические системы

27.5. Биометрические поведенческие системы
- 27.5.1. Распознавание подписи
- 27.5.2. Распознание личности
- 27.5.3. Распознание голоса
- 27.5.4. Другие биометрические поведенческие системы

27.6. Управление рисками в биометрии
- 27.6.1. Внедрение биометрических систем
- 27.6.2. Уязвимости биометрических систем

27.7. Осуществление политики в хостах
- 27.7.1. Прокладка питающей и защитной кабельной сети
- 27.7.2. Расположение оборудования
- 27.7.3. Вывод оборудования за пределы помещения
- 27.7.4. IT-оборудование без присмотра и политика свободного места

27.8. Защита окружающей среды
- 27.8.1. Системы пожарной безопасности
- 27.8.2. Системы защиты от сейсмических воздействий
- 27.8.3. Системы защиты от землетрясений

27.9. Безопасность в центре обработки данных
- 27.9.1. Двери безопасности
- 27.9.2. Системы видеонаблюдения (CCTV)
- 27.9.3. Контроль безопасности

27.10. Международные правила физической безопасности
- 27.10.1. IEC 62443-2-1 (Европа)
- 27.10.2. NERC CIP-005-5 (США)
- 27.10.3. NERC CIP-014-2 (США)

Модуль 28. Политика безопасной коммуникации в компаниях

28.1. Управление безопасностью в сети
- 28.1.1. Контроль и мониторинг сети
- 28.1.2. Разделение сетей
- 28.1.3. Системы безопасности в сети

28.2. Протоколы безопасной связи
- 28.2.1. Модель TCP/IP
- 28.2.2. Протокол IPSEC
- 28.2.3. Протокол TLS

28.3. Протокол TLS 1,3
- 28.3.1. Фазы процесса TLS 1.3
- 28.3.2. Протокол *Handshake*
- 28.3.3. Протокол о регистрации
- 28.3.4. Отличия от TLS 1.2

28.4. Криптографические алгоритмы
- 28.4.1. Криптографические алгоритмы, используемые в коммуникациях
- 28.4.2. *Cipher-suites*
- 28.4.3. Криптографические алгоритмы, разрешенные для TLS 1.3

28.5. Функции дайджеста
- 28.5.1. MD6
- 28.5.2. SHA

28.6. PKI. Инфраструктура открытых ключей
- 28.6.1. PKI и ее подразделения
- 28.6.2. Электронный сертификат
- 28.6.3. Типы цифровых сертификатов

28.7. Туннельный и транспортный режимы коммуникации
- 28.7.1. Туннельный режим
- 28.7.2. Транспортный режим
- 28.7.3. Реализация зашифрованного туннеля

28.8. SSH. *Secure Shell*
- 28.8.1. SSH. Безопасная капсула
- 28.8.2. Как работает SSH
- 28.8.3. SSH-инструменты

28.9. Аудит криптографических систем
  28.9.1. Проверка целостности
  28.9.2. Тестирование криптографических систем
28.10. Криптографические системы
  28.10.1. Уязвимости криптографических систем
  28.10.2. Защитные меры в криптографии

Модуль 29. Организационные аспекты политики информационной безопасности

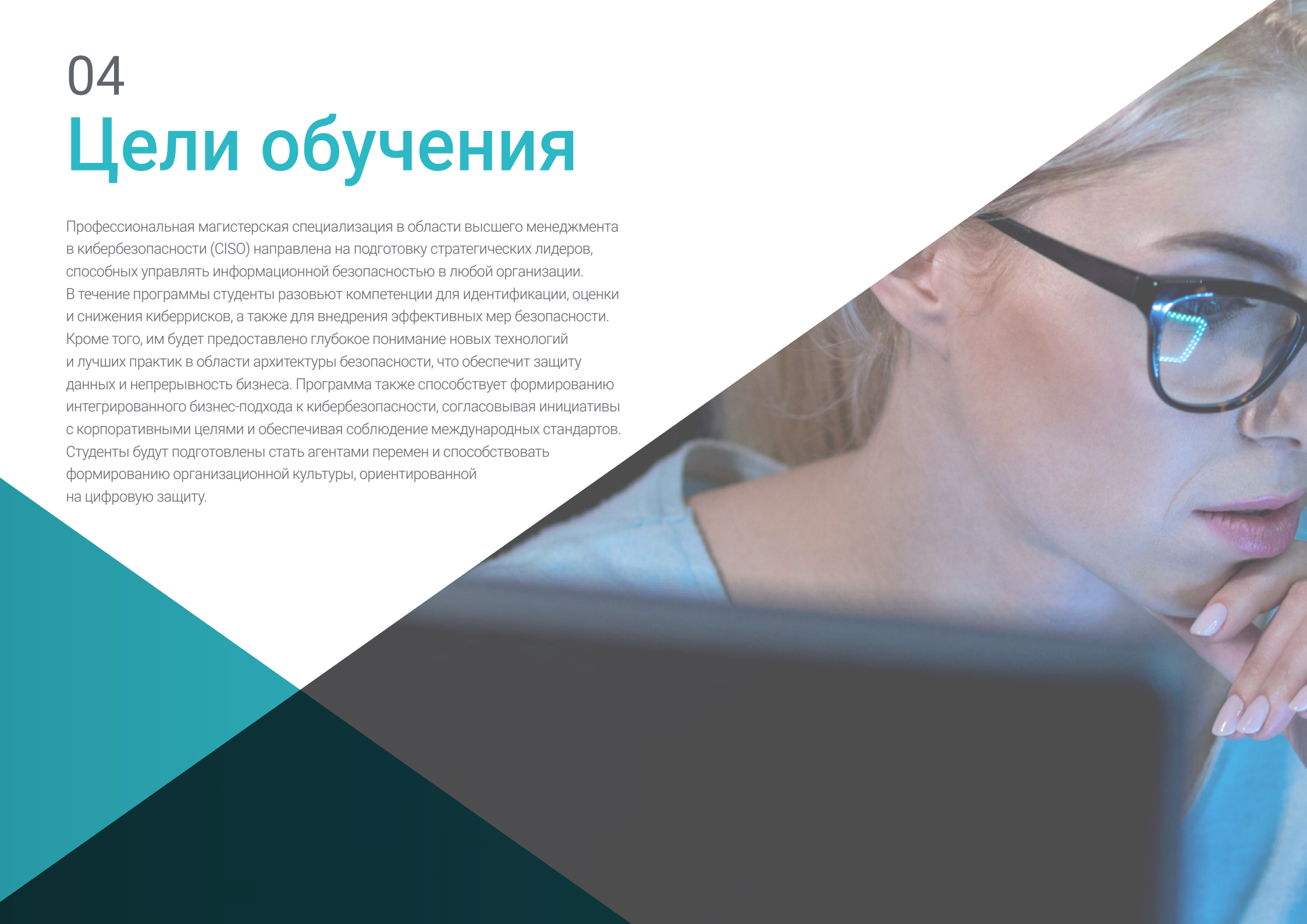
29.1. Внутренняя организация
  29.1.1. Распределение обязанностей
  29.1.2. Разделение обязанностей
  29.1.3. Контакты с органами власти
  29.1.4. Информационная безопасность в управлении проектами
29.2. Управление активами
  29.2.1. Ответственность за активы
  29.2.2. Классификация информации
  29.2.3. Обращение с носителями информации
29.3. Политики безопасности в бизнес-процессах
  29.3.1. Анализ уязвимых бизнес-процессов
  29.3.2. Анализ влияния на бизнес
  29.3.3. Классификация процессов по степени влияния на бизнес
29.4. Политики безопасности, связанные с человеческими ресурсами
  29.4.1. До приема на работу
  29.4.2. Во время приема на работу
  29.4.3. Увольнение или изменение должности
29.5. Политика безопасности управления
  29.5.1. Руководство по управлению информационной безопасностью
  29.5.2. BIA — анализ воздействия
  29.5.3. План восстановления как политика безопасности
29.6. Приобретение и обслуживание информационных систем
  29.6.1. Требования к безопасности информационных систем
  29.6.2. Безопасность данных разработки и поддержки
  29.6.3. Данные тестирования
29.7. Безопасность в отношениях с поставщиками
  29.7.1. IT-безопасность с поставщиками
  29.7.2. Управление предоставлением услуг с гарантией
  29.7.3. Безопасность цепи поставок
29.8. Эксплуатационная безопасность
  29.8.1. Обязанности в процессе эксплуатации
  29.8.2. Защита от вредоносного кода
  29.8.3. Резервные копии
  29.8.4. Записи о деятельности и мониторинге
29.9. Управление безопасностью и нормативно-правовым регулированием
  29.9.1. Соблюдение требований законодательства
  29.9.2. Проверки информационной безопасности
29.10. Безопасность в обеспечении непрерывности бизнеса
  29.10.1. Непрерывность информационной безопасности
  29.10.2. Увольнения

Комплексная программа обучения TECH научит вас быть дальновидным лидером, обеспечивающим долгосрочную защиту организации"

04

Цели обучения

Профессиональная магистерская специализация в области высшего менеджмента в кибербезопасности (CISO) направлена на подготовку стратегических лидеров, способных управлять информационной безопасностью в любой организации. В течение программы студенты разовьют компетенции для идентификации, оценки и снижения киберрисков, а также для внедрения эффективных мер безопасности. Кроме того, им будет предоставлено глубокое понимание новых технологий и лучших практик в области архитектуры безопасности, что обеспечит защиту данных и непрерывность бизнеса. Программа также способствует формированию интегрированного бизнес-подхода к кибербезопасности, согласовывая инициативы с корпоративными целями и обеспечивая соблюдение международных стандартов. Студенты будут подготовлены стать агентами перемен и способствовать формированию организационной культуры, ориентированной на цифровую защиту.



В этой программе на 100% в онлайн-формате вы найдете самые актуальные учебные материалы и исследования на университетской сцене"

Общие цели

- Развивать стратегических лидеров в области кибербезопасности, способных управлять защитой цифровых активов и технологической инфраструктуры глобальных организаций
- Интегрировать кибербезопасность в корпоративную стратегию, согласовывая инициативы цифровой защиты с глобальными целями организации
- Обучать внедрению политик и нормативных рамок кибербезопасности, обеспечивающих соблюдение регуляторных требований и защиту информации в цифровых средах
- Содействовать развитию лидерства и управлению командами по кибербезопасности, повышая способность принимать стратегические решения в кризисных ситуациях и управлять проектами безопасности на организационном уровне

Присоединяйтесь к TECH и развивайте навыки, необходимые для того, чтобы стать лидером, который предвидит угрозы и использует возможности”

Конкретные цели

Модуль 1. Кибербезопасность и кибербезопасность

- Развивать необходимые навыки для внедрения стратегий кибербезопасности и кибербезопасности
- Защищать информационные системы от киберугроз посредством сбора, анализа и использования цифровой разведки

Модуль 2. Безопасность хоста

- Обучать внедрению мер безопасности в хост-системы
- Обеспечивать защиту серверов и устройств от уязвимостей, *вредоносного ПО* и несанкционированного доступа

Модуль 3. Сетевая безопасность (периметр)

- Предоставлять необходимые знания для защиты информационных сетей на периферии
- Осваивать техники и инструменты безопасности, такие как межсетевые экраны, VPN и системы обнаружения вторжений

Модуль 4. Безопасность *смартфонов*

- Предоставлять полное понимание безопасности мобильных устройств
- Углублять защиту от угроз, таких как *вредоносное ПО*, потеря данных и атаки через мобильные приложения

Модуль 5. Безопасность в IoT

- Обучать внедрению политик безопасности для устройств IoT
- Обеспечивать защиту инфраструктуры и данных, генерируемых устройствами, подключенными через сети и платформы IoT

Модуль 6. Этичный хакинг

- Развивать необходимые компетенции для проведения тестов на проникновение и аудита безопасности с использованием техник этичного хакинга
- Уметь выявлять уязвимости и предотвращать атаки

Модуль 7. Реверс-инжиниринг

- Осваивать техники обратного проектирования для анализа и понимания работы программного обеспечения и *аппаратного обеспечения*
- Выявлять возможные уязвимости и предлагать решения по безопасности

Модуль 8. Безопасная разработка

- Обучать лучшим практикам безопасной разработки программного обеспечения
- Применять принципы безопасности на всех этапах жизненного цикла разработки для минимизации рисков и уязвимостей в приложениях

Модуль 9. Практическое внедрение политик безопасности в программное обеспечение и *аппаратное обеспечение*

- Предоставлять необходимые знания для разработки и реализации надежных политик безопасности в программном обеспечении и аппаратном обеспечении
- Обеспечивать защиту от внутренних и внешних угроз

Модуль 10. Судебная экспертиза

- Развивать компетенции в области цифровой судебной экспертизы
- Анализировать сбор, сохранение и анализ цифровых доказательств в случаях инцидентов информационной безопасности

Модуль 11. Безопасность при проектировании и разработке систем
- Подходить к интеграции мер безопасности с этапов проектирования и разработки информационных систем
- Гарантировать защиту от возможных уязвимостей с самого начала проекта

Модуль 12. Архитектуры и модели информационной безопасности
- Предоставлять необходимые знания об архитектурах и моделях информационной безопасности
- Разрабатывать и внедрять надежные системы, которые защищают данные и ресурсы организации

Модуль 13. Система управления информационной безопасностью (СУИБ)
- Внедрять систему управления информационной безопасностью
- Эффективно защищать корпоративную информацию, обеспечивая соблюдение нормативных требований и лучших практик

Модуль 14. Управление ИТ-безопасностью
- Предоставлять необходимые знания для эффективного управления безопасностью технологической инфраструктуры компании
- Минимизировать риски и обеспечивать непрерывность операционной деятельности

Модуль 15. Политика управления инцидентами безопасности
- Обучать созданию и применению эффективных политик управления инцидентами безопасности
- Устанавливать четкие протоколы для обнаружения, анализа и реагирования на утечки безопасности

Модуль 16. Анализ рисков и среды ИТ-безопасности
- Предоставлять необходимые знания для проведения анализа рисков в ИТ-среде, выявляя угрозы и уязвимости
- Применять стратегии смягчения для обеспечения безопасности технологической инфраструктуры

Модуль 17. Политики безопасности для анализа угроз в информационных системах
- Обучать разработке политик безопасности для выявления, анализа и смягчения угроз в информационных системах
- Использовать соответствующие инструменты и методы для защиты цифровых активов организации

Модуль 18. Практическая реализация политики безопасности перед угрозой атак
- Внедрять эффективные политики безопасности против возможных атак
- Обеспечивать защиту систем и критически важной информации в организации

Модуль 19. Криптография в ИТ
- Обучать основам и применениям криптографии в области информационных технологий
- Внедрять алгоритмы шифрования и обеспечения безопасности при передаче данных

Модуль 20. Управление идентификацией и доступом в ИТ-безопасности
- Развивать необходимые навыки для управления идентификацией и доступом в ИТ-системах
- Устанавливать политики аутентификации и контроля доступа для защиты ресурсов и данных организации

Модуль 21. Безопасность в коммуникациях и работе программного обеспечения

- Обучать защите цифровых коммуникаций и внедрению мер безопасности при работе с программным обеспечением
- Гарантировать конфиденциальность, целостность и доступность информации

Модуль 22. Безопасность в облачных средах

- Внедрять политики безопасности в облачных вычислениях
- Обеспечивать защиту данных и приложений от несанкционированного доступа и атак

Модуль 23. Инструменты мониторинга в политиках безопасности информационных систем

- Обучать использованию инструментов мониторинга для оценки эффективности политик безопасности в информационных системах
- Углубленно изучать методы раннего выявления уязвимостей и атак

Модуль 24. Безопасность в коммуникациях между устройствами интернета вещей (IoT)

- Развивать компетенции в области внедрения мер безопасности для защиты коммуникаций между IoT-устройствами
- Минимизировать риски, связанные с обменом данными между подключенными устройствами

Модуль 25. План по обеспечению непрерывности бизнеса, связанный с безопасностью

- Разрабатывать план обеспечения непрерывности бизнеса, который гарантирует защиту и быструю восстановляемость систем
- Устанавливать протоколы для обеспечения сохранности критически важных данных в случае инцидентов безопасности

Модуль 26. Практическая политика аварийного восстановления системы безопасности

- Создать политики восстановления после катастроф
- Обеспечить быструю реставрацию систем и защиту данных в случае серьезных инцидентов безопасности

Модуль 27. Внедрение политики физической и экологической безопасности в компании

- Обучить внедрению политик физической и экологической безопасности для защиты материальных ресурсов организации
- Обеспечить соответствующие условия для безопасного функционирования технологических систем

Модуль 28. Политика безопасной коммуникации в компаниях

- Предоставить знания для разработки политик безопасных коммуникаций внутри организации
- Защитить сети и каналы связи от шпионажа и утечки информации

Модуль 29. Организационные аспекты политики информационной безопасности

- Предоставить инструменты для внедрения организационных политик в управлении информационной безопасностью
- Определить роли, обязанности и процессы для защиты информационных активов

05

Возможности карьерного роста

По завершении Профессиональной магистерской специализации в области высшего менеджмента в кибербезопасности (CISO) выпускники университета будут полностью подготовлены к выполнению ключевых ролей в области защиты и управления информационной безопасностью в различных организациях. Кроме того, они смогут разрабатывать и возглавлять стратегии безопасности в многонациональных компаниях, эффективно управляя и минимизируя киберриски. Также они будут готовы занимать позиции, требующие навыков лидерства в инициативах по кибербезопасности и обеспечению защиты цифровых активов в любых отраслях.

Пройдя эту Профессиональную магистерскую специализацию, вы станете менеджером, способным предвидеть риски и защищать важную информацию”

Профиль выпускника

Выпускник Профессиональной магистерской специализации в области высшего менеджмента в кибербезопасности (CISO) станет стратегическим лидером с глубоким пониманием информационной безопасности в контексте глобальных организаций. Он будет подготовлен к разработке и внедрению передовых политик безопасности, а также к руководству мультидисциплинарными командами. Кроме того, выпускник будет обладать прочными навыками управления и корпоративного контроля, что позволит ему эффективно решать вызовы в области кибербезопасности в различных секторах, обеспечивая защиту цифровых активов. Эта программа предоставит ему все необходимые инструменты для отслеживания последних технологических тенденций и адаптации к стремительным изменениям в цифровой среде.

Подготовьтесь к тому, чтобы стать одним из лучших профессионалов, минимизировать последствия кибератак и быстро вернуться к привычной работе.

- **Стратегическое лидерство и адаптивность:** Способность руководить мультидисциплинарными командами и управлять политиками безопасности, адаптируясь к стремительным технологическим изменениям и новым вызовам в сфере кибербезопасности
- **Управление рисками и обоснованное принятие решений:** Навык выявления, оценки и минимизации киберрисков с принятием решений, основанных на данных и детальном анализе
- **Критический анализ и управление инцидентами:** Способность выявлять уязвимости, управлять инцидентами безопасности и координировать реагирование на кризисные ситуации, обеспечивая непрерывность бизнес-процессов
- **Эффективная коммуникация и стратегическое мышление:** Навык четкого донесения информации о рисках и решениях до различных заинтересованных сторон, а также формирование глобального стратегического подхода к защите цифровых активов

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

1. **Chief Information Security Officer (CISO):** Стратегический лидер, отвечающий за защиту информации и кибербезопасность во всей организации, разрабатывающий политики и контролирующий цифровую инфраструктуру безопасности.
2. **Директор по кибербезопасности:** Отвечает за управление и контроль работы команд информационной безопасности, разработку и внедрение стратегий для защиты технологической инфраструктуры компании.
3. **Менеджер по информационной безопасности:** Отвечает за управление и координацию политик цифровой безопасности, контроль защиты данных и информационных систем от потенциальных угроз.
4. **Консультант по кибербезопасности:** Эксперт, консультирующий компании по вопросам внедрения и управления мерами кибербезопасности, помогая минимизировать риски и соблюдать международные нормативные требования.
5. **Менеджер по управлению ИТ-рисками:** Отвечает за выявление, оценку и минимизацию киберрисков, которые могут повлиять на безопасность информации и технологических систем организации
6. **Руководитель службы информационной безопасности:** Лидер, координирующий и контролирующий все инициативы, связанные с защитой данных и информационных систем в организации

Вы в одном шаге от того, чтобы улучшить свою профессиональную жизнь с помощью Профессиональной магистерской специализации, которую может предложить только TECH"

06

Методика обучения

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

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

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

Студент — приоритет всех программ TECH

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

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

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

Самые обширные учебные планы на международном уровне

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

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

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

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

Case studies или метод кейсов

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

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

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

Метод *Relearning*

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

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

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

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

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

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

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

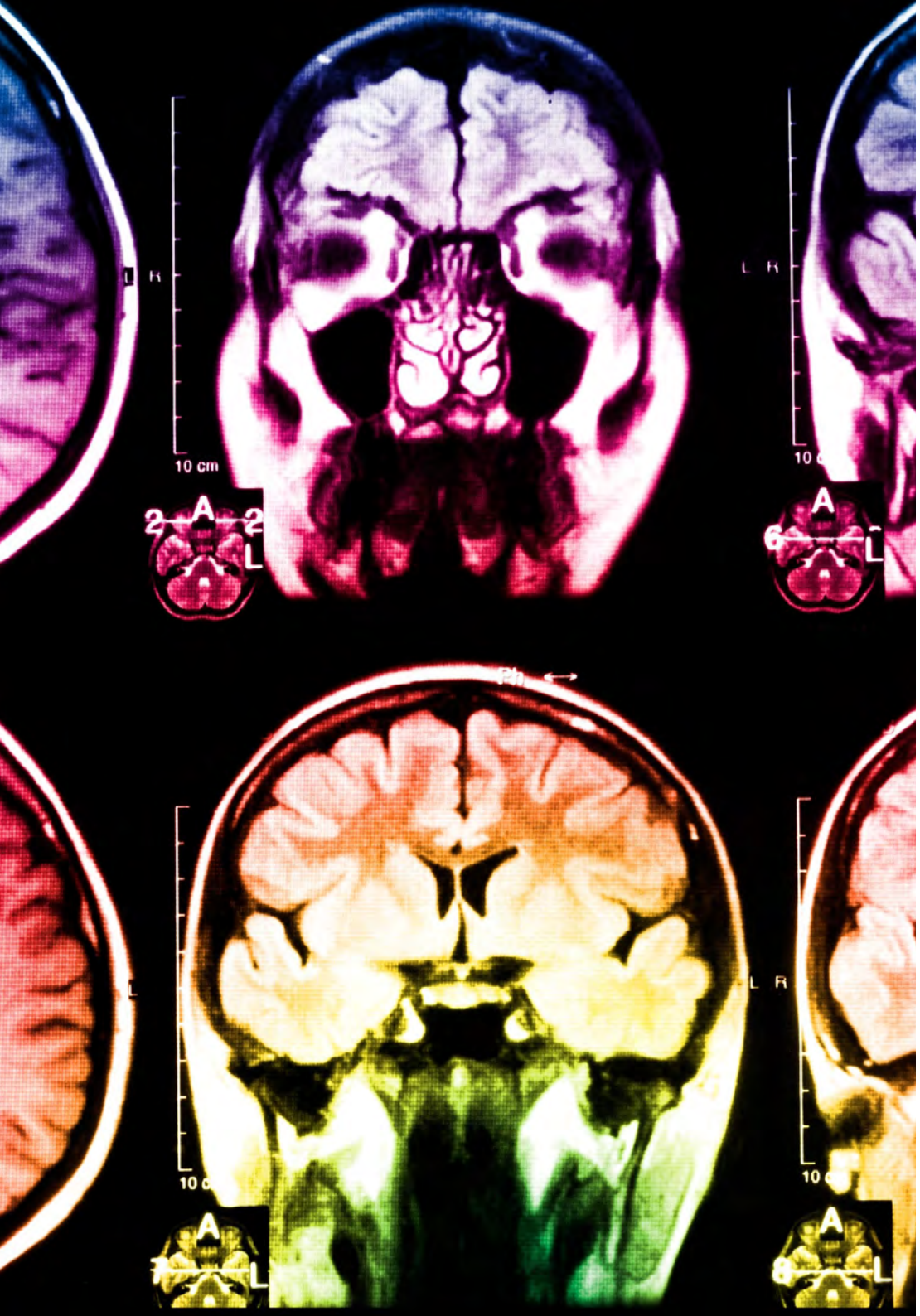
Кроме того, для максимального содействия взаимодействию между наставником и студентом предоставляется широкий спектр возможностей для общения как в реальном времени, так и в отложенном (внутренняя система обмена сообщениями, форумы для обсуждений, служба телефонной поддержки, электронная почта для связи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

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

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

Эффективность метода обосновывается четырьмя ключевыми достижениями:

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



Методика университета, получившая самую высокую оценку среди своих студентов

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

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

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

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

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

Учебные материалы

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

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

Практика навыков и компетенций

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

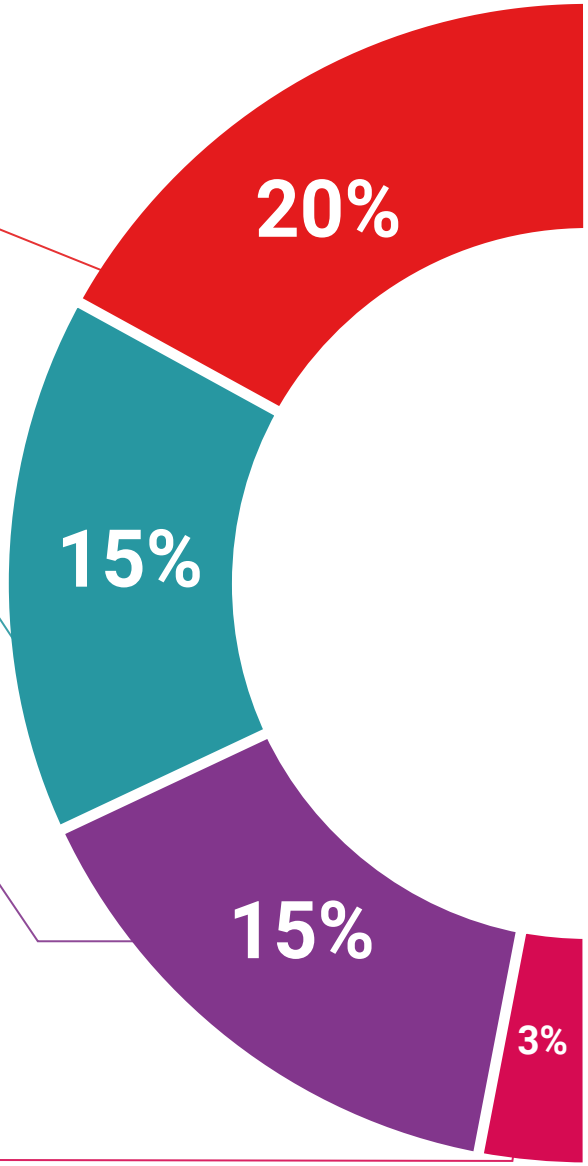
Интерактивные конспекты

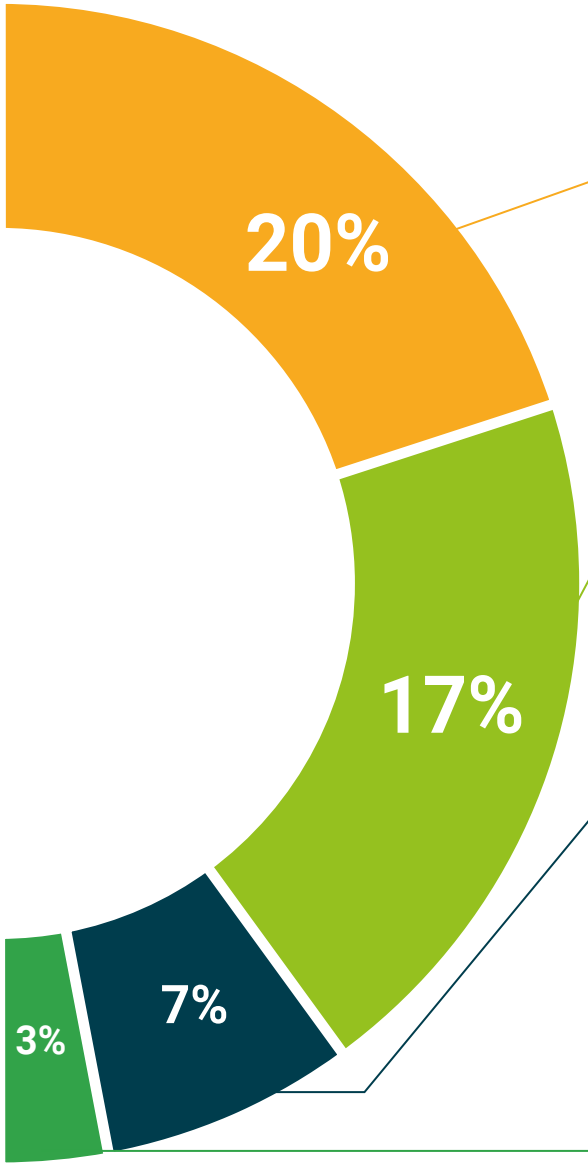
Мы представляем содержание в привлекательной и динамичной форме для воспроизведения на мультимедийных устройствах, которые включают аудио, видео, изображения, диаграммы и концептуальные карты для закрепления знаний.

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

Дополнительная литература

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





Кейс-стади

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

Тестирование и повторное тестирование

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

Мастер-классы

Существуют научные данные о пользе экспертного наблюдения третьей стороны.

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

Краткие справочные руководства

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

07

Преподавательский состав

Эта Профессиональная магистерская специализация в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer) включает преподавательский состав, состоящий из действующих специалистов, которые в совершенстве владеют актуальными знаниями в данной сфере. Таким образом, студенты программы получают доступ к самым последним достижениям в области кибербезопасности благодаря высококвалифицированным преподавателям, отобранным TECH.

TECH предлагает вам самых специализированных экспертов и преподавателей, чтобы ваш подход и обучение были самыми лучшими"

Приглашенный лектор международного уровня

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

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

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

Д-р Лемье, Фредерик

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

Благодаря TECH вы сможете учиться у лучших мировых профессионалов"

Руководство

Г-жа Фернандес Сапена, Соня

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

Г-н Олайа Бональ, Мартин

- Старший менеджер практики *блокчейн* в компании EY
- Технический специалист по *блокчейн*-клиентам в IBM
- Директор по архитектуре компании Blocknitive
- Координатор группы по нереляционным распределенным базам данных в WedoIT, дочернее предприятие IBM
- Архитектор инфраструктуры в Bankia
- Руководитель отдела верстки в компании T-Systems
- Координатор отдела Bing Data España SL

Преподаватели

Г-жа Маркос Сбарбаро, Виктория Алисия

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

Г-н Энтренас, Алехандро

- Руководитель проекта по кибербезопасности. Entelgy Innotec Security
- Консультант по кибербезопасности. Entelgy
- Аналитик информационной безопасности. Innovery, Испания
- Аналитик по информационной безопасности. Atos
- Степень технического инженера в области компьютерных систем в Университете Кордовы
- Степень магистра в области управления информационной безопасностью в Мадридском политехническом университете
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

Г-н Катала Барба, Хосе Франсиско

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

Г-н Перальта Алонсо, Йон

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

Г-н Гонсало Алонсо, Феликс

- Генеральный директор и учредитель Smart REM Solutions
- Руководитель отдела риск-инжиниринга и инноваций в Dynargy
- Руководитель и партнер-основатель технологической консалтинговой компании Risknova
- Степень магистра в области управления страхованием в Институте сотрудничества страховых компаний
- Степень бакалавра в области промышленной электроники в Папском университете Комильяс

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

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

Г-н Ногалес Авила, Хавьер
- Старший консультант по корпоративному облаку и сорсингу в Quint
- Консультант по облачным технологиям в Indra
- Ассоциированный консультант по технологиям в Accenture
- Степень бакалавра в области организации производства в Университете Хаэна
- MBA в области делового администрирования и менеджмента в ThePower Business School

Г-н Гомес Родригес, Антонио
- Главный инженер по облачным решениям для Oracle
- Соорганизатор Malaga Developer Meetup
- Специалист-консультант для Sopra Group и Everis
- Руководитель команды в компании System Dynamics
- Разработчик программного обеспечения в компании SGO Software
- Степень магистра в области электронного бизнеса в бизнес-школе Ла-Салье
- Последипломное образование в области информационных технологий и систем в Каталонском технологическом институте
- Степень бакалавра в области высшей телекоммуникационной инженерии в Политехническом университете Каталонии

Г-н Родриго Эстебанес, Хуан Мануэль
- Соучредитель компании Ismet Tech
- Менеджер по информационной безопасности в Ecix Group
- *Сотрудник по операционной безопасности* в Atos IT Solutions and Services A/S
- Преподаватель по управлению кибербезопасностью в университете
- Степень бакалавра в области инженерии Университета Вальядолида
- Степень магистра в области интегрированных систем управления в Университете CEU Сан-Пабло

Г-н Дель Валье Ариас, Хорхе

- Инженер по телекоммуникациям с опытом работы в области развития бизнеса
- Smart City Solutions & Software Business Development Manager Испания. Itron, Inc
- Консультант по вопросам IoT
- Временный директор по бизнесу IoT. TCOMET
- Руководитель бизнес-подразделения IoT, Индустрия 4.0. Diode Испания
- Региональный менеджер по продажам в области IoT и телекоммуникаций. Aicox Soluciones
- Главный технический директор (CTO) и менеджер по развитию бизнеса. Консалтинг TELYC
- Основатель и генеральный директор компании Sensor Intelligence
- Руководитель отдела операций и проектов. Codio
- Главный операционный директор в компании Codium Networks
- Главный инженер по разработке аппаратного и микропрограммного обеспечения. AITEMIN
- Региональный руководитель отдела радиочастотного планирования и оптимизации - сеть LMDS 3,5 ГГц. Clearwire
- Диплом инженера в области телекоммуникаций в Политехническом университете Мадрида
- Бизнес-магистратура в International Graduate School Ла-Салье в Мадриде
- Степень магистра в области возобновляемых источников энергии. CEPYME

Г-н Госало Фернандес, Хуан Луис

- Менеджер по продуктам на основе блокчейна для Open Canarias
- Директор по блокчейн DevOps в Аластрии
- Директор по технологиям уровня обслуживания в Santander, Испания
- Руководитель направления разработки мобильных приложений Tinkerlink в компании Cronos Telecom
- Директор по технологиям управления ИТ-услугами в Barclays Bank Spain
- Степень бакалавра в области высшей компьютерной инженерии в UNED
- Специализация в области *глубокого обучения* в DeepLearning.ai

Г-жа Хурадо Хабонеро, Лорена

- Ответственная за информационную безопасность (CISO) в компании Grupo Pascual
- Менеджер по кибербезопасности в KPMG. Испания
- Консультант по контролю и управлению проектами в области ИТ-процессов и инфраструктуры в Bankia
- Инженер по средствам эксплуатации в Dalkia
- Разработчик в Banco Popular Group
- Разработчик приложений в Мадридском политехническом университете
- Степень бакалавра в области компьютерной инженерии в Университете Альфонсо X Мудрого
- Технический инженер в области компьютерного менеджмента в Политехническом университете Мадрида
- Сертифицированный инженер по решениям в области конфиденциальности данных (CDPSE) в ISACA

Г-н Ортега Эстебан, Октавио

- Специалист по маркетингу и веб-разработке
- Внештатный программист компьютерных приложений и *веб-разработчик*
- *Операционный директор* в Smallsquid SL
- Администратор электронной коммерции в компании Ortega y Serrano
- Преподаватель курсов по получению сертификата специалиста в области компьютерных технологий и коммуникаций
- Преподаватель курсов по компьютерной безопасности
- Степень бакалавра психологии Открытого университета Каталонии
- Профессиональное среднее образование в области анализа, проектирования и решения *программного обеспечения*
- Профессиональное среднее образование в области перспективного программирования

Г-н Эмбид Руис, Марио

- Юрист, специализирующийся на ИКТ и защите данных в Martínez-Echevarría Abogados
- Менеджер по правовым вопросам в Branddocs SL
- Аналитик по рискам в сегменте малого и среднего бизнеса BBVA
- Преподаватель в университетской аспирантуре, связанной с правом
- Степень бакалавра в области права в Университете короля Хуана Карлоса
- Степень магистра в области делового администрирования и менеджмента в Университете короля Хуана Карлоса
- Степень магистра права со специализацией в области новых технологий, Интернета и аудиовизуального права Центра университетских исследований Вильянуэва

08

Квалификация

Профессиональная магистерская специализация в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer) гарантирует, помимо самого строгого и современного обучения, получение диплома о прохождении Профессиональной магистерской специализации, выдаваемого TECH Технологическим университетом.

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

Данная **Профессиональной магистерской специализации в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer)** содержит самую полную и современную программу на рынке.

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

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

Профессиональной магистерской специализации в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer)

Формат: **онлайн**

Продолжительность: **2 года**


tech технологический университет

Настоящий

ДИПЛОМ

свидетельствует о том, что

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

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

ПРОФЕССИОНАЛЬНАЯ МАГИСТЕРСКАЯ СПЕЦИАЛИЗАЦИЯ

в области

высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer)

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

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

17 июня 2020 г.

Д-р Tere Guevara Navarro
Ректор

unique TECH code: AFWOR23S techtitute.com/certificates


Профессиональная магистерская специализация в области высшего менеджмента в кибербезопасности (CISO, Chief Information Security Officer)

Общее распределение учебного плана

Курс	Предмет	Часы	Характер
1º	Киберразведка и кибербезопасность	110	Обязат
1º	Безопасность хоста	110	Обязат
1º	Сетевая безопасность (периметр)	110	Обязат
1º	Безопасность смартфонов	110	Обязат
1º	Безопасность в IoT	110	Обязат
1º	Этичный хакинг	110	Обязат
1º	Реверс-инжиниринг	110	Обязат
1º	Безопасная разработка	110	Обязат
1º	Практическое внедрение политик безопасности в программное обеспечение и аппаратное обеспечение	110	Обязат
1º	Судебная экспертиза	110	Обязат
1º	Безопасность при проектировании и разработке систем	100	Обязат
1º	Архитектуры и модели информационной безопасности	100	Обязат
1º	Система управления информационной безопасностью (СУИБ)	100	Обязат
1º	Управление ИТ-безопасностью	100	Обязат
1º	Политика управления инцидентами безопасности	100	Обязат
1º	Анализ рисков и среды ИТ-безопасности	100	Обязат
1º	Политики безопасности для анализа угроз в информационных системах	100	Обязат

Курс	Предмет	Часы	Характер
2º	Практическая реализация политики безопасности перед угрозой атак	100	Обязат
2º	Криптография в ИТ	100	Обязат
2º	Управление идентификацией и доступом в ИТ-безопасности	100	Обязат
2º	Безопасность в коммуникациях и работе программного обеспечения	100	Обязат
2º	Безопасность в облачных средах	100	Обязат
2º	Инструменты мониторинга в политиках безопасности информационных систем	100	Обязат
2º	Безопасность в коммуникациях между устройствами интернета вещей (IoT)	100	Обязат
2º	План по обеспечению непрерывности бизнеса, связанный с безопасностью	100	Обязат
2º	Практическая политика аварийного восстановления системы безопасности	100	Обязат
2º	Внедрение политики физической и экологической безопасности в компании	100	Обязат
2º	Политика безопасной коммуникации в компаниях	100	Обязат
2º	Организационные аспекты политики информационной безопасности	100	Обязат

Д-р Tere Guevara Navarro
Ректор

tech технологический университет

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

tech технологический университет

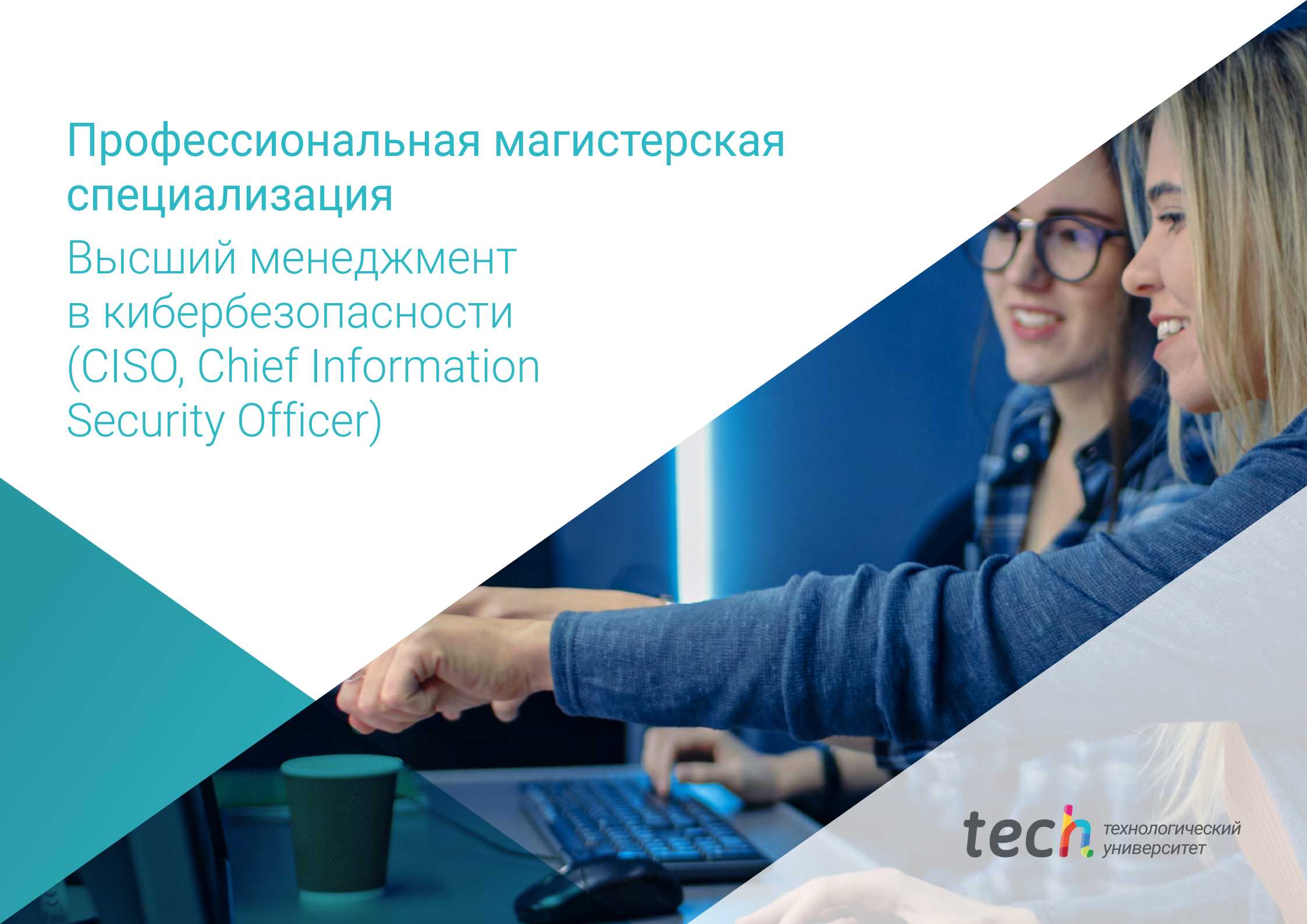
Профессиональная магистерская специализация

Высший менеджмент в кибербезопасности (CISO, Chief Information Security Officer)

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

Профессиональная магистерская специализация

Высший менеджмент в кибербезопасности (CISO, Chief Information Security Officer)



tech технологический университет