Специалист по информационной безопасности

11 месяцев
продолжительность курса

4 проекта
в портфолио

Модуль 1. Настройка корпоративных IT-сервисов в среде эмуляции	Спринт 1. Настройка локальной корпоративной сети в эмуляторе Спринт 2. Настройка операционной системы Спринт 3. Развёртывание инфраструктурных сервисов Спринт 4. Запуск прикладных сервисов с корректировкой конфигурации Спринт 5. Проектная работа 1	10 недель
Модуль 2. Обеспечение безопасности корпоративных сервисов	Спринт 1. Моделирование угроз Спринт 2. Обеспечение сетевой безопасности корпоративной сети Спринт 3. Безопасности конечных устройств Спринт 4. Обеспечение безопасности входящей электронной почты Спринт 5. Сетевая безопасность веб-приложений Спринт 6. Выявление угроз и внедрение требуемого средства защиты информации Спринт 7. Проектная работа 2	14 недель
Модуль 3. Администрирование и поддержка средств защиты информации	Спринт 1. Администрирование и поддержка средства защиты Спринт 2. Анализ и решение проблем работоспособности бизнес-приложений, сети или средств защиты (траблшутинг) Спринт 3. Проектная работа 3	6 недель
Модуль 4. Разработка и внедрение политик безопасности	Спринт 1. Применение требований стандартов Спринт 2. Поиск альтернативных решений	4 недели
Модуль 5. Виртуализация и контейнеризация	Спринт 1. Виртуализация и контейнеризация	2 недели
Дипломная работа		3 недели

Настройка корпоративных IT-сервисов в среде эмуляции

01

[10 недель],
[4 домашних задания],
[1 проект]

Настроите эмуляцию корпоративной сети с основными бизнес-сервисами — почтой, веб-порталом и файловым сервером.

Настройка корпоративной сети

Настроите корпоративную сеть с основными бизнес-сервисами (почта, веб-портал, файловый сервер) и инфраструктурными сервисами в эмуляторе, наладите мониторинг работоспособности сервисов.

Инструменты

Эмулятор сети с виртуальными образами сетевого оборудования

Инструменты анализа сетевого трафика

Образы операционных систем Windows и Linux (Desktop и Server)

Командные оболочки Bash/PowerShell

Прикладные сервисы (веб-сервер, почтовый сервер, файловый сервер, система IT-мониторинга) на базе опенсорс-решений

Содержание модуля

Спринт 1. Настройка локальной корпоративной сети в эмуляторе

Спринт 2. Настройка операционной системы

Спринт 3. Развёртывание инфраструктурных сервисов

Спринт 4. Запуск прикладных сервисов с корректировкой конфигурации

Спринт 5. Проектная работа 1

Обеспечение безопасности корпоративных сервисов 02

[14 недель],
[6 домашних заданий],
[1 проект]

Выявите и оцените актуальные угрозы корпоративной сети. Внедрите средства защиты информации, которые требуются, чтобы нейтрализовать выявленные угрозы.

Анализ и внедрение средств защиты информации
Изучите и проанализируете бизнес-процессы компании, оцените актуальные угрозы, внедрите необходимые средства защиты информации и меры обеспечения безопасности.

Инструменты

Средства сетевой безопасности: Firewall, IPS/IDS, NTA

Endpoint security: антивирусное ПО, EDR, безопасная настройка операционной системы (харденинг)

Защита веб-приложений: WAF, безопасная настройка веб-сервера

Защита почты: антиспам, почтовый антивирус, песочница (sandbox)

Содержание модуля

Спринт 1. Моделирование угроз

Спринт 2. Обеспечение сетевой безопасности корпоративной сети

Спринт 3. Безопасности конечных устройств

Спринт 4. Обеспечение безопасности входящей электронной почты

Спринт 5. Сетевая безопасность веб-приложений

Спринт 6. Выявление угроз и внедрение требуемого средства защиты информации

Спринт 7. Проектная работа 2

Администрирование и поддержка средств защиты информации

03

[6 недель], [3 домашних задания], [1 проект]

Изучите полный цикл администрирования и поддержки средств защиты — от выполнения рутинных задач по настройке и поддержке до решения проблем работоспособности самого средства или бизнес-сервисов.

Поддержка средства защиты

Решите несколько обращений пользователей и IT-специалистов корпоративной сети, выявите причины, по которым возникают разные типы аварий и ошибок конфигурирования и их природу.

Инструменты

Инструменты анализа сетевого трафика и базовой диагностики сетевой связности

Средства самодиагностики операционных систем

Средства мониторинга состояния статусов разных сервисов компьютерной сети, серверов и сетевого оборудования

Средства мониторинга веб-приложений

Содержание модуля

Спринт 1. Администрирование и поддержка средства защиты

Спринт 2. Анализ и решение проблем работоспособности бизнес-приложений, сети или средств защиты (траблшутинг).

Спринт 3. Проектная работа 3

Разработка и внедрение политик безопасности

04

[4 недели], [2 домашних задания]

Оцените, насколько применимы требования в стандарте. Если требования неприменимы — предложите альтернативное решение.

Инструменты

Нормативно-правовые акты (НПА)

Международные стандарты

Фреймворки популярных стандартов

Командные оболочки Bash/PowerShell

Содержание модуля

Спринт 1. Применение требований стандартов

Спринт 2. Поиск альтернативных решений

Виртуализация и контейнеризация

05

[2 недели], [1 домашнее задание]

Узнаете, как используется виртуализация и контейнеризация в корпоративных сетях.

Содержание модуля

Спринт 1. Виртуализация и контейнеризация

Дипломная работа

[3 недели],
[1 проект]

Разработаете и настроите защиту корпоративной сети в соответствии с бизнес-требованиями и стандартами.