MERION

Программа курса

ОНЛАЙН-КУРС ПО КИБЕРБЕЗОПАСНОСТИ

ПРОГРАММА КУРСА

🌐 Блок 1

Сетевые концепции

Содержимое блока:

- Функции сетевых уровней
- Эталонная модель OSI
- Набор протоколов TCP/IP
- Протокол управления передачей (TCP)
- IP-адреса

Научишься:

- Понимать структуру сетевых уровней
- Различать модели OSI и TCP/IP
- Использовать анализ сетевых сообщений

🛠️ **Практика в блоке:**

- Лабораторная работа №1: Проверка сообщений ICMP с помощью Wireshark

☑️ **Тестирование по блоку Сетевые концепции**

⚙️ Блок 2

Сетевые компоненты и системы безопасности

Содержимое блока:

- Address Resolution Protocol (ARP)
- Domain Name System (DNS)
- DHCP
- Типы сетевых устройств
- Системы сетевой безопасности

Научишься:

- Работать с сетевыми сервисами
- Анализировать сетевую инфраструктуру
- Понимать основы защиты сетей

🛠️ **Практика в блоке:**

- Лабораторная работа №2: Определение DNS
- Лабораторная работа №3: DNS-анализ с помощью Wireshark

☑️ **Тестирование по блоку Сетевые компоненты и системы безопасности**

🛡️ Блок 3

Концепции безопасности

Содержимое блока:

- Принципы защиты
- Конфиденциальность, целостность, доступность
- Модели управления доступом
- Развертывание компонентов безопасности

Научишься:

- Применять базовые принципы защиты данных
- Использовать модели управления доступом

☑️ **Тестирование по блоку Концепции безопасности**

🧰 Блок 4

Принципы безопасности

Содержимое блока:

- Ландшафт атак и уязвимости
- NetFlow
- Списки контроля доступа
- NAT, PAT, туннелирование, шифрование
- P2P, TOR
- Балансировка нагрузки
- Мониторинг сетевого трафика

Научишься:

- Анализировать сетевые угрозы
- Использовать методы мониторинга трафика
- Работать с сетевыми технологиями безопасности

🛠️ **Практика в блоке:**

- Лабораторная работа №4: Использование tcpdump для захвата сетевого трафика

☑️ **Тестирование по блоку Принципы безопасности**

⚔️ Блок 5

Методы атак

Содержимое блока:

- DoS, DDoS
- Man-in-the-middle
- Атаки на веб-приложения (SQL-инъекция, XSS)
- Социальная инженерия
- Атаки на конечные точки
- Вредоносное ПО

Научишься:

- Определять различные виды атак
- Понимать методы социальной инженерии
- Противостоять современным сетевым угрозам

☑️ **Тестирование по блоку Методы атак**

🔒 Блок 6

Работа с криптографией и PKI

Содержимое блока:

- Основы криптографии
- Хеширование
- Симметричное и асимметричное шифрование
- PKI и цифровые подписи

Научишься:

- Работать с шифрованием и сертификацией
- Понимать криптографические алгоритмы

🛠️ **Практика в блоке:**

- Лабораторная работа №5: Сравнение хешей
- Лабораторная работа №6: Наблюдение за обменом цифровыми сертификатами через Wireshark

☑️ **Тестирование по блоку Работа с криптографией и PKI**

📋 Блок 7

Анализ угроз для конечных точек

Содержимое блока:

- Антивирусные технологии
- Хостовые межсетевые экраны
- Мониторинг и защита конечных устройств

Научишься:

- Защищать конечные устройства от угроз
- Использовать хостовые средства безопасности

☑️ **Тестирование по блоку Анализ угроз для конечных точек**

📌 Блок 8

Погружение в Endpoint Security

Содержимое блока:

- Файловые системы Windows и Linux
- CVSS
- Работа с вредоносным ПО

Научишься:

- Понимать файловые системы в контексте безопасности
- Использовать песочницы для анализа вредоносных программ

🛠️ **Практика в блоке:**

- Лабораторная работа №7: Использование ADS для скрытия файла
- Лабораторная работа №8: Создание песочницы для анализа вредоносных программ

☑️ **Тестирование по блоку Погружение в Endpoint Security**

🚨 Блок 9

Компьютерная криминалистика

Содержимое блока:

- Сбор и хранение цифровых доказательств
- Инструменты криминалистики

Научишься:

- Проводить сбор цифровых доказательств
- Работать с forensic-инструментами

🛠️ **Практика в блоке:**

- Лабораторная работа №9: Создание образа диска в Linux
- Лабораторная работа №10: Использование FTK Imager для создания образа диска в Windows

☑️ **Тестирование по блоку Компьютерная криминалистика**

📝 Блок 10

Анализ вторжений

Содержимое блока:

- IDS/IPS
- Межсетевые экраны
- Анализ сетевого трафика

Научишься:

- Выявлять события вторжения
- Работать с сетевыми журналами

🛠️ **Практика в блоке:**

- Лабораторная работа №11: Анализ пакетов с помощью Wireshark

☑️ **Тестирование по блоку Анализ вторжений**

🔑 Блок 11

Методы управления безопасностью

Содержимое блока:

- Активы и уязвимости
- Управление мобильными устройствами
- Регулярные выражения

Научишься:

- Управлять безопасностью ИТ-активов
- Автоматизировать поиск информации

🛠️ **Практика в блоке:**

- Лабораторная работа №12: Использование регулярных выражений для поиска данных

☑️ **Тестирование по блоку Методы управления безопасностью**

🆘 Блок 12

Действия при реагировании на инциденты

Содержимое блока:

- Процесс реагирования на инциденты
- Профилирование сетей и серверов
- Стандарты соответствия (PCI DSS, HIPAA)

Научишься:

- Организовывать ответ на инциденты
- Работать с профилированием сетевой инфраструктуры

☑️ **Тестирование по блоку Действия при реагировании на инциденты**

🛠️ Блок 13

Обработка инцидентов

Содержимое блока:

- Модели анализа инцидентов (Diamond Model, Cyber Kill Chain)
- Сбор доказательств и идентификация данных

Научишься:

- Использовать модели анализа вторжений
- Понимать процесс сбора цифровых доказательств

☑️ **Тестирование по блоку Обработка инцидентов**

🏗️ Блок 14

Внедрение решений Cisco для обеспечения безопасности

Содержимое блока:

- AAA в Cisco
- Развертывание межсетевого экрана
- Настройка IPS

Научишься:

- Настраивать решения Cisco в целях безопасности
- Использовать Cisco Packet Tracer

🛠️ **Практика в блоке:**

- Лабораторные работы на базе Cisco Packet Tracer по внедрению технических средств безопасности

☑️ **Тестирование по блоку Внедрение решений Cisco для обеспечения безопасности**

🏁 Финальное тестирование

☑️ **Обобщающее тестирование по всем блокам курса**

- Проверь свои знания, закрепи ключевые темы и убедись, что готов применять новые навыки на практике

Изучишь технологии и инструменты:

Cisco Packet Tracer | Cisco | Cisco CLI | Putty

Wireshark | FTK Imager | Kali Linux | Linux

Получишь сертификаты:

Настоящее удостоверение свидетельствует о том, что

Добронравов Алексей Олегович

прошел(а) повышение квалификации в (на)

ООО "Мерион Нетворкс"

по дополнительной профессиональной программе

Кибербезопасность

в объеме

40 академических часов

УДОСТОВЕРЕНИЕ

О ПОВЫШЕНИИ КВАЛИФИКАЦИИ

Документ о квалификации

Регистрационный номер

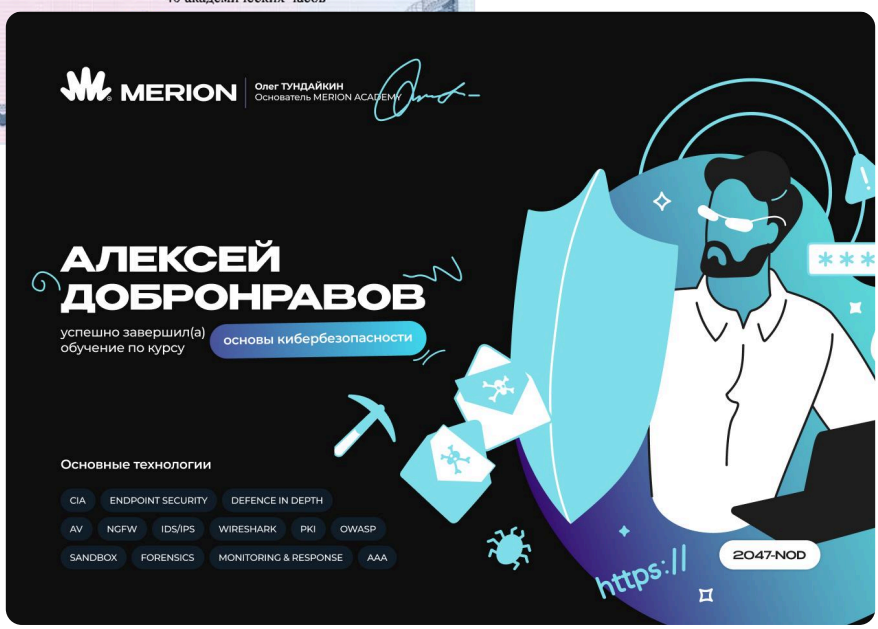
12

Город

Москва

Дата выдачи

09.03.2023



ОБ АВТОРЕ

Александр Ахремчик

Computer Security Incident Response Team (CSIRT) Lead Analyst

- Skills: IR, Threat Hunting, OSINT, Network & Host Forensics
- Products: ArcSight ESM (Micro Focus), QRadar SIEM (IBM), MP SIEM (Positive Technologies), FortiSIEM (Fortinet)

ЧТО ГОВОРЯТ НАШИ СТУДЕНТЫ

Денис ц

10 февраля 2025

★★★★★

Не первый курс прохожу у данной компании, самое сложное - заставить себя. Подача норм, контент в целом актуален либо доступен, самое крутое - всегда можно вернуться и что-то вспомнить, пройти повторно. Поддержка работает тоже хорошо, в общем негатива не вызвали =)

Зайдулин В.

2 февраля 2025

★★★★★

Отличный курс, всё отлично объясняют. Буду учиться дальше! Всем советую пройти его и устроиться на удаленную работу из дома. Кибербезопасность рулит!

Edmond Atoyan

27 декабря 2022

★★★★★

Прошел курс по основам информационной безопасности и остался доволен результатом. Курс представлен весьма информативно и цена вполне соответствует полученным знаниям. Особенно порадовали практические задания в Cisco Packet Tracer и примеры с использованием открытых решений по информационной безопасности. Надеюсь, что в будущем добавят лабораторные работы по комплексной защите сети с использованием различных открытых решений, таких как антивирусы, системы обнаружения вторжений, интегрированные платформы безопасности и др., а также уроки по форензике с применением открытых инструментов на реальных примерах. Практика – основа всего, и я уверен, что такие упражнения значительно обогатили бы опыт обучения. Рекомендую этот курс новичкам – он информативен, интересен и оправдывает свою стоимость.

ЗДЕСЬ РАБОТАЮТ НАШИ ВЫПУСКНИКИ

Для нас это не просто логотипы, а истории повышения зарплаты, получения новой должности и масштабирования бизнеса.

Т БАНК · Ростелеком · ВКонтакте · МГТС

OZON · Selectel · МТС · ТАТТЕЛЕКОМ · FLOCKTORY

ПУЛКОВО Аэропорт Санкт-Петербурга · TATNEFT · РУСАГРО группа компаний · Газпром · ТЕПЛОСЕТЬ САНКТ-ПЕТЕРБУРГА

ГЛАВСТРОЙ · DATALINE

ЗАПИСАТЬСЯ

Перейди по ссылке, или отсканируй QR-код, чтобы записаться на курс

Перейти по ссылке >