карта 2

F-402: Инженер по информационной безопасности (Security Engineer)

F-106: Основы. Введение в информационную безопасность (Introduction to InfoSec)

Без РТ бонусов

С ИТМО бонусами

- Умение устанавливать ПО
- Умение читать техническую литературу на английском со словарем

- Современные тренды и проблемы ИБ, роль специалистов
- Механизм повышения защищенности ИТ-инфраструктуры
- Устройства ИТ-инфраструктуры компаний и, связанные с ней угрозы
- Опасность целевых атак (APT)
- Основные стандарты в области ИБ

F-108: Операционная система Linux (OS Linux)

Без РТ бонусов

С ИТМО бонусами

- Умение устанавливать ПО и работать с виртуализацией
- Базовое понимание работы сетей

- Терминал Linux: управление файлами, правами доступа, пользователями
- Сетевые сервисы: настройка Apache2, SSH, FTP, SMB и др.
- Сетевая настройка ОС Linux и удалённое подключение по SSH
- Безопасность: аудит системы, инструменты защиты, настройка межсетевого экрана

F-109: Локальные сети (Local Area Network)

С ИТМО бонусами

Без РТ бонусов

- Работа с Windows/Linux (RDP, SSH, установка ПО, настройка)
- Владение системами виртуализации (VirtualBox/VMware)
- Умение работать с правами в Linux (sudo/su)

- Расчет параметров сети и базовая настройка маршрутизаторов Cisco
- Настройка сетевых сервисов: DHCP, DNS, NAT
- Построение VPN-подключений (настройка клиентов и серверов)
- Моделирование сетевой инфраструктуры и планирование IP-адресации
- Контроль сетевого доступа к объектам инфраструктуры
- Проведение атак на сетевые протоколы и защита от них

F-110: Доменная структура Windows (Windows Domain Infrastructure)

С ИТМО бонусами

- Администрирование Windows и виртуализация (VirtualBox)
- Установка ПО и настройка ОС
- Чтение технической документации на английском

- Серверы DHCP, DNS, GPO и как их конфигурировать
- Процессы аутентификации в доменных средах
- Как происходит обмен файлами в доменной инфраструктуре
- Базы данных уязвимостей, критичность уязвимостей
- Процесс выявления уязвимых узлов в инфраструктуре
- Анализ событий ОС Windows

F-111: Администрирование СЗИ (Administration of Information Security Tool)

С ИТМО бонусами

- Администрирование Windows и виртуализация (VirtualBox)
- Установка ПО и настройка ОС
- Чтение технической документации на английском

- Типовая архитектура средств защиты информации в корпоративной инфраструктуре
- Роль и место систем SIEM, IDS/IPS, NAF в обеспечении информационной безопасности
- Организационные процессы интеграции средств защиты в инфраструктуру
- Применение бесплатного ПО для защиты информационной инфраструктур

F-113: Эксплуатация средств и процессов информационной безопасности(Security Tools and Processes Operation)

С ИТМО бонусами

- Уверенно работать в командной строке Linux (bash): управление файлами, пользователями, правами доступа, сервисами, настройка сети;
- Администрировать ОС Window, понимание журналов событий.
- Понимать базовые сетевые протоколы (ARP, DHCP, DNS, TCP/UDP)
- Уметь развораивать и настраивать виртуальные машины в VirtualBox/VMWare.

- Внедрение и эксплуатация средств защиты информации в корпоративной инфраструктуре
- Настройка журналирования и мониторинг событий безопасности на конечных узлах
- Понимание моделей атак и векторов компромитации инфраструктуры с использованием MITRE ATT&CK
- Представление о нормативных требованиях и основах менеджмента информационной безопасности

Введний курс, обзор ключевых этапов пентеста:

- разведка внешней инфраструктуры;
- базовые веб-атаки;
- привилегии в Linux/Windows;
- пробросс трафика, защита от обнаружения.

Курс покажет, как можно развиваться в этой области: через принципы и тренировку мышления, практику.

R-101: «Профессия — Белый Хакер» (White Hacker Profession)

Без РТ бонусов

С ИТМО бонусами

- Базовые навыки работы с ПК и интернетом
- Администрирование Windows/Linux
- Владение виртуализацией и контейнерами
- Знание основ сетей
- Чтение техдокументации на английском

- Имитация атак на ИТ-инфраструктуру и поиск уязвимостей с использованием специализированных инструментов
- Анализ сетевого трафика, протоколов и клиент-серверного взаимодействия
- Повышение привилегий: в информационных системах, веб-сайтах, операционных системах, сетевых инфраструктурах

Углубленная версия R-101

Это полный профессиональный трек пентестера (разведка, первичные векторы, подготовка инструментов, повышение привилегий, внутрисетевые атаки и АД):

- переход от junior до mid pentester/Red Team Specialist;
- навыки написания и модификации эксплойтов, управления C2, скрытого исполнения и обхода детекторов;
- инструменты Nmap, Burp Suite, Metasploit, Scapy, BloodHound и др.

Курс по использованию Python для задач пентеста дайт возможность автоматизировать, писать собственные скрипты и эксплойты, ускорить работу:

- работа с протоколами;
- парсинг;
- Scapy;
- многопоточность;
- многопроцессность.

R-218: Программирование на Python для пентестеров (Python Programming For Penetration...

С ИТМО бонусами

- Знание основ работы сетей
- Навыки работы с Linux/Windows на уровне продвинутого пользователя
- Опыт работы с виртуализацией (VirtualBox/VMWare)
- Умение читать техническую документацию на английском

- Программирование скриптов для работы с файлами и сетью
- Работа с сетевыми протоколами, парсингом и многопоточностью
- Автоматизация пентеста и исследований безопасности

R-220: Анализ безопасности мобильных приложений (Mobile Application Security Analysis)

С ИТМО бонусами

- Знание основ сетевого взаимодействия
- Администрирование Linux/Windows
- Работа с PowerShell/bash
- Навыки программирования
- Опыт работы с VirtualBox/VMWare

- Разработка простых Android-приложений
- Реверс-инжиниринг APK/IPA
- Динамический анализ iOS
- Поиск и эксплуатация уязвимостей
- Извлечение данных из мобильных ОС

R-319: Анализ защищенности веб-приложений (Web Application Security Analysis)

С ИТМО бонусами

- Опыт программирования (PHP, Python, Java и др.)
- Понимание сетевых протоколов (IP, TCP, DNS, HTTP)
- Опыт разработки веб-приложений (мин. динамические страницы)
- Навыки работы с Linux/Windows на уровне продвинутого пользователя (установка пакетов, работа с терминальной оболочкой, менеджмент прав доступа)
- Опыт работы с VirtualBox/VMWare

- Работа с Burp Suite и другими инструментами пентеста
- Обнаружение и эксплуатация основных уязвимостей серверной и клиентской части веб-приложений(SQLi, OS Command Injection, XSS, CSRF, SSRF, XXE, LFI/RFI, Prototype Pollution и др.)
- Оценка корректности реализации механизмов аутентификации и управления сессиями
- Использование техник обхода фильтраций и защиты
- Подготовка отчётов с описанием уязвимостей и рекомендациями

Углубленное изучение веб-пентеста:

- ручная и автоматическая эксплуатация веб-уязвимостей, шаблонов обхода фильтров;
- работа с Burp Suite/Ffuf/sqlmap и другими инструментами;
- оформление отчётов.

Отдальная ветка для тех, кому интересна мобильная безопасность:

- ОС Android и iOS;
- создание простых приложений;
- анализ данных в закрытых приложениях;
- реверс-инжиниринг пакетов .apk и .ipa;
- поиск и эксплуатация типовых уязвимостей.

R301: Пентестер (Penetration Testing Specialist)

С ИТМО бонусами

- Опыт программирования на языке высокого уровня
- Понимание работы веб-страниц и взаимодействия с сервером
- Знание сетевых протоколов (TCP/IP)
- Умение устанавливать ПО в Windows/Linux
- Навыки работы с командной строкой (ls, pwd, cat, cd, scp, ssh и др.)
- Умение запускать инструменты в командной строке Linux/Windows
- Навыки использования VPN
- Умение работать с технической документацией на английском

- Разведка и сбор информации об инфраструктуре
- Эксплуатация уязвимостей веб-приложений, сервисов и ОС
- Проведение атак социальной инженерии и обход защитных средств
- Повышение привилегий в Windows, Linux и контейнерных средах
- Атаки на Active Directory и горизонтальное перемещение
- Применение более 100 техник пентеста в виртульных лабораторях
- Формирование отчётов с оценкой рисков и рекомендациями для компаний

R301-M1 Исследование целей тестирования

- Установка программного обеспечения в ОС Windows и Linux
- Знание базовых команд командной строки (ls, pwd, cat, cd, scp, ssh)
- Запуск инструментов и утилит через командную строку
- Работа с VPN
- Перевод технической документации с английского языка
- Поиск информации в технической документации

- Сканирование сетей
- Сбор информации о домене
- Поиск учетних информации об организации
- Поиск email-адресов сотрудников организации
- Поиск известных уязвимостей программного обеспечения

R301-GM1 Внешний периметр

- Установка программного обеспечения в ОС Windows и Linux
- Владение базовыми командами командной строки (ls, pwd, cd, scp, ssh)
- Запуск инструментов и утилит через командную строку
- Настройка и использование VPN-соединений
- Перевод технической документации с английского языка
- Поиск и анализ информации в технической документации
- Понимание информации на языке высокого уровня
- Понимание файловой структуры ОС Linux
- Понимание принципов работы веб-страниц и передачи данных на сервер

R301-M2 Получение первичного доступа через атаки на аутентификацию

- Компромитация учетных записей
- Проверка надёжности пароля
- Восстановление зашифрованных паролей

R301-M3 Получение первичного доступа через атаки на веб-приложения

- Сбор информации о веб-приложении
- Идентификация и оценка уязвимостей в веб-приложениях
- Эксплуатация наиболее опасных уязвимостей для захвата управления приложением

R301-M4 Получение первичного доступа через атаки социальной инженерии

- Разработка системы фишинговой рассылки для проверки уровня осведомлённости сотрудников
- Проведение типовых атак социальной инженерии для компромитации компьютеров сотрудников
- Подготовка инфраструктуры фишинговых атак и зеркал веб-сайтов

R301-M5 Эксплуатации известных уязвимостей

- Эксплуатация известных уязвимостей из списка популярных CVE
- Подготовка и поиск актуальных CVE для информационной системы
- Поиск и применений эксплойтов для известных уязвимостей
- Доработка и изменение эксплойтов для известных уязвимостей

R301-M6 Подготовка инструментов тестирования

- Обход антивирусных средств и средств защиты
- Применение техник скрытого исполнения нагрузок
- Использование популярных средств управления и контроля скомпромитированной системы (C&C)

- Проведение разведок и сбор информации (доменов, IP, подсетей, e-mail, учетки), использование инструментов Nmap, Shodan, Amass, Burp Suite, Wfuzz, Metasploit, Nessus
- Атаки на аутентификацию (brute force, password spraying, восстановление хешей)
- Тестирование веб-приложений (SQLi, OS Command Injection, Directory Traversal, File Upload и др.)
- Эксплуатация известных уязвимостей (Log4Shell, PrintNightmare, EternalBlue и др.)
- Проведение атак социальной инженерии (фишинг, подготовка инфраструктуры рассылок)
- Обход антивирусов, AMSI и динамического анализа, применение безфайловых техник
- Использование C2-инфраструктуры и скрытое исполнение нагрузок

- Навык получения шеллов
- Умение использовать полезные нагрузки
- Навыки обхода средств защиты
- Понимание модели клиент-сервер

После получения первичного доступа нужно закрепиться в системе и развить атаку

- Установка программного обеспечения в ОС Linux
- Владение базовыми командами командной строки (ls, pwd, cat, cd, scp, ssh)
- Понимание файловой системы Linux
- Понимание системы прав доступа в Linux
- Запуск инструментов и утилит через командную строку Linux
- Работа с VPN
- Перевод технической документации с английского языка
- Поиск информации в технической документации
- Опыт программирования на языке высокого уровня
- Понимание сетевых протоколов TCP/IP

R301-GM2 Повышение привилегий

R301-M7 Повышение привилегий в Linux

- Сбор информации о системах Linux
- Поиск и эксплуатация локальных уязвимостей в системе Linux
- Эксплуатация уязвимостей в привилегированных системных сервисах Linux
- Анализ конфигурации Linux на возможности несанкционированного повышения привилегий
- Применение эксплойтов к ядру Linux

R301-M8 Повышение привилегий в контейнерных средах

- Исследование окружения контейнера Docker
- Повышение привилегий в docker-контейнерах и побег из контейнеризации
- Исследование окружения Kubernetes

R301-M9 Повышение привилегий в Windows

- Сбор информации и разведка в ОС Windows
- Извлечение учётных данных в операционной системе Windows
- Манипулирование учётными записями и сессиями
- Повышение привилегий через misconfigurations в сервисах Windows
- Повышение привилегий через уязвимости ядра Windows

- Анализ конфигураций и сбор информации в Linux и Windows
- Эксплуатация локальных уязвимостей в Linux (SUID, Cron, Sudo, переменные окружения, ядро)
- Использование инструментов LinPEAS, linux exploit suggester, nuclei, metasploit local exploit suggester
- Повышение привилегий и побег из Docker-контейнеров, исследование окружения Kubernetes
- Извлечение учётных данных и хешей в Windows (LSASS, SAM)
- Эксплуатация уязвимостей сервисов, автозапуска и ядра Windows
- Использование инструментов LaZagne, Sharpdp, Impacket, Sliver, hashcat

- Полный контроль над хостами
- Навыки извлечения учетных данных
- Понимание внутреннего устройства ОС

Дальше нужно распространяться по внутренней сети

- Понимание Active Directory и сетевых протоколов TCP/IP
- Установка ПО в ОС Linux и Windows
- Владение базовыми командами и утилитами командной строки
- Навык работы с VPN
- Перевод технической документации с английского языка
- Поиск информации в технической документации

R301-GM3 Локальные сети

R301-M10 Проброс сетевого трафика (Pivoting)

- Обеспечение доступа к внутренним ресурсам через использование встроенных функций операционных систем и прикладных программ
- Получение доступа к внутренним ресурсам через jump host
- Туннелирование трафика

R301-M11 Проведение атак на локальные сети

- Перехват трафика
- Анализ трафика сети
- Расшифровка TLS-трафика
- Проведение атак Man-in-The-Middle

R301-M12 Проведение атак на Active Directory

- Сбор информации в сети Windows-машин
- Проведение атак типа «Relay»
- Проведение атак Pass-the-Hash
- Горизонтальное перемещение в сети Windows-машин
- Проведение атак на протокол аутентификации Kerberos
- Проведение атак на службы сертификатов

- Настройка туннелей и прокси-цепочек (SSH, Chisel, Gost, proxychains4)
- Проброс трафика и обход сетевых ограничений
- Перехват и анализ сетевого взаимодействия (Wireshark, tcpdump, NBTscan)
- Проведение атак ARP Spoofing, LLMNR/NetBIOS/mDNS Poisoning
- Расшифровка TLS-трафика и атаки MITM
- Сбор информации в Active Directory с использованием BloodHound и PowerView
- Атаки Pass-the-Hash и Relay, Kerberoasting, ASREPRoasting, Zerologon
- Повышение привилегий через ESC1/ESC4/ESC8, злоупотребление ACL и LAPS
- Выполнение атак DCsync и горизонтальное перемещение в сетях Windows
- Построение комплексной методики тестирования внутренней инфраструктуры компании

R301-M13 Формирование отчета

- Составление отчетов о проведении тестирования

Полезно для специалистов направления защиты, желающих глубже понять тактика атакующих и повысить эффективность оборонительных мер:

- понимание TTP атакующих;
- артефакты локальной эскалации;
- понимание методов обхода EDR.

Введний курс Blue Team дайт практику разворачивания мониторинга и базовые навыки аналитики:

- развёртывание SIEM/агентов;
- чтение логов Windows и Linux;
- первичная forensic-практика.

B-101: Специалист по противодействию кибератакам (Cyber Security Threat Specialist)

Без РТ бонусов

С ИТМО бонусами

- Базовые навыки ПК: работа с компьютером, установка ПО
- Администрирование Windows/Linux (терминал, права, пакеты)
- Владение виртуальными средами (VirtualBox/VMware)
- Знание основ сетей и чтение технической документации на английском

Стартовые навыки:

- развертывание защищенной инфраструктуры;
- анализ и мониторинг киберугроз;
- реагирование на инциденты;
- криминалистический анализ.

Полный цикл обучения SOC-аналитика для выявления атак:

- обнаружение атак (XSS, фишинг, Kerberos);
- анализа логов;
- обнаружение в АД(бесподписные сетяк.

Выпускники трека смогут уверенно работать аналитиками SOC, проводить расследования и повышать защищённость инфраструктуры компаний.

Курс разбирает векторы атак на инфраструктуру:

- разведка и анализ инфраструктуры (OSINT, сканирование, перечисление);
- тестирование веб-приложений и защита от атак;
- пост-эксплуатация и анализ вредоносного ПО;
- безопасность сетей (VPN, туннелирование, Wi-Fi).

Практическая программа по системам информационной безопасности и настройкам ключевых систем защиты:

- межсетевые экраны, IDS/IPS, прокси, VPN;
- антивирусная защита, групповые политики AD, защита на уровне ОС;
- работа с SIEM, анализ трафика, развертывание Honeyfrut.

Для AppSec/DevSecOps S-235 дайт основные концепции кибербезопасности и принципы защиты приложений:

- ключевые уязвимости веб-приложений;
- безопасность окружения и инструменты защиты ПО;
- интеграция безопасности на всех этапах разработки;
- снижение количества уязвимостей и итерацией доработки.

Обучение SOC-аналитика:

- обнаружение атак на внешний периметр (XSS, CSRF, SQLi, фишинг);
- выявление аномальной активности во внутренней сети Windows/Linux;
- детектирование атак на АД (Kerberoasting, Pass-the-Hash, DCSync);
- анализ вредоносного сетевого трафика и выявление скрытого атакующего.

Прямое применение настроенных систем в операционной деятельности SOC

Прямое развитие тем администрирования и защиты:

- изучение угроз и методов атак;
- разработка и внедрение стратегии защиты периметра и внутренней сети;
- настройка средств защиты (firewall, IDS/IPS, DLP, SIEM);
- интеграция мониторинга.

Программа по работе аналитиком SOC:

- работа с SIEM, корреляция событий;
- обнаружение и расследование атак;
- настройка правил корреляции, плейбуки;
- практические методы противодействия кибератакам.

S-235: Основы безопасной разработки (Secure Development Fundamentals)

С ИТМО бонусами

- Опыт работы в ИТ
- Понимание процесса разработки ПО
- Навыки администрирования ОС (VMWare, VirtualBox)
- Опыт работы с Unix-подобными ОС
- Базовые знания сетей (DNS, TCP)
- Навыки программирования на любом языке
- Умение читать техническую документацию на английском
- Навыки анализа логов и поиска решений по ошибкам

- Основные концепции кибербезопасности
- Методологии устранения угроз веб-приложений
- Стандарты и практики защиты веб-приложений
- Принципы безопасной разработки
- Безопасная настройка окружения и компонентов приложений
- Статический и динамический анализ кода

Профессиональный трек с практикой построения security-pipeline, оркестрацией, контейнерной безопасностью и примерами эталонных конфигураций.

Для углубленного изучения процессов и инструментов

Это углубление в процессы SDLc для интеграции безопасности в разработку:

- SDL, DevSecOps;
- применение инструментов анализа: SAST, DAST, SCA, Fuzzing;
- безопасность инфраструктуры: управление секретами, контейнерами и CI/CD;
- создание AppSec-процессов: дорожная карта и обучение команд.

Знание уязвимостей приложений помогает понимать, почему правильная конфигурация окружения важна и какие конкретные настройки предотвратят эксплуатацию уязвимостей:

- управление конфигурациями с использованием Ansible и Vagrant;
- хардинг Linux-систем;
- настройка и защита Nginx;
- работа с Docker и обеспечение его безопасности;
- развертывание и защита Kubernetes;
- безопасное хранение секретов с Hashicorp Vault;
- конфигурирование безопасности в облачных средах (IaaS, PaaS, SaaS).

B-301: Аналитик Центра противодействия кибератакам (Security Operations Center Analyst)

С ИТМО бонусами

- Знание сетевых протоколов и веб-технологий
- Навыки работы в Linux (bash): базовые команды (ls, cd, ssh и др.)
- Опыт работы с виртуализацией
- Понимание прав доступа к файлам и каталогам (rwx)
- Умение читать техническую документацию на английском

- Обнаружение атак на внешний периметр (сканирование, XSS, CSRF, SQLi, фишинг)
- Выявление аномальной активности во внутренней сети Windows/Linux
- Детектирование атак на Active Directory (Kerberoasting, Pass-the-Hash, DCSync)
- Анализ вредоносного сетевого трафика и выявление закрепления атакующего
- Работа с инструментами SOC: SIEM (Elastic), Suricata, Wireshark, Sysmon
- Построение личной базы знаний и методик реагирования на инциденты

B301-M1 Обнаружение атакующего на этапе работы с внешним периметром

- Обнаружение атак на внешний периметр и его защиту
- Обнаружение атак на веб-приложения и внедрение механизмов их защиты
- Обнаружение фишинговых атак и снижение рисков от них

B301-M2 Обнаружение атакующего на этапе разведки во внутренней сети

- Выявление эксплуатации уязвимостей Windows и Linux
- Обнаружение различных атак на беспроводные сети
- Анализ активности системных процессов

B301-M3 Обнаружение атак на доменную инфраструктуру, построенную на базе Windows Active Directory

- Обнаружение различных атак на Active Directory
- Обнаружение и предотвращение эксплуатации уязвимостей
- Обнаружение классических атак на Kerberos
- Предотвращение компромитации сети и обеспечение соответствия требованиям безопасности

B301-M4 Обнаружение закрепления атакующего на хостах и анализ сетевого трафика

- Обеспечение безопасности информационной системы
- Выявление закрепления на Windows-машинах и Linux-машинах
- Выявление аномальной активности в сегменте рабочих станций

B301-M5 Дополнительный. Техники атак хакера

- Позволяет специалисту SOC лучше понять действия атакующего и посмотреть на свои действия с двух сторон, увидеть что конкретно делает хакер

Для углубленного понимания защиты инфраструктуры

B-410: Специалист по защите корпоративной инфраструктуры (Corporate Infrastructure Protection Specialist)

С ИТМО бонусами

- Знание английского для работы с технической документацией
- Понимание основ сетевого взаимодействия
- Навыки работы с Linux/Windows (на уровне продвинутого пользователя)
- Опыт работы с виртуализацией (VirtualBox, VMWare)

B-207: Угрозы корпоративной инфраструктуры (Cyber Infrastructure Threats)

- Моделирование корпоративной инфраструктуры
- Проведение тестирования инфраструктуры по основным векторам атак
- Работа с инструментами OSINT, сетевыми сканерами, сканерами уязвимостей

B-208: Системы Информационной Безопасности (Information Security Systems)

- Linux: администрирование ОС и гипервизоров, настройка сетей/SSH/пользователей, Bash-скрипты и сервисы, межсетевой экран
- Windows: развёртывание AD и контроллера домена, настройка DNS/GPO, управление пользователями, PowerShell/cmd
- Сети: анализ трафика, межсетевые экраны и IDS/IPS, прокси-серверы, VPN с 2FA, аудит безопасности ОС

- Сегментирование и разделение сетей
- Настройка межсетевых экранов, прокси-серверов, VPN
- Развертывание проактивной антивирусной защиты
- Детектирование сетевых атак и аномального трафика
- Настройка расширенного аудита Windows
- Управление инцидентами и событиями ИБ
- Настройка систем HoneyPot и HoneyNet

B-228: Аналитик SOC (Security Operations Center Analyst)

- Linux: администрирование ОС и гипервизоров, настройка сетей/SSH/пользователей, Bash-скрипты и сервисы, межсетевой экран
- Windows: развёртывание AD и контроллера домена, настройка DNS/GPO, управление пользователями, PowerShell/cmd
- Сети: понимание сетевых протоколов (IP/TCP/DNS/HTTP), управление сетями Cisco, настройка маршрутизации и VLAN/Trunk-портов

- Моделирование угроз
- Развертывание SIEM
- Мониторинг и сбор данных
- Создание правил корреляции
- Работа с IDS/IPS
- Расследование инцидентов
- Обнаружение скрытых каналов связи
- Тактики реагирования на инциденты
- Разработка плейбуков

Безопасная разработка может требовать понимания инфраструктуры(уменьшение рисков на стыке разработки и эксплуатации)

S-410: Специалист по безопасной разработке приложений (Specialist in secure application development)

С ИТМО бонусами

- Знание английского для работы с технической документацией
- Опыт программирования (PHP, Python, Java и др.)
- Понимание сетевых протоколов (IP, TCP, DNS, HTTP)
- Опыт разработки веб-приложений (мин. динамические страницы)
- Навыки работы с Linux/Windows (установка ПО, терминал, управление правами)
- Опыт работы с виртуализацией (VirtualBox, Docker, LXD)

- Выстраивания безопасности окружений правильным конфигурациям инструментов Docker, Kubernetes, AWS IAM
- Выстраивания взаимодействия в отделе обеспечения безопасности разработки ПО в соответствии с особенностями процессов безопасной разработки и инструментов, применяемых в SDLC-цикле
- Созданием Security Pipeline на основе GitLab и инструментов SAST, DAST, SCA и пр.

S-232: Безопасная разработка приложений в рамках SDL цикла (Security Development Lifecycle)

С ИТМО бонусами

- Умение читать техническую документацию на английском
- Опыт программирования (PHP, Python, Java и др.)
- Понимание сетевых протоколов (IP, TCP, DNS, HTTP)
- Опыт разработки веб-приложений (мин. динамические страницы)

- Формулирование требований и процессов в цикле безопасной разработки ПО
- Разработка дорожной карты развития SSDLc
- Применение инструментов DAST, SAST, SCA в CI/CD
- Автоматизация анализа безопасности окружения приложений
- Обнаружение типовых уязвимостей веб-приложений OWASP Top 10 с использованием автоматизированных средств.

S-224 дайт практические реализации этих мер в окружении:

- практические навыки работы с инфраструктурой (Linux hardening, Nginx, Docker, Kubernetes, Vault);
- понимание уязвимостей конфигурации окружения;
- автоматизация через Ansible, Vagrant, CI/CD.

S-232 объясняет, какие меры нужны в SDLC:

- понимание требований безопасности на этапе проектирования;
- настройка security-пайплайна в Jenkins;
- работа с SAST/SCA/DAST-инструментами;
- моделирование угроз для приложений;
- управление security-requirements.

S-224: Безопасность окружения приложений (Applications Environment Security)

С ИТМО бонусами

- Умение читать техническую документацию на английском
- Навыки анализа логов и поиска решений по ошибкам
- Администрирование Linux/Mac
- Опыт работы с виртульными средами (VirtualBox, Docker, LXD)

- Автоматизация развертывания (Ansible, Vagrant)
- Построение безопасных конфигураций (Nginx, Docker, Kubernetes, AWS IAM)
- Автоматизация поиска уязвимостей в конфигурации ПО Nginx, Docker, Kubernetes, AWS IAM

Понимание уязвимостей помогает точнее выстраивать процесс безопасной разработки, определять, какие проверки должны быть обязательными, и где внедрять контроль (SAST, DAST, SCA, SBOM и т.д.):

- знание методов атак;
- практический опыт тестирования;
- глубокое понимание уязвимостей.

Специалисты ПОМОГУТ, как моделировать угрозу для организации на основе ландшафта угроз:

- TTP и цепочки атак для построения TI-отчётов;
- работа с моделями и платформами Threat Intelligence;
- создание правил детектирования и поиск угроз;
- анализ угроз и данных.

SOC-аналитики научатся составлять ландшафт угроз, чтобы самостоятельно приоритизировать написание правил корреляции:

- работа с моделями и платформами Threat Intelligence;
- создание правил детектирования и поиск угроз;
- анализ угроз и данных;
- построение процессов TI.

B-236: Реагирование на инциденты и компьютерная криминалистика в ОС Windows (Digital Forensics and Incident Response in Window...

С ИТМО бонусами

- Понимание принципов работы вредоносного ПО
- Навыки работы с Linux/Windows (на уровне продвинутого пользователя)
- Знание тактик злоумышленников (MITRE ATT&CK)
- Опыт работы с виртуализацией (VirtualBox, VMWare)

- Построение процесса реагирования на инциденты
- Сбор и анализ артефактов (реестр, NTFS, Prefetch, JumpList, логи)
- Анализ снимков RAM и дисков (Volatility, FTK Imager, KAPE)
- Выявление и анализ ВПО, IOC-артефактов и persistence-механизмов
- Анализ сетевого трафика и браузерных артефактов (Wireshark, NetFlow)
- Подготовка отчётов по расследованиям

Фундаментальный курс DFIR по Windows:

- сбор цифровых улик: реестр, логи, дампы памяти и дисков с помощью FTK Imager KAPE, Volatility;
- расследование атак: поиск вредоносного ПО и следов взлома;
- анализ артефактов: трафик, браузеры, корреляция событий.

Фундаментальный курс DFIR по Windows даст понимание, где и как защита могла не сработать, как оценить пробелы:

- сбор цифровых улик: реестр, логи, дампы памяти и дисков с помощью FTK Imager KAPE, Volatility;
- расследование атак: поиск вредоносного ПО и следов взлома;
- анализ артефактов: трафик, браузеры, корреляция событий.

Специалисты DFIR помогут эффективность расследования за счет навыков атрибуции (понимания, кто атаковал):

- работа с моделями и платформами Threat Intelligence;
- создание правил детектирования и поиск угроз;
- построение процессов TI.

Курс TIA поможет выстраивать операционную деятельность ИБ-подразделения, действовать проактивно, планировать, внедрять и реализовывать защитные меры, ориентируясь на актуальный ландшафт угроз:

- работа с моделями и платформами Threat Intelligence;
- создание правил детектирования и поиск угроз;
- анализ угроз и данных;
- построение процессов TI.

TIA: Threat Intelligence

С ИТМО бонусами

- Понимание работы веб-страниц и сетевых протоколов (TCP/IP)
- Умение устанавливать и запускать ПО в Windows/Linux
- Навыки работы с командной строкой и VPN
- Умение работать с технической документацией на английском
- Понимание действий атакующих
- Предпосылки: опыт в Blue Team/Red Team или прохождение курса B301 "Аналитик SOC"

- Владение инструментами Threat Intelligence
- Применение процессов и методов TI
- Построение ландшафта угроз
- Написание правил детектирования
- Взаимодействие с командами ИБ