

Требования к квалификации поступающего на обучение по программе повышения квалификации № 33 «Техническая защита информации. Анализ архитектуры и экспертиза исходных кодов программного обеспечения»

К освоению программы повышения квалификации допускаются лица, имеющие высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук (в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации), подтвержденное документом об образовании.

Дополнительные требования к поступающим на обучение:

1. Уверенное знание языков C/C++, ассемблера x86.
2. Знание основ программной инженерии.
3. Навыки работы с ОС Linux, умение работать с интерфейсом командной строки.
4. Базовые навыки работы со средствами дизассемблирования и декомпиляции (IDA Pro, HexRays и т.п.).
5. Навыки работы с QEMU/KVM на уровне уверенного пользователя.
6. Навыки работы со средствами контейнеризации, в частности, docker (понимание основных команд, формирующих docker-файл, в том числе FROM, RUN, CMD, WORKDIR; понимание основных команд самого docker-процесса (run, build, exec); понимание принципов получения терминала для управления контейнером, проброса каталогов между хостом и контейнером).
7. Базовые знания об основных принципах формирования сетевого трафика, сетевых протоколах IP\TCP\UDP\SSL\TLS\HTTP. Умение записать трафик с сетевого интерфейса с помощью tcpdump. Умение открыть просмотр трафика в сетевом анализаторе Wireshark, настроить фильтры отбора сессий, сшить сессию высокоуровневого протокола.
8. Базовые навыки построения SQL запросов.
9. Понимание принципов хранения информации в базах данных, поддерживающих стандарт ANSI/ISO SQL.
10. Понимание принципов XML разметки.

Прибывающим на обучение необходимо иметь с собой ноутбук, удовлетворяющий следующим требованиям к аппаратной части и программному обеспечению:

1. ОЗУ 8+ ГБ, CPU 4+ ядра, 100 ГБ HDD.
2. ОС Linux Ubuntu 18.04.
3. docker, docker-compose.
4. Wireshark на хостовой ОС (для работы с pcap-трассами сетевого трафика).
5. Просмотрщик pdf/docx-файлов.