Карьера
после диплома

"Защита информации для инженера. Основные направления профессиональной области, чем в них занимаются инженерные кадры, что нужно уметь для того что бы работать в выбранном направлении."

Александр Аржанцев

О докладчике

МТУСИ Радиотехника
Опыт работы в качестве :
Инженера в частях войск связи РФ;
Инженер разработчик РЭА;
Инженер специальных исследований в области технических каналов утечки информации (последние 6 лет).

Хобби ИБ
Занимаюсь изучением безопасности сетевых технологий и web программирования, стажер в пентест команде PentestIT.

Основные направления рынка технической защиты информации

- Технические каналы утечки
- Шифрование
- Защита сетей
- Специальные проверки
- Разработка и выпуск оборудования защиты информации
- Испытание, тестирование средств и систем

Технические каналы утечки

- проведение специальных исследование (лабораторные объектовые);
- аттестация помещений ;

Необходимые знания

- знания документации ФСБ, ФСТЭК (нормы и методики);
- измерительное оборудование, специальные комплексы;
- Умение читать схемы, основы радиотехники;
- Знания протоколов исследуемых сигналов.

Шифрование

- разработка аппаратной части;
- разработка программной части;
- внедрение решений.

Необходимые знания

- знание ГОСов по шифрованию;
- основы криптографии;
- знание языка низкого уровня и высокого уровня;
- сетевые технологии на уровни CCNA;
- знание Windows, Linux.

Защита сетей

- работа в ИБ компании (Linux, Windows, CCNA SEC, основы pentest, один язык программирования(например Java), знание законодательства: по конфиденциальной информации, о персональных данных, понимание основ расследований инцидентов);
- работа в интеграторе (знание Linux, Windows, CCNA SEC, вендорские сертификаты по ИБ);
- проектирование защищенных сетей (CCNA SEC, ЕСКД, ГОСТы по проектированию защищенных сетей).

Специальные проверки

- специальных проверки;
- специальные обследования.

Необходимые знания

- знания документации ФСБ (нормы и методики);
- измерительное оборудование, специальные комплексы, рентген;
- Умение читать схемы;
- Знания протоколов исследуемых сигналов, видов и форм сигналов.

Разработка и выпуск аппаратуры защиты информации

- разработка программных, аппаратных или смешенных средств

Необходимые знания

- CCNA;
- ЕСКД;
- ГОСТы по проектированию защищенных средств(в зависимости от вида разработки)
- система автоматизированного; проектирования (напр. “Компас”);
- Linux, Windows, язык программирования

Испытание, тестирование средств и систем.

- сертификационные испытания;

Необходимые знания

- знания документации ФСБ, ФСТЭК (нормы и методики);
- измерительное оборудование, специальные комплексы;
- умение читать схемы;
- знания протоколов исследуемых сигналов
- умение разобраться в алгоритме работы устройства и составить план тестирования.

- тестирование на проникновение.

Необходимые знания

- Linux (**Kali Linux**), Windows, CCNA SEC;
- Основы SQL;
- Знание основных векторов атаки;
- Умение быстро разбираться в технологиях;
- Знания хотя бы одного языка программирования(Ruby,Java);
- Знание PHP, Java, HTML; (Понимание принципов OWSP , топ 10);
- NIST и др. стандарты и методики тестирования.

Что делать что бы быть актуальным для работодателя после окончания института ?

- Знание Windows;
- Linux;
- CCNA SEC (в любом случае CCNA);
- Знание хотя бы одного языка программирования(Java, Ruby и т.д.);
- Нормативная база.

Нет $$$? Не беда учим бесплатно см. ниже!!!

- Знание Windows ;
- Linux (https://stepic.org – обучение Linux,тут же C++,Pyhton);
- CCNA (http://habrahabr.ru/post/134892/ и дальше все темы курса «Сети для самых маленьких»);
- Знание одного языка программирования (http://www.codecademy.com HTML, Java, Ruby);
- https://www.owasp.org OWASP все о безопасности веба;
- http://www.sans.org/ SANS (Demo)-рассылка;
- https://vk.com/pentestit - петест команда, обучение а так же разное интересное по ИБ.

Отдельно обращаю внимание, если есть возможность развиваться и изучать область «облачной» безопасности, то стоит попытаться т.к. просматривается тенденция на большой спрос на данную категорию специалистов в ближайшем будущем

Спасибо за внимание!

aarzhancev@gmail.com