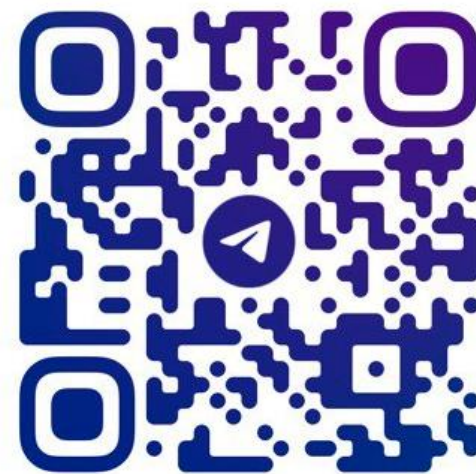


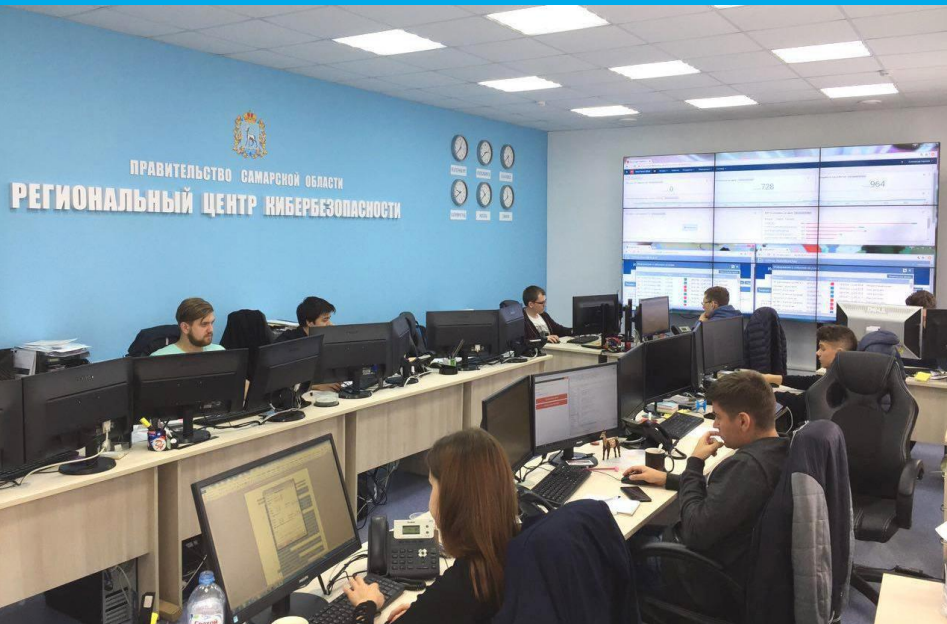


РЕГИОНАЛЬНЫЙ ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

УПРАВЛЕНИЕ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ЦЕНТР
ЦИФРОВОЙ



@DIGITALREG63



О НАС ЦЕНТР ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ И РЕСУРСЫ САМАРСКОЙ ОБЛАСТИ

- Обнаружение и выявление инцидентов ИБ
- Анализ и обработка выявленного инцидента ИБ
- Установление причин и источника инцидента
- Визуализация угроз ИБ, основанная на анализе событий, поступивших в режиме реального времени
- Экспертный анализ событий ИБ
- Реагирование и ликвидация последствий инцидентов информационной безопасности
- Разработка рекомендаций, направленных на устранение уязвимостей и предупреждение подобных инцидентов в будущем
- Проведение аудита безопасности государственных информационных систем Самарской области

ГОССОПКА



У ВАС ЕСТЬ ОПЫТ РАБОТЫ?

У МЕНЯ ЕСТЬ КОЕ-ЧТО ПОЛУЧШЕ!

ЦЕЛЕУСТРЕМЛЕННОСТЬ, КОММУНИКАбельНОСТЬ,
БЫСТРАЯ ОБУЧАЕМОСТЬ...

Что делать дальше после выпуска?

Количество вакансий в Самарской области для специалистов инженеров информационной безопасности по состоянию на сентябрь 2023 года (данные с hh.ru)

Специалист по информационной безопасности 47

Опыт работы

- Не имеет значения
- От 1 года до 3 лет 26
- От 3 до 6 лет 18
- Нет опыта 3

Вакансии без опыта работы:

- Инженер 1 линии технической поддержки мониторинга
- Инженер 1 линии технической поддержки сопровождения СЗИ
- Специалист по информационной безопасности



Собеседование – ОТДЕЛЬНЫЙ ВИД ИСПЫТАНИЯ

- Будь увереннее и не волнуйся
- Умей изложить свои мысли четко и структурировано
- Не ответить на вопрос – не страшно, это нормально
- Самый ценный кандидат для работодателя тот, у которого «горят» глаза

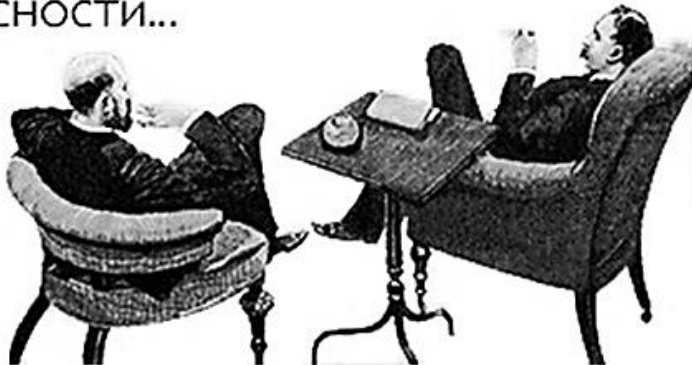
Формула успеха после ВУЗа:

- Умение общаться с людьми
- Уметь работать в команде
- Инициативность

Не нужно быть идеальным, чтобы найти работу!

Первое получение опыта

- У нас дыра в безопасности.
- Слава богу, хоть что-то у нас в безопасности...



- Широкий спектр средств защиты информации от шлюзов безопасности до узконаправленных средств защиты от DDoS-атак
- Объемная инфраструктура состоящая из серверов, систем хранения данных, различных видов сетевого оборудования и ряда специфических устройств
- Бесконечное множество специализированного программного обеспечения: анализаторы сетевого трафика, системы контроля защищенности, защита от НСД, анализаторы исходного кода
- Правовая база, регуляторы – ФСТЭК, ФСБ, Минцифра

Цифровой



ИБ – это про командную игру



Первые проблемы



- Слабо уделено внимание информационным технологиям
- В учебных программах не предусмотрены, либо слабо раскрыты курсы по темам:
 - SOC
 - ГосСОПКА
 - КИИ
 - Защита АСУ ТП
- Навыки проведения различных видов сетевых атак отсутствуют
- Абстрактные знания без практического применения
- Преподаваемые программы быстро устаревают



Алексей Лукацкий
Бизнес-консультант по безопасности



Вся нормативка по ИБ
Что надо знать?



**POSITIVE
HACK
DAYS 12**

ДОВЕРИЕ К ТЕХНОЛОГИЯМ



30/05/2024

ЕЖЕГОДНАЯ
КОНФЕРЕНЦИЯ

IT IS CONF

ПРЯМАЯ ТРАНСЛЯЦИЯ



Спасибо за
внимание!



Контакты:
Андрей
Григорьев

Начальник
управления
информационной
безопасности ГБУ СО



digitalre
g.ru



info@digitalre
g.ru