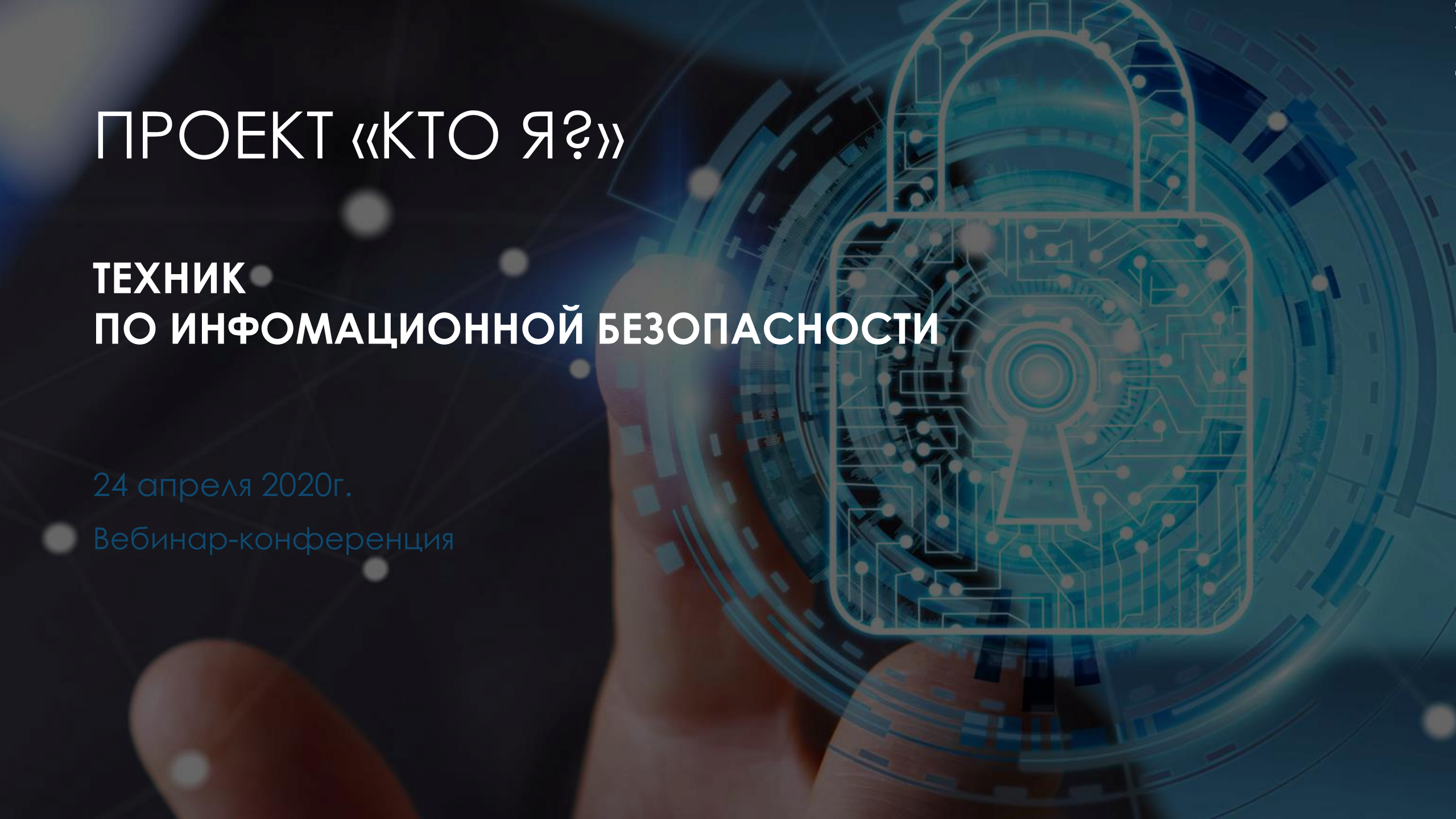
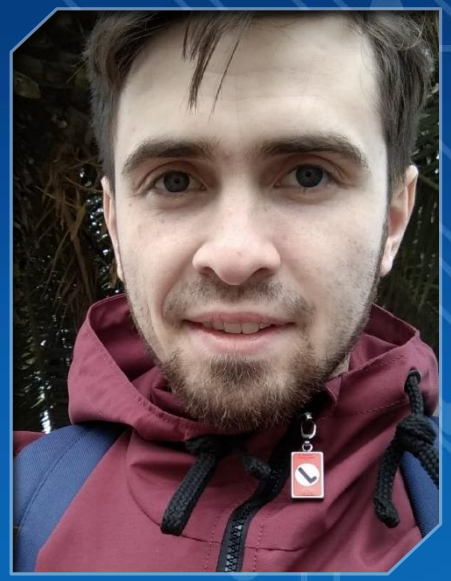
ПРОЕКТ «КТО Я?»

ТЕХНИК
ПО ИНФОМАЦИОННОЙ БЕЗОПАСНОСТИ

24 апреля 2020г.

Вебинар-конференция





Оболенский Борис Вячеславович

Группа ИТС-9.2. В 2016 г закончил КС54, в 2020 г. закончил МТУСИ
Работает в ООО «Лайтигард» на должности «Специалист по оценке соответствия требованиям безопасности информации».

“Советы наверное прозвучат достаточно банально, ...но:

- ✓ Нужно ставить себе цели и стремиться к их достижению, разобраться в своих желаниях и идеях, понять чего ты хочешь добиться и потом ставить правильную цель.
- ✓ *Чтобы строить карьеру, нужно, естественно, много общаться с людьми, предлагать руководителям свои идеи и рассказывать о своих желаниях, не боятся высказать своё мнение, проявлять себя, показывать свой профессионализм, постоянно обучаться и развиваться.*
- ✓ Постоянно нужно учиться. Очень важно, найдя свою нишу, не сидеть на одном месте без развития, а постоянно развиваться и получать новые знания. За последние пару лет я прошел не менее 10 различных курсов, как онлайн, так и очных.
- ✓ *На счет ВУЗа каждый должен решить сам для себя. Я, закончив колледж, для себя решил, что мне необходимо продолжить обучение и получить высшее образование. После колледжа некоторое время может показаться что ты уже и так все знаешь. Особенно это начнет подтверждаться в первые пару месяцев обучения в институте, но это только в начале 😊. Через какое-то время вы начнете получать новые полезные знания.*

Что могу сказать на счёт данного направления сейчас? Учиться и работать в направлении ИБ сейчас даже более актуально, чем тогда, когда я поступал в колледж. Но я бы наверное выбрал более техническую часть сейчас, а не организационную, хотя каждому своё.

Перспектив в ИБ достаточно, рост большой. Сейчас, в связи со сложившейся ситуацией в мире, многие ушли на удаленную работу и вопросы безопасности конфиденциальных данных и защиты каналов связи стоят очень остро. Компаниям нужны хорошие специалисты.”

ОПИСАНИЕ ПРОФЕССИИ

Техник по защите информации - специалист, который занимается администрированием и эксплуатацией систем защиты информации и DLP систем, мониторингом технического состояния оборудования и сетей, систем защиты информации компании, своевременной их проверкой, испытанием, техническим обслуживанием, обеспечением технически исправного состояния.

СФЕРА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ
— ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
— СВЯЗЬ

ТРЕБОВАНИЯ К ИНДИВИДУАЛЬНЫМ ОСОБЕННОСТЯМ СПЕЦИАЛИСТА

К профессионально важным качествам техника по защите информации относятся:

- хорошая память
- гибкость и динамичность мышления
- аналитические способности
- высокий уровень концентрации внимания
- способность грамотно выражать свои мысли
- математические способности

- профессионализм
- увлеченность (мотивация)
- желание учиться
- ответственность
- креативность
- высокий уровень развития технических способностей

ТЕХНИК ПО ЗАЩИТЕ ИНФОРМАЦИИ ДОЛЖЕН УМЕТЬ

- осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем
- использовать и оформлять техническую документацию в соответствии с действующими нормативными правовыми актами
- организовывать и конфигурировать компьютерные сети, работать с протоколами разных уровней

- устанавливать и настраивать параметры современных сетевых протоколов, проводить монтаж компьютерных сетей;
- осуществлять диагностику компьютерных сетей, устранять неисправности компьютерных сетей;
- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись.

ОПЫТ РАБОТЫ ???

Колледж = знания + умения

Где взять опыт опыт работы во время обучения ?

- ✓ Практика
- ✓ Олимпиады и конкурсы
- ✓ Исследовательская работа
- ✓ Студенческие конференции
- ✓ Стажировки
- ✓ Чемпионаты

КОНКУРСЫ

✨ВСЕРОССИЙСКАЯ ОЛИМПИАДА
"ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ»
http://профконкурс.рф/index/0-83

- Олимпиада НТИ **https://nti-contest.ru/profiles/infobez/**

Участникам профиля «Информационная безопасность» предстоит на время стать кибердетективами:

- искать уязвимости в веб-приложениях и бинарных файлах;
- разобраться, как работает операционная система и какие недостатки в себе содержит;
- изучить криптоалгоритмы и проанализировать, так ли безопасен интернет вещей;
- разработать новые инструменты и подходы к комплексному обеспечению безопасности.

КОНКУРСЫ

- Всероссийский кейс-чемпионат по информационной безопасности — **https://teachingame.ru/case**

- ✓ CTF – соревнования по информационной безопасности, целью которой является совершенствование навыков в области компьютерной безопасности. **https://kmb.cybber.ru/**
- ✓ **Hack the Box** -это онлайн-платформа, позволяющая вам проверить свои навыки тестирования на проникновение и обмениваться идеями и методологиями с тысячами людей в области безопасности.

СТАЖИРОВКИ

Преимущества стажировки для студентов

- Ценный опыт, новые знания
- Погружение в профессию
- Короткий рабочий день
- Полезные связи (Networking)
- Рекомендации от наставников
- Прокачать себя и получить опыт от коллег
- Возможность заработать

СТАЖИРОВКИ

- *попасть на стажировку в одну из ведущих компаний на рынке — необыкновенно важно!*
- *для некоторых стажировка плавно превращается в первую полноценную работу.*

- https://edu.infosec.ru/
- https://dsec.ru/about/traineeship/
- https://www.infowatch.ru/company/career/traineeship
- https://tssolution.ru/stazhirovka
- https://v.ok.ru/interns.html

СТАЖИРОВКИ

Лаборатория Касперского

kaspersky

Ты определенно нам подходишь, если ты:

- Студент (техническое направление) и заканчиваешь обучение не раньше 2021 года
- можешь работать 25-35 часов в неделю (желательно в промежутке 10:00-18:30)
- знаешь английский язык на уровне pre-intermediate и выше
- можешь документировать инструкции (Microsoft Word, Excel, Power Point)
- хочешь развиваться в сфере Информационной Безопасности
- готов активно коммуницировать с командой и другими отделами, следить за выполнением дедлайнов
- стрессоустойчив

На данной позиции предстоит:

- ***Участие в анализе требований информационной безопасности к ИТ-сервисам***
- ***Участие в обработке запросов ИБ, подготовке и анализе запрашиваемой информации***
- ***Обработка заявок по направлению***

СТАЖИРОВКИ

КОМАНДА ISO QIWI ХОРОШО ИЗВЕСТНА В ПРОФЕССИОНАЛЬНОМ СООБЩЕСТВЕ. ИМЕНИТЫЕ СПИКЕРЫ, УЧАСТНИКИ CTF И ОРГАНИЗАТОРЫ РАЗЛИЧНЫХ ХАКЕРСКИХ СОРЕВНОВАНИЙ.

Администратор информационной безопасности

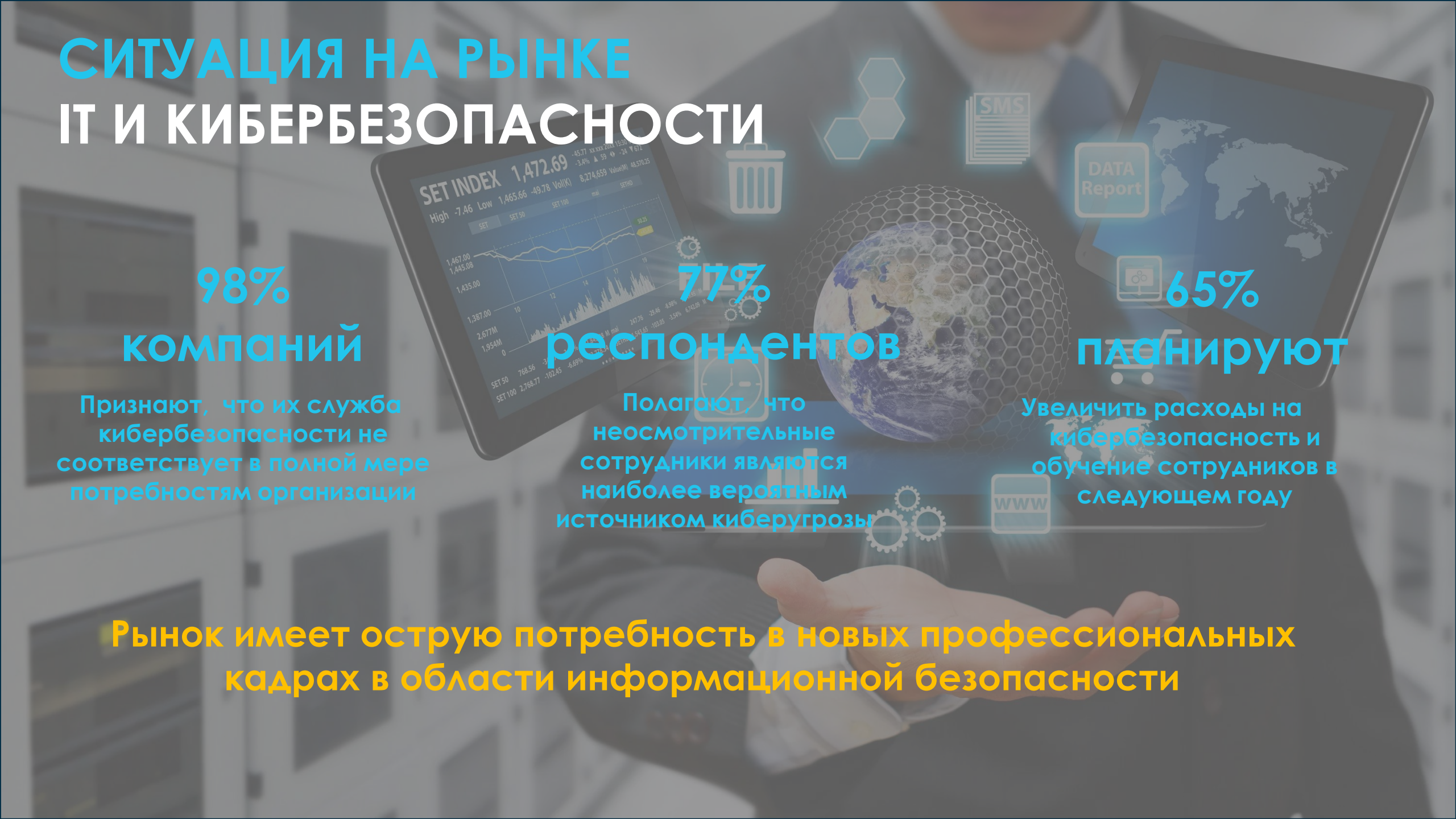
Чем ты будешь заниматься:

- Контролировать цикл жизни учетных записей сотрудников компании. Создавать УЗ в системах, насыщать правами, пересматривать полномочия и менять учетные данные.
- Обрабатывать запросы по предоставлению доступов в системы с разными ролевыми моделями, анализировать правомерности запрашиваемых полномочий и принимать итоговые решения по ним.
- Искать информацию о пользователях и их действиям в домене и базах на уровне приложения/операционной системы.
- Реагировать на сообщения систем SIEM, NGFW, ATP и разбирать инциденты безопасности.
- Настройкой банков-клиентов и криптопровайдеров, выпускать сертификаты.
- Консультировать сотрудников компании по вопросам ИБ.

ЧЕМПИОНАТЫ

- Всероссийский кейс-чемпионат по информационной безопасности от Russian Information Security Club
- Чемпионат AtomSkills
- Региональные чемпионаты WorldSkills

СИТУАЦИЯ НА РЫНКЕ IT И КИБЕРБЕЗОПАСНОСТИ



98%
компаний

Признают, что их служба кибербезопасности не соответствует в полной мере потребностям организации

77%
респондентов

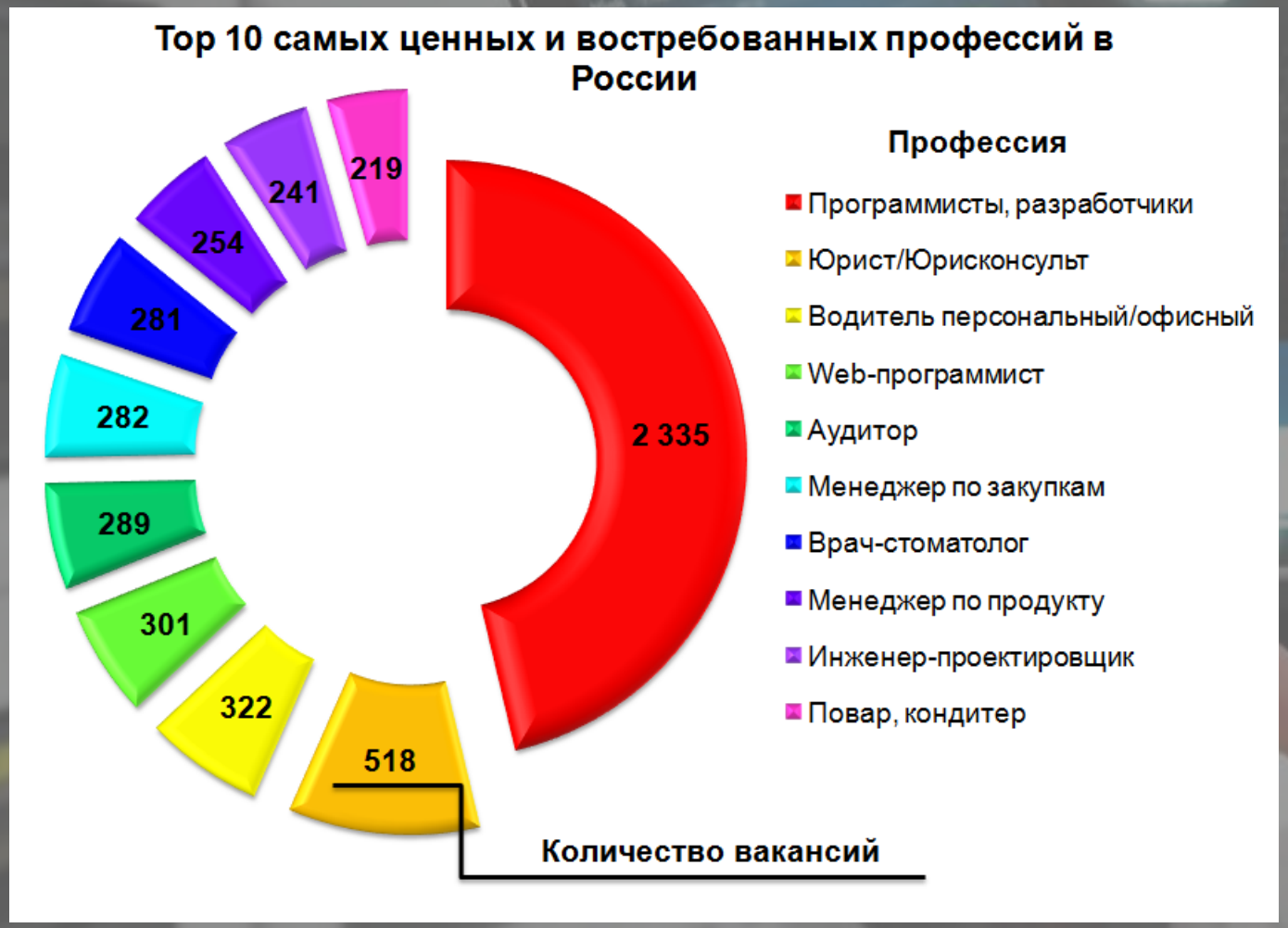
Полагают, что неосмотрительные сотрудники являются наиболее вероятным источником киберугрозы

65%
планируют

Увеличить расходы на кибербезопасность и обучение сотрудников в следующем году

Рынок имеет острую потребность в новых профессиональных кадрах в области информационной безопасности

СИТУАЦИЯ НА РЫНКЕ IT И КИБЕРБЕЗОПАСНОСТИ



Специалисты по информационной безопасности требуются во многих организациях, начиная с банков, больниц и любых учреждений, использующих компьютерные сети (а сейчас это почти любая организация), до фирм, специализирующихся на разработке программного обеспечения.


КРИПТОПРО
KASPERSKY lab
BI.ZONE
PT
GROUP IB
GLOBAL CYBER SECURITY COMPANY
КОД БЕЗОПАСНОСТИ
СБЕРБАНК ТЕХНОЛОГИИ
pwc
infotecs
ГРУППА КОМПАНИЙ МАСКОМ
КРОК
РОСАТОМ
Jet
КОМПАНИЯ АКТИВ
Эшелон
комплексная безопасность

СИТУАЦИЯ НА РЫНКЕ IT И КИБЕРБЕЗОПАСНОСТИ

Информационная безопасность – очень перспективная, но закрытая область

Находится на стадии роста. Особенно сейчас, в ситуации роста удаленной работы

Большинство компаний предпочитает вкладывать в обучение и развитие своих безопасников, в усиление своего контура безопасности

СТУПЕНЬКИ КАРЬЕРЫ И ПЕРСПЕКТИВЫ

- На выходе из учебного заведения будущий безопасник либо никому не нужен, либо воспринимается как отличный стажер для крупного бизнеса.

  Причина в том, что всё в работе зависит от конкретного окружения и конкретных угроз и обучиться можно только на практике именно в той компании, где предполагается дальнейший рост.

- **Чем раньше вы начнёте знакомиться с будущей компанией — тем лучше. Оптимально — проходить практику прямо в ней.**

Дальше, два варианта:

- *первый — вы медленно растёте в одной компании.*
- *Второй — набиваете кучу шишек на первом месте работы, и уже будучи опытным и настороженным, начинаете работать на больший оклад в другом месте.*

СТУПЕНЬКИ КАРЬЕРЫ И ПЕРСПЕКТИВЫ

Начать карьеру в данной сфере могут IT-специалисты со средним, неполным или законченным высшим образованием, опытом администрирования средств защиты информации и операционных систем Windows или Unix.

Требования работодателей к профессиональным навыкам и умениям начинающих специалистов достаточно серьезные: даже претенденты на сравнительно невысокий доход должны знать законодательство РФ по информационной безопасности, принципы работы сетей и средства криптозащиты, современные программные и аппаратные средства защиты информации, а также технологии обеспечения информационной безопасности.

Зарплата, на которую могут рассчитывать молодые специалисты в столице, от 40 т.руб.

СТУПЕНЬКИ КАРЬЕРЫ И ПЕРСПЕКТИВЫ

- Новичку в информационной безопасности стоит начать с самостоятельного изучения OpenSourse-инструментария, прежде, чем переходить к платным инструментам.
- Широкий спектр программных продуктов, которые нужны в ежедневной работе, есть в Kali Linux, Parrot OS. Нужно освоить Wireshark, SqlMap, Nmap, John the Ripper и многие другие вещи.

- Каждый день нужно выделять время на образование: это единственный шанс оставаться в целом подготовленным к тому, что происходит с технологиями.
- Нужно постоянно читать конкретику по известным ситуациям взломов, осваивать новые системы.
- Хороший источник информации – специализированные сайты и форумы (Habr)

КУДА ПОЙТИ ВЫПУСКНИКУ

Огромное множество крупных и небольших компаний, на рынке, в области организации защиты информационных технологий, нуждаются в молодых специалистах, а именно выпускниках ВУЗов и СУЗов, в области информационной безопасности.

kaspersky

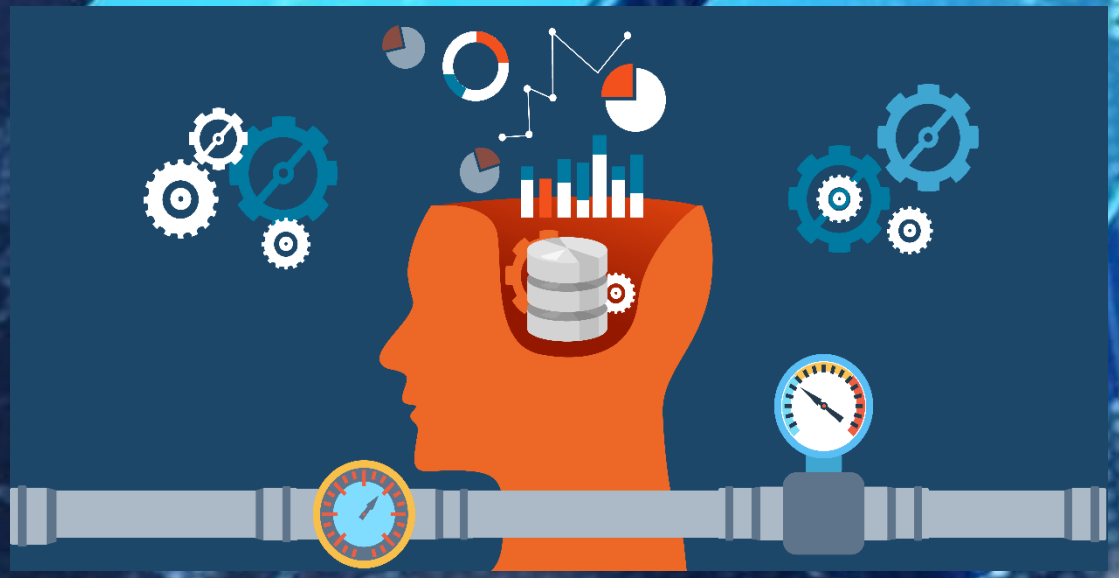
Ростелеком

ГРИНАТОМ

ЭНЕРГИЯ ЭФФЕКТИВНЫХ РЕШЕНИЙ

ВОСТРЕБОВАННОСТЬ НА РЫНКЕ ТРУДА

Вопреки мнению многих выпускников о том, что без высшего образования, Вас не возьмут на работу по специальности , мы покажем вам результаты мониторинга рынка труда, согласно тем навыкам, которые Вам дали в колледже по направлению- Информационная безопасность



Мы рассмотрим:

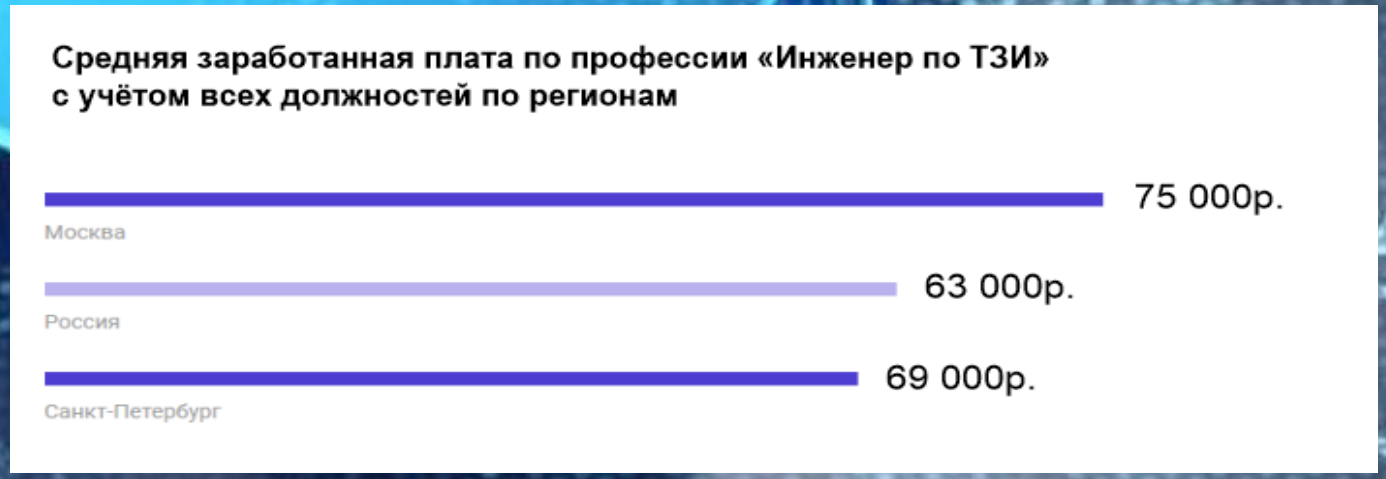
- ***требования работодателей***
- ***необходимые навыки для трудоустройства***
- ***условия работы***
- ***уровень заработной платы***

ТЕХНИК ПО ЗАЩИТЕ ИНФОРМАЦИИ

- Техник по защите информации — специалист, занимающийся проверкой технического состояния, установкой, наладкой и регулировкой аппаратуры и приборов телекоммуникационных систем, их профилактическим осмотром и текущим ремонтом.

ИНЖЕНЕР ПО ТЗИ

- Настраивает многоуровневую систему защиты информации (логины и пароли, идентификацию по номерам телефона, по отпечатку пальца, по сетчатке глаза и др.)
- Исследует составные части системы (сайта, сервиса, автоматизированной системы в компании) на наличие уязвимостей
- Устраняет выявленные поломки и уязвимости
- Устраняет последствия взломов, если они произошли
- Разрабатывает и внедряет новые регламенты по обеспечению защиты информации
- Проводит работу с пользователями системы, чтобы объяснить важность и виды защитных мер
- Ведет документацию
- Готовит отчеты по состоянию IT-систем
- Взаимодействует с партнерами и поставщиками оборудования в сфере обеспечения безопасности



ВАКАНСИЯ - СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - СТАЖЕР

- Участие в проектах в роли специалиста по информационной безопасности;
- Возможность приобрести практический опыт в IT компании и принять участие в реальных проектах;
- Возможности карьерного и профессионального развития.

Обязанности

- Изучение и настройка средств защиты информации от ведущих зарубежных и российских производителей (Palo Alto, Check Point, Континент, Cisco и многих других);
- Разработка мер повышения информационной безопасности.

Требования

- Базовые знания об информационных технологиях (в областях администрирования, защиты периметра, сетевой инфраструктуры);
- Понимание принципов работы AD, DNS, DHCP, Vlan, VPN, PKI, FW, TCP/IP(OSI);
- Понимание принципа построения сетей передачи данных;
- Навыки сбора и анализа большого объема информации.

МЛАДШИЙ АНАЛИТИК / СПЕЦИАЛИСТ ОТДЕЛА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Опыт работы с ОС Windows, *nix;**
- **Знание английского языка (чтение технической литературы, написание деловых писем разговорный английский будет плюсом);**
- **Грамотная устная и письменная речь;**
- **Внимательность, способность быстро переключаться между задачами;**
- **Понимание работы базовых интернет-технологий и принципов работы вредоносного ПО.**

СПЕЦИАЛИСТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИИ

- Участие в экспертизе проектов локальных нормативных актов, организационно-распорядительных документов, регламентирующих вопросы защиты информации
- Подготовка проектной документации на информационные и автоматизированные системы
- Мониторинг изменений, вносимых регуляторами области информационной безопасности
- Участие в проведении проверок по выполнению требований информационной безопасности в соответствии с планом проверок
- Участие в испытаниях на соответствие требованиям безопасности информации создаваемых объектов информатизации

Пожелания к кандидату:

Наличие компетенций в составлении и согласовании организационно-распорядительных документов и проектной документации;

Навыки деловой переписки

Личностно-деловые качества (компетенции):

- Системное/стратегическое мышление;
- Ориентация на результат;
- Планирование и организация деятельности;
- Работа в команде;
- Эффективная коммуникация;

Опыт участия в проектах по направлениям информационных технологий и/или информационной безопасности

Предложение :

Требуемый опыт работы: не требуется

Официальное трудоустройство в соответствии с ТК РФ стандартный 8-часовой рабочий день, график работы 5/2, сб и вс – вых.

ДМС (со стоматологией), полный соцпакет, оплата больничных листов;

ЗП от 52 000 рублей

ИНЖЕНЕР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗП от 60 000 рублей

- Разработка проектной и исполнительной документации по ГОСТ 34;
- Внедрение и эксплуатация комплексных систем ИБ;
- Поиск и устранение неисправностей, связанных с работой оборудования и ПО информационной безопасности (преимущественно решения Инфотекс, Kaspersky, Код безопасности, Safe Phone, Positive Technologies);
- Ведение переговоров с технической поддержкой вендора;
- Стендирование решений по информационной безопасности

- Понимание основ построения локальных сетей (на уровне CCNA);
- Самообучаемость, целеустремленность, нацеленность на результат;
- Умение излагать мысли на бумаге;
- Английский язык - на уровне чтения профессиональной литературы и технической документации
- Приветствуются Сертификаты Cisco: CCNA/CCNA Security;
- Приветствуются Сертификаты Инфотекс.

Предложения:

- Работа в динамично развивающейся компании.
- Высокий уровень заработной платы, который оговаривается с каждым соискателем индивидуально.
- Оформление по ТК РФ с первого рабочего дня, ДМС.
- Возможность применения своих знаний и способностей для решения интересных и сложных задач.
- Обучение за счет компании.
- Реальные возможности профессионального и карьерного роста!

ИНЖЕНЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ

Требуемый опыт работы: **не требуется**
Официальное трудоустройство с первых дней работы;
- Обучение за счет компании 5 дней;
- Командировки полностью оплачиваются Компанией;
- Заработная плата: оклад + ежемесячные премии;
- Испытательный срок до 3х месяцев;

Пожелания к кандидату:
Наличие оконченного высшего / средне-профессионального образования в сфере защиты информации;
- Знание Российского законодательства в области защиты информации;
- Знание принципов и механизмов защиты информации;
- Быстрая обучаемость;
- Коммуникабельность;
- Грамотная техническая речь;
- Готовность к командировкам;

- Наличие базовых навыков администрирования ОС Windows Server
- Наличие базовых навыков администрирования сетей на основе TCP/IP
- Наличие базовых навыков программирования
- Наличие базовых навыков в сфере защиты информации

Чем Вам предстоит заниматься:
- Установка и настройка средств защиты информации;
- Разработка организационно-распорядительной документации по вопросам информационной безопасности;
- Разработка, оформление документов, таблиц

Мы рассмотрели вакансии для студентов-выпускников не имеющих опыта работы и высшего образования.

Далее мы рассмотрим перспективы и возможности при условии саморазвития, повышения квалификации и карьерного роста

КАК ПОВЫСИТЬ СВОЮ ЦЕННОСТЬ НА РЫНКЕ ТРУДА

В первую очередь все работодатели смотрят на профессионализм соискателей, их техническую грамотность, знания и опыт работы в конкретной сфере.

Отсюда следует, что в среднем для продвижения по карьерной лестнице требуется опыт работы от 1 до 3 лет, большим плюсом будет опыт работы от 3 до 6 лет.

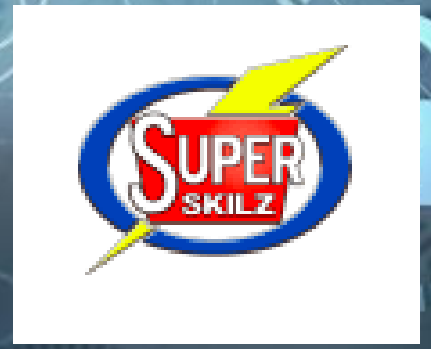
С таким опытом работы вы уже можете претендовать на вакансию руководителя проектов по информационной безопасности. Заработная плата по таким вакансиям составляет около 110 000-130 000 рублей.

ОПРЕДЕЛЕНИЕ СФЕРЫ РАЗВИТИЯ

В начале карьеры, получив определенный опыт, Вы будете понимать, какие пробелы возникают в процессе освоения профессии.

После того как появился опыт работы и какое либо мнение, нужно определиться в какой конкретно сфере вы хотите трудиться.

Требования работодателей в различных сферах информационной безопасности часто разнятся, в зависимости от их специфики



С ЧЕГО НАЧАТЬ КАРЬЕРНЫЙ РОСТ ?

Начать с себя

Определившись, в какой сфере вы хотите трудиться, нужно проделать работу по сбору первичной информации. Хотите работать в банке – изучите открытые вакансии на порталах рекрутинговых агентств. Проанализируйте, какие навыки «мелькают» чаще, какие сертификаты востребованы и т.д.

Нет знакомых из нужной сферы – идите на тематические ресурсы, форумы, группы в соцсетях.

Выпускникам колледжей для продвижения по карьерной лестнице необходимо высшее техническое образование в области «Информационной безопасности».

BANKIR.RU

RISC
Russian Information Security Club

INFORMATION SECURITY
SearchInform

ЧТО НУЖНО ЗНАТЬ БЕЗОПАСНИКУ, ПРЕДОТВРАЩАЮЩЕМУ УТЕЧКИ ИНФОРМАЦИИ ?

Первое, с чем придётся столкнуться на этой должности – нормативка.

ГОСТы, отраслевые стандарты, федеральные законы, приказы ведомств и т.д.

Обрабатываете персональные данные? – должны «знать и уметь» ФЗ-152.

Связаны с государственными информационными системами? – не забывайте о приказах ФСТЭК №17 и №21.

Чтобы быть востребованным специалистом и повышать свою квалификацию нужно постоянно изучать нормативную документацию, различные поправки, свежевышедшие приказы и нормы.

НАВЫКИ

- В идеале нужно быть немного юристом (а им придётся стать, выполняя разнарядку по нормативной документации), немного психологом (работа с людьми в стиле следователя МВД) и много аналитиком, ведь основная деятельность связана с выявлением, предотвращением и расследованием утечек.

- Это минимальный набор который поможет вам в развитии карьеры. В дальнейшем он будет пополняться специфическими знаниями и опытом, характерными для конкретной компании.

НАВЫКИ

Сейчас нужно быть «профессиональнее» всех, чтобы успеть за изменениями технологий

https://www.specialist.ru/section/information-security
https://itsecurity.ru/services/
https://www.infowatch.ru/services/education/dlp
https://infotecs.ru/services/obuchenie-i-sertifikatsiya.php
https://habr.com/ru/
https://www.academyit.ru/courses/fields/itsecurity/

ПОМОЖЕТ ДОБИВАТЬСЯ ПЕРСПЕКТИВ И КАРЬЕРНОГО РОСТА:

- Умение работать в команде, грамотно распределять обязанности между участниками.
- Высокие коммуникационные навыки.
- Опыт работы с технологией «Межсетевых экранов».
- Знания в области антивирусной защиты.
- Навыки выявления возможных каналов утечки информации.
- Работа в крупных проектах.
- Стрессоустойчивость. Опыт работы в условиях «дедлайна».
- Самостоятельность. Полное понимание своей части работы.
- Высокая производительность.

— Знание английского языка на уровне чтения технической литературы и научных статей, предпочтение отдается кандидатам со свободным разговорным языком;

Специалист по информационной безопасности широкого профиля.

Здесь речь о профессионалах, которые могут быть экспертами в 2-3 направлениях информационной безопасности и хорошо разбираться еще в 4-5 смежных направлений.

Такие профессионалы могут погружаться в экспертизу и выступать в качестве консультантов или архитекторов сложных высоконагруженных проектов.

Специалист по безопасной разработке приложений.

- Ищет потенциальные уязвимости используя готовые инструменты или тулзы собственной разработки.
- Он способен разобраться в коде проектов, написанных на разных языках программирования, определить типовые ошибки кода и указать разработчикам на их наличие.
- Использует различные инструменты, использует статический и динамический анализ кода, знает разные инструменты и способен выступать в качестве эксперта для команды разработки.
- Может указать разработчикам на потенциально уязвимые части кода, которые необходимо переписать.

Пентестер (penetration tester)

- По сути, белый хакер. Его задача — исследование безопасности веб-сайтов, мобильных приложений, программных платформ и т.п.
- В отличие от злоумышленников, которых за их деятельность ждет наказание, пентестеры за обнаружение уязвимости получают бонусы. Среди пентестеров есть и фрилансеры — это, зачастую, охотники за Bug Bounty, вознаграждением, предлагаемым какой-либо компанией за обнаружение уязвимости в ее сервисе или приложении.

РУКОВОДИТЕЛЬ ПРОЕКТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗП от 110 000 до 130 000 рублей
Опыт работы: 1-3 года

Обязанности: Руководство проектами в сфере информационной безопасности;
Проведение предпроектного обследования автоматизированной системы;
Создание модели угроз и нарушителя в АС;
Анализ уязвимостей АС, организация сетевого поиска уязвимостей («сетевого сканирования»);
Составление частного технического задания на СЗИ;
Подготовка документации технического проекта;
Участие в подготовке рабочей документации на СЗИ;
Организация и проведение аттестации рабочих мест в соответствии с приказом ФСТЭК России от 11.02.2013г. №17;
Ввод в эксплуатацию и сопровождение СЗИ;

Требования:

- Высшее техническое образование (информационные технологии/информационная безопасность).
- Ответственность, пунктуальность, внимательность, последовательность в действиях.
- Высокая производительность.
- Высокие коммуникационные навыки.
- Знание предметной области по направлениям: межсетевые экраны, НСД, недекларированные возможности, антивирусная защита;
- Знание и умение применять на практике методы и инструменты управления проектами.
- Широкий кругозор в ИБ. Понимание состава и специфики работ по информационной безопасности, аттестации объектов информатизации, обеспечения безопасности информационных систем, систем персональных данных и критической информационной инфраструктуры, сертификации продуктов по линии ФСТЭК России;
- Знание ГОСТ 34 серии;

АДМИНИСТРАТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗП 120 000-140 000 рублей.

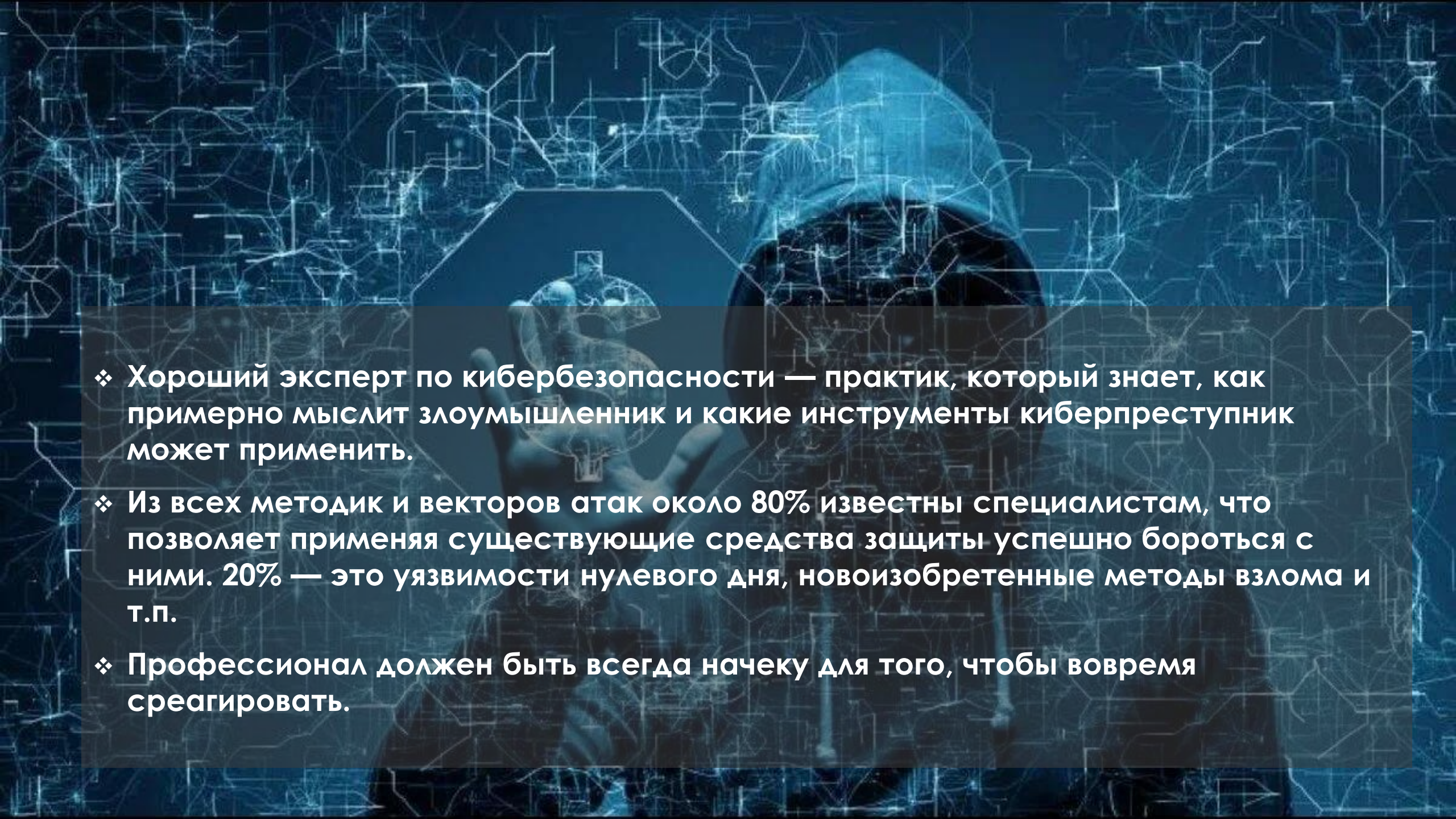
Опыт работы: 1-3 года

Задачи:

- Планирование политики, систем и мероприятий информационной безопасности предприятия
- Администрирование и эксплуатация систем защиты информации и DLP систем.
- Выявление, реагирование и участие в расследовании инцидентов информационной безопасности
- Проведение регулярного анализа состояния информационных систем
- Подготовка технических заданий, участие в заключении и сопровождении договоров на выполнение работ по внедрению и сопровождению средств защиты информации
- Участие в формировании бизнес-планов по направлению «информационная безопасность»
- Разработка регламентов и локальных нормативных документов по организации и обеспечению информационной безопасности
- Реализация организационных и технических мероприятий по комплексной защите информации
- Мониторинг технического состояния оборудования и сетей систем защиты информации компании, своевременная их проверка, испытание, техническое обслуживание, обеспечение технически исправного состояния

Требования:

- Высшее (плюсом будет образование в области информационной безопасности, также рассматриваются кандидаты с образованием в области информационные технологии)
- Знание нормативной базы в части защиты информации: законов и иных нормативных правовых актов РФ, регулирующих отношения, связанных с защитой информации, руководящих документов ФСТЭК, ФСБ, Роскомнадзора, 152-ФЗ, 398-ФЗ
- Знание принципов построения средств защиты информации от "утечки" по техническим каналам
- Знание принципов работы средств обеспечения безопасности (антивирусы, WAF, системы обнаружения вторжений и т.д.)
- Опыт выявления угроз информационной безопасности на основе сведений об уязвимостях (классификация угроз, формирование рекомендаций по устранению уязвимостей и минимизации рисков)
- Опыт проведения анализа защищенности web-проектов
- Опыт участия в проектах по проектированию и внедрению систем информационной безопасности
- Опыт расследования инцидентов безопасности, сбор доказательной базы
- Опыт настройки параметров безопасности системных компонентов на уровне сети, ОС, прикладного ПО. Опыт работы с профильным ПО (UTM/NGFW, DLP, SIEM, IDM, WAF, VPN, IDS/IPS, PKI, СЗИ от НСД, СКЗИ, и т.п.), СКУД и системами видеонаблюдения
- Опыт разработки технической и аналитической документации.
- Знания в области сетевой архитектуры, понимание принципов построения и функционирования сетей; знание сетевых протоколов, стека TCP/IP, модели ISO/OSI
- Windows и Linux на уровне администратора
- Хорошее знание и опыт администрирования Active Directory и GPO, Terminal



- Хороший эксперт по кибербезопасности — практик, который знает, как примерно мыслит злоумышленник и какие инструменты киберпреступник может применить.
- Из всех методик и векторов атак около 80% известны специалистам, что позволяет применяя существующие средства защиты успешно бороться с ними. 20% — это уязвимости нулевого дня, новоизобретенные методы взлома и т.п.
- Профессионал должен быть всегда начеку для того, чтобы вовремя среагировать.

Напоследок

Разумеется, выше описан некий собирательный образ построения карьеры в области «Информационной безопасности», который может радикально отличаться от того, что есть в какой-либо компании.

У каждого свои потребности и свои исторически сложившиеся принципы, поэтому подход к безопасности может быть очень разным.

МЫ, КОМАНДА ОТДЕЛА СОДЕЙСТВИЯ ТРУДОУСТРОЙСТВУ, ПОМОЖЕМ ТЕБЕ!

Обращайся : г. Москва, ул. Б.Каменщики, д.7, каб. 507 , телефон: 8-495-134-12-34 (доб. 1326), e-mail: ks54ot@mail.ru

ТАК ЖЕ ДЛЯ ТЕБЯ МОЖЕТ ОКАЗАТЬСЯ ПОЛЕЗНА ИНФОРМАЦИЯ В ГРУППЕ ВК

https://vk.com/club77163460

Тут ты можешь найти:
-Карьерные мероприятия
-Горящие вакансии
-Интересные статьи и рекомендации

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ
Центральный административный округ

Государственное бюджетное профессиональное образовательное учреждение города Москвы "Колледж связи № 54" имени П.М. Вострухина

РЕЗУЛЬТАТЫ РАБОТЫ РЕСУРСА «ОБРАЩЕНИЯ ГРАЖДАН К РУКОВОДИТЕЛЮ ДЕПАРТАМЕНТА ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ»

Есть вопросы по дистанционному образованию в Вашей школе?
ЗАДАЙТЕ ИХ ЗДЕСЬ

ГЛАВНАЯ
НОВОСТИ
СВЕДЕНИЯ ОБ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ
ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ
ГАЛЕРЕИ
ДИСТАНЦИОННОЕ ОБУЧЕНИЕ
ДИСТАНЦИОННОЕ ВОСПИТАНИЕ

Главная / Вакансии

Вакансии

Рекомендации по поиску работы

1. Пробуйте искать работу разными способами. Определите на практике наиболее эффективные для Вас способы с учетом Вашей профессии и квалификации.
2. Используйте одновременно несколько способов поиска работы.
3. Применяйте активные варианты поиска в сочетании с пассивными (например, поиск вакансий в сети «Интернет» и размещение резюме на сайтах).
4. Занимайтесь поиском работы каждый день.
5. Продолжайте поиск, пока не получите конкретного предложения о работе.

Подготовьтесь к мероприятию заранее: обновите резюме на hh.ru или в формате word/pdf, поймите, в какое время вам будет удобно откликаться на вакансии, решите, на какой вебинар вы хотите пойти. Будьте максимально активны — все работодатели, которые будут в эти дни на «Ярмарке…», готовы к диалогу! До встречи!

Ссылки на сайты, посвященные поиску работы. Заходите, читайте, оставляйте резюме!

www.jobrapido.ru

www.e-Graduate.ru