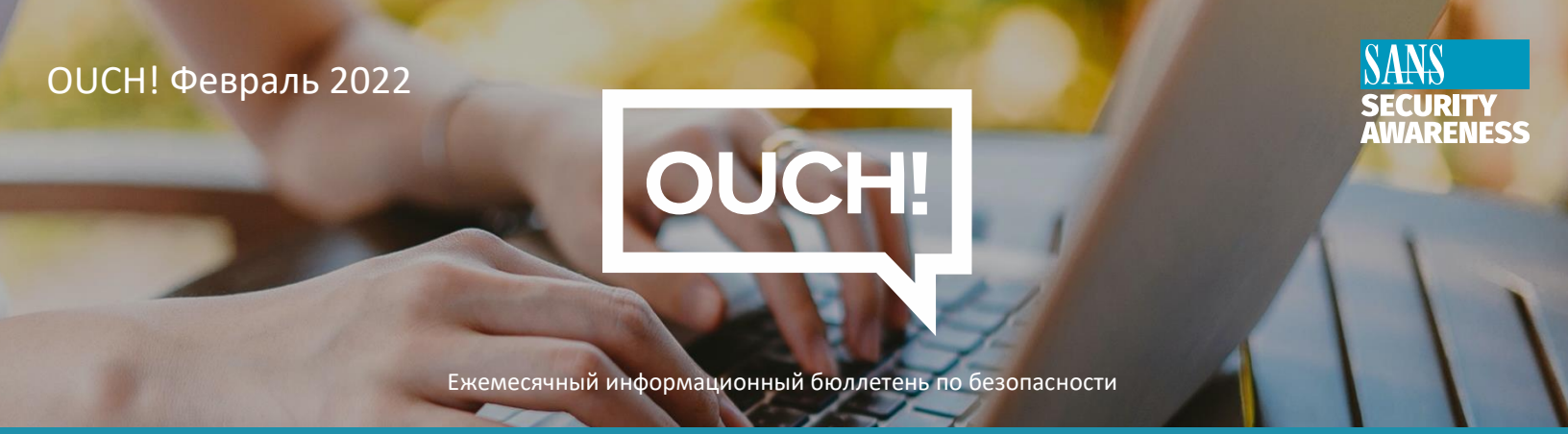

Ежемесячный информационный бюллетень по безопасности

Начать карьеру в сфере кибербезопасности может каждый

Обзор

Мы читаем о кибербезопасности в новостях почти каждый день, поскольку организации и правительства по всему миру продолжают подвергаться атакам программ-вымогателей, мошенничества и кибератак. Существует огромный спрос на людей, обученных кибербезопасности, для защиты от этих растущих угроз. На самом деле, по оценкам недавних исследований, во всем мире существует почти 3 миллиона вакансий в области кибербезопасности.

Вы рассматривали бы карьеру как профессионал в области кибербезопасности? Это быстро развивающаяся, высокодинамичная область с огромным количеством интересных специальностей на выбор. Эти должности включают в себя такие области, как судебная экспертиза, осведомленность и обучение, безопасность конечных точек, критическая инфраструктура, реагирование на инциденты, безопасное кодирование и политика. Кроме того, карьера в области кибербезопасности позволяет вам работать практически в любой точке мира с удивительными преимуществами и возможностью добиться реальных результатов.

Нужно ли вам образование в области компьютерных наук?

Абсолютно нет! Многие из лучших специалистов по безопасности не имеют технического образования. Ключом является страсть к обучению; как только вы поймете, как технологии работают (и ломаются), вы сможете лучше защитить их. Что интересного в кибербезопасности, так это то, что вы можете изучать, как технологии работают когда вам это удобно, не выходя из собственного дома.

С чего начать?

Начните изучать различные области, чтобы узнать свои интересы. Часто вы можете начать только с компьютеров или устройств, которые есть у вас дома.

- **Кодирование**: изучите основы программирования. Python, HTML или JavaScript — все это хорошие программы для начала. Подумайте о сайте онлайн-обучения или возьмите любую книгу для начинающих по программированию.
- **Системы**: изучите основы администрирования операционной системы, такой как Linux или Windows. Если вы действительно хотите стать лучше, накапливайте опыт с помощью интерфейса командной строки и сценариев.
- **Приложения**: узнайте, как настраивать, запускать и поддерживать приложения, такие как веб-сервер или DNS-сервер.

- **Сеть**: узнайте, как компьютеры и устройства взаимодействуют друг с другом, перехватывая и анализируя сетевой трафик. Это может быть очень весело, так как ваш дом, скорее всего, уже является сетевым окружением со всеми видами устройств, подключенных к нему.
- **Облачные технологии**: Узнайте, как работают облачные сервисы и как их можно использовать.

Устройте дома свою лабораторию. Вы можете создать несколько виртуальных операционных систем на одном физическом компьютере или настроить лабораторию, используя облачные ресурсы, такие как Amazon AWS или Microsoft Azure. Если вы хотите работать напрямую с оборудованием, купите простые и дешевые компьютеры, такие как Raspberry Pi или Arduino. Как только вы настроите и запустите свои системы, начните с ними взаимодействовать и узнайте все, что можно, об их настройке и оптимизации или начните программировать и создавать код в этих системах. Нет правильного или неправильного способа начать, просто следуйте за своими интересами.

Другим вариантом является встреча и работа с другими людьми в сфере кибербезопасности. Подумайте о том, чтобы посетить местную конференцию по кибербезопасности или виртуальную конференцию, такую как Bsides или SANS New2Cyber. Самое сложное - найти такое мероприятие или встречу. После того, как вы примете участие, свяжитесь с другими участниками и расширьте свою профессиональную сеть.

Другие варианты обучения включают видео YouTube, онлайн-форумы, подписку на блоги от специалистов по безопасности или участие в онлайн-мероприятиях Capture the Flag (CTF). В конце концов, не позволяйте вашему образованию или прошлому вам препятствовать. Страсть к обучению и помощи другим, а также способность «мыслить нестандартно» являются ключевыми качествами. После того, как вы начнете развитие ваших навыков, и вы начинете общаться с другими в этой области у вас появятся новые возможности.

Приглашенный редактор

Лодрина Черне (@hexplates) является главным защитником безопасности в Cybereason, продвигая инновации и разрабатывая передовой опыт, связанный со стандартами и политикой кибербезопасности. Она также является сертифицированным инструктором в Институте SANS, где помогает специалистам по информационной безопасности углублять их фундаментальное понимание цифровой криминалистики и реагирования на инциденты (DFIR).

Ресурсы

Конференции по безопасности : http://www.securitybsides.com/
Женщины в кибербезопасности: https://www.wicys.org/
Плейлист New2Cyber на YouTube : https://youtube.com/playlist?list=PLtgaAEEmVe6BQkZiJC5nIk9xx74QTGtsZ
Киберакадемии SANS : https://www.sans.org/scholarship-academies/
Кибер-асы SANS : https://www.cyberaces.org
Подкасты о кибербезопасности : https://www.sans.org/blog/cybersecurity-podcast-roundup/

Роман Полаков