Статья про ИКиЗИ на сайте Министерства науки и высшего образования

В рамках Года науки и технологий руководитель и сотрудники Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого (СПбПУ) рассказали о том, что такое кибербезопасность, почему цифровую гигиену должен соблюдать каждый, а также — о востребованности специалистов в этой области.

Ваши гаджеты интересны хакерам

Раньше защита информации на компьютерах была актуальна только для таких областей, как, например, оборонная промышленность, деятельность банков, так как это могло быть связано с государственной информацией. Сейчас все изменилось — считает директор Института кибербезопасности и защиты информации СПбПУ, доктор технических наук Дмитрий Зегжда.

«Теперь надо заниматься защитой «умных» автомобилей, кофеварок, и так далее. Хотя у большинства этих устройств нет интересной секретной информации, но зато есть программное обеспечение. А там, где есть программное обеспечение, есть управление, там идет борьба за то, кто будет управлять этим программным обеспечением, а значит сможет сделать с его помощью что угодно», — предупреждает Дмитрий Зегжда.

По мнению его коллеги, доцента Института кибербезопасности и защиты информации Дмитрия Москвина, одним из основных заблуждений пользователей персональных компьютеров, смартфонов и прочих гаджетов является то, что их устройства будто бы не интересны хакерам.

«Кибербезопасность — дело каждого. Например, известны атаки на государственные службы, которые проводятся с так называемых бот-сетей. А кто такие бот-сети? Это сети, состоящие из зараженных вредоносным ПО компьютеров и гаджетов обычных граждан. Чем их больше, тем нарушителю лучше: он не подставляет себя, а подставляет обычных пользователей, к которым потом в случае чего и придут правоохранительные органы», — объясняет ученый.

Цифровая гигиена

Таким образом, пользователь персонального компьютера может стать не только жертвой мошенничества, но и его источником. Вредоносные действия могут совершать с устройства добропорядочного гражданина, который даже не будет подозревать об этом. Для того, чтобы избежать таких ситуаций, очень важно соблюдать цифровую гигиену.

«Главный совет — не думать, что в интернете могут быть какие-то секреты. Относитесь ко всему, что вы передаете через интернет, публикуете в нем, храните в облаке, как к тому, что уже находится в общем доступе. Один мой коллега очень хорошо сказал: все, что вы указали в сети, будет храниться вечно и может быть использовано против вас», — предупреждает Дмитрий Москвин.

По его словам, очень важно соблюдать правила безопасности: использовать разные пароли на разных сервисах, периодически менять эти пароли, причем лучше применять двухфакторную идентификацию. Нельзя ничего запускать с сомнительных сайтов и скачивать файлы, присланные по почте от незнакомых отправителей. И нужно пользоваться только лицензионным программным обеспечением.

О том, как не стать жертвой финансовых мошенничеств в интернете рассказывает доцент Института кибербезопасности и защиты информации СПбПУ Артем Коноплев.

«Например, лучше не держать на карте денег до той поры, пока нам не надо совершить по ней какую-то операцию, покупку онлайн. Если на карте ноль, даже если наши данные утекли к мошенникам, деньги у нас украсть не могут. Второй вариант — сегодня все банковские приложения позволяют хоть по 100 раз в день блокировать карту и выпускать новую. А еще можно завести отдельную банковскую карту для онлайн-транзакций. Не светите карту, на которую вы получаете зарплату, не надо расплачиваться ей, вводить данные и тому подобное», — говорит он.

Но самое главное, по мнению доцента СПбПУ, не торопиться и перепроверять информацию.

«Мы часто слышим истории, когда звонят бабушке и говорят, что ее внук попал в беду, она начинает переживать и тут же переводит деньги. Не надо торопиться, нужно взять и позвонить внуку, дочке, еще куда-то и проверить информацию. Не надо сразу доверять и полагаться на первоисточник, найдите способ проверить информацию», — добавляет Артем Коноплев.

Востребованная специальность

Как отмечает Дмитрий Зегжда, специалисты в области кибербезопасности очень востребованы.

«У нас в вузе каждый год растут цифры приема и выпуска таких специалистов, — рассказывает он. — В этом году в Политех мы приняли 160 человек для обучения по этой специальности, в следующем году увеличим прием и к нам поступит еще больше ребят, но все равно специалистов пока не хватает. Уже начиная со второго-третьего курса наших студентов начинают звать на работу, все находят работу по специальности — это важный показатель».

Работа в этой области становится все более интересной: пока IT-специалисты придумывают новые способы защиты, злоумышленники придумывают новые способы атак. Отсюда востребованность специалистов становится все более высокой не только в России, но и во всем мире.

«Раньше кибербезопасность была неким вторичным фактором, а сейчас из-за того, что цифровизация проникает всюду, потребители говорят: вы, прежде чем внедрять вот это свое новое цифровое решение, пожалуйста, обеспечьте нам безопасность», — объясняет Дмитрий Зегжда.

Оригинал статьи на сайте МинОбрНауки: https://minobrnauki.gov.ru/press-center/news/?ELEMENT_ID=34670