#НастоящиеВеликие: как защититься от киберугроз

Знаете, какую проблему надо решить, чтобы оказаться в фантастическом цифровом мире с беспилотным транспортом и вездесущим искусственным интеллектом? Проблему кибербезопасности. Современные технологии уже позволяют претворить самые смелые замыслы ученых в жизнь, но для их реализации нужно обеспечить самое главное – безопасность наших личных данных. Как сохранить их в целости и сохранности, знает новый герой спецпроекта #НастоящиеВеликие.

Дмитрий Петрович ЗЕГЖДА, профессор РАН, директор Высшей школы кибербезопасности и защиты информации, директор научно-образовательного центра «LG-Политехник», стоял у истоков развития кибербезопасности не только в Политехе, но и во всей России. Возглавляемая им высшая школа, а раньше кафедра «Информационная безопасность компьютерных систем», стала первой в России кафедрой в гражданском вузе, на которой начали готовить специалистов по информационной безопасности.

Мы встретились с Дмитрием Петровичем и узнали, как развивалась

кибербезопасность, чем специалист по кибербезопасности отличается от программиста, в каком проекте «Сбербанка» участвовала научная группа Дмитрия Петровича, и поговорили о многом другом – даже о социальной миссии киберзащитников. А в конце интервью вы найдете правила безопасности в Сети от нашего эксперта.

- Дмитрий Петрович, сейчас все компании, да и целые государства, стремятся к тотальной цифровизации. И этот процесс, конечно, обостряет вопрос защиты информации.

- Совершенно верно. Цифровизация предполагает повсеместное внедрение компьютерных технологий и «умных» устройств. И первое, о чем задумываются пользователи или потребители цифровых технологий, это об угрозах информационной безопасности. Если раньше говорили о защите информации как о конфиденциальности, целостности и доступности данных, то теперь, когда сеть Интернет объединила в единое киберпространство не только компьютеры пользователей и центры обработки данных, но и «умные» дома и города, цифровое производство, автомобили и беспилотники, на первый план выходит угроза захвата управления киберфизическими системами и устройствами.

Человечество намерено доверить искусственному интеллекту самое дорогое – здоровье, репутацию, финансы… Существуют злоумышленники, которые

хотят воспользоваться этими технологиями для реализации своих недобрых намерений. Проблема кибербезопасности – это барьер, который человечеству нужно преодолеть, чтобы компьютеризация дальше развивалась и проникала в новые области. Поэтому весь мир ищет решение этой проблемы, но технологии развиваются так быстро, и сама проблема кибербезопасности настолько сложна, что пока до ее решения еще очень далеко. Россия на сегодняшний день многого достигла в этой сфере, наши специалисты и решения в этой области занимают лидирующие позиции.

- И надо отметить, что Политех первым из гражданских вузов стал готовить специалистов по информационной безопасности. Как тогда, больше 20 лет назад, удалось понять, что эта сфера будет суперактуальной и востребованной?

- Это была эпоха персональных компьютеров, а самой распространенной угрозой для них, впрочем, как и сейчас, были компьютерные вирусы – тогда они представлялись как искусственная жизнь. Уникальная особенность нашей кафедры состоит в том, что она выросла из Специализированного центра защиты информации, в котором велись работы по этой тематике. Кафедру «Информационная безопасность компьютерных систем» создал мой отец – Петр Дмитриевич Зегжда. В 1993 году к нему обратились специалисты из Министерства обороны, для которого в те годы защита информации была малоизученной, но при этом крайне актуальной задачей. Начав научную работу в этой области, мы поняли, что это очень важное и перспективное направление. К решению таких задач и тогда, и сейчас тянулась молодежь, потому что информационная безопасность была и остается на переднем крае развития технологии и применения научных методов для решения практических задач. В 1997 году на базе Специализированного центра защиты информации была открыта кафедра «Информационная безопасность компьютерных систем», и если начинали мы с набора в 20 студентов, то в этом году мы приняли на первый курс 180 человек.

- Раз уж мы заговорили о студентах, расскажите, специалистов по кибербезопасности обучают так же, как программистов, или есть какие-то особенности?

- Безусловно, специалист по кибербезопасности должен знать, что он защищает, следовательно, должен разбираться в аппаратном и программном обеспечении компьютерных и киберфизических систем не хуже их разработчиков. Фактически мы учим студентов, как устроены современные системы и как их разрабатывать. Это первое. Кроме этого, специалист в сфере кибербезопасности должен хорошо понимать, от чего именно необходимо защищать системы и их пользователей, поэтому он должен изучать как средства защиты, так и механизмы реализации угроз.

И третье: поскольку эта сфера находится на переднем крае науки и развивается на наших глазах, он должен уметь постоянно обновлять знания. Поэтому мы стараемся учить не конкретным технологиям, а основам, которые не меняются на более длительную перспективу. Это поможет выпускникам самостоятельно изучать новые продукты. На мой взгляд, это три самых важных момента.

- Я знаю, что студенты вашей высшей школы нарасхват среди работодателей.

- Да, и мы считаем, что это самая высокая оценка нашей работы. К четвертому курсу все, без исключения, студенты нашей кафедры работают, причем по специальности! Наши выпускники трудятся в Яндексе, Google, Cisco, Oracle, Siemens, в государственных структурах… Многие из них достигли значительных успехов: среди наших выпускников – директор по безопасности Яндекса, консультант по безопасности Bloomberg, многие открыли собственные компании и успешно занимаются бизнесом.

- Чем же ваши студенты и выпускники так привлекают работодателей?

- Надеюсь, что тем, как мы их учим. В нашу высшую школу поступить непросто, а учиться еще сложнее. Среди самых сложных предметов – специальные разделы математики на старших курсах, где изучается криптография, и системное программирование. Например, каждый третьекурсник должен написать свой компилятор, то есть не просто создать программу, а сделать инструмент для ее разработки.

- Технологии в вашей сфере развиваются настолько стремительно, что их даже сложно отследить – не то что обучать им студентов. Как справляетесь с этой ситуацией?

- У нашей высшей школы очень много партнеров. Наиболее показательным

является взаимодействие с компанией LG, с которой мы создали научно-образовательный центр и сотрудничаем уже около 20 лет. Компания финансирует и образование, и научные исследования. Благодаря этому мы учим студентов самым современным технологиям. Кстати, после первого курса они проходят практику в LG, а многие впоследствии устраиваются туда на работу. В рамках научного взаимодействия мы помогаем LG прорабатывать будущие проекты, которые пойдут в реализацию в следующем году или через год.

- Дмитрий Петрович, исследовательская активность вашей научной группы поражает. Каждый год вас отмечают на самых высоких уровнях – премиями Правительства России и Петербурга, президентскими и правительственными грантами. Расскажите о самом ярком и влиятельном проекте.

- Мы действительно очень много работаем, потому что находимся на острие развития технологий и у нас очень много молодежи. В среднем мы реализуем от двух до четырех проектов в год, включая федеральные целевые программы, сотрудничество с самыми передовыми компаниями, такими как Bosch, Cisco, Лаборатория Касперского и многими другими. История нашей кафедры богата различными проектами во всех сферах информационной безопасности, и сложно выделить какой-то один проект.

За последние годы я бы отметил два направления научных и практических разработок. Первое – это кибербезопасность цифрового производства и киберфизических систем. Если рассматривать эту проблему с точки зрения теории управления, то мы переходим от противодействия кибератакам к обеспечению киберустойчивости. Мы не можем предотвратить все кибератаки и заблокировать их источники, поэтому должны строить систему таким образом, чтобы, несмотря на злонамеренные воздействия, она продолжала функционировать. Такой подход объединяет нас с современной индустрией и расширяет круг наших партнеров: кроме традиционных IT-компаний мы работаем и с производственными, такими как «Трансмашхолдинг», «Газпромнефть», Bosch и другие.

Второе направление – это применение методов искусственного интеллекта и машинного обучения для выявления компьютерных атак. В этом направлении мы сотрудничаем со «Сбербанком», и эта работа была удостоена премии Правительства Российской Федерации. В авторский коллектив входили ведущие специалисты «Сбербанка», я и мой коллега профессор Максим Олегович Калинин.

- Расскажите об этом проекте, он уже внедрен?

- Да. «Сбербанк» как самая большая российская IT-компания уделяет вопросам кибербезопасности огромное внимание. Разработанные нами решения используются в самом большом в Европе SOC – Security Operation Centre – Центре реагирования на компьютерные инциденты «Сбербанка». Это совершенно фантастический проект: огромная круглая комната, где на всю площадь стен проецируется вся информация, имеющая значение для кибербезопасности «Сбербанка».

- А какую роль во всем этом высокотехнологичном и автоматизированном процессе играет человек?

- Для обеспечения кибербезопасности недостаточно даже суперсовременных технологий, потому что самым уязвимым звеном в системе защиты является человек. Так всегда было и так будет. Поэтому один из самых эффективных

способов обеспечения кибербезопасности – это обучение как специалистов, так и пользователей. Мы прекрасно понимаем важность этой миссии и стараемся донести наши знания не только до узкого круга специалистов, но и до более широкой общественности. Поэтому ежегодно мы публикуем несколько книг о разных аспектах кибербезопасности.

- Это своего рода социальная миссия вашей высшей школы. А что касается ваших личных установок, я знаю, что часть средств из премии правительства вы пожертвовали в Эндаумент-фонд Политеха.

- Образование всегда нуждается в ресурсах, а Эндаумент-фонд – один из механизмов финансирования этого процесса. Образование – не та отрасль, где можно оценить эффект от затраченных ресурсов так, как это делают в бизнесе. Эффект от образования может прийти через поколение или два. Сколько есть примеров, когда люди занимались тем, что, казалось бы, на тот момент было никому не нужно, но через 100 лет из этого вырастали целые направления науки и отрасли промышленности.

Хочу рассказать о еще одном нашем проекте, имеющем гуманитарное значение. Мы сейчас работаем с Роскомнадзором над решением очень важной задачи – это борьба с призывами к детскому суициду в социальных сетях. Это действительно страшное явление, когда возможности соцсетей используются злоумышленниками для воздействия на детскую аудиторию с

самыми низменными целями. Мы применяем наши технологии работы с соцсетями и методы искусственного интеллекта для автоматического распознавания постов, содержащих угрозу детям.

- К сожалению, в цифровом мире опасности поджидают ребенка на каждом шагу. Взрослые тоже нередко становятся жертвами киберпреступников, чаще всего это связано с финансовыми махинациями. Поделитесь, пожалуйста, основными правилами безопасности в Сети.

- Знаете, абсолютно безопасный компьютер – это тот, который выключен из розетки. Как только вы его включили и тем более вошли в сеть Интернет, то сразу подверглись опасности. Об этом надо помнить постоянно, так же как мы следим за ситуацией, когда мы переходим дорогу. А в интернете многие этого пока не ощущают. Надо отдавать себе отчет в том, что если мы что-то выложили в Сеть, пусть даже на свою персональную страницу, и даже если доступ к этой информации сейчас закрыт для других пользователей, то рано или поздно эта информация станет доступной всем.

Никто не позаботится о нашей безопасности, кроме нас самих. Многие думают: вот, установлю замечательную программу, и всё будет хорошо и безопасно! Нет, не будет, надо, как минимум, регулярно ее обновлять и менять пароли.

- Как часто?

- Чем чаще, тем лучше.

- Заодно память разовьем…

- Это действительно проблема, потому что у нас есть интернет-банки, соцсети, приложения, каждый магазин старается, чтобы мы создали на его сайте личный кабинет. В итоге мы получаем огромное множество логинов и паролей, которые нам не запомнить и которые мы путаем. Некоторые используют один пароль для всего – это неправильно. Корректнее придумать свое индивидуальное правило генерации паролей. То есть в зависимости от сайта или соцсети, куда человек хочет войти, он и создает пароль. Это может быть комбинация названия сайта, личных данных и других параметров. Таким образом, не нужно запоминать много паролей – необходимо запомнить один алгоритм их генерации.

- Когда начинаешь обо всем этом думать, невольно может развиться паранойя. Имеет ли смысл так волноваться?

- Это зависит от того, что вы доверили информационным системам. Если это незначительная вещь, то и не надо волноваться, но если это финансы, здоровье и так далее, то задуматься стоит. Тут мы опять приходим к тому, что проблема обеспечения кибербезопасности – это серьезный барьер на пути внедрения в нашу жизнь цифровых технологий, который человечество должно преодолеть. Ключевая роль в преодолении этого барьера принадлежит научным исследованиям и образованию.

- Дмитрий Петрович, я уверена, что с такой высшей школой и с вашими студентами, нас ждет светлое и, что самое главное, безопасное цифровое будущее. Спасибо за интересный разговор!

Беседовала Илона ЖАБЕНКО

Дата публикации: 2019.11.27

>>Перейти к новости

>>Перейти ко всем новостям