STARTALK PROJECT: Choose to Study Russian for Professional Needs

Russian, Cryptography, and Cybersecurity

Криптография и компьютерная безопасность. Интервью с профессором Александрой Болдыревой, Технологический институт Джорджии

Биография: Александра Болдырева — профессор Технологического института Джорджии, координатор магистерской программы по информационной безопасности в Колледже вычислительной техники, исследователь в области криптографии и информационной безопасности. Родилась и выросла в Санкт-Петербурге, где получила степень бакалавра и магистра наук в области прикладной математики в Санкт-Петербургском политехническом университете. Защитила диссертацию и получила докторскую степень в области компьютерных наук в Калифорнийском университете в Сан-Диего.

Профессор Болдырева является автором многочисленных работ по открытому ключу и другим методам шифрования. За свои исследования была удостоена двух наград «Испытание временем». Она также является членом Института информационной безопасности и конфиденциальности (IISP) и программы «Алгоритмы, комбинаторика и оптимизация» (ACO), а в прошлом участвовала в работе предшественника IISP – Центра информационной безопасности Georgia Tech.

1. **Расскажите, пожалуйста, о себе.**

Александра Болдырева (А.Б.): Я родилась и выросла в Санкт-Петербурге, в России. Правда, когда я родилась, они назывались Ленинград и Советский Союз. В старших классах я училась в математической школе, а потом я училась в Ленинградском политехническом институте, сейчас он называется Санкт-Петербургский политехнический университет. Я училась на физико-механическом факультете на кафедре прикладной математики, но нас учили тому, что здесь называется компьютерные науки, но тогда такой термин не использовался. После окончания института я несколько лет работала программистом, и в какой-то момент я узнала о возможности поступить в аспирантуру в США, и мне это показалось очень интересным. Я подготовилась и поступила в аспирантуру на докторскую программу в Калифорнийский университет в Сан-Диего. И там я получила докторскую степень по компьютерным наукам в области криптографии. После окончания университета я получила работу профессора в университете Georgia Tech. И когда я начинала, я начинала работу на факультете по компьютерным наукам, но несколько лет назад мы создали новый факультет по компьютерной безопасности и приватности, один из первых факультетов такого типа в мире. И там я сейчас и работаю.

2. **Почему вы решили заниматься проблемами компьютерной безопасности?**

А.Б.: Когда я училась в России, я прочитала статью в каком-то научно-популярном журнале о криптографии, и мне это показалось очень интересным. Ну, действительно, шифрование, секретность – это

всё звучит очень интригующе. Но моя учёба там и работа там никак не были связаны с криптографией. А когда я начала учиться в аспирантуре в США, там у нас как у студентов была возможность выбрать область вначале. И я не совсем была уверена, чем я буду заниматься, я только знала, что мне нравятся более теоретические области. И на первом курсе я прослушала несколько курсов у профессора Михира Белларе, очень известного криптографа, но тогда я это ещё не очень в этом разбиралась. Но мне очень понравились его курсы, и содержание, и стиль преподавания. Я ему сказала, что меня интересует криптография, и он предложил мне попробовать работать в этой области. И с тех пор я работаю в области криптографии.

3. Для чего нужна криптография?

А.Б.: Криптография – это наука о том, как обезопасить передачу или хранение цифровой информации. И под безопасностью тут можно понимать несколько целей. Наверное, самая главная цель – это обеспечить конфиденциальность или приватность данных, то есть чтобы ваши данные никто не мог прочитать, кроме тех, для кого они предназначены. И для того, чтобы достичь эту цель, используются различные системы шифрования. Другая очень важная цель криптографии – это как обеспечить, чтобы никто не смог изменить или подделать данные без ведома тех, для кого эти данные предназначаются.

Помимо этих двух основных целей в криптографии есть много других, я упомяну ещё две. Одна – это о том, как несколько участников могут вычислить что-то базируемое на секретных данных, которые им принадлежат, но так, чтобы никто не узнал об их личных секретных данных. А как пример – известная проблема, как несколько очень богатых людей могут встретиться и выяснить, кто из них самый богатый, не раскрывая суммы своих состояний. И в криптографии есть протоколы, которые помогают этого достичь.

И ещё одна цель, с которой криптография помогает справиться, – доказать истинность какого-то утверждения, не выдавая никакой информации о том, что вы знаете. И пример будет о том, как доказать, допустим, что вы знаете решение для какой-то головоломки, и убедить в этом других, но не выдать ничего об этом решении. И на первый взгляд может показаться, что это невозможно, но это не так, и криптография показывает, что решение возможно для таких задач. Это здорово.

4. Где используется криптография?

А.Б.: Если я спрошу наших слушателей: “Кто из вас сегодня пользовался криптографией?” – наверное, немногие ответят утвердительно. Но, скорее всего, это не так, и если, например, вы смотрите это видео на YouTube, то вы прямо сейчас используете криптографию. И вообще в наши дни около девяноста пяти процентов всего трафика в интернете зашифровано, то есть используется криптография. И помимо YouTube, если вы что-то делаете в интернете и если в браузере, вы видите буковки по-английски https, это значит, что используется криптографический протокол TLS и ваше сообщение зашифровано. И помимо интернета криптография используется, когда вы платите кредитными или дебетными карточками в магазине. Многие слышали о криптовалютах, они используют криптографию, и также криптография используется в других приложениях.

5. Что такое криптография как наука?

А.Б.: Криптография – это довольно старая дисциплина. Говорят, что еще Юлий Цезарь использовал криптографию, чтобы зашифровать свои приказы. И, наверное, многие слышали об Энигме, криптографической машине, которая широко использовалась в нацистской Германии во время Второй

мировой войны. Но криптография как наука – это довольно молодая наука, потому что почти все достижения современной криптографии случились в последние 50 лет или даже меньше.

Наверное, одно из самых важных достижений современной криптографии – это открытие криптографических систем с открытым ключом. Потому что древние шифры, включая Энигму и самые простые шифры, когда буквы заменяются цифрами или другими буквами – это всё примеры криптографических систем с закрытым ключом. То есть для того, чтобы зашифровать и расшифровать данные, то у того, кто посылает и кто получает, должен иметься какой-то один секретный ключ, какая-то информация, известная только им. Но для развития электронной коммерции этого было недостаточно, потому что, например, если я хочу купить что-то в интернет-магазине и хочу послать номер своей кредитной карты, и я хочу сделать это секретно, я не могу использовать только традиционную криптографию, потому что у меня с интернет-магазином нет никакого секретного ключа. Вот для этого очень было важно создать системы с открытым ключом, когда стало возможно пересылать информацию секретно, тогда как у того, кто посылает и кто получает не было изначально никакого секретного ключа. Звучит довольно неправдоподобно, что безопасность возможна в такой ситуации. Поэтому, когда учёные пытались создать такие криптографические системы с открытым ключом, многие не верили, что у них это получится. Но, к счастью, они были настойчивы и теперь мы все пользуемся такими системами, и это, конечно, помогает в безопасности в интернете и в других приложениях.

Ещё очень важное, по моему мнению, достижение современной криптографии – это возможность доказать безопасность. Я объясню, что я имею в виду. Традиционно криптографические протоколы создавались методом проб и ошибок, то есть криптографы создавали криптографический протокол, пробовали его взломать и, если не получалось, тогда протокол внедрялся в практику. Иногда кто-то другой взламывал, тогда создателям надо было подправить протокол, и цикл повторялся. И если в течении нескольких лет никто не мог взломать протокол, то … Что мы знали о безопасности? В общем-то только то, что никто ещё не смог взломать этот протокол, но мы не знали, вдруг кто-то сможет взломать его в будущем. Но в современной криптографии есть методы, которые позволяют нам математически доказать, что никто не сможет взломать протокол, если только не найдутся решения для каких-то очень трудных задач. Многие верят, что это очень трудные задачи без решения, например, факторизация больших чисел. И тогда математическое доказательство безопасности криптографического протокола даёт нам гарантии, что никто не сможет его взломать, если только не найдутся решения для очень трудных задач. Это гораздо лучше, чем метод проб и ошибок. Ну, конечно, в криптографии много всего другого происходит, но, наверное, это всё-таки больше интересно для специалистов.

6. Расскажите, пожалуйста, над какими исследованиями вы работаете.

А.Б.: Конечно, одна из тем, над которой я работаю уже несколько лет, это системы шифрования баз данных с возможностью поиска. Допустим, вы хотите хранить свои данные, базу данных или документы на сервере на облаке. И, допустим, вы не хотите, чтобы если вдруг этот сервер будет взломан, кто-то смог прочитать ваши данные, и тогда, конечно, имеет смысл хранить данные в зашифрованном виде. Но проблема в том, что традиционные системы шифрования настолько хороши, что никакие функции невозможны над зашифрованными данными. А вам бы хотелось, допустим, извлечь какие-то конкретные записи из базы данных или запросить документы, содержащие какое-то определённое слово. Так вот это будет невозможно, если данные зашифрованы, невозможно с традиционными системами шифрования. Но есть специализированные системы шифрования, которые позволяют зашифровать и дать возможность

поиска. И вот над такими системами шифрования я работаю. И, честно говоря, мы всё еще не знаем самые лучшие способы, как это делать. Мы знаем, как это делать, чтобы получить очень быстрые системы, но не с самой хорошей безопасностью. И наоборот, мы знаем, как достичь отличной безопасности, но тогда системы будут довольно медленные, то есть мы всё ещё работаем над тем, как найти лучший баланс в этом смысле.

И несколько примеров протоколов, которые я анализировала: один – это протокол QUIC, который был разработан компанией Google как альтернатива популярному протоколу TLS. Другой пример – это протокол FIDO, разработанный альянсом FIDO, который использует методологию, позволяющую нам отказаться от использования паролей, потому что с использованием паролей есть много проблем. И ещё один протокол, который я недавно анализировала, – это протокол для того, как сгенерировать и сертифицировать ключи для протокола, используемого машинами-беспилотниками.

7. На ваш взгляд, какие важные задачи стоят сейчас перед учёными в криптографии?

А.Б.: Может быть, вы слышали, что квантовые компьютеры, когда и если они будут разработаны в полную силу, то они смогут взломать почти все традиционные криптографические системы с открытым ключом. Это потому, что квантовые компьютеры могут эффективно решать проблемы, на которых базируется безопасность этих систем. Я уже упоминала как пример проблему факторизации больших данных – это трудная задача, но не для квантовых компьютеров. Поэтому, конечно, квантовые компьютеры представляют угрозу для безопасности криптографических систем. Но у нас было и всё ещё есть время подготовиться. И криптографы уже много лет работают и продолжают работать над разработкой новых криптографических систем, которые квантовые компьютеры не смогут взломать. И с 2016 года исследования в этом направлении проводились под руководством Национального института стандартов и технологий. И вот в прошлом году были выбраны четыре победивших кандидата криптографических систем с открытым ключом, которые квантовые компьютеры не смогут взломать.

8. Как в Вашей работе совмещаются научные исследования, преподавание и административная работа?

А.Б.: Я сейчас работаю профессором на факультете по компьютерной безопасности и приватности в Georgia Tech. Многие думают, что профессора главным образом читают лекции. Мы действительно преподаём, но помимо преподавания мы также занимаемся научной работой, я уже говорила про это. И ещё в дополнение мы занимаемся административной работой. Например, решаем, какие курсы должны студенты выбрать для конкретных программ, каких профессоров и аспирантов нанимать к нам на факультет и так далее. И, как я уже упоминала, наш факультет по компьютерной безопасности и приватности был создан всего пару лет назад. И он необычен тем, что на нашем факультете сотрудничают профессора и студенты из разных областей, не только из компьютерных наук, но из инженерии, политологии, юриспруденции и бизнеса. Поскольку наш факультет такой новый, конечно, он требует немножко больше административной работы.

9. Какие карьерные возможности открываются перед студентами, изучающими криптографию и компьютерную безопасность?

А.Б.: Наши студенты, действительно, нарасхват в индустрии. Ну и также есть, конечно, работа в академии. А в индустрии наши выпускники работают во всех больших известных компаниях, как то Google, Facebook, Amazon, Apple, Intel, Qualcomm и в других. Также работают в меньших специализированных

компаниях, в банках, в государственных организациях, в стартапах. Я слышала, проводились исследования, что в недавние годы по Америке больше шестисот тысяч позиций для специалистов по компьютерной безопасности. А по всему миру счёт идёт на миллионы и спрос продолжает расти, потому что компьютерные системы, которые мы используем, становятся всё сложнее и сложнее. И это даёт возможность для подрыва безопасности, и поэтому специалисты по компьютерной безопасности очень важны почти для всех организаций.

10. Какое слово вы бы назвали “словом года” в вашей области?

А.Б.: Я выберу слово постквантум – от постквантовой криптографии. Это потому, что сейчас для криптографов очень важно разработать новые криптографические системы с открытым ключом, которые квантовые компьютеры, когда они будут построены, не смогут взломать.

Блицопрос

- **Книги или кино?**

А.Б.: У вас трудные вопросы! Если можно, я не буду выбирать что-то одно, потому что я считаю и то, и другое: и книги, и кино, потому что это разные жанры и прекрасные жанры. И может быть хорошая книга, и по ней можно снять плохое кино, и наоборот. И может быть, наоборот. И да, пусть будет и то, и то.

- **Ваша любимая книга на русском языке**

А.Б.: Опять-таки, я не смогу ответить очень конкретно. У меня нет любимой книги на любом языке. Я люблю много книг, но, как пример, недавно, чтобы поднять настроение, я перечитала “Двенадцать стульев” Ильфа и Петрова. И действительно, настроение поднялось. И удивительно, что книге почти сто лет, и она до сих пор звучит очень современно и очень смешно.

- **Русскоязычный учёный или исследователь, который вас вдохновил**

А.Б.: А я назову Леонарда Эйлера. И многие могут удивиться: это совсем не русское имя. И действительно, он родился в Швейцарии, но Эйлер провёл много лет, работая в Российской академии наук в Санкт-Петербурге, в моём родном городе. И он, мне кажется, один из самых продуктивных учёных в мире. Он написал какое-то немыслимое количество научных статей, по-моему, около восьмисот. Он создал очень многое для математики и для других областей, и даже в моей области, в криптографии, функция Эйлера используется, например, в одной из самых известных криптографических систем – криптосистеме с открытым ключом RSA. Эйлер работал даже после того, как он полностью потерял зрение, и даже работал в день своей смерти. Он похоронен в Санкт-Петербурге.

- **Три совета будущим специалистам по криптографии**

А.Б.: Если вы любите математику, логические головоломки и подумываете над тем, чтобы стать криптографом, то, первое, что я посоветую: поступать в университет на компьютерные науки. И второе: там попробовать взять курс по криптографии и, если это возможно, попробовать поработать над каким-нибудь маленьким научным проектом. Это даст вам понять, нравятся ли вам научные исследования. А если нет, то

наверняка знания из курса пригодятся для работы в индустрии. А если понравятся научные исследования, тогда я советую попробовать поступить в аспирантуру и продолжать обучение.

- **Не могли бы вы дать несколько практических советов по компьютерной безопасности?**

А.Б.: Да, они будут очень простыми, но мне кажется, они очень важные. Первое – это не доверять всем электронным письмам и всегда спрашивать себя, можно ли верить этому электронному письму. Второе – не нажимать на всякие неизвестные ссылки, особенно если вы не уверены в том, кто прислал вам это электронное письмо. И последнее – не лениться и обновлять компьютерные программы, не игнорировать сообщения, когда ваш компьютер напоминает, что программы надо обновлять. Это действительно очень важно для компьютерной безопасности.

Ноябрь 2023