Можно ли спрятаться от всевидящего киберока?

Значение кибербезопасности в современном мире растет с каждым днем. Всё больше используя возможности цифровых технологий, мы приобретаем привычку жить «в цифре» – и отказаться от благ цивилизации уже нельзя, и всё сложнее сохранять приватность, спрятаться от всевидящего киберока. О преимуществах и угрозах высоких технологий мы поговорили с директором Института кибербезопасности и защиты информации СПбПУ доктором технических наук, профессором и членом-корреспондентом РАН Дмитрием Зегждой.

- Дмитрий Петрович, в этом году вас избрали членом-корреспондентом РАН по Отделению нанотехнологий и информационных технологий. Расскажите, пожалуйста, чем занимается отделение, какое место в его структуре занимает раздел науки, который вы представляете, – кибербезопасность.

- Сегодня микроэлектроника является одним из важнейших направлений, от которого зависит устойчивость критической инфраструктуры, банковской сферы, обороноспособность страны, развитие всех отраслей экономики. Если говорить упрощенно, микроэлектроника – это основа всех современных высоких технологий, и как любая высокотехнологическая отрасль она уязвима для злоумышленников. Отделение нанотехнологий и информационных технологий РАН – это самые передовые научные исследования в сфере микроэлектроники и ПО, подготовка кадров для отрасли, разработка не имеющих сегодня в России аналогов программных и аппаратных комплексов, интеграция разработок для создания готовых к внедрению решений. В процессе развития микроэлектроники естественным образом появились киберугрозы, способные через уязвимости микросхем внедриться в их работу практически на любом этапе – от проектирования до непосредственной сборки. Кибербезопасность противостоит таким угрозам, так что объединение кибербезопасности и микроэлектроники – это в некотором роде закономерный синтез двух наиболее передовых направлений.

- В предыдущем интервью, которое вы дали журналу «Наука. Политех» чуть более года назад, вы уже говорили, что потребность в специалистах по кибербезопасности выше, чем в программистах. И что в 2022 году набор в Институт кибербезопасности и защиты информации увеличится на 40 мест. Меж тем, недавно аналитики HeadHunter подсчитали, что спрос на них еще вырос – в 6,5 раз по сравнению с прошлым годом. И какой, кстати, был в эту приемную кампанию конкурс?

- Спрос на специалистов по информационной безопасности значительно выше предложения. По свежим данным наших коллег из Сбера, в стране работают около пяти тысяч специалистов по кибербезопасности, а потребность в несколько раз превышает эту цифру. Специалисты по кибербезопасности требуются не только в специализированные компании или госслужбу, но и на все те предприятия, где идет процесс цифровизации и где занимаются передовыми информационными технологиями. Важна не только специализация сотрудника, но его высокая квалификация – этого не достигнешь без фундаментального образования. Несколько лет назад мы принимали на первый курс около 50 студентов, сейчас больше 200. Конкурс в эту приемную кампанию был традиционно высоким, около 17 человек на место. Я хочу отметить, что прием 2022 года в Институте кибербезопасности отличается большим количеством абитуриентов из петербургских физико-математических школ. Мы начинаем работать со школьниками с 10-х классов – ежегодно проводим летнюю практику, стараемся дать представление о том, что такое кибербезопасность и чем занимаются специалисты – в результате получаем нацеленных именно на нашу сферу абитуриентов.

- В Политехе два года назад была введена система электронных трудовых книжек. Насколько защищены сейчас электронные ресурсы, такие как портал «Госуслуги»? Не приведет ли очередная кибератака к утрате важных документов? Известны ли вам случаи, когда в результате кибератак безвозвратно терялись какие-то данные?

- Защищенность «Госуслуг» обычно оценивается высоко, и я согласен с этим – «Госуслуги» сложная и нагруженная система, которой пользуются миллионы людей. В мире не так много аналогов этому ресурсу. Как правило, большинство инцидентов безопасности связаны с человеческим фактором – злоумышленники используют методы социальной инженерии, психологическое давление, выясняя нужную информацию. Не нужно никому сообщать номер банковской карты, пароли, коды подтверждения из смс. Однако бывают и целенаправленные атаки на ресурс – в конце 2021 года Минцифры зафиксировало самую мощную за всё время функционирования атаку на «Госуслуги» и вплоть до настоящего времени продолжаются попытки вывести из строя как сайт, так и мобильное приложение, и другие государственные порталы. Специалисты по кибербезопасности «Госуслуг» успешно справляются с высокой нагрузкой на все ресурсы – насколько мне известно, серьезных нарушений в работе не было зафиксировано. В Институте кибербезопасности на направлении «Информационно-аналитические системы безопасности» мы готовим специалистов, которые умеют защищать банковские, государственные и другие высоконагруженные системы.

- Давайте поговорим о безопасности информационного пространства. Оно много дает человеку, но при этом также представляет угрозу, оно способно дезориентировать, создать ложную картину мира. Как, например, отличить в Интернете живого собеседника от бота? Есть у ботов какие-то маркеры?

- Если мы говорим именно о ботах, а не о рядовом фишинге, при котором кибермошенничеством вполне может заниматься и обычный человек, в чьих интересах вести переписку максимально правдоподобно, с соблюдением всех тонкостей деловой или личной коммуникации (в большинстве случаев у злоумышленников не получается и этого), то главный маркер искусственности интернет-коммуникаций – лингвистический. Поскольку в интернет-диалоге, как правило, паралингвистические средства общения (тембр и темп интонации, жесты, заполнители речи) недоступны, пользователям остается только текст. Понятно, что его замаскировать проще. Но бот, например, часто не способен распознавать грамматически неправильно построенные предложения, не считывает инверсию и перифраз, плохо ориентируется в местоимениях, не отличает типы вопросов. Один из самых ярких маркеров ботов, по которому их обычно и отличают – неспособность удерживать в памяти весь диалог. Чаще всего боты разговаривают шаблонами (присылают ссылку в ответ на наш вопрос или выдают стандартную форму) или используют метод отзеркаливания.

Вообще, существует метод определения навыков коммуникации ИИ – тест Тьюринга. Принцип у него такой: экспериментатор общается одновременно с компьютером и с человеком. Если он не может определить, где компьютер, значит, искусственный интеллект смог выдать себя за человека. Есть программы, которые вполне успешно этот тест проходят. Чат-бот Kuki побеждал в нем несколько лет подряд. Но это своего рода рекламный ход для компаний, конечно. В случае с Kuki за каждым предметом разработчики закрепляли еще его качества (плита – металлическая, стол – деревянный), так что ответы он давал более или менее адекватные.

- Хотя люди уже научились отличать фейковые новости от реальных, многие по-прежнему на них «ведутся». Можно ли автоматизировать систему распознавания фейков?

- В принципе, можно написать программный код, который будет распознавать такие заметки и новости, в которых есть признаки ложных сообщений. Для этого нужно собрать базу данных по фейкам и классифицировать их, чтобы обучить нейронную сеть. На самом деле, это довольно сложная задача, потому что, если мы пишем такую программу, то должны быть уверены, что она сможет отфильтровать и ошибки. За борьбой с фейками во многих случаях скрывается возможность манипулирования общественным мнением. Многие компании заявляют, что пишут или создают нейросети для борьбы с фейками, но на практике это пока реализуется плохо.

- Как отличить информационную кампанию от обычных новостей?

- У информационной кампании, как правило, есть несколько отличительных признаков – длительность и интенсивность. Что такое информационная кампания? Это прицельный, спланированный поток информации, который должен склонить аудиторию к какому-то решению или выбору. Так, например, информационная кампания – обычный термин для предвыборного периода, когда все кандидаты рекламируют себя. Рядовая новость, появившись в информационном пространстве, живет несколько дней, а, может быть, и часов. Информационная кампания способна длиться годами, если требуется. Чаще всего, конечно, она тоже чуть более краткосрочная. Если о событии, его последствиях, причинах и деталях массово пишут во всех СМИ, во всех социальных сетях, то скорее всего идет информационная кампания. Вести ее не так уж просто, аудитория склонна терять интерес к событию. Поэтому, как правило, такую кампанию можно сравнить с марафоном – пресса экономит силы и выдает новости дозированно, но постоянно, не скупясь на эмоции, чтобы пользователи запомнили инцидент и прониклись к нему. С чисто технической точки зрения информационную кампанию можно выявить прежде всего по частоте упоминаний того или иного события и чрезмерной эмоциональности его описания.

- Известно, что люди охотнее верят всяким небылицам, чем правде, которая не вписывается в их представления о реальности. Тогда получается, что дезинформация – это эффективное оружие в информационной войне? В чем опасность использования заведомо ложной информации?

- Опасность, как ни банально, в том, что всё тайное рано или поздно становится явным. Когда одна из сторон проводит дезинформацию, она должна полностью владеть всеми видами фиксации информационной среды в том социуме или в той локации, где осуществляет обман. В современном мире так сделать почти невозможно, учитывая наблюдение со спутников и банальное наличие почти у всех смартфонов с возможностью фиксации. Сейчас есть куда более элегантные способы скрыть правду. Один из них – белый шум. Разные СМИ выдают разные наборы и версии события, эксперты дают противоречащие друг другу комментарии, очевидцы сообщают противоположные факты. У аудитории тогда создается ощущение полуправды. За беспорядочным набором гипотез в этом случае легко скрыть реальное положение дел.

- Какие существуют эффективные стратегии ведения информационной войны? Блокирование сайтов, ограничение доступа к информации, рекомендательные системы можно отнести к таковым?

- Современный мир сложно себе представить без информационной войны, это важнейший фактор дезинтеграционных процессов, в таких войнах так или иначе участвуют все игроки политической арены. Дискредитация образа противника и героизация образа правительства/армии/союзника происходят повсеместно. Информационные войны обычно делят на открытые (когда происходит явное или скрытое противостояние массмедиа) и закрытые (в них работают над взломами систем хакеры). Нужно понимать, что блокировка сайтов и ограничение доступа к информации – это своего рода оборонительные элементы информационной войны. Используя их, государство пытается не пустить условного «врага» на свою территорию. Да, в идеале система должна быть выстроена так, чтобы граждане одного государства не становились жертвами информационных атак другого, но одних запретов скорее всего недостаточно, нужно, кроме того, укреплять собственное влияние.

- Какие психофизиологические особенности человека используются в гибридной информационной войне, и можно ли от этого защититься?

- Информационно-психологическое оружие направлено на изменение сознания – как массового, так и индивидуального. Противоборствующие стороны стараются укрепить свое влияние через некую господствующую идею – универсальную мировоззренческую систему, которая вбирает в себя набор принципов и ценностных установок, сформулированных максимально просто. При навязывании идеи или образа эксплуатируются сильные эмоции – чувство гордости, вины, ненависти, стыда. Стороны стараются транслировать свои установки всеми возможными способами – не только через средства массовой информации или социальные сети, но и через объекты искусства, кино, литературу, даже детские книжки. Образ врага лучше всего демонизировать через радикальные, даже ужасающие установки.

Способность сопротивляться информационно-психологическому воздействию во многом зависит от убеждений, личностной или гражданской позиции, уровня осведомленности, просвещенности. Нельзя защититься от информационных атак целиком, но можно попытаться выработать иммунитет – всегда проверять новости в нескольких источниках, читать каналы разной политической ангажированности, не верить сразу слишком эмоциональным сообщениям.

- Существующая система борьбы с проявлениями агрессии в Интернете с помощью искусственного интеллекта вызывает много нареканий у пользователей. Почему у нее столько изъянов? За какими-то блогерами роботы буквально охотятся и блокируют их по ничтожным поводам, а кто-то позволяет себе всё и остается безнаказанным. Можно ли

создать идеальную цензуру в Интернете?

- Технически очень трудно ввести не только идеальную, но и вообще какую-либо цензуру в Интернете усилиями одного государства. Успешно вводят подобные ограничения Китай, Северная Корея и Иран, хотя, за исключением первого случая, все из них имеют множество явных и пока не решаемых изъянов – скорость, обособленность, обход ограничений.

В том, что касается нейросетевых моделей распознавания агрессии, нужно учитывать, насколько разные модальности могут быть у деструктивных действий пользователей. Большинство современных социальных сетей так или иначе вынуждено вводить ограничения в отношении юзеров, занимающихся разжиганием ненависти, и модерировать публичные переписки. Другое дело, что не всегда получается идеальный результат. Нейросеть сложно научить считывать сарказм, например. Пользователи в свою очередь всегда могут прибегнуть к частичной маскировке оскорблений – использовать *, например.

- При удалении файлов чрез файловый менеджер сам файл не удаляется полностью, его можно в дальнейшем восстановить. Что можно использовать для тотального удаления файлов?

- Для полного удаления файлов лучше всего использовать специальные программы, выбрав функцию «без возможности восстановления».

- В прошлом интервью вы упоминали компьютерные устройства, которые также являются объектами кибератак, хотя и не связаны с ценной информацией, – кондиционеры, автомобили и так далее. А известны ли случаи взлома кардиостимуляторов? Могут ли такие действия злоумышленников причинить вред человеку?

- Риск кибератак на персональные медицинские устройства, среди которых кардиостимуляторы и инсулиновые помпы, крайне низкий, но он, тем не менее, существует. Эти устройства используют программное обеспечение, а значит, могут быть взломаны. В 2017 году FDA (Управление по санитарному надзору за качеством продуктов и медикаментов из США) [redacted] около 500 тысяч кардиостимуляторов, которые посчитало уязвимыми для взлома. Однако никаких сообщений о фактическом взломе не поступало. За безопасность персональных медицинских устройств несут ответственность их производители, и, конечно, они закладывают в них функцию защиты от кибератак.

- Много шума наделал взлом защиты Яндекс.Еда и слив данных пользователей в открытый доступ. Это неприятный инцидент, но не слишком серьезный. При этом кибератак на серьезную инфраструктуру разных стран, например, «обвала» серверов железнодорожной компании, блокировки движения поездов, пока не наблюдается. Почему этого не происходит? Хакеры не настолько продвинутые? Или атаки происходят, но криптозащита на очень хорошем уровне?

- Социальные объекты и объекты критической важности охраняются довольно серьезно: чтобы их взломать, нужно потратить слишком много ресурсов, времени и сил. Хотя, например, все мы помним, как вывели из строя ядерные центрифуги Ирана с помощью сетевого червя Stuxnet. То есть такие серьезные атаки уже случались. Другое дело, что чаще всего определяющим в них является все же человеческий фактор. Куда проще убедить сотрудника втайне пронести флешку и заразить через нее компьютер, чем «ломать» почти идеальную систему защиты.

- Возвращаясь к взлому Яндекс.Еды. У таких ситуаций должны быть правовые последствия? Компания несет ответственность за недостаточную киберзащиту данных своих клиентов?

- У таких ситуаций не только должны быть, но и уже есть правовые последствия. Из-за последней крупной утечки персональных данных пользователей Яндекс.Еды зарегистрирован коллективный иск к компании. И таких исков много. Фирмы несут существенные убытки из-за недостаточной киберзащиты. Эти финансовые и репутационные издержки – последствия того, что зачастую компании все же уделяют не слишком много внимания кибербезопасности.

- Насколько сейчас развит дипфейк? Можно ли уже с его помощью обходить биометрическую защиту?

- С помощью дипфейков уже обходят биометрическую защиту, но пока это редкие случаи, они связаны скорее не с совершенствованием системы самих дипфейков, а с уязвимостями безопасности. В Китае в 2021 году [redacted] довольно крупную

аферу с распознаванием лиц. Мошенники там использовали смартфоны, которые позволяли для идентификации пользователей использовать записанное видеоизображение, а не снимок с фронтальной камеры. Преступники таким образом обманывали налоговую службу. Основная угроза дипфейков действительно связана с гипотетической подменой одним человеком другого. Хороший способ защиты – многофакторная авторизация, когда, кроме изображения, нужно ввести также пароль или другие данные. Кроме того, некоторые системы работают по принципу «вопрос-ответ»: они просят улыбнуться или помахать в камеру, или выполнить другое действие, чтобы убедиться, что перед ними не дипфейк.

Понятно, что с развитием дипфейков будут развиваться и алгоритмы их распознавания. Они работают с очень тонкими вещами – отслеживают моргание, расстояние от центра зрачка до края оболочки, сдвиг ключевых антропометрических точек. По прогнозам, к 2024 году точность выявления дипфейков программами по распознаванию контента достигнет 70 %, а к 2030 году – и 90 %. Сам процесс создания дипфейков станет в таком случае абсолютно не рентабельным.