Лекция 3. Безопасность больших данных

История и современность

Необходимость защищать данные появилась вместе с самими данными, когда эти данные создали угрозу неприкосновенности частной жизни. Одним из таких случаев является первая в истории перепись, которую организовал царь Давид для того, чтобы вполне наглядно увидеть свои успехи в деле завоевания мира. Надо сказать, результат его приятно удивил, хотя сама перепись не одобрялась церковью.

Второй известный случай переписи был во время правления императора Августа в 28 году до н. э. Судя по ней, население Римской империи составляло 4 036 000 человек. Скорее всего, это было число взрослых свободных мужчин, которыми и интересовались власти, так что общее количество людей могло составлять порядка 10 миллионов человек, не считая рабов. Хотя ряд историков придерживаются мнения, что переписчики считали всех свободных граждан.

Вернемся к теме безопасности. Средневековые историки придерживались мнения, что именно перепись населения стала причиной гибели детей, то есть избиения младенцев по приказу царя Ирода.

Члены британского парламента, хорошо знавшие Библию, проголосовали против переписи населения, предложенной правительством в 1753 году. Многие признавали, что она может принести немало пользы, но, с другой стороны, вспоминали исторический опыт и опасались, что эта статистика попадет во вражеские страны. А это даст врагам Англии информацию о ней, которую разглашать было ни в коем случае нельзя. Это вопрос безопасности страны. Именно из-за таких опасений перепись отвергали многие европейские страны. Враг не должен знать ни количество населения в целом, ни количество взрослых мужчин, способных участвовать в войне. Первые статистические данные в Швеции были опубликованы в 1744 году. Исследование проводилось в одном городе (Упсале), но он нигде не упоминался.

Также жители не хотели, чтобы государство имело о них больше информации. Они не сомневались, что перепись приведет к новым налогам, а молодых людей, о которых станет известно государству, станут забирать в армию, «вырывая» их из семейного дела или с земли, где всегда требуются лишние руки. Необходимость переписи населения в Великобритании была признана только в 1801 году после недостатка продуктов питания в 1800 году по всей стране. Для их распределения государству требовалось знать, какое количество людей в нем живет.

До сих пор люди во всех странах не горят желанием участвовать в переписи. Возможно, срабатывает историческая память. Но скорее, как и в прошлом, мы просто не хотим, чтобы правительство имело о нас лишнюю информацию и каким-то образом использовало ее против нас. Хотя в современном мире необходимость борьбы с терроризмом заставляет людей понимать и необходимость раскрытия данных.

Следует отметить, что такие компании, как *Amazon, Apple, Google,* не желают добровольно делиться информацией с правительством и правоохранительными органами. Например, только за вторую половину 2016 года *Apple* получила около 6 000 требований, касающихся национальной безопасности. Но в компании твердо убеждены, что национальная безопасность может быть обеспечена без нарушения конфиденциальности.

В компанию регулярно поступают официальные просьбы о раскрытии информации и выполнении определенных действий. Это могут быть запросы от властей, правоохранительных органов и частных компаний. Запросы от частных лиц

обычно связаны с судебными разбирательствами. В компании каждый из них рассматривается отдельно.

Строя взаимоотношения с партнерами и поставщиками услуг, компания требует от них следовать тем же стандартам, которым следует сама в ответ на требования государственных органов. Юристы компании тщательно проверяют, есть ли законные основания для требования о предоставлении данных. Если они есть, то данные предоставляются только в необходимом объеме. Если запрос не обоснован, нечетко сформулирован или некорректен, никакой информации не предоставляется.

В продукты и сервисы *Apple* никогда не встраивались универсальные ключи и средства несанкционированного доступа. В компании говорят, что никогда не предоставят прямого доступа к их сервисам правоохранительным органам.

Когда правоохранительные органы присылают запросы в отношении устройств (в случае потери и кражи), компания старается помочь. Компания получает запросы по финансовым идентификаторам, например, использованию данных чужих кредитных карт для покупки продукции *Apple.* Доступ к пользовательскому контенту предоставляется только при наличии ордера на обыск, если дело происходит в США.

Если компания получает международные запросы на доступ к контенту, хранящемуся в центрах обработки данных в США, то для их рассмотрения они должны соответствовать требованиям закона США «О защите информации, передаваемой при помощи электронных систем связи». Если компания предоставляет информацию правоохранительным органам о данных, хранящихся в *iCloud,* то предварительно оповещает об этом пользователя, если оповещение не запрещено законом.

Интересный случай, связанный с *Apple,* произошел в 2016 году. Компания отказалась взламывать телефон по требованию ФБР после теракта в Сан-Бернардино. Стрельба в Сан-Бернардино произошла 2 декабря 2015 года. Сайед Фарук и его жена Ташфин Малик открыли огонь в центре для людей с ограниченными возможностями. 14 человек погибли, еще 21 получил травмы разной степени тяжести. По данным ФБР, Фарук имел контакты с двумя зарубежными террористическими организациями — «Джебхат ан-Нусра» и «Аш-Ша-баб». В США случившееся признали терактом. Глава компании *Apple* Тим Кук заявил, что этот прецедент может ударить по другим гражданам, а они должны быть уверены в безопасности своих данных. На сайте компании было опубликовано обращение к клиентам и выражен протест на требования властей о получении доступа к айфону и поступившим на него сообщениям стрелку Сайеду Фаруку. По мнению компании, запрос угрожал безопасности клиентов *Apple,* и последствия прецедента «выходят далеко за рамки правового поля». Окружной суд Лос-Анджелеса постановил 16 февраля, что *Apple* должна обеспечить «разумную техническую помощь» для того, чтобы сотрудники ФБР получили доступ к данным айфона Фарука. ФБР потребовала от компании снять ограничение на количество попыток ввести пароль, тогда система автоматического взлома паролей взломает смартфон Фарука. Тим Кук назвал это созданием «лазейки к айфонам». Кук написал на сайте на следующий день после принятия решения судом (17 февраля 2016 года): «Правительство попросило *Apple* взломать аппараты наших собственных пользователей и подорвать десятилетия работы над системой защиты клиентов, в том числе американских граждан, от изобретательных хакеров и киберпреступников».

В дальнейшем Министерство юстиции США объявило, что правоохранительным органам удалось взломать защиту смартфона Фарука (там ведь тоже работают талантливые люди). Таким образом, спор между *Apple* и ФБР, требовавшим от компании содействия в разблокировке, был прекращен. *Apple* содействия не оказала.

Apple — не единственная американская компания, от которой ФБР или правительство требовали содействия во взломе смартфонов. Такие требования получала и *Google,* например, в 2015 году, когда велось расследование дела, связанного с торговлей наркотиками. Калифорнийский суд обязал привлечь компанию к разблокировке телефонов. Подобные решения принимались в Алабаме, Северной Дакоте и ряде других штатов, но неизвестно, подчинялась ли *Google* этим требованиям.

Представитель *Google* официально объявил, что компания никогда не получала требований создать дополнительный инструмент, ставящий крест на безопасности ее продуктов, как было в случае *с Apple.* «Если бы такое требование поступило, мы бы его решительно оспорили,» — заявили в *Google.* То есть *Apple* и *Google* выступают против политики правительства США, но за строгую конфиденциальность данных своих клиентов.

За нами наблюдают

Если вы смотрите детективные сериалы по телевизору или триллеры в кино, то обязательно видели полицейских или следователей, внимательно просматривающих записи с камер видеонаблюдения. Так они пытаются засечь или автомобиль, или какого-то человека. Когда мы произносим слова «большие данные», то в первую очередь на ум приходят цифры. Но видеозаписи — это такие же данные, как какая-нибудь сводная таблица или ведомость, в особенности цифровое видео. Человек чувствителен к визуальным данным.

Конечно, кто-то лучше воспринимает письменный текст, кто-то — информацию на слух, но мы все способны обрабатывать информацию, получаемую органами зрения. Это часть человеческой природы. Но способность ухудшается при большой зрительной нагрузке. Например, если полицейскому нужно просмотреть много часов записи, у него неизбежно снизится внимание. Человек устает. И поэтому анализ видеозаписей является прекрасной возможностью для использования алгоритмов *Big Data.* И в наши дни они все больше и больше используются в работе правоохранительных органов, как, впрочем, и в работе ритейлеров. Видеокамеры наблюдения есть везде, даже там, где мы их не замечаем и не догадываемся об их наличии. То есть сейчас наши города, по крайней мере, в развитых странах, будто накрыты гигантским куполом.

Есть соответствующие программы, помогающие вычленить нужный час у какого-то здания или, например, пассажиров определенного рейса. Сейчас никого не удивляют работающие камеры в супермаркетах и других магазинах. Мы скорее удивимся, если их не увидим, по крайней мере, в США. Мы предполагаем, что эти камеры установлены в целях безопасности, и с их помощью за посетителями наблюдает служба безопасности супермаркета или даже государственные правоохранительные органы с какого-то центрального пункта наблюдения. Но большие данные обеспечивают не только возможность наблюдения за посетителями. С их помощью магазин следит, какие полки привлекают наибольшее внимание.

Так же работает система распознавания лиц — и отслеживает не только людей, объявленных в розыск (которые интересуют правоохранительные органы), но и постоянных покупателей (которые интересуют магазин). Эта же система распознавания лиц в дальнейшем соотносит постоянных покупателей данного магазина сети или многих магазинов сети с аккаунтами в социальных сетях, и им направляется целевая реклама или предложения. Подобное стало возможно только благодаря технологиям *Big Data.*

Еще одна интересная система сбора данных установлена в сети *7-Eleven,* работающей в 18 странах мира и имеющей более 36 000 торговых точек — небольших супермаркетов. У них установлена система, собирающая информацию по потокам покупателей и по тому, сколько человек проходит через каждую кассу. Система соотносит количество покупателей в целом и количество покупателей, обслуженных каждым кассиром, вычисляется наиболее напряженное время и спокойные часы. В ряде стран это круглосуточные магазины, потому что, например, на курортах в Таиланде, есть круглосуточный спрос на их услуги. Имея в распоряжении всю эту информацию, можно увеличить количество продавцов-кассиров в часы наибольших потоков покупателей и убрать в те часы, когда покупателей нет. И эти часы различаются в разных странах и городах одной и той же страны. Технологии *Big Data* в этом очень помогают.

Также эти технологии, использующие видеонаблюдение, помогают определить, какие продавцы хорошо работают вместе, а кого лучше не ставить в одну смену. Не нужно нанимать психологов, проводить дорогостоящее тестирование. Все это сделает алгоритм! Кто-то лучше работает в солнечные дни, а кто-то в дождливые. Это можно учесть. Систему придумали в американской компании *Percolata,* которая предлагает различные решения для оптимизации маркетинга. В компании посчитали, что в магазинах, где их система используется, удалось поднять выручку от 10 до 30%. Конечно, подобный подход не радует сотрудников, как и любая работа, которой управляет алгоритм. Ведь начинаются сокращения или сотрудники вынуждены работать в неудобные для них часы, без четкого графика, а тогда, когда система посчитала выгодной их загрузку для нанимателя. С другой стороны, с такой системой хороших сотрудников можно поощрять и награждать, а от плохих избавляться. И конечно, система «ловит» воров.

Подобные системы наблюдения уже давно используются на улицах, по крайней мере, в развитых странах. Они стали необходимой частью работы полиции и властей. Конечно, нельзя представить ни один современный аэропорт или вокзал без круглосуточной системы наблюдения и системы распознавания лиц. Сейчас уже говорят, что мы живем в «обществе наблюдения». Видеокамеры не только висят на улицах и в помещениях, наши автомобили оснащены видеорегистраторами, на некоторых официальных лицах вы тоже можете их увидеть (например, на сотрудниках дорожной полиции), и наше местоположение можно отследить с помощью телефона.

Уверены ли мы, что видеоданные, попадающие в системы *Big Data,* будут использованы правильно? Конечно, нет. С их помощью можно все больше и больше контролировать нашу жизнь, наши действия, которые мы совершаем ежедневно. В некоторых частях Америки власти не ограничиваются видеонаблюдением — на скамейках на улицах и в парках уже установлены микрофоны. Разговоры анализируют с помощью технологий *Big Data.*

Наверное, никто не будет спорить с тем, что видеонаблюдение — это важная часть работы полиции. И видеодоказательства более весомы в суде. Они более надежды, здесь никак не мешает человеческий фактор, хотя во время слушаний в суде до сих пор учитываются показания свидетелей-людей и на их основании судьи и присяжные принимают решения. Но на них нельзя полагаться! Не потому, что люди преднамеренно лгут, а потому, что каждый человек по-своему видит ситуацию.

Для примера можно вспомнить эксперимент австрийского и немецкого юриста, специалиста в области уголовного и международного права Франца фон Аиста (1851-1919), проведенный в далеком 1901 году. Во время семинара в Берлине разразился жаркий спор (специально спровоцированный исследователем), потом прозвучал выстрел — и один из студентов (участник эксперимента) «упал замертво». Все замерли

в ужасе. Через несколько минут «убитый» студент встал, а фон Лист объяснил, что никто не пострадал и случившееся — часть программы семинара. Потом он попросил каждого студента детально описать то, что произошло в аудитории у них перед глазами.

Это были будущие юристы и описывали они то, что случилось только что, а не несколько недель или даже месяцев назад, как бывает при даче показаний в суде. Студенты успокоились, поняв, что никто не пострадал, от их показаний не будет зависеть ни жизнь, ни судьба другого человека, невиновный не отправится в тюрьму и обвинять вообще некого.

Наверное, сам Франц фон Аист не ожидал такого результата — он получил совершенно разные описания случившегося. Большинство студентов ошиблись с временным фактором. Часто неправильно указывалась последовательность событий. Некоторые описывали, как убийца выбежал из аудитории, а он никуда не убегал. И студентам еще нужно было назвать имя «убийцы» (еще одного помощника фон Листа). Было названо восемь разных человек. Так можно ли после этого верить показаниям людей?!

Человеческая память несовершенна. Видеозапись не может помнить неправильно. На ней зарегистрировано именно то, что произошло. Только одна запись. А когда запись вводится в систему *Big Data,* то появляются и дополнительные возможности ее использования. Несчастных полицейских, часами просматривающих километры пленки, можно избавить от этого изнурительного труда. И полицейские тоже люди, как и свидетели. Они устают, они могут пропустить на записи важный момент: срабатывает человеческий фактор. Здесь нельзя говорить о непрофессионализме или даже невнимательности. Он смотрел внимательно и напряженно, но шесть или восемь часов подряд! Если же поиск за нас осуществляет искусственный интеллект, мы можем рассчитывать на гораздо лучший результат. Нельзя сказать, что системы *Big Data* идеальны, но они значительно облегчают работу людей, например, вычленяют из нескольких часов записей несколько важных минут, которые уже внимательно просматривают люди.

С помощью программного обеспечения для распознавания лиц или автомобилей просто отследить перемещение человека или автомобиля по городу. Камеры висят не на каждом шагу, но путь от камеры к камере проследить не сложно. Современные системы позволяют узнать о ваших перемещениях в мельчайших деталях! Например, в США и Великобритании подобные отслеживания используются для того, чтобы ловить незарегистрированные автомобили. Также эти системы активно используются для поиска пропавших людей. И масса людей была найдена таким образом.

Постоянная слежка за нами — это хорошо или плохо? В какой степени мы готовы терпеть вторжение в нашу частную жизнь ради потенциальной пользы и безопасности? Поиск пропавших людей, ловля преступников — да. Если данные будут использоваться правильно и только для обеспечения доказательств в законных расследованиях, это кажется разумным.

Предсказывание наших действий

Мы можем ожидать, что спецслужбы будут знать о нас все. Но дело в том, что они смогут знать и то, где мы будем завтра, через месяц, а то и год. И в этом им помогут большие данные. Спецслужбы всего мира сейчас очень интересуются новыми технологиями и привлекают к работе молодых специалистов, которые в этих технологиях прекрасно разбираются. И они не только собирают данные обо всех, но и занимаются передовыми разработками по моделированию поведения отдельных людей

или групп людей. Пока еще нет технологий, позволяющих абсолютно точно предсказывать, где в ближайшее время начнутся беспорядки, революция или что-то подобное, но такие разработки ведутся, и в них уже инвестированы огромные средства. Хотим ли мы этого? Можно ли отдавать развитие интеллекта на откуп спецслужб? Не получится ли в результате большого перекоса?

Давай вернемся в прошлое, в XIX век. Эпидемия холеры началась в Лондоне в 1854 году, в районе Брод-стрит (в настоящее время Бродвик-стрит). Благодаря этому событию прославился и вошел в историю лондонский врач Джон Сноу, который смог определить источник заражения. Это была вода из совершенно определенной водозаборной колонки. Сноу смог связать вспышку холеры с загрязнением питьевой воды. Сноу не верил в господствовавшую в то время теорию миазмов, в соответствии с которой причиной болезней типа холеры и чумы считался нездоровый воздух. Джон Сноу опрашивал жителей всех домов в районе Сохо, один за другим, и наносил на карту источники, в которых они брали воду (водопровода, как вы понимаете, еще не было, а вместо канализации использовались выгребные ямы). Исследовать воду лабораторными методами он не мог, но смог определить «вредоносную» водозаборную колонку. Он составил так называемую «карту холеры». На ней были отмечены водозаборные станции и количество заболевших в том или ином здании, и Сноу смог доказать местным властям связь между источником воды и распространением заболевания. После того как власти сняли с колонки рукоять насоса, эпидемия пошла на спад. Местное население очень высоко оценило работу доктора Сноу. Чуть позже появилось еще одно доказательство его правоты. В расположенном недалеко от той самой водозаборной колонки монастыре никто не умер. Но оказалось, что монахи пили только пиво, сваренное на монастырской пивоварне. Расследование Сноу считается главным событием в истории эпидемиологии, медицинской географии и важной вехой в истории здравоохранения и обеспечения безопасности людей в целом.

А метод, использованный Сноу, стали использовать в различных областях знаний. Сейчас уже появились и используются программные продукты для предсказывания преступлений. Они снова и снова используют принцип анализа, который применил для составления своей «карты холеры» Джон Сноу, только работают с большими массивами данных. Один из самых известных «предсказателей» вероятных мест совершения преступлений — *PredPol.* Это программный комплекс, разработанный с участием Калифорнийского университета и в тесном сотрудничестве с полицией. Это «предсказание преступлений», аналитический инструмент, который подсказывает сотрудникам полиции, на что следует обратить внимание. Он позволяет с большой долей вероятности определить, когда и где случится преступление: кража, ограбление, ДТП, преступление, связанное с наркотиками, увеличение активности уличных банд. То есть дается предсказание о виде преступления, месте и времени, но не личности преступника. О точности предсказаний данных нет: разработчики и производители предпочитают об этом умалчивать. Хотя полиция Кента (Великобритания) официально заявила о раскрытии на месте и предотвращении гораздо большего (в 10 раз!) количества преступлений и правонарушений с использованием *PredPol,* чем при обычном патрулировании.

Алгоритм использует отчеты о преступлениях за годы и десятилетия и определяет районы с наибольшей вероятностью совершения следующего. На карте города он отмечает такие участки красными квадратами. В реальности их величина 150 х 150 метров. Учитывается расположение банкоматов, места охвата уличными камерами и «серые» зоны, места проживания людей с криминальным прошлым, людской поток на улицах в то или другое время дня. Время дня, день недели, национальные и религиозные праздники тоже учитываются. В район, который система

посчитает потенциально опасным, можно отправить полицейского или патрульную машину. Сотрудники могут обнаружить, что кто-то пытается взломать замок на двери пустующего дома, открыть чужую машину, спасти прохожего от нападения. Но этого может и не случиться. Кликните на выделенный район — и можете ознакомиться с историей правонарушений.

Но для лучшей работы этой системы нужно, чтобы в полицию сообщали обо всех правонарушениях, а этого не происходит, в особенности из районов, где жители селятся по этническому признаку. Или люди просто не хотят тратить время на общение с полицией, понимая, что им все равно не вернут украденный бумажник. В бумажнике были только банковские карты, ни одного наличного доллара. Человек звонит в банк, блокирует карты, ему вскоре выдают новые — или бесплатно, или за минимальную плату. Далеко не все драки попадают в полицейскую базу данных, а драки в районах, где проживают национальные меньшинства, попадают только в случае, если есть жертвы, и то не всегда.

Компания *PredPol* основана антропологом Джеффри Брэнтингемом, который изучает криминальный мир, опираясь на статистику, из Калифорнийского университета, и математиком Джорджем Молером из университета Санта-Клары. Придуманная система основана на работах, выполнявшихся по заказу Армии США. Ученые создавали модели прогнозирования количества потерь во время боевых действий и поведения террористов в Афганистане и Ираке. Это был проект, о котором рассказывается на сайте Министерства обороны США. Он назывался «Применение пространственно-временной нелинейной фильтрации в целях информационной поддержки и борьбы с проявлениями терроризма». В нем участвовал Джеффри Брэнтингем, который с 2008 года занимался построением статистических моделей криминальной активности.

В США система используется в подразделениях полиции в Калифорнии, Флориде, Мэриленде, Пенсильвании, Алабаме и Вашингтоне. Она используется полицией Лос-Анджелеса с 2014 года. За пределами США использовалась в городе Кент (Великобритания), о чем уже было сказано, и Монтевидео (Уругвай). Стоимость лицензирования разная в разных городах: для Колумбии (столица штата Южная Каролина с населением 134 000 человек) — это 37 500 долларов в год; для Алхамбры в Калифорнии (85 000 человек) — это 22 000 долларов в год.

У *PredPol* немало противников, которые считают эффективность системы недоказанной, а популярность — хорошей работой маркетологов. Но полиция приняла этот инструмент и использует его.

Hitachi, производитель бытовой техники, электроники и медицинского оборудования, предложила свой модуль *PCA (Predictive Crime Analytics)* для прогнозирования преступлений в составе комплекса для работы «умного города». Комплекс называется *Hitachi Visualization Suite (HVS),* это облачная платформа, которая использует данные, поступающие от службы 911, камер наблюдения, считывателей автомобильных номеров и датчиков выстрелов. Используется в Техасе и Калифорнии.

Разработчики Марк Джулс и Дэррин Липскомб занимались вопросами безопасности. Их компанию в 2014 году купила *Hitachi.* PCA использует данные о криминальной активности, погоде, дорожном движении, маршрутах общественного транспорта, записи с камер видеонаблюдения, сообщения в социальных сетях. Система анализирует твиты с учетом местного сленга — так можно понять, что происходит в том или ином городе. Все странные сообщения улавливаются. Разработчики приводят пример. PCA ловит сообщение с предложением купить насос в Макдоналдсе. Это

ненормально. Система мгновенно реагирует, проводит анализ местного сленга и приходит к выводу, что в Макдоналдсе идет торговля амфетамином.

На карте города в этой системе появляются цветные блоки, чем он темнее, тем выше вероятность криминальной активности. Шкала от 0 до 100. Размер квадрата 200 х 200 метров. Разработчики PCA говорят и о возможности определения личности вероятного преступника. Система не справляется с предсказанием преступлений как *PredPol.* Она мало помогает оперативным работникам на улицах, хотя сидящие в кабинетах аналитики высоко ее оценивают.

В Нью-Йорке используется разработка компании *Microsoft* под названием *Domain Awareness System,* разработана по заказу полиции Нью-Йорка. Система имеет доступ к более чем 3 000 камерам видеонаблюдения, полицейским отчетам, записям звонков в спасательную службу, базе автомобилей и датчикам радиации. Она снабжает полицию города полезной информаций о подозрительной активности, обобщает и визуализирует данные. Но эта система не делает выводов о том, где и когда произойдет следующее преступление.

То есть полиция получает мгновенный доступ к записям с видеокамер, следователи наблюдают за арестом подозреваемых, полиция отслеживает похожие преступления в том же районе, выявляет преступные схемы, похожие и связанные между собой события, можно отследить, где находилась машина преступника вчера, месяц назад. В зависимости от криминальной активности в районе руководители могут правильно распределить силы. Если где-то обнаружена подозрительная сумка, можно отмотать назад запись и увидеть, кто ее принес.

В Китае компания *China Electronics Technology Group,* производитель локационного оборудования и электронных компонентов для военных нужд Китая, работает над созданием системы предотвращения террористических актов, но она по доступным описаниям больше похожа на систему тотального контроля за людьми.

Эта система может анализировать данные о выполняемой человеком работе, движении денег по карточкам и банковским счетам, хобби, видах и частоте покупаемых товаров и услуг и сопоставлять эти данные с данными камер видеонаблюдения. Эти сведения будут использоваться для обнаружения необычных для человека действий: вдруг кому-то падает на счет крупная сумма денег, вдруг кто-то начинает регулярно звонить в США.

Все эти системы используют большие данные. Подобная компьютерная система автоматизирует методики, наработанные десятилетиями, то, чем правоохранительные органы занимались «вручную», «внезапные озарения» после часов размышлений и просмотра фотографий и записей теперь происходят гораздо быстрее.

В американских детективных фильмах такое озарение детектива часто показано очень эффектно. Теперь это делает машина и без многих часов анализа. Человек для обработки больших массивов данных использует подсознание, возможности которого ограничены, а тут работает машина, которую можно подправить, перенастроить, и она станет еще эффективнее.

И эти системы помогают обеспечить безопасность простых граждан. Например, система подсказывает, что в таком-то районе или квадрате следует ожидать вспышки преступлений. Там появляются полицейские и предотвращают или раскрывают преступления на месте, даже те, о которых при других обстоятельствах люди не стали бы сообщать. Преступность снижается.

В крупных городах в систему загружают только серьезные правонарушения, иначе в таком городе, как Нью-Йорк, полиции будет просто не справиться. А в Кенте загружают все, даже самые мелкие правонарушения. Результат впечатляющий.

Что наше, а что не наше

Масса людей в разных странах зависит от иностранного программного обеспечения, чаще всего американского, и теоретически очень даже возможно, что в какой-то стране (например, России) будет заблокирована *Windows.* Сейчас и почти весь софт, и почти все «железо», то есть почти любое программное обеспечение и оборудование имеют удаленное управление. То есть они привязаны к поставщику. В большинстве случаев имеются встроенные модули, которые обращаются к поставщику за какой-то информацией. Это означает, что на систему можно влиять удаленно и даже отключить.

Поставщик хочет оставить себе доступ к системе. Это понятно. Ему нужно обеспечивать техническую поддержку. Современные технологии позволяют налаживать систему удаленно, если в ней что-то сломалось или сбилось. Также поставщик хочет привязать к себе клиентов, держать их на крючке.

Поэтому любая страна, заботящаяся о своей безопасности, просто не имеет права иметь инфраструктуру, зависимую от технологий других стран, в особенности тех, с которыми у нее не самые лучшие отношения. Угрозами кибератак в наши дни никого не удивить. Но некоторые почему-то до сих пор не верят в их реальность. А зря. Да, простому человеку сложно представить, что одна страна может отключить другой свет. Может! Если в энергосистеме есть управляемые модули, связанные с Интернетом, то это означает низкий уровень защищенности. Талантливые хакеры вполне могут в эту систему проникнуть. Да и поставщик может вмешаться.

Программное обеспечение открывает возможность слежки за пользователем. И иностранное государство, из которого это программное обеспечение поступило, может следить за гражданами другого государства, в котором это программное обеспечение используют. Это может быть массовая слежка. Данные пользователей в той или иной степени собирают смартфоны, социальные сети, фитнес-браслеты, все современные гаджеты. Данные собираются на какой-то платформе, анализируются, чаще всего они передаются партнерам для адресной рекламы. Как было сказано выше, ни *Apple,* ни *Google* не желают передавать данные ФБР, наоборот, они выступают за защиту данных своих пользователей. Но в современном мире мы не можем быть уверены в защите данных. Ведь ФБР смогло взломать смартфон Сайеда Фарука, хотя *Apple* категорически отказалась разрабатывать универсальный ключ.

Можно следить и за конкретным человеком, который по каким-то причинам интересен заказчику, например иностранному государству. Это может быть политик или чиновник, или бизнесмен, который знает что-то важное для заказчика. Сейчас несложно запустить вирус или троянскую программу в смартфон — с помощью предложения перейти по ссылке, поучаствовать в розыгрыше призов, просто через СМС. Разработчики средств подсаживания троянских программ — это специалисты по социальной инженерии. Это настоящие профессионалы, которые придумывают предложения, на которые клиент кликает — и все. Шпионская программа засела в смартфоне нужного человека и следит за всем, что происходит. Можно подключиться и к чужому компьютеру, в особенности, если человек повсюду ходит с ноутбуком. Вам он обязательно нужен в кафе? Если вы будете цепляться к *Wi-Fi* в любых местах, то обязательно подцепите какую-нибудь виртуальную гадость. Пусть вы не хранитель государственных секретов и даже корпоративных секретов, но деньги-то у вас какие-то есть. Вам же будет жалко их потерять. Поэтому неудивительно, что сейчас самые богатые и высокопоставленные люди на нашей планете вернулись к простым кнопочным телефонам.

Можно запустить шпиона не только в личные гаджеты, но и в корпоративную сеть. Хотя это гораздо сложнее, чем подключиться к конкретному смартфону или компьютеру. Если компьютер подключен к корпоративной сети и никуда не выносится из офиса, для внедрения в него троянской программы нужно взламывать корпоративную сеть.

Русских хакеров обвинили во взломе сервера демократической партии США перед выборами. Так ли виноваты русские хакеры, если они на самом деле получили информацию? Ведь перед тем как они что-то взломали (если взломали), были грубо нарушены правила безопасности. Не русские хакеры виноваты в том, что конфиденциальная информация была вынесена из секретной сети. Секретные данные оказались на домашнем компьютере. Разве в этом виноваты русские хакеры?

Сейчас много говорят о том, что хакеры могут реально влиять на происходящие в мире события. Да, могут! Кибервойна — это написание вирусных программ или кодов с целью выведения из строя инфраструктуры противника или воровства информации. В 2017 году кибератаки блокировали работу организаций в 150 странах мира, причем это были самые разные организации — операторы мобильной связи, государственные учреждения, больницы. Подобные атаки в современном мире анонимны, трудно установить организатора или инициатора. Отсюда и появляются обвинения «русских хакеров». Чаще всего атаки организуются на финансовые структуры, их количество растет. Инструменты, разработанные государствами для борьбы со своими противниками, могут быть похищены, причем иностранному шпиону теперь не нужно физически выезжать в чужую страну. Примером может служить кибератака, совершенная в 2017 году, в результате которой был похищен вирус *WannaCry,* разработанный в ЦРУ. Эта программа-вымогатель денежных средств даже получила титул «вирус года». От нее в общей сложности пострадало более 500 тысяч компьютеров.

Один из первых и самых известных примеров кибероружия — это вирус *Stuxnet.* Это компьютерный червь, поражающий компьютеры под управлением операционной системы *Microsoft Windows.* Этот компьютерный червь может быть использован для несанкционированного сбора данных и диверсий на промышленных предприятиях, электростанциях, в аэропортах. Это первый случай в истории, когда вирус физически разрушал инфраструктуру. Это очень высококвалифицированная разработка, в которой признались спецслужбы США и Израиля. Считается, что она была направлена против ядерного проекта Ирана. Американский журналист Дэвид Сангер в своей книге «Противостоять и скрывать: тайные войны Обамы и удивительное использование американской силы» утверждает, то это часть антииранской операции «Олимпийские игры», разработанной американским правительством. В 2011 году госсекретарь США Хилари Клинтон заявила, что проект по разработке *Stuxnet* оказался очень успешным, а иранская ядерная программа была отброшена на несколько лет назад. Израильтяне утверждали, что испытывали его в своем центре в пустыне Негев.

Вирус использовал четыре уязвимости системы *Microsoft Windows* и был обнаружен только через три года (от момента разработки до момента обнаружения). Это сделал белорусский эксперт Сергей Уласень из компании «ВирусБлокАда». За время действия вирус успел не только вывести из строя центрифуги на заводе по обогащению урана в Иране, но и заразить целый ряд объектов в разных частях света, например в Великобритании и России.

Обычно вирус обнаруживают гораздо быстрее — за несколько часов, а то и минут. Ситуация с *Stuxnet* — необычная и единственная в своем роде. Вероятно, дело в очень высокой квалификации разработчиков. Но в дальнейшем ни один разработчик не имеет контроля над вирусом — после того, как его «выпускает». И вирус может

поражать объекты не только в стране, против которой разрабатывался, но и в любой другой, включая страну-разработчика. Да и в большинстве случаев авторство компьютерных вирусов установить не удается. Если разработчик не хочет, то «национальность» вируса определить невозможно.

В большинстве развитых (и не только) стран мира в настоящее время созданы специализированные центры или подразделения, которые занимаются защитой от киберугроз, работают государственные системы обнаружения, предупреждения и ликвидации компьютерных атак. В первую очередь там занимаются угрозами, которые могут нанести урон государству как прямо, так и косвенно.

В Китае работает так называемый «Великий китайский файервол», который также называют золотым щитом. Он фильтрует всю поступающую извне информацию по Интернету. Разработка проекта началась в 1998 году, а внедрен он был по всей стране в 2003 году. В системе есть несколько подсистем, например, управление безопасностью, информирование о правонарушениях, управление трафиком, контроль за вводом информации и т. д.

Золотой щит ограничивает доступ к ряду иностранных сайтов с территории КНР. Например, в Китае не работает *Facebook.* Сайты, базирующиеся на территории КНР, не имеют права публиковать новости и даже ссылаться на новости с зарубежных сайтов или СМИ без специального предварительного одобрения. Фильтрация идет по ключевым словам, связанным с государственной безопасностью. Также есть черный список адресов сайтов.

То есть у китайцев получилась блокировка больших платформ, и извне управлять Китаем через информационные технологии невозможно. В Китае есть собственные социальные сети и различные системы. Но Интернет — это в любом случае международная сеть, и какие-то угрозы все равно будут распространяться.

Советы простому человеку

Если вы пользуетесь социальными сетями и любыми облачными хранилищами данных, вы должны понимать, что эта информация — публичная. Вы считаете, что вы никому не интересны, кроме родственников, друзей и работодателей. Вы пользуетесь смартфоном и регулярно заходите в социальные сети. Вы абсолютно уверены, что публикуемая вами информация никому не интересна?

Вы считаете, что общаетесь в социальных сетях только с узким кругом друзей. Нет. Вы выносите информацию на публику. До этой информации могут добраться миллионы людей. И у вас нет возможности контролировать дальнейшую жизнь вашей публикации. Даже если вы ее удалили, а кто-то успел скопировать, она будет жить своей жизнью без вас, и вы не можете на это повлиять. Вы что-то публиковали для узкого круга друзей, а ваш друг возьмет и представит эту публикацию миллионам или конкретным заинтересованным людям. И вы опять ничего не можете сделать. Так что очень хорошо думайте перед тем, как что-то выкладывать в Сеть. Ваши старые фото в стиле ню или просто фривольные через несколько лет могут помешать вам устроиться на хорошую работу.

Также не забывайте, что любой ваш современный гаджет принадлежит разработчику технологии. Что он в него встроил? Как он отреагирует, если вы попытаетесь внести изменения в операционную систему? У производителей платформ и разных приложений есть доступ к информации, которую вы храните в своих устройствах. По телефону можно определить ваше местоположение. Это кладезь информации о вас.

Что мы обычно загружаем на сайты типа *Facebook*? Там можно найти наши демографические данные, место жительства, семью и друзей, друзей друзей, интересы, пристрастия, образование, домашних животных, фотографии, видеозаписи и многое другое. Наш современник, выдающийся математик Стивен Вольфрам, создатель «вычислительного двигателя знания», известного так же, как *Wolfram Alpha,* разработал потребительский программный продукт, известный как «личная аналитика для *Facebook».* В течение всего лишь одной минуты этот программный продукт выдает колоссальный набор данных и графиков о вас и ваших социальных связях. Сам Вольфрам назвал это «приборной доской для жизни». Если вы зарегистрированы на *Facebook,* то советую вам посмотреть ваш личный вариант, это бесплатно: *http://www.wolframalpha.com/facebook/.* От того, что вы увидите, может стать немного неуютно, поскольку программа извлекает всю информацию, которую вы когда-либо размещали на *Facebook,* создает облачное хранилище данных из всех ваших постов, точного времени вашего захода и образа действий, ваших лайков и комментов, поста, который больше всего понравился, поста, который получил наибольшее количество комментов, демографических данных по всем вашим друзьям, включая карту мира с их местонахождением, местное время у них и дни рождения, карты ваших социальных связей, выделяя друзей и семью, влияния, соседей, социальные элементы соединения, случайных и близких людей.

Вы хотите, чтобы любой желающий мог это узнать? Если нет, думайте перед тем, как что-то пишете в Интернете или загружаете на своей страничке в социальной сети, даже для самого узкого круга.

Список использованных источников:

1. Просто Big Data. — СПб.: Страта, 2019. — 148 с.