УМНЫЕ УСТРОЙСТВА, КИБЕРСТРАХОВАНИЕ И УТЕЧКИ ДАННЫХ: НОВЫЕ ПРОБЛЕМЫ И НОВЫЕ РЕШЕНИЯ

Иванова Ангелина Петровна

Старший лаборант Отдела правоведения Института научной информации по общественным наукам РАН (ИНИОН РАН), (Москва, Россия)

Аннотация. *Практически повсеместные в настоящее время контакты людей с «умными» устройствами подвергают персональные данные пользователей множеству новых угроз. Для того чтобы справиться с информационными рисками, компании начали приобретать полисы киберстрахования. Помимо этого, представляется целесообразным введение уникального индивидуального идентификатора на основе технологии блокчейн и / или биометрических данных.*

Ключевые слова: *Интернет вещей; информационная безопасность; персональные данные; киберстрахование; блокчейн.*

Для цитирования: Иванова А.П. Умные устройства, киберстрахование и утечки данных: новые проблемы и новые решения // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 143–148.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.11

Введение

На сегодняшний день почти вся жизнь людей проходит во взаимодействии с интеллектуальными устройствами. Цифровизация создает особый взаимосвязанный мир, в котором люди подключены к Интернету вещей, включающему в себя «умные» телевизоры, термостаты, мобильные телефоны, автомобили и даже промышленные системы управления. Интеллектуальные помощники, такие как Siri, Google Now и другие, не отключаются никогда, реагируя в любое время на голосовые команды, например, «Okay, Google» [Privacy and liberty …, 2017, p. 36]. Однако вместе с удобствами гаджеты привносят в нашу жизнь и новые угрозы – угрозы кибербезопасности. Увеличивается опасность кибератак, которые могут иметь различные формы в зависимости от цели их совершения.

Информационная безопасность

В целом понятие «Интернет вещей» довольно неоднозначно и различается в зависимости от того, какой ученый или правительственное учреждение дает ему определение. Один из подходов представляет Интернет вещей как «расширение глобальной инфраструктуры за счет развивающихся информационно-коммуникационных технологий, которые включают в себя взаимосвязь физических и виртуальных систем с другими системами» [DiGrazia, 2018, p. 257]. И хотя большинство людей слышали об Интернете вещей, не все из них понимают, как он влияет на них. Многие потребители могут вовсе не осознавать объем данных, собираемый их устройствами. В большинстве случаев они не знают, какие возможности есть у постоянно активных девайсов. В то время как эти устройства являются частью Интернета вещей и могут быть каналом для проникновения хакеров в дома своих владельцев.

Угроза раскрытия личной информации становится все более реальной в жизни современного общества. В сентябре 2017 г. бюро кредитных историй Equifax объявило, что его база данных была взломана. В результате этого под угрозу была поставлена конфиденциальная информация примерно 143 млн американских потребителей, что составляет около 44% населения. Хакеры смогли получить доступ к «именам людей, социальным сетям, номерам социального страхования, датам рождения, адресам, и, в некоторых случаях, номерам водительских удостоверений» [Marcus, 2018, p. 556]. В результате атаки вируса-шифровальщика WannaCry хакеры смогли за несколько дней взломать более 300 тыс. компьютеров более чем в 150 странах мира, включая компьютеры многих больниц, которые лишились доступа к медицинским записям пациентов. Вирус использовал уяз-

вимости операционной системы Microsoft Windows и шифровал файлы в компьютерах до тех пор, пока пользователь не платил «выкуп» [DiGrazia, 2018, p. 269].

Эти два инцидента иллюстрируют потенциал катастрофического воздействия, которое один хакер может оказать на миллионы людей по всему миру. Основными целями субъектов киберпреступлений являются банковские и валютно-обменные платформы. По официальным данным, в 2015 г. в результате киберкраж было похищено более 300 млн долл. Однако, по оценкам компании «Лаборатория Касперского», специализирующейся в области компьютерной безопасности, реально эта сумма может быть в три раза больше [DiGrazia, 2018, p. 268].

Первостепенное значение для обеспечения национальной безопасности имеет отражение кибератак на автоматизированные системы управления, которые рассматриваются в качестве одной из самых больших угроз. Автоматизированные системы управления обычно определяются как «различные типы систем управления и связанных с ними контрольно-измерительных приборов, которые включают в себя устройства, системы, сети и средства управления, используемые для автоматизации производственных процессов» [DiGrazia, 2018, p. 270]. В настоящее время они применяются практически во всех сферах человеческой деятельности, от сферы общественного питания до фармацевтики. В 2014 г. хакеры продемонстрировали, что имеют возможность получить доступ к автоматизированным системам. Так, была взломана система немецкого сталелитейного завода, а также система управления дамбой в северной части штата Нью-Йорк [DiGrazia, 2018, p. 271].

Согласно отчету страховой компании Lloyd Emerging Risk за 2015 г., кибератака на энергосистему США может обойтись национальной экономике в более чем 1 трлн долл и более чем 70 млрд долл – для страховых компаний. Основная проблема киберрисков (которая не была отражена в данном отчете) заключается в том, что они не ограничены физическими границами и могут причинить огромный вред при минимальных затратах со стороны хакера – достаточно всего нескольких строк вредоносного кода [DiGrazia, 2018, p. 267].

Причин успешности кибератак множество. Главная из них – недостаток знаний о том, как управлять кибербезопасностью (неосведомленность о методах борьбы с манипулятивной деятельностью или отсутствие соответствующих навыков правоприменения), что приводит к недостатку внимания, уделяемого этим вопросам.

Способы противостояния киберугрозам

По данным страховой компании Allianz, киберпреступность обходится мировой экономике в 445 млрд долл. в год [DiGrazia, 2018, p. 261]. Для того чтобы справиться с киберрисками, многие компании начали приобретать полисы *киберстрахования*.

Страхование помогает частным лицам и компаниям справиться с неизбежными и постоянными рисками. Полисы киберстархования – это относительно новый страховой продукт, предназначенный для освобождения застрахованного лица от расходов, связанных с хакерством, кибератаками и утечками данных. Они обычно подразделяются на две основные категории: страхование «первой» и «третьей» стороны. Первое подразумевает покрытие расходов на уведомления о нарушении конфиденциальности данных, кредитный мониторинг, операционные расходы, смягчение репутационного ущерба. Второе включает покрытие расходов, связанных с привлечением к ответственности (штрафы, мировые соглашения и т.д.).

Необходимость киберстрахования в последнее время стала предметом многочисленных дискуссий. Некоторые считают, что суммы денежных средств, которые компании платят в качестве страховых премий, сопоставимы с суммами, которые они вынуждены заплатить для устранения последствий кибератак и утечек данных. Более того, компании, возможно, могли бы предотвратить кибератаки, если бы использовали деньги, потраченные на киберстрахование, для укрепления защиты своих информационных сетей [DiGrazia, 2018, p. 260]. Другие считают, что киберстрахование является хорошей инвестицией для малого и среднего бизнеса, который может серьезно пострадать от кибератак, но не имеет финансовых возможностей для проведения аудита IT-рисков и предотвращения кибервторжений.

На самом деле, малый и средний бизнес стали главной мишенью для хакеров, потому что не имеют опыта или средств, которыми располагают крупные компании для защиты своих сетей. Киберстрахование может быть ценным вложением и для крупных компаний, которые имеют дело с большим количеством данных, таких как организации розничной торговли, медицинские организации, финансовые компании и т.д. При этом фирмы, приобретающие киберстраховки, должны понимать, какие расходы будут покрывать их страховые полисы, а какие могут дублировать страховые покрытия, и какие риски остались незастрахованы.

Например, в США большинство действующих полисов страхования гражданской ответственности основаны на стандартных формах, разработанных Управлением в сфере страхования (Insurance Service Office – ISO). Современные полисы охватывают три области расходов: имущественная ответственность и ответственность за причинение вреда здоровью; ответственность за нарушения в сфере рекламы; медицинские выплаты. Несмотря на то что сфера киберстрахования является относительно новой, базовые элементы страховых полисов неоднократно пересматривались страховыми компаниями и судами. Ввиду этого ISO определило, что раз в несколько лет необходимо менять стандартные формы полисов.

Модели потерь, используемые страховыми компаниями для таких полисов, как страхование автомобилей, страхование жизни и страхование жилых помещений, позволяют предсказать ожи-

даемый убыток на основе агрегирования большого числа независимых рисков, неоднократно повторяющихся в течение длительного периода времени. В настоящее время страховые компании разработали сложные инструменты моделирования и, как правило, имеют возможность предвидеть убытки, связанные со стихийными бедствиями. Хотя в 2005 г. некоторые из них были застигнуты врасплох и понесли серьезные убытки в результате урагана «Катрин». Вместе с тем потери от крупного инцидента в цифровом мире, например потери от утечки данных, могут не быть локализованы на территории одной стороны, что делает такие инциденты гораздо опаснее для страховых компаний [DiGrazia, 2018, p. 269].

Пример вируса WannaCry продемонстрировал, что даже при наличии надежного рынка перестрахования масштабная кибератака может привести к банкротству как первичных страховых компаний, выпускающих полисы, так и перестраховщиков. Это происходит потому, что страховые компании пытаются выпускать полисы для покрытия угроз, создаваемых людьми, которые, как правило, трудно моделировать и страховать.

Используемая в киберпреступлениях уязвимость провоцирует массовый каскадный эффект, приводящий к триллионам застрахованных убытков. В результате возникают значительные проблемы у страховых компаний, которые оформляют полисы киберстрахования. Хакерские действия могут вызвать цепь событий, влекущих за собой выплату страхового возмещения по разным видам страхования: киберстрахованию, страхованию жилых помещений и даже полисам автострахования. Вероятность массовых правонарушений, связанных, например, с использованием номеров социального страхования в США, ставит под угрозу компании, хранящие эти данные. Отрицательные последствия имеют место и для потребителей: им приходится тратить значительные средства на оплату постоянного кредитного мониторинга, предотвращение рисков кражи личных данных и возможность быстрого замораживания счетов.

Диверсификация рисков на рынке киберстрахования потребовала углубленного сценарного анализа потенциальных рисков, связанных с киберпреступлениями. Как выяснилось, действующие в настоящее время страховые полисы не соответствуют миру с Интернетом вещей. Ввиду несовершенства существующих методов идентификации отдельных лиц в гражданском обороте высказывается мнение о необходимости перейти к альтернативным способам.

Одним из наиболее популярных вариантов, предлагаемых экспертами по обеспечению безопасности, является *использование многофакторной биометрии* для идентификации человека, такой как распознавание голоса / лица, сканирование радужной оболочки и т.д. Другая альтернатива – это *применение технологии блокчейн*, которая позволяет создать «публичный регистр транзакций» [DiGrazia, 2018, p. 272].

Технология блокчейн уже применяется Эстонией в качестве основы для цифровой идентификационной системы в сфере медицинских услуг, на контрольно-пропускных пунктах, а также для голосования на выборах. Такие компании, как IBM и SecureKey, используют блокчейн при разработке идентификационных решений, основанных на «ориентированной на пользователя модели, также известной как суверенная идентичность», которая позволяет пользователям контролировать количество лиц, имеющих доступ к их личной информации [DiGrazia, 2018, p. 276].

Переход на систему идентификации на основе блокчейн, возможно, был бы оптимальным решением для стран с большой численностью населения, поскольку она не требует от правительства сбора биометрических данных граждан, но позволяет предотвратить мошеннические транзакции. Преимущество использования алгоритмов блокчейн заключается также в том, что по мере совершенствования технологий взлома алгоритмы могут совершенствоваться вместе с ними.

Одним из наиболее значимых препятствий на пути внедрения блокчейн-технологий является опасение, что цифровые записи будут умышленно изменены или уничтожены. Однако данный аргумент носит спорный характер, поскольку зашифрованный публичный реестр, в котором хранятся данные, технически не может быть уничтожен или переписан.

Заключение

Благодаря Интернету вещей возник мир, где почти все, что делают люди, зависит от информации и взаимосвязанных компьютерных систем. При этом растущее количество и масштабы кибератак свидетельствуют о значительности ущерба, к которому приводят инциденты в цифровой сфере. Вместе с тем в настоящее время существуют и меры, которые государства, бизнес и физические лица могут предпринять для своей защиты.

Во-первых, компании могут использовать альтернативный уникальный идентификатор пользователей на основе технологии блокчейн и / или биометрических данных. Во-вторых, страховые компании могут стимулировать организации к повышению уровня безопасности данных, предлагая более выгодные тарифы тем, кто внедряет более надежные механизмы защиты. Однако следует помнить о массовом каскадном эффекте, которым обладают инциденты в цифровой сфере ввиду высокого уровня ее взаимосвязанности.

Список литературы

DiGrazia K. Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach // Journal of Business & Technology Law. – Baltimore, 2018. – Vol. 13, N 2. – P. 255–277.

Marcus D.J. The data breach dilemma: proacrtive solutions for proptecting consumers' personal information // Duke law journal. – Durham, NC, 2018. – Vol. 68, N 555. – P. 555–593.

Privacy and liberty in an alaways-on, always-listening world / Bohm A.S. and other // The Columbia science and technology law review. – New York, 2017. – Vol. 19, N 1. – P. 1–45.