ТЕХНОЛОГИИ 02.07.2021 08:31

Побочное явление цифровизации: как в России крадут и продают персональные данные



Анастасия Скрынникова

Forbes Staff

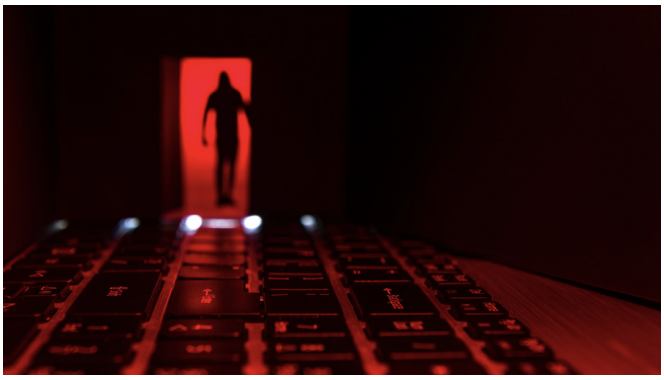

Фото Getty Images

В 2020 году в судах было рассмотрено 43 дела о сливе личных данных россиян, а за первое полугодие 2021-го было всего пять таких дел. Однако опрошенные Forbes эксперты утверждают, что черный рынок персональных данных растет в России каждый год, а его лидерами остаются финансовый сектор и телеком-компании

Сколько данных утекло

С января по сентябрь 2020 года в России утекло 96,5 млн записей персональных данных и платежной информации (по данным компании

InfoWatch). При этом доля утечек, связанных с мошенническими действиями, превышает 10% — в мире этот показатель втрое ниже.

Черный рынок персональных данных постоянно растет, а основной причиной этого являются инсайдеры — сотрудники компаний, которые продают или отдают бесплатно конфиденциальные данные своих клиентов, говорится в исследовании ИТ-компании «Крок» (есть у Forbes). В 2020 году общий ущерб от утечек личных данных превысил 3 млрд рублей, следует из материалов «Крок».

Количество публикаций о раскрытых делах, связанных с хищениями данных, в 2020 году выросло в два раза по сравнению с 2019 годом, рассказывал технический директор DeviceLock и владелец Telegram-канала «Утечки информации» Ашот Оганесян. Абсолютный лидер по краже данных в 2020 году — сотрудники сотовых операторов и салонов мобильной связи, как и в 2019 году, писал Оганесян. В 2020 году доля этого сегмента выросла с 44% до 67%, а доля банковских работников, занимающих второе место, наоборот, упала с 27% до 18%.

У такого роста операторских хищений есть несколько причин, указывает Оганесян: низкий уровень зарплат сотрудников фронт-офисов и салонов связи, а также легкость, с которой можно вычислить преступников. Злоумышленники, которые работали в салонах связи, продавали украденные данные не скрываясь и часто своим знакомым. Это позволяло правоохранителям без труда находить таких продавцов, а потом производить контрольную закупку, рассказывал эксперт.

За «Глазом Бога»: кто создал главный в России сервис для поиска персональных данных и почему его не закрывают

Как сливают данные

Проблема криминального пробива данных сегодня актуальна для всей России, хотя чаще всего этим промышляют сотрудники операторов связи, менеджеры банков и госслужащие в регионах, рассказал Forbes руководитель направления аналитики и спецпроектов ГК InfoWatch Андрей Арсентьев. Это связано как с более низким уровнем защищенности информационных ресурсов, так и с невысокими

зарплатами, рассуждает Арсентьев. Его слова подтверждают данные системы ГАС «Правосудие»: согласно информации из нее, в 2020 году было рассмотрено 43 дела по уголовной статье 138 ч. 2 — нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. В этом году таких дел пока только пять.

В мае 2020 года специалист офиса «Вымпелкома» в Казани Бурлак М.В. получил штраф в размере 120 000 рублей за то, что пробивал и отправлял своему знакомому данные о звонках его бывшей жены, следует из материалов суда. Бурлак делал это бесплатно, а также привлек к пробиву свою коллегу, имя которой не раскрывается. Информацию о звонках Бурлак пересылал заказчику через мессенджер WhatsApp. Когда потерпевшая поняла, что бывший муж в курсе деталей ее общения по мобильному телефону, она написала жалобу в «Вымпелком». Позже с ней связалась служба безопасности оператора и ФСБ, говорится в материалах дела. Судебные дела в отношении бывшего мужа потерпевшей и еще одной сотрудницы «Вымпелкома», фигурировавшей в деле, еще ведутся.

Другой похожий случай произошел в Якутии, где в июне 2020 года продавец офиса одного из мобильных операторов Патранжел В.О. получил наказание в виде 200 часов общественных работ за то, что слил звонки абонента за один месяц. В июле 2019-го Патранжелу написал интернет-пользователь с просьбой прислать список исходящих и входящих звонков с определенного номера за июнь того же года. Патранжел вошел в программу просмотра детализации звонков ССВО, использовав свой служебный логин и пароль, ввел номер телефона и получил информацию о звонках. После этого преступник скопировал данные в Excel, загрузил на свой мобильный телефон и отправил заказчику. Сколько денег за такую «работу» получил Патранжел, в документах суда не указано, его разработкой также занималось ФСБ. Личность заказчика установить не удалось.

«Большинство сотрудников не задумываются о том, что их мессенджеры контролируют»: как в России сливают конфиденциальную информацию и что за это бывает

Сколько стоят данные

Пробив — это побочное явление цифровизации: она повысила качество жизни, но создала новые риски, говорит Арсентьев из InfoWatch. Каждая единица персональных данных сейчас имеет цену на черном рынке, указывает он. Услуга мобильного пробива, то есть продажа данных об абонентах сотовых компаний, пользуется устойчивым спросом в даркнете, добавляет эксперт. В зависимости от объема детализации справка об одном абоненте может стоить от 500 рублей до нескольких десятков тысяч, говорит он.

Основные факторы расцвета мобильного пробива — высокий спрос на услугу, менеджеры с невысокими зарплатами, дыры в информационной безопасности сотовых компаний и не слишком строгая ответственность за подобные преступления, отмечает Арсентьев. Как правило, осужденные пробивщики отделываются штрафом в размере до 100 000 рублей или условным сроком.

Огромной популярностью в даркнете пользуются базы данных, которые были украдены в различных государственных и коммерческих организациях, добавляет ведущий специалист отдела аудита Infosecurity a Softline Company Анатолий Сазонов. По его словам, цены на такие базы персональных данных зависят от состава и количества данных, их стоимость в среднем начинается от $100-$200. Стоимость данных клиентов банков варьируется от трех рублей до 120 рублей за запись, цена за разворот российского паспорта начинается от $1, заграничного — от $2,5 (по данным Infosecurity a Softline Company).

Новые объявления о продаже баз данных появляются в даркнете каждый день, однако далеко не всегда это какие-то ценные сведения, рассказал Forbes автор Telegram-канала в сфере инфобезопасности In4security. Часто это результат компиляции из более старых утечек или парсинг открытой информации, добавил он.

Прохудившиеся банки: можно ли остановить утечки персональных данных

Что делают операторы и банки

Продажа или передача персональных данных клиентов для компаний — это в первую очередь репутационные потери, говорит гендиректор «ТМТ Консалтинга» Константин Анкилов. Но на решение этой

проблемы операторы тратят и деньги — они вынуждены держать увеличенный штат службы безопасности, который занимается проблемой утечек, а также тратиться на судебные издержки, когда такие дела доходят до суда, говорит эксперт. Чтобы снизить число утечек, нужно перестраивать систему доступа сотрудников к данным абонентов, считает гендиректор Telecom Daily Денис Кусков. По его словам, нужно внедрить такие решения, чтобы никто не мог получить информацию о звонках клиентов, например, без предъявления специальных кодов, которые бы показывали целесообразность получения данных. Если этого не сделать, то рынок мобильного пробива будет существовать еще много лет, сетует Кусков.

Сейчас для предупреждения утечек компании внедряют системы, использующие машинное обучение, чтобы определить наиболее вероятные каналы утечек и сотрудников, которые потенциально могут стать инсайдерами, говорит ведущий эксперт направления информационной безопасности «Крок» Александр Черныхов. Для расследования утечек сейчас разрабатываются системы цифровой маркировки документов и интерфейсов, это помогает и в поиске инсайдеров, отметил он.

Представитель «Сбера» рассказал Forbes, что за 2020 год в компании не обнаружили ни одного случая утечки персональных данных от сотрудников банка. Это стало возможным благодаря «новой архитектуре процессов по противодействию утечкам», отметили в «Сбере», но не раскрыли подробности работы с этой проблемой. В МТС есть архитектурное разграничение доступов к информации, также разработан полный комплекс технической защиты от распространения персональных данных — это программно-технические средства контроля доступа и постоянный мониторинг, рассказал представитель оператора. Он добавил, что компания также рассказывает сотрудникам о том, что нельзя допускать посторонних к защищаемой информации, и о том, что за это грозит уголовная ответственность.

Представитель «Вымпелкома» рассказал, что оператор не терпит никакие формы нарушения приватности персональных данных своих пользователей. Компания готова сотрудничать с уполномоченными органами в части расследования подобных нарушений, добавил он. Представитель «Мегафона» отказался от комментариев.

Представитель «Т2 РТК Холдинга» (бренд Tele2) не ответил на запрос Forbes.

Утечка данных и риск отзыва лицензии: банки назвали главные угрозы от кибератак

Чем грозит продажа личных данных

Как правило, незаконные действия с персональными данными в текущей практике используются в рамках уголовных дел о мошеннических действиях (в основном дистанционным способом), объясняет партнер фирмы «Рустам Курмаев и партнеры» Дмитрий Горбунов. Согласно официальной статистике, только в 2020 году суды рассмотрели более 36 500 дел о мошенничестве, что на треть выше уровня 2019 года, при этом в 60% суды выносили обвинительный приговор. Пока за 2021 год не появилось такой же статистики, но вполне можно ожидать рост подобных дел на 25-30%, предполагает Горбунов.

Если обнаружится утечка несущественных персональных данных, человеку грозит штраф до 50 000 рублей, а юридическому лицу — до 6 млн рублей, говорит управляющий партнер юридической компании AVG Legal Алексей Гавришев.

Наказание за нарушение тайны телефонных переговоров и переписки может составлять до четырех лет лишения свободы, отметил Гавришев. Кроме того, информация, которая проходит через оператора связи, чаще всего является коммерческой тайной, а ее разглашение карается лишением свободы на срок до пяти лет, добавил юрист.