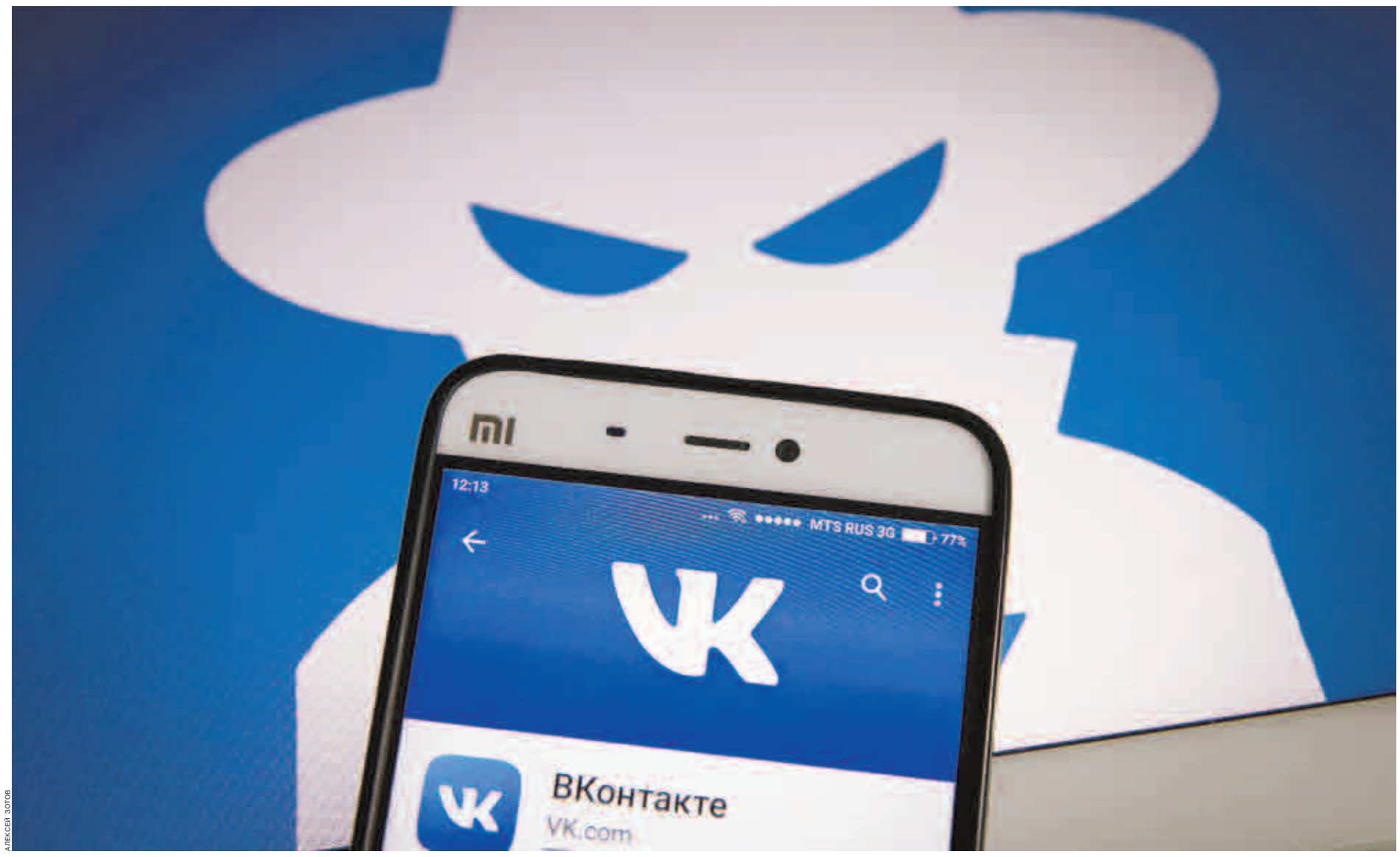
Опасные сети

В конце апреля основатель Facebook Марк Цукерберг объявил о первом в истории соцсети масштабном преобразовании: он пообещал, что изменится не только дизайн страницы, но и уровень конфиденциальности. К этому моменту руководство соцсети уже несколько раз признавало утечку персональных данных своих пользователей. Но если в Европе и США Facebook и другим IT-гигантам грозят серьезные штрафы за «утерю» паролей и адресов электронной почты, то в России за такое нарушение нет строгой ответственности. Параллельно с этим мир потрясают скандалы, вызванные небезопасностью интернета вещей: взламывая «умные» устройства, злоумышленники превращают их в шпионов и даже получают контроль над финансами пользователей.



АЛЕКСЕЙ ЗОТОВ

Граждане не относятся к персональным данным с должным вниманием, и строгой ответственности за нарушение их хранения не предусмотрено

— информбезопасность —

«Скандал на миллионы евро»

540 млн записей пользователей Facebook стали доступны для скачивания на открытой облачной платформе Amazon, сообщила в начале апреля австралийская компания по кибербезопасности UpGuard. Названия учетных записей, действия пользователей, их лайки и другую личную информацию собирала мексиканская цифровая платформа Cultura Colectiva: эта информация хранилась в облаке Amazon. База другой, уже не работающей площадки — приложения At the Pool — содержала имена, пароли, информацию о любимых фильмах и книгах, фотографии, а также адреса электронной почты 22 тыс. пользователей соцсети. Доступ к базам был закрыт уже после того, как журналисты Bloomberg предупредили Facebook об утечке.

Штраф Facebook выписало в конце 2018 года и антимонопольное ведомство Италии, обязав соцсеть заплатить €10 млн за использование в коммерческих целях данных своих пользователей. Затем к числу стран, которые недовольны действиями соцсети, присоединилась Турция: управление по защите персональных данных оштрафовало Facebook на $270 тыс. за нарушения конфиденциальности фотографий пользователей. При этом большую часть суммы компания должна заплатить за то, что не приняла мер после того, как получила предупреждение о нарушении закона.

В будущем соцсети могут грозить новые выплаты: в апреле расследование против Facebook начала прокуратура Нью-Йорка из-за несанкционированного хранения электронных почт и контактных данных 1,5 млн пользователей. Перед этим Facebook призналась, что может непреднамеренно загружать контакты в электронных почтах пользователей, которые регистрировались в соцсети с мая 2016 года.

Помимо ущерба компании такие утечки непосредственно влияют на безопасность пользователя. Данные — особенно те, что связаны с платежной информацией, — могут монетизировать злоумышленники, поэтому интерес со стороны киберпреступного мира к ним по-прежнему высокий, рассказывает руководитель российского исследовательского центра «Лаборатории Касперского» Юрий Наместников. Личные данные пользователей могут использовать фишеры (технически подкованные злоумышленники): имея подробную информацию о человеке, намного легче как провести успешную целенаправленную кибератаку на него самого, так и в дальнейшем попасть в сеть компании, в которой он работает, добавляет эксперт.

Радионяня-шпион

Facebook — не единственный IT-гигант, который сталкивается с проблемами, связанными с защитой и хранением конфиденциальной информации. Google и ее «дочки» также вынуждены защищаться от критики, вызванной утечкой персональных данных. Камеры видеонаблюдения, радионяни, дроны, «умные» колонки, бытовые приборы с выходом в интернет — эти устройства все чаще используют семьи по всему миру. Такие гаджеты становятся новыми мишенями для хакерских атак, особенно в США, где каждый третий потребитель владеет двумя и более устройствами для «умного» дома.

На рубеже 2018 и 2019 годов Америку потрясли скандалы, вызванные взломами камер фирмы Nest (принадлежит Google), установленных в радионянях. Например, в январе в Калифорнии американка Лаура Лайонс находилась дома, когда ее «умная» камера предупредила, что на Лос-Анджелес, Чикаго и Огайо были направлены три северокорейские ракеты. В сообщении говорилось, что США принимают ответные меры, а люди в зоне поражения должны быть эвакуированы в течение трех часов. Когда Лайонс включила телевизор, чтобы узнать подробности, то не нашла никакой информации о предстоящей атаке. Ничего о ней не знали и в службе спасения. После звонка в службу поддержки Nest женщина поняла, что стала жертвой хакерского взлома.

Если злоумышленники взломают устройство «умного» дома, то они могут долгое время записывать информацию о пользователях — таким образом, помощники под управлением мошенников становятся шпионскими устройствами, предупреждает аналитик ГК InfoWatch Андрей Арсентьев. Домашний интернет вещей может быть использован для дестабилизации комфортного существования: взломав «умные» датчики температуры, злоумышленники получают контроль над изменением климата в комнате, а взломанный «умный» замок кардинально меняет свою функцию и становится отмычкой к дверям дома, отмечает он. «Страшно представить, к каким последствиям приведет внешнее управление „умным“ автомобилем или подключенным к сети кардиостимулятором»,— говорит эксперт.

После серии взломов устройств Nest в начале текущего года компания разослала своим пользователям предупреждение и попросила придумать «сильный» пароль к домашней камере видеонаблюдения и защитить ее двухфакторной аутентификацией.

Деньги пользователя могут оказаться под угрозой в том случае, если взломанные устройства интегрированы с платежными системами, при этом не требуют подтверждения трансакции, отмечают в InfoWatch. Если холодильник запрограммирован на автоматический заказ молока, то, когда в нем не останется ни одного пакета, теоретически возможно изменить параметры оплаты и совершить мошеннический платеж. Выход для пользователя здесь в использовании технологии токенизации: она позволяет совершать безопасные мобильные платежи путем шифрования данных, заключает господин Арсентьев.

Инциденты с нарушением прав пользователей в области персональных данных подтолкнули европейских законодателей начать заботиться о своих гражданах: после четырех лет обсуждений в 2018 году в ЕС вступил в силу закон об усилении ответственности за нарушения в области персональных данных (General Data Protection Regulation). Санкции за его неисполнение грозят компании максимальным штрафом до €20 млн или 4% от глобального оборота компании. Из-за этого суммы, которые начали выплачивать компании, значительно выросли.

Заткнуть утечку

Говорить о том, какая индустрия больше всего страдает от утечек данных, сложно, так как личную информацию клиентов сегодня хранит и обрабатывает большое количество организаций, работающих совершенно в разных областях, говорит Юрий Наместников. При этом в России компании действительно стали аккуратнее относиться к обработке и хранению данных — это произошло после принятия законов «О персональных данных» и «О безопасности критической информационной инфраструктуры».

В 2018 году в мире наиболее громкие случаи утечек, связанные, в частности, с платежными данными пользователей, происходили в финансовых организациях и онлайн-магазинах, а также в ресторанных и отельных сетях, через которые ежедневно обрабатывают большое количество платежных данных пользователей, добавляет господин Наместников. Но защита собственных данных особенно актуальна для российских пользователей: если в Европе и США за утечку информации пользователей компаниям грозят большие штрафы, то в России такая практика еще не сложилась: и сами граждане не относятся к персональным данным с должным вниманием, и строгой ответственности за нарушение их хранения не предусмотрено, говорит адвокат Forward Legal Данил Бухарин.

Административный штраф в России значительно меньше, чем в Европе: для организации он ограничен суммой 75 тыс. руб., отмечает юрист. За весь 2018 год Роскомнадзор составил всего 30 административных протоколов в случаях, когда оператор персональных данных не обеспечил безопасные условия их хранения и это привело к неправомерному доступу к личной информации. Отдельный вид ответственности за нарушение требований к сбору и хранению персональных данных россиян — это блокировка иностранного интернет-ресурса по требованию Роскомнадзора и решению суда. Например, в августе 2016 года в России был заблокирован LinkedIn.

Более серьезные санкции предусмотрены в Уголовном кодексе, но к уголовной ответственности возможно привлечь только физических лиц. За неправомерное копирование персональных данных могут лишить свободы на срок до семи лет, однако доказать наличие состава такого преступления крайне сложно, подчеркивает господин Бухарин. Если же компания незаконно передаст третьим лицам персональные данные клиента, с нее могут потребовать возмещения убытков или компенсации морального вреда. Суды удовлетворяют подобные иски, но суммы взысканий небольшие: моральный вред оценивается не дороже 30 тыс. руб.

Ирина Юзбекова

РОССИЙСКИЙ РЫНОК ВЫСОКОТЕХНОЛОГИЧНЫХ ХИЩЕНИЙ

ИСТОЧНИКИ: GROUP-IB, ДАННЫЕ ЗА 2-Ю ПОЛОВИНУ 2017 — 1-Ю ПОЛОВИНУ 2018 ГОДА.

Сегмент рынка	Количество групп	Успешные атаки в день	Средняя сумма одного хищения (руб.)	Средняя сумма хищений в день (руб.)	H2 2017 — H1 2018 (руб.)
Хищения у юрлиц с троянами для ПК	3	2	1,1 млн	2,2 млн	547,8 млн
Хищения у физлиц с Android-троянами	8	100	7 тыс.	770 тыс.	191,73 тыс.
Целевые атаки на банки	3		118 млн		1303,9 млн
Фишинг	26	108	1 тыс.	1,008 млн	251 млн
Обналичивание похищенных средств				1,336 млн	919,5 млн
ИТОГО				**3,114** млн	**3214** млн

Сага о Big Data

— большие данные —

с16

Регулировать нельзя оставить

Считая саморегулирование больших данных недостаточным, власти настаивают на регулировании этой сферы. Законопроект, закрепляющий определение больших пользовательских данных, их оператора и вводящий правила их обработки, был внесен в Госдуму еще в октябре 2018 года депутатом от «Единой России» Михаилом Романовым. Однако отрасль раскритиковала документ: по мнению экспертов, это увеличит нагрузку на бизнес и может усугубить технологическое отставание России. В результате комитет Госдумы по информполитике решил вернуть законопроект его автору.

Помимо этого, в госпрограмме «Цифровая экономика» предусмотрена разработка законопроекта, устанавливающего правила и порядок доступа к общедоступным данным. Минэкономики планировало внести документ в правительство до конца 2018 года, но он так и не был подготовлен. Власти рассматривали три концепции регулирования. Первая закрепляла за площадкой, собирающей данные, права на управление размещенными на ней данными. Модель поддерживали крупные игроки. Вторая концепция предусматривала свободную обработку общедоступных данных, размещенных на платформах, без согласия их субъектов. Это было бы выгодно стартапам, которые зарабатывают на сборе данных и оказании услуг по их анализу.

Третий вариант не предусматривал введения дополнительного регулирования, а ограничивался введением дополнительных соглашений между крупными интернет-площадками и третьими лицами. Но власти до сих пор однозначно не определились в выборе модели. Сейчас концепцию управления данными готовит центр компетенций «Сколково», а предложения к ней были подготовлены АНО «Цифровая экономика».

Бизнес борется за Data

Параллельно с инициативами в части регулирования выступают и другие бизнес-объединения. Так, в январе ФРИИ подготовил законопроект, вводящий в законодательство термин «персонализированные данные» и предлагающий обеспечить их свободное обращение на рынке. Иными словами, граждане смогут предлагать бизнесу свои данные с определенной целью и сроками за вознаграждение в различных формах и тем самым зарабатывать до 60 тыс. руб. в год. Пользователь сам должен распоряжаться своими данными, решать, кому их передавать, согласна Светлана Белова. «Для этого надо предоставить гражданину удобный интерфейс для доступа к своим данным, хранящимся в ГИСах и у бизнеса, как это уже реализовано у „ВКонтакте“, Facebook, Telegram и других платформ»,— считает она. «Все, что может привести к возможности нарушения прав и свобод владельцев персональных данных, должно быть четко урегулировано, в том числе их оборот, а все, что касается собственно данных, которые не могут содержать информацию ограниченного доступа, в том числе персональных данных, очевидно, может быть отдано на откуп отрасли»,— полагает Александра Орехович.

Созданная в октябре прошлого года АУРБД (объединяет «Ростелеком», «Яндекс», Mail.ru Group, Сбербанк, Газпромбанк, Тинькофф-банк, «Мегафон», oneFactor и Qiwi), напротив, выступает за саморегулирование в сфере оборота Big Data. «Мы совместно с Институтом развития интернета готовим кодекс использования данных, который станет обязательным для всех участников организации»,— напомнила Анна Серебряникова. По ее словам, он должен стать актом отраслевого саморегулирования, закрепляющим не предусмотренные законодательством правила работы с массивами данных.

По оценке Николая Легкодимова, основная опасность в регулировании этой сферы заключается как в расширительном толковании того, что такое большие данные по отношению к человеку, так и в возможности выводить приватную информацию о человеке исходя из данных, которые сами по себе персональными не являются. Объемы обработки Big Data и современные механизмы позволяют, например, на основе знаний о районе проживания и истории пары покупок идентифицировать человека с точностью до ФИО, отмечает он: «В США были случаи, когда использование таких технологий приводило к поимке преступников». В то же время, если говорить о России, в силу модели взаимодействия гражданина и государства наши власти всегда будут стремиться к тому, чтобы быть владельцем и контролером таких данных, считает он: «Это неудивительно, ведь, например, аналитикой, которую дают телекомкомпании, можно пользоваться для управления электоратом». Именно в таком скрытом влиянии на предвыборный процесс обвиняют Cambridge Analytica и сторонников «Брексита», напоминает эксперт.

Юлия Тишина

Генеральный директор АО «Коммерсантъ», главный редактор газеты «Коммерсантъ» Владимир Желонкин | **Руководитель дирекции по развитию** Владимир Лавицкий | **Директор фотослужбы** Сергей Вишневский | **Генеральный директор АО «Коммерсантъ-Сибирь»** Ольга Добарская | **Главный редактор АО «Коммерсантъ-Сибирь»** Елена Морозова | **Выпускающий редактор** Лолита Белова | **Верстка** Тамара Крохолева | **Корректура** Юлия Носырева | **Дирекция по рекламе** Наталья Артемова тел. (383) 223-03-93, 209-34-42 | **Цветное приложение «Технопром» является составной частью газеты АО «Коммерсантъ»** | Учредитель АО «Коммерсантъ» | Адрес: 127055, г. Москва, Тихвинский пер., д. 11, стр. 2 | **Адрес редакции:** 630099, г. Новосибирск, ул.Октябрьская, д. 52, 4-й этаж, тел. (383) 223-03-93 | Отпечатано в Владивостокском филиале ООО «Типографии «Комсомольская правда», Приморский край, г. Владивосток, улица Жигура, 11 | Тираж 3800 экз.