Опасно. Еще опаснее!

Марат САФИУЛИН,
управляющий
Федеральным фондом
по защите прав вкладчиков
и акционеров

Комплекс разнообразных проблем, которые породили санкции, может обострить ситуацию с безопасностью частных инвесторов и потребителей финансовых услуг.

МАСШТАБ ПРОБЛЕМЫ

Во второй половине 2020 года интернет-ресурс Cybersecurity Ventures сделал прогноз, что в 2021 году ущерб от киберпреступности в мире должен составить $6 трлн. Это составляет примерно $755 на каждого жителя планеты. Издание описывает базовый сценарий, по которому в ближайшей перспективе рост киберпреступлений составит не менее 15 % в год. К 2025 году мировые издержки от киберпреступности составят $10.4 трлн, то есть примерно по $1300 на каждого из нас. Кстати, сегодняшние $6 трлн — это больше, чем ВВП Германии или Японии, полученный в 2021 году.

Не все противоправные деяния имеют непосредственную финансовую мотивацию. Есть атаки, совершаемые против государственных учреждений, попытки получения информации, которая не предназначена для извлечения денежных средств, например в целях шпионажа. И все же, по данным сайта csoonline.com, в 2021 году 86 % подтвержденных утечек данных были связаны непосредственно с финансовыми целями преступников.

На сегодняшний день фишинг остается одной из самых распространенных угроз в сфере кибербезопасности. Количество фишинговых сайтов, выявленных Google, к январю 2021 года выросло по сравнению с январем 2020 года на 27 % и превысило 2 млн.

Существенное ухудшение ситуации специалисты связывают с пандемией, которая в значительной мере увеличила долю дистанционных коммуникаций, в том числе финансовых.

Автор упомянутого выше материала в Cybersecurity Ventures Стив Морган рассматривает ситуацию скорее с точки зрения перспектив рынка цифровой безопасности. Уже сегодня в США в сфере кибербезопасности занято 925 тыс. человек и открыто примерно полмиллиона вакансий. Рост глобального рынка кибербезопасности предполагается в ближайшей перспективе на уровне 12–15 % в год.

Профессионалам будет где развернуться. Однако масштаб проблем в данном случае не до конца осознается мировым сообществом и большинством национальных правительств. По оценкам, которые приведены в публикации Брайана Финлэя в ресурсе Stimson, «торговля наркотиками и людьми, кража нефти, незаконная добыча полезных ископаемых, рыболовство, незаконный оборот оружия приносят от $1.6 до 2.2 трлн в год». То есть все вместе эти беды не покрывают и половину киберущерба.

Уровень взаимодействия между различными государствами в борьбе с криптопреступниками остается низким

При этом уровень взаимодействия между различными государствами в борьбе с криптопреступниками остается низким. Преступный интернационал в сфере кибермошенничества сложился, он эффективно использует преимущества давно сформированной глобальной финансовой системы. А противостоят ему в основном национальные институты финансового надзора и правоохранительные органы. Однако чувствительное поражение глобальному преступному сообществу может нанести только консолидированная и эффективная система международной финансовой и информационной безопасности. В настоящее время надзорным и правоохранительным органам приходится выполнять роль пожарников, которые вынуждены занимать пассивную позицию, решая проблемы, продуманные и созданные криминалом.

Данные по киберпреступности в России существенно отличаются от общемировых, что, по всей видимости, связано с различными методологиями подсчета, а также с разницей в масштабах цен и стоимости интеллектуальной собственности.

По данным МВД России, количество преступлений, совершенных с использованием «информационно-телекоммуникационных технологий или в сфере компьютерной информации», в 2021 году увеличилось по сравнению с 2020 годом всего на 1.4% (518 тысяч). Но в сравнении с 2019 годом (294 тысячи) количество киберпреступлений увеличилось на 76%. Большинство экспертов считают такой скачок результатом пандемии. Однако мы не исключаем, что определенную роль в итоговой статистике за 2021 год могли сыграть изменения в перечне статей УК РФ, которые используются для формирования отчетности министерства.

В 2021 году в 41% случаев киберпреступлений правоохранительные органы открывали дела по 159-й статье УК РФ («Мошенничество»), в 33% — по статье 158 («Кража»), в 26% случаев — по другим статьям. Основными способами хищений называют «дистанционное подписание фиктивного договора», «инвестиции в фейковые биржи и розыгрыши», а также «фишинговые атаки».

В 2022 году фиксируется спад IT-преступности, что, в первую очередь, эксперты связывают с жесткими санкциями в финансовой и информационной сферах. В первой половине года зафиксировано снижение показателей киберпреступности более чем на 8% (249 тысяч).

Доля раскрытых преступлений в 2019–2021 годах оставалась низкой (22–23%), что почти соответствовало уровню раскрытия преступлений по 159-й статье («Мошенничество») — 20%. Однако в 2022 году доля раскрытых киберпреступлений выросла почти до 30%. Возможно, этот позитивный сдвиг произошел в связи с «суверенизацией» интернета и систем финансовых расчетов.

Статистика МВД России описывает только часть свершившихся правонарушений. По сведениям Банка России, в 2021 году было зарегистрировано более миллиона операций, совершенных без согласия клиента. Почти все эти операции — мошеннические, но далеко не по всем были возбуждены уголовные дела. По сравнению с 2020 годом рост составил почти 34%, а по сравнению с 2019-м зафиксирован скачок на 79%. Еще плачевнее выглядит статистика по финансовому ущербу. Потери клиентов от несанкционированных безналичных переводов, сделанных с помощью банковских карт либо дистанционных приложений управления счетом, составили в 2021 году почти 13.6 млрд рублей. По сравнению с 2020 годом рост составил 38%, а с 2019-м — 111%.

Несмотря на существующие нормы ФЗ «О национальной платежной системе», которые возлагают серьезную материальную ответственность за карточное мошенничество на кредитные организации, доля возвращенных банками денежных средств остается крайне низкой и, более того, продолжает снижаться (2019 год — 14.5%, 2020 год — 11.3%, 2021 год — 6.8%). Банки слабо заинтересованы в развитии систем безопасности безналичных расчетов, пока почти все издержки можно возложить на клиентов.

Не спасает ситуацию и страхование рисков мошенничества, которое банки чуть ли не навязывают клиентам при выдаче карт. В год с клиентов собирается премия примерно 9–10 млрд рублей. Но по статистике ИА «Эксперт РА», сумма страховых выплат составляет примерно 3% от собранных страховых премий (без учета Сбербанка). При таком уровне страховых выплат страховка скорее выглядит завуалированной комиссией.

Все это подвигло Банк России к разработке мер, стимулирующих банки к борьбе с карточным мошенничеством. В декабре 2021 года регулятор предложил внести изменения в ФЗ «О национальной платежной системе», которые обязывали бы банки возвращать украденные со счетов граждан деньги. Предполагается, что сумма возврата будет зависеть от эффективности систем защиты от мошенников банка. Чем

Ряд крупных банков создал достаточно эффективные антифрод-системы, позволяющие, в частности, оперативно выявлять подозрительные счета, которые используют мошенники

Санкционный финансовый шок, который испытали десятки миллионов российских домохозяйств, создал для мошенников дополнительные возможности

эффективнее система, тем меньше банк возвращает денег клиенту.

Ряд крупных банков создал достаточно эффективные антифрод-системы, позволяющие, в частности, оперативно выявлять подозрительные счета, которые используют мошенники. Это дает кредитным организациям возможность временно блокировать поручения на перевод денежных средств на эти счета или запрашивать дополнительные подтверждения от держателя карты. Но есть банки, которые экономят на создании антифрод-систем. Мошенники, как правило, рекомендуют пользоваться картами именно таких банков.

В соответствии с действующей редакцией ФЗ «О национальной платежной системе» банки обязаны возместить денежные средства на карточных счетах, если клиент оперативно проинформировал кредитную организацию, что транзакция не была им санкционирована. Но в законе содержится спасительная для банков оговорка: эта обязанность действует, «если» банк «не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента — физического лица». Данная оговорка позволяет банкам избегать финансовой ответственности практически во всех случаях «социальной инженерии», когда человек сам передает мошенникам данные, необходимые для несанкционированного списания.

Предложение Банка России должно стимулировать кредитные организации к тому, чтобы совершенствовать меры защиты клиентов от их собственных ошибок. Такой подход нам представляется разумным, поскольку в руках банков находятся самые эффективные каналы оперативных коммуникаций. Они же располагают информационными и вычислительными ресурсами, необходимыми для выявления подозрительных счетов и транзакций.

Впрочем, допускаем, что у регулятора есть механизмы улучшения ситуации и без изменений законодательства. За период с 2019-го по 2021 год доля несанкционированных операций, совершенных с помощью социальной инженерии, снизилась с 68.6 % до 49.4 %. А это означает, что банки в 2021 году умудрялись избегать выплат по несанкционированным операциям, совершенным без социальной инженерии, как минимум в 85 % случаев.

По оценкам RTM Group, ущерб от киберпреступлений в России в 2021 году составил 150 млрд рублей, а в 2022 году прогнозировался на уровне 165 млрд. Правда, с учетом числа киберпреступлений в первой половине года ущерб в этом году может и не вырасти.

Если сравнивать российский ущерб с глобальными оценками, то он окажется значительно ниже, чем в других странах ($15–17 против $755). Однако скорее всего столь большая разница в значительной степени определяется разницей в методологии подсчета.

ЧТО ДАЛЬШЕ?

Несмотря на противоречивость представленных данных, они позволяют подтвердить вывод о том, что киберриски в последние два года значительно возросли. Некоторое стабилизирующее влияние в России на ситуацию оказала санкционная «суверенизация» финансовой системы 2022 года. В частности, в марте-мае сократилась активность мошеннических колл-центров, занимавшихся социальной инженерией. Но к началу лета активность начала восстанавливаться. Криминальные группы создают внутри страны новые сети «инкассаторов», а также активно используют для расчетов криптовалюту.

В целом санкционный финансовый шок, который испытали десятки миллионов российских домохозяйств, создал для мошенников дополнительные возможности. Некоторые из последствий этого шока вполне могут способствовать росту киберрисков. События весны 2022 года в определенной степени девальвируют в глазах инвесторов и потребителей значимость государственных финансовых учреждений, в первую очередь Центробанка. В результате международных финансовых санкций в ряде случаев люди, которые предпочли нелицензированные площадки, оказались в более выигрышном положении по сравнению с теми, кто доверился лицензиям.

В данном случае речь идет о реализовавшихся политических рисках. Однако их следствием стала довольно сильная дезориентация инвесторов. Этим, очевидно, воспользуются криминальные структуры, которые обязательно предложат россиянам новые перспективные формы вложений. В этой связи мы ожидаем дальнейшую активизацию фишинговых атак в сочетании с методами социальной инженерии.

КРИПТОБУДУЩЕЕ?

Интересы потребителей финансовых услуг и инвесторов на крипторынке в основном касаются операций с наиболее известными и капитализированными активами: биткоином, эфиром, а также основными стейблкоинами. Но такие активы легальные российские операторы информационных систем предложить не могут, поэтому потребителям приходится искать площадки вне российской юрисдикции со всеми возникающими рисками, в том числе с криптори сками.

Как бы Центробанк ни стремился уберечь население от вложений в криптовалюту, сделать это будет практически невозможно. По данным профессора, президента АНО «Центр защиты вкладчиков и инвесторов» Артема Генкина, российскими пользователями по состоянию на начало текущего года зарегистрировано 12–17 млн кошельков. Это не означает, что на рынке 12–17 млн криптоинвесторов, так как у одного пользователя может быть много кошельков. Объем вложений в криптовалюту составляет примерно 2 трлн рублей. При этом около 60 % «российских» кошельков относятся к «спящим», то есть по ним редко совершаются операции. Это, как подчеркивает профессор Генкин, говорит о том, что российский пользователь настроен на средне- и долгосрочные вложения.

Массовый интерес к вложениям в криптовалюту подтверждается статистикой Яндекса. Начиная с конца 2020 года ежемесячно фиксируется 0.8–2.1 млн запросов «курс биткоина». Информационный спрос в значительной степени зависит от динамики курса: чем выше курс биткоина, тем выше интерес (коэффициент корреляции 0.65). Это позволяет с высокой долей уверенности предположить, что очередной взлет стоимости биткоина увеличит не просто интерес к криптомонете, но и частоту использования

криптовалютной легенды мошенниками, а соответственно, будет увеличивать криториски, в первую очередь из-за роста числа фишинговых ресурсов.

Несколько иная картина с запросами «криптокошелек» и «криптобиржа». Общее количество таких запросов на порядок меньше, чем о курсе биткоина, что неудивительно, поскольку выбор или оценка институтов криптоинфраструктуры не требует регулярности. Здесь мы также видим определенную, хотя и значительно менее выраженную, корреляцию с курсом биткоина (0.34 и 0.51 соответственно). Но оба запроса буквально выстреливают в шоковые месяцы 2022 года (март, апрель). Затем происходит значительное снижение количества запросов, однако оно все равно остается на относительно высоком уровне, несмотря на обвал курса биткоина. Это скорее всего отражает стратегический тренд на интерес новой аудитории к цифровым активам.

При выборе институтов инфраструктуры крипторынка люди попадают в зону повышенных рисков. В условиях практически полного отсутствия регулирования, общепринятых стандартов предоставления криптоуслуг, а также алгоритмов оценки институтов криптоинфраструктуры выход гражданина на крипторынок превращается в экскурсию по минному полю. В интернете можно найти качественные материалы о том, как выбирать кошельки, обменники, биржи, на что обращать внимание. Однако для того, чтобы найти эти материалы, нужно обладать хорошими навыками отделения зерен от плевел. На человека, который проявит минимальный интерес к крипторынку, обрушится мощный поток рекламы разного рода школ и экспертов, готовых «за один вечер» онлайн научить зарабатывать деньги на крипте. В результате рекомендаций подобных гуру криптоинвесторы часто попадают на недобросовестные, а иногда и откровенно фишинговые интернет-ресурсы.

Вполне понятным представляется желание регулятора максимально ограничить доступ на крипторынок массового инвестора. И в этом отношении жесткая позиция по поводу легализации этого рынка в российской юрисдикции может быть оправданной. Однако в ситуации, когда государство не в силах ограничить уход в «крипту» денег через нероссийские сетевые ресурсы, возможно, следует занять более активную позицию Российской ассоциации криптоиндустрии и блокчейна (РАКиБ). По крайней мере, профессионалы должны играть более активную роль в цифровом просвещении населения, в предупреждении о рисках мошенничества.

УХОД В РИСК?

Финансовый шок конца февраля — апреля 2022 года стимулировал интерес россиян к использованию высокорисковых инструментов, и в данном случае речь не только о криптовалюте. В течение последних нескольких лет наблюдался относительно стабильный информационный интерес к такому рискованному финансовому инструменту, как торговля на рынке Форекс. Он всегда оставался довольно высоким, но стабильным (500–700 тысяч запросов в месяц). В феврале этого года бесстрастный Яндекс неожиданно фиксирует 1 млн 300 тысяч запросов, а в марте — более 4.6 млн. Летом информационный спрос стабилизировался, но на уровне примерно в 1.5 раза выше, чем сформировавшийся за последние годы.

С чем связан взрывной рост интереса к Форексу? С одной стороны, напрашивается предположение, что в условиях схлопывания привычного валютного рынка многие потребители проявили интерес к внебиржевому рынку валютных пар. В пользу этой гипотезы говорит то обстоятельство, что похожий по динамике рост наблюдался по запросам «наличная валюта», «валюта на бирже». Однако общее количество запросов про «наличную валюту» оказалось меньше запросов «Форекс» примерно в 20–30 раз, а про «валюту на бирже» — в 15–20 раз. Получается, что при возникновении проблемы россияне предпочли в качестве решения самый рискованный инструмент и институт финансового рынка.

За неполные полгода о рынке Форекс было сделано примерно 7 млн сверхнормативных запросов. Несколько миллионов человек проявили к нему интерес, который они не проявляли к этому сегменту как минимум несколько лет. Возможно, что значительная часть этих людей ранее были участниками рынка Форекс. С учетом малочисленности легального рынка получается, что большинство этих людей были клиентами нелегальных форекс-брокеров. Скорее всего у них есть негативный опыт торговли, но несмотря на это они в проблемный период вспомнили о сомнительных возможностях Форекса.

В любом случае взрывной рост интереса к Форексу создает серьезные риски активизации недобросовестных компаний, риски прямого мошенничества, в первую очередь путем создания фишинговых сайтов.

При выборе институтов инфраструктуры крипторынка люди попадают в зону повышенных рисков