зу в продаже конкретного вида кредитов и скоринге клиентов, может испытывать проблемы с капиталом и обслуживанием кредитов. В таком случае ему выгоднее продать, чем держать на балансе портфель кредитов (потребительских, ипотечных или автокредитов).

Продажа кредитного портфеля — это возможность прежде всего быстро увеличить ликвидность, если, например, кредитная организация испытывает кассовый разрыв и срочно нуждается в деньгах, отмечает господин Ковязин. «Еще одна причина продажи кредитного портфеля — желание привлечь средства под какой-то новый проект или более выгодный кредит,— рассказывает эксперт.— Также банк может пересмотреть свою политику развития и уйти из какого-то отдельного региона или с рынка розничного кредитования в целом, как это сделал в 2011 году „БНП Париба Восток“, который закрыл розничный бизнес в России, продав свой портфель банку „Уралсиб“ за 1,3 млрд рублей».

СЮРПРИЗ ДЛЯ КЛИЕНТА Продажа кредитных портфелей, как правило, затрагивает не только банки, но и третье лицо — заемщиков. Как поясняет господин Рыков, по Гражданскому кодексу согласия заемщика на цессию не требуется. Таким образом, новый кредитор приобретает право требования в том же объеме и на тех же условиях, что и у прежнего цессионера. При этом федеральный закон «О потребительском кредите» защищает заемщиков — физических лиц от продажи кредитных портфелей непрофессиональным участникам рынка.

Вне зависимости от того, кто будет новым цессионером, все условия кредитного договора сохраняются неизменными, подчеркивает госпожа Крючкова. «Бывают случаи, когда условия даже улучшаются (например, больше сеть отделений, лучше развиты дистанционные сервисы, больше способов оплаты). Однако с того момента, как заемщик был уведомлен о продаже своего кредита, он обязан платить за него новому кредитору. Единственное, что меняется для заемщика,— реквизиты оплаты»,— рассказывает эксперт.

По словам господина Рыкова, цессия зачастую становится для заемщика шансом на реструктуризацию задолженности даже в том случае, если первоначальный кредитор отказал в ней. «Поскольку портфели выкупаются с дисконтом, новый кредитор, как правило, заинтересован в быстрой оборачиваемости активов без необходимости формирования резерва на длительный срок. Однако, даже если это не так, кредитная и рисковая политики цессионария могут отличаться от таковых в кредитной организации, с которой заключался договор, в связи с чем при необходимости предпринять попытку реструктуризации задолженности однозначно стоит»,— резюмирует господин Рыков.

«Обрыва» в кредитной истории заемщика тоже не должно быть: договор будет отмечен как закрытый со статусом «переуступка прав» и появится информация о том, кому были они переуступлены, говорит господин Турпитько. «Новый кредитор становится источником формирования кредитной истории и обязан передавать сведения в бюро кредитных историй. Причем в то самое бюро, в котором кредитная история была сформирована изначально»,— уточняет он. ■

СКРЫТАЯ УГРОЗА

РОССИЯ ПОКА ЗНАЧИТЕЛЬНО ОТСТАЕТ ОТ ЗАПАДНЫХ СТРАН В СФЕРЕ КИБЕРСТРАХОВАНИЯ, А ОСНОВНЫЕ МЕТОДИКИ ОЦЕНКИ РИСКОВ И РАСЧЕТА ТАРИФОВ В ЭТОЙ ОБЛАСТИ ТОЛЬКО ФОРМИРУЮТСЯ. ОДНАКО, НЕСМОТРЯ НА ДОРОГОВИЗНУ И РИСКИ ЭТОГО ПРОДУКТА, ЕГО ПРОНИКНОВЕНИЕ ПОСТЕПЕННО БУДЕТ РАСТИ.

ГЕОРГИЙ КАРЧИК

В мире регулярно происходят кибератаки, которые приводят к массовым сбоям дорогой техники. Например, экономические потери от вирусов Wannacry и Petya в 2017 году, по данным Reuters, составили $8 млрд по всему миру. Резкий рост интереса к страхованию от киберугроз происходит именно после таких атак.

Более свежий пример — утечка данных клиентов Сбербанка, о которой стало известно в начале октября этого года. Официально в открытый доступ попали сведения 200 человек, но неофициально проблема может коснуться около 60 млн кредитных карт. Тем не менее, в отличие от вируса Petya, существенного всплеска интереса к данному виду страхования эта утечка не вызвала. Заместитель гендиректора страхового брокера «СиЛайн» Владимир Новак говорит, что корпорации фактически не несут ответственности перед третьими лицами за разглашение их персональных данных, поэтому утечка прошла безнаказанно для банка. Эксперты отмечают, что подобные инциденты скорее приводят к росту спроса на решения в области кибербезопасности, то есть на инструменты снижения вероятности наступления таких событий.

«По сравнению с прошлым годом прирост, безусловно, есть — около 20–30% по количеству запросов. Основные запросы приходят от IT-компаний, которым понятно страхование киберрисков в силу их рода деятельности, а также от финансовых институтов. Помимо этого, увеличивается количество полисов по международным клиентам: они покупают глобальные страховые программы, которые теперь включают и Россию»,— говорит директор по страхованию финансовых линий АО СК «Альянс» Вадим Михневич.

ИГРА В ЗАЩИТЕ Одна из сложностей при заключении договора страхования в этой сфере — выбор рисков, так как речь идет о комплексном продукте. Это не только финансовые убытки, связанные с потерей прибыли из-за перерыва в деятельности, но и материальные, вызванные выходом техники из строя.

В перечень рисков также можно добавить расходы на восстановление программного обеспечения (ПО), расследование киберинцидента, мониторинг проблемных зон. Есть еще юридические расходы, связанные со штрафами за утерю данных, судебными исками и процедурами замены скомпрометированных документов, ответственность перед третьими лицами за аналогичный ущерб, причиненный киберинцидентами. «В отличие от большинства видов имущественного страхования, в страховании киберрисков важную роль играет сервисная составляющая и перечень консультантов, которые будут действовать при наступлении киберинцидента. Также заключению договоров предшествует серьезная работа по анализу необходимых покрытий и его формированию, подготовка андеррайтинговой информации»,— отмечает начальник департамента страхования финансовых институтов компании «Греко ДжейЭлТи. Страховые брокеры» Дмитрий Грузинцев.

Неудивительно, что основные клиенты в этой сфере — крупные компании, бизнес которых в той или иной степени завязан на многочисленные диджитал-решения. «Большой экспертизы требует сама оценка риска,— добавляет управляющий директор по имущественным видам страхования компании «Ренессанс Страхование» Марина Зюганова.— Как правило, страховщики нанимают для аудита клиента независимую IT-компанию, которая оценивает сильные и слабые стороны информационной безопасности». Также опрошенные эксперты отмечают, что клиенты часто выбирают компанию через международного страхового брокера. Последние обычно рекомендуют международные страховые компании, так как они лучше подготовлены к организации страховой защиты по страхованию киберрисков, у них есть доступ к экспертизе и наработкам из США и Европы, а также опыт урегулирования убытков.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР Если говорить о сегменте b2c, то одним из лидеров в страховании киберрисков является «Сбербанк страхование». В компании отмечают, что около 300 тыс. клиентов ежемесячно приобретают продукт, защищающий банковские карты, куда включено страхование от киберинцидентов. По данным компании, сегодня этим видом в нашей стране занимаются около 10 страховщиков. И если за рубежом киберриски составляют около 1% от страхования имущества юридических лиц, в России общий портфель застрахованных от киберрисков юрлиц с начала 2019 года оценивается примерно в 50 млн рублей при потенциале этого рынка около 1 млрд рублей в год. «Нам известны случаи, когда кредиторы требуют киберстрахование в качестве обеспечения залога»,— говорит руководитель СК «Сбербанк страхование» Дмитрий Попов.

Впрочем, из-за сложности продукта этот вид страхования достаточно дорогой, так как требует покупки перестраховочной защиты, андеррайтинга и оценки риска. Страховой тариф может варьироваться от 0,5–2% до 10%, считают «Греко ДжейЭлТи. Страховые брокеры» и «СиЛайн». Также из-за сложности данного вида страхования существуют проблемы с выплатами. «Мошенничество в киберстраховании пока наблюдается в основном со стороны страховщиков,— уверен директор по отраслевым решениям в страховании IT-компании KPOK Андрей Крупнов.— Например, страховщики отказывают в выплате, если к киберинциденту привела человеческая ошибка, а такую причину можно подвести практически под любой случай. В то же время клиенту мошенничество реализовать сложно, так как речь идет об электронных сетях, в которых достаточно просто обнаружить все следы действий и их хронологию». «По этой причине также не удастся заявить события, произошедшие до даты заключения договора страхования,— полагает господин Новак.— Помимо общих исключений, также присутствует целый ряд более специфических, таких как работа с нелицензионным ПО, трейдинговые операции, расходы на лицензионные платежи и прочее».

Проникновение киберстрахования через пять лет можно оценить в 30–35% крупных корпоративных клиентов, 5–10% розничных и представителей малого и среднего бизнеса, считает господин Крупнов. Но поскольку речь идет о новом виде страхования, то существенной проблемой для него является отсутствие накопленной статистики для расчета рисков, а также неприменимость традиционных методов андеррайтинга. Это связано с сильной изменчивостью киберугроз и средств противодействия им. Если на Западе методики оценки рисков и расчета тарифов по киберстрахованию постепенно появляются, то в России они пока находятся только в стадии разработки.

При этом данный вид страхования уже нельзя назвать экзотикой. Для зарубежных компаний он уже стал распространенной практикой, в России его популярность также растет. «Именно страхование может выступать одним из вариантов обработки киберрисков, согласно проекту Положения Банка России „О требованиях к системе управления операционным риском в кредитной организации и банковской группе“»,— заключает старший консультант центра информационной безопасности компании «Инфосистемы Джет» Ирина Павлова. ■