УДК 343.985

Д.Н. Лахтиков

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ХИЩЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ОНЛАЙН-ПЛАТЕЖА

В настоящее время наиболее распространенными являются технологии онлайн-платежей на основе банковских платежных карточек, электронных денег, интернет-банкинга. Обращение электронных денег осуществляется в сети Интернет, их можно использовать при помощи виртуальных кошельков, интернет-банкинга, устройств, работающих с банковскими платежными карточками, и т. д. Интернет-банкинг же является системой дистанционного банковского обслуживания (СДБО), позволяющей осуществлять управление счетами с использованием сети Интернет, а также предоставлять посредством программно-аппаратных средств и компьютерной сети Интернет банковские услуги.

При совершении хищений с использованием средств онлайн-платежа преступники изучают особенности функционирования этих средств, в том числе программно-техническое обеспечение, с целью использования различных технологических особенностей в преступных целях, разрабатывают соответствующее программное обеспечение либо приобретают его на специализированных интернет-ресурсах, в том числе в даркнете. Эксплуатируя выявленную технологическую особенность (уязвимость), похищаются финансовые средства и перемещаются на счета, контролируемые преступниками (например, используются дропы и т. д.), после чего осуществляется их вывод с указанного счета и обналичивание.

Основными тенденциями совершаемых хищений в рассматриваемой сфере в 2020 г. являются: увеличение количества преступлений с использованием социальной инженерии (фишинг, вишинг, взлом учетных записей пользователей в социальных сетях); звонки в результате утечки персональных данных на маркетплейсе Joom; наличие фактов компрометации СДБО клиентов в рамках социальной инженерии, в результате чего преступники получали учетные данные (логины, пароли и ключи) доступа к СДБО; мошенничество по токенам, когда преступники с использованием социальной инженерии выманивали не только реквизиты банковской платежной карточки и пароль 3-D Secure, но и данные, необходимые для присвоения токена к банковской платежной карточке, привязывали токен держателя на свое мобильное устройство; рассылка в социальных сетях уведомлений о выигрышах, когда держатели сами вводили реквизиты банковских платежных карточек для получения выигрыша; увеличение количества мошеннических операций на онлайн-сервисах, которые занимались продажей цифровых товаров (компьютерные игры и программное обеспечение (взлом аккаунтов учетной записи Google, осуществление операции оплаты Google-сервисов в пределах остатка баланса на счете)); вещевой кардинг; мошеннические онлайн-возвраты; смещение мошенничества с использованием платежных инструментов и сервисов все больше в сферу электронной коммерции.

Основными участниками технологии онлайн-платежей могут являться: покупатель (владелец счета, электронных денег и др.); продавец (интернет-магазин, предприятие торговли (услуг); платежная система; платежный агрегатор; платежный шлюз; эмиссионный банк (осуществляет выпуск и в отдельных случаях обслуживание банковских платежных карточек); банк-эквайер (обеспечивает расчеты по банковским платежным карточкам в торгово-сервисных организациях); процессинговый центр (обеспечивает технологическое и информационное взаимодействие между участниками расчетов). Например, совершая платеж, покупатель вводит платежные данные через веб-интерфейс интернет-магазина, после чего информация передается через платежный шлюз в банк-эквайер, который отправляет запрос на платеж в платежную систему, получает запрос на авторизацию, отправляет этот код назад в платежную систему, совершающую операцию, код авторизации возвращается в платежный шлюз и этот же код уходит в интернет-магазин с результатом операции.

Платежная система является финансовой инфраструктурой, обеспечивающей совершение финансовых транзакций между банками и иными участниками финансовых операций. С позиции технической составляющей – это аппаратно-программный комплекс со своей технической инфраструктурой, сводом правил и процедур, обеспечивающих бесперебойное совершение финансовых транзакций согласно международному, национальному законодательству и своим правилам. Ключевой задачей платежной системы является оперативное проведение взаиморасчетов между участниками. Платежная система может работать как на уровне одной страны, так и обеспечивать интересы нескольких стран, т. е. быть локальной (например, SEPA в Европе) или быть международной (например, SWIFT). В отдельных случаях под международной платежной системой имеют в виду только системы, обслуживающие банковские платежные карточки (VISA, MasterCard и др.). В Республике Беларусь наиболее распространенными электронными платежными системами являются «Яндекс.Деньги» (один из сервисов «Яндекс»), WebMoney, PayPal, Qiwi. Функционируют также национальные платежные системы, например IPay-сервис, интегрированный с названными выше платежными системами, а также с Единым расчетным информационным пространством (ЕРИП) и мобильными операторами. Национальным банком Республики Беларусь создана система-провайдер «Расчет», с помощью которой осуществляется поддержка при проведении онлайн-платежей. ЕРИП позволяет проводить различные виды расчетов, включая коммунальные услуги, покупки в интернет-магазинах, билеты в кино и др. Возможно подключение системы ЕРИП как напрямую, так и с помощью платежных агрегаторов.

Платежный агрегатор обрабатывает онлайн-платежи. Так, владелец интернет-магазина либо самостоятельно организовывает прием платежей с каждой из платежных систем, либо заключает договор с платежным агрегатором, у которого имеются технические решения для работы с платежными системами. Наиболее распространенными платежными агрегаторами в Республике Беларусь являются WebPay, bePaid, Assist.

Платежный шлюз является сервисом, который осуществляет маршрутизацию платежа. С технической точки зрения платежный шлюз является программным модулем, который распределяет (осуществляет маршрутизацию) платеж между участниками транзакции: интернет-магазин, банки и третьи стороны, вовлеченные в процесс (например, предоставляющие услуги эквайеринга). Платежный шлюз является интегратором платежных решений, который не выполняет какой-либо

расчетно-финансовой функции. Однако платежные агрегатор и шлюз осуществляют интеграцию платежных инструментов для проведения онлайн-платежей посредством широкого набора разных опций (банковские платежные карточки, электронные кошельки, оффлайн-платежи и др.). Основное отличие заключается в том, что платежный шлюз является технологическим партнером, который маршрутизирует платеж, не взаимодействуя с финансовыми средствами клиентов, в то время как платежный агрегатор их аккумулирует у себя.

Почти все платежные системы и платежные агрегаторы обладают своими антифрод-решениями. Цель антифрод-системы заключается в том, чтобы убедиться, что, например, пользователь является реальным владельцем банковской платежной карточки, совершающим покупку в интернет-магазине. В случае выявления подозрительной активности, т. е. превышения какого-либо значения параметра, система автоматически блокирует возможность совершения платежа либо отправляет покупателя на дополнительную проверку.

Преступники стараются, чтобы их цифровой след максимально совпадал с владельцем аккаунта (банковской платежной карточки), совершают хищение, ставят цель быть максимально похожими на реального покупателя со всеми возможными данными.

Общий механизм работы антифрод-системы можно свести к следующему. Сервер банка переадресовывает сведения о транзакции в антифрод-систему и ожидает разрешения на проведение платежа. Антифрод-система анализирует сведения, чтобы принять решение о легитимности этой транзакции. Обрабатывается платеж, оценивается его риск, при необходимости инициируется проверка другими сервисами, например, дополнительная аутентификация клиента, после чего решение передается назад. В результате финансовая транзакция оказывается подтвержденной или отклоненной. В момент совершения финансовой транзакции сканируются браузер, IP-адрес, куки-файлы на предмет подозрительной активности, а также собирается несколько показателей (у каждой антифрод-системы они различные) – начиная от IP-адреса компьютера, версии браузера и заканчивая статистикой платежей и др.Осуществляется проверка на использование виртуальной машины или VPN, анализируется поведение клиента, проверяется информация о платежной системе, используется собственная база мошеннических действий и др.

Эффективность предупреждения мошенничества данного вида во многом зависит от надежности программно-аппаратного обеспечения, используемого в организациях кредитно-финансовой сферы, способности систем безопасности противостоять компьютерным атакам, профессиональной подготовки сотрудников информационной безопасности и правоохранительных органов.

Таким образом, борьба с хищениями, совершаемыми с использованием средств онлайн-платежей, должна начинаться с эмиссионного банка и присутствовать на всех этапах финансовой транзакции. Для эффективного противодействия хищениям необходима реализация комплекса профилактических мер, среди которых можно выделить меры, повышающие трудность совершения преступлений; направленные на повышение уровня цифровой финансовой грамотности всех участников, активное внедрение антифрод-систем; обеспечивающие передачу платежных данных только посредством защищенных каналов.

УДК 343

П.В. Лутович

СОВЕРШЕНСТВОВАНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ РАСЧЕТНЫХ ОТНОШЕНИЙ В СОВРЕМЕННЫХ ЭКОНОМИЧЕСКИХ УСЛОВИЯХ

Современные международные экономические отношения предполагают совершение большого количества денежных операций путем использования валют различных государств. Несмотря на то что международные расчеты являются необходимым и важным элементом внешнеэкономических связей, они отличаются большой сложностью в силу особого субъектного состава и отсутствия унифицированного источника их правового регулирования.

Развитие интеграционных процессов, обусловленных глобализацией общественных отношений в мировой экономике, требует четкой и прозрачной организации расчетных отношений между отечественными хозяйствующими субъектами и зарубежными партнерами. Сильное влияние на проведение международных расчетов оказывает существующий уровень развития национальной кредитно-финансовой системы, которая динамично и последовательно развивается, внедряя в свою деятельность инновационные достижения современной банковской сферы.

С развитием информационных технологий оптимизируется порядок осуществления расчетных операций за счет появления цифровых валют. В научной литературе разновидностью цифровой валюты выступает криптовалюта, предусматривающая учет внутренних расчетных единиц и работающая в полностью автоматическом режиме.

Особенностью большинства существующих криптовалют является то, что их эмиссия происходит при отсутствии контролирующих органов со стороны государства. Они не могут быть учтены в совокупной денежной массе соответствующего государства, так как не являются национальными либо наднациональными денежными единицами той или иной страны. Кроме того, криптовалюты лишены каких-либо гарантий со стороны государства, поскольку центральные банки обычно не имеют отношения к их созданию.

Вместе с тем применение таких технологий позволит сократить издержки финансовых организаций на десятки миллиардов долларов США за счет экономии на трансграничных платежах, торговле ценными бумагами и др. Специалисты отмечают перспективность их применения в других направлениях банковской деятельности: потребительское кредитование, операции с наличными деньгами, корпоративное кредитование, торговое финансирование, ипотека, депозиты, розничные и международные платежи.