

Е. А. Гопка

Институт бизнеса БГУ, Минск, Беларусь, gopka@sbmt.by

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ПЛАТЕЖНЫХ УСЛУГ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Век цифровых технологий предъявляет повышенные требования к обеспечению безопасности платежных услуг. В работе обсуждаются проблемы функционирования платежных систем и регулирования отношений, возникающих при оказании платежных услуг.

Ключевые слова: *цифровизация, безопасность, интернет-мошенничество, платежные услуги, страхование карты, аутентификация*

E. Gopka

School of Business of BSU, Minsk, Belarus, gopka@sbmt.by

PROBLEMS OF USING PAYMENT SERVICES IN THE DIGITAL SPACE

The age of digital technologies imposes increased requirements for ensuring the security of payment services. The paper discusses the problems of the functioning of payment systems and the regulation of relations arising in the provision of payment services.

Keywords: *digitalization, security, internet fraud, payment services, card insurance, authentication*

В период стремительного развития глобальной информатизации общество столкнулось с серьезной и злободневной проблемой обеспечения безопасности использования платежных услуг в цифровом пространстве.

В соответствии с Законом Республики Беларусь «О платежных системах и платежных услугах» определяются правовые и организационные основы функционирования платежных систем в Республике Беларусь, регулируются отношения, возникающие при оказании платежных услуг. Так платежная – это услуга, оказываемая поставщиком платежной услуги. В соответствии со ст. 9 настоящего Закона определены следующие виды платежных услуг: услуги оператора платежной системы по организации платежной системы; расчетные услуги; инициирование платежа; эквайринг платежных операций; эмиссия (создание) или распространение платежных инструментов; платежные услуги по операциям с электронными деньгами; услуги клиринга; услуги процессинга; информационные платежные услуги [1].

Следует отметить, что поставщик платежных услуг обязан (ст. 10 Закона) использовать многофакторную аутентификацию пользователей в случаях и порядке, установленных Национальным банком.

Кроме того, поставщик платежных услуг обязан обеспечить возможность возврата денежных средств (электронных денег) получателем денежных средств (электронных денег) плательщику в соответствии с порядком, установленным законодательством, в случае, если: денежные средства уплачены излишне; платеж осуществлен ошибочно.

Как указывается в Законе, поставщик платежных услуг должен предоставить пользователю информацию (ст. 23 Закона) о безопасности оказания платежных услуг. Информация о платежной услуге (платежных услугах) поставщика платежных услуг включает в себя: форму и порядок получения согласия на платежную операцию, отзыва такого согласия. Информация о безопасности оказания платежных услуг включает в себя: перечень требований к пользователю, на-

правленных на обеспечение сохранности платежных инструментов, и описание процесса уведомления поставщика платежных услуг в случаях, предполагаемого или выявленного факта неправомерных действий либо угрозы для безопасности оказания платежной услуги; условия приостановления оказания платежной услуги, блокировки платежного инструмента в одностороннем порядке; ответственность пользователя (плательщика) за осуществление неавторизованной платежной операции, включая предоставление информации о сумме нанесенного ущерба; способ и сроки информирования пользователем поставщика платежных услуг о неавторизованной, неправильно инициированной или проведенной платежной операции, а также ответственность поставщика платежных услуг за неавторизованные платежные операции; ответственность поставщика платежных услуг за нарушение порядка инициирования, порядка проведения платежных операций; описание процедуры гарантирования завершения расчетов по принятым платежам, исполнения платежных обязательств; условия возмещения ущерба, причиненного по вине поставщика платежных услуг.

В последнее время в Беларуси зафиксирован значительный рост количества преступлений, связанных с хищениями денежных средств посредством обманных действий в Интернете и с использованием компьютерной техники. Если до 2022 г. тенденция была менее ощутима и увеличение было незначительное, то уже в прошлом году количество случаев интернет-мошенничества возросло в 2 раза и каждое второе из числа зарегистрированных преступлений было совершено с использованием Интернета. Это обусловлено доступностью технологий, которой активно пользуются злоумышленники. Ущерб от деятельности мошенников в 2022 г. в нашей стране достиг почти 9 млн белорусских рублей [2].

Поставщик платежных услуг обязан в соответствии с Законом (ст. 33) принимать необходимые меры по исключению конфликта интересов и условий его возникновения, возможности совершения преступлений и иных противоправных деяний при осуществлении своей деятельности.

Пользователь имеет право (ст. 39) обжаловать действия (бездействие) поставщиков платежных услуг по осуществлению платежа (детали платежа) в случаях, предусмотренных платежным соглашением и (или) договором между поставщиком и пользователем платежных услуг, настоящим Законом и иными актами законодательства. Кроме того пользователь имеет право получить полную информацию по платежу в соответствии с требованиями ст. 23 настоящего Закона.

Остановимся далее на фишинге (англ. «phishing» от «fishing» – рыбная ловля, выуживание) – виде мошенничества с использованием сети Интернет, целью которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т. д.) [3].

О способах защиты интересов пользователей от интернет-мошенничества сообщалось неоднократно многими средствами массовой информации, банками, правоохранительными органами.

Следует отметить, что мошенники все время идут вперед, придумывая новые схемы. Так в феврале текущего года проблемы возникали даже при оплате коммунальных услуг – через поддельные сайты, являющиеся полной копией интернет-ресурсов банков. Более 50 случаев потери денег при оплате коммунальных услуг в Интернете зафиксировали органы МВД Беларуси, в то время как ранее коммунальными услугами злоумышленники не интересовались [4].

В соответствии с Законом (ст. 40) пользователь платежного инструмента обязан: с момента получения платежного инструмента принять меры по обеспечению защиты своих персональных данных и аутентификационных данных, к которым предоставляется доступ посредством эмитируемого поставщиком платежных услуг платежного инструмента, согласованные с поставщиком платежных услуг, в том числе обеспечить защиту от несанкционированного доступа к указанным данным третьих лиц.

Согласие на осуществление платежной операции (ст. 50 Закона) предоставляется в соответствии с требованиями, установленными законодательством, в форме и посредством инструмен-

тов, согласованных поставщиком платежных услуг, осуществляющим указанную операцию, с пользователем-плательщиком в соответствующем договоре на оказание платежных услуг. Согласие на осуществление платежной операции может быть предоставлено пользователем – получателем платежа или поставщиком платежной услуги инициирования платежа. Процедура предоставления согласия на осуществление платежной операции должна быть согласована поставщиком (поставщиками) соответствующих платежных услуг и пользователем.

Приведенные статьи Закона и тенденция динамики случаев интернет-мошенничества позволяют сделать вывод о необходимости разработки и использовании банками действенных методов для снижения и элиминации негативных последствий от действий злоумышленников. Потребителям банковских услуг для защиты своих средств можно активно использовать такой инструмент как страхование карты. Специалистам банков следует более действенно отслеживать опасные сайты и предпринимать действия по их блокировке. Кроме того, для защиты своих клиентов банкам не допустимо упрощать процедуры предоставления платежных услуг в цифровом пространстве, например, возможность снятия SMS-подтверждения при совершении платежа любого размера через мобильное приложение. Такие упрощения и мнимые сокращения времени совершения платежной операции могут быть на руку только мошенникам. Таким образом, только совместные усилия поставщиков и пользователей могут привести к хорошим результатам по обеспечению безопасности платежных услуг.

Список использованных источников

1. О платежных системах и платежных услугах [Электронный ресурс] : Закон Респ. Беларусь, 19 апр. 2022 г. № 154-З // Нац. центр правовой информ. Респ. Беларусь. – Режим доступа: <https://pravo.by/document/?guid=12551&p0=H12200164&p1=1%20/>. – Дата доступа: 15.03.2023.
2. В Беларуси в прошлом году каждый второй случай мошенничества совершен через Интернет [Электронный ресурс]. – Режим доступа: <https://www.belta.by/society/view/v-belarusi-v-proshlom-godu-kazhdyy-vtoroj-sluchaj-moshennichestva-sovershen-cherez-internet-549245-2023/>. – Дата доступа: 15.03.2023.
3. Борьба с мошенничеством на сетях электросвязи [Электронный ресурс]. – Режим доступа: <https://www.oac.gov.by/fighting-telecom-fraud/phishing>. – Дата доступа: 15.03.2023.
4. Новая схема мошенничества в Интернете: в Беларуси пострадало более 50 человек [Электронный ресурс]. – Режим доступа: <https://officelife.media/news/41061-novaya-skHEMA-moshennichestva-v-internete-v-belarusi-postradalo-bolee-50-chelovek/>. – Дата доступа: 15.03.2023.