МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ СИСТЕМ И МЕРЫ ЕГО ПРЕДУПРЕЖДЕНИЯ

Авторы: *Устинова Валерия Георгиевна (Курганский государственный университет)*

Аннотация: *С января по сентябрь 2019 года в России было зарегистрировано в четыре с лишним раза больше преступлений, квалифицированных по ст.159.3 Уголовного кодекса Российской Федерации, чем за аналогичный период прошлого года. Это свидетельствует об отсутствии эффективных мер по предупреждению данного вида преступлений. На основе системно-структурного анализа способов мошенничества в экономической сфере сформированы авторские предложения – меры предупреждения мошенничества с использованием платежных систем. Предложены рекомендации по снижению рисков попадания в сети мошенников.*

Ключевые слова: *мошенничество, мошенничество с использованием платежных систем, траппинг, скимминг, финансовая грамотность.*

Annotation: *From January to September 2019, more than four times more crimes were registered in Russia, qualified under Article 159.3 of the Criminal Code of the Russian Federation, than for the same period last year. This indicates the absence of effective measures to prevent this type of crime. On the basis of a system-structural analysis of methods of fraud in the economic sphere, author’s proposals have been formed - measures to prevent fraud using payment systems. Recommendations are offered to reduce the risks of getting into the network of scammers.*

Keywords: *fraud, fraud using payment systems, trapping, skimming, financial literacy.*

В настоящее время происходит активное развитие экономической сферы жизни общества в России, усложняются уже имеющиеся и создаются новые финансовые инструменты, рассматриваются ранее не существовавшие варианты использования финансовых услуг. Однако это обуславливает и увеличение количества случаев мошенничества, поскольку с января по сентябрь 2019 года в России было зарегистрировано 10,3 тыс. преступлений, квалифицированных по ст. 159.3 Уголовного кодекса Российской Федерации («Мошенничество с использованием электронных средств платежа»), что в четыре с лишним раза больше, чем за аналогичный период прошлого года. Именно поэтому данная тема является особенно актуальной.

Наиболее распространенными способами мошенничества с использованием платежных систем являются: траппинг, скимминг, фишинг и «наперстки».

Для преступников траппинг (от англ. – заманивать) является самым простым способом получить карту клиента банка, не прилагая при этом особых усилий. Этот способ заключается в том, что злоумышленники вставляют в картридер небольшой кусок пластика с прорезью в центре. Карта попадает в эту прорезь и остается в банкомате, затем к владельцу карты подходит мошенник, который указывает на то, что с ним случались подобные ситуации и необходимо ввести пин-код. После нескольких неудачных попыток владелец карты уходит, а мошенник, запомнивший

пин-код, достает карту с помощью специальных инструментов.

Скимминг (от англ. – скользить) – еще одна из разновидностей мошеннической деятельности с банковскими картами, которая заключается в считывании информации с магнитной полосы с помощью специального технического устройства. Такой прибор мошенники-скиммеры могут прикрепить к банкомату камеры, чтобы фиксировать нажатия клавиш клиента банка, когда он вводит пин-код. Для борьбы со скиммингом, банки обычно используют три способа - физический мониторинг, пассивный антискимминг и активный антискимминг. Физический мониторинг заключается в периодической проверке банкоматов сотрудниками банка, при этом работниками ведется журнал, где записывается время и состояние банкомата, чтобы в случае появления инородного устройства была возможность выявить промежуток времени. Данный метод является самым ненадежным, поскольку возникает большая вероятность совершения мошенничества между проверками. При пассивном антискимминге на банкомат устанавливается накладки, которые препятствует установки инородных устройств. Но эти такие накладки являются видимыми, поэтому многие люди могут опасаться пользоваться данным банкоматом. Активный антискимминг - это самый эффективный метод, который также является и самым дорогостоящим. В этом случае антискиммингговое устройство устанавливается внутри банкомата.

Другим способом мошенничества является фишинг (от англ. – рыбалка). Это незаконная схема, которая была разработана специально для компьютерного финансового мошенничества. Суть ее заключается в том, что киберпреступники создают сайт, по всем параметрам схожий с сайтом банка или интернет-магазина, предусмотрев на нем возможность проводить денежные расчеты через Интернет. Постепенно на этот фальшивый сайт завлекаются владельцы банковских карт, которые впоследствии оставляют там свои конфиденциальные данные, платежные реквизиты. После чего преступники крадут деньги со счетов «покупателей». В качестве привлечения пользователей на фальшивый сайт может применяться массовая рассылка электронных сообщений от имени банков и интернет-магазинов со ссылкой на ложный сайт. Наиболее продвинутые финансовые мошенники распространяют вирусные программы через различные интернет-ресурсы. Владелец банковской карты, компьютер которого заражен вирусной программой, при попытке войти в личный кабинет перенаправляется на фальшивые сайты, где также вводит личную информацию и отправляет ее непосредственно в руки кибермошенников.

Набирает популярность среди мошенников и «наперстки» - способ, в котором задействована преступная группа. У банкомата один из злоумышленников оставляет свою банковскую карту в картоприемнике. Следующий клиент (жертва) подходит к устройству и вынимает карту. Далее появляется хозяин банковской карты, который заявляет, что с его счета пропала крупная сумма денежных средств, и требует их вернуть. В качестве свидетеля привлекается еще один злоумышленник, а жертве начинают угрожать полицией. «Это похоже на схему с игрой в наперстки. Также разыгрывается сценка», - рассказал газете «Известия» полковник МВД в отставке Евгений Черноусов. Гражданам необходимо помнить, что на банкоматах есть камеры, а все операции фиксируются кредитным учреждением, поэтому у мошенников нет

шансов доказать «вину» потенциальной жертвы.

Одной из наиболее действенных мер противодействия мошенничеству с использованием платежных систем является его профилактика, а именно, предупреждение данного вида преступления. Такие действия могут осуществляться как общими, так и специальными субъектами.

К числу общих субъектов можно отнести все федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления и их должностных лиц, чья деятельность непосредственно не направлена на борьбу с преступностью, например, Департамент социальной политики Администрации города Кургана. Также к числу общих субъектов предупреждения преступлений относятся общественные объединения, юридические и физические лица, чья деятельность направлена на улучшение общественной жизни, например, благотворительные фонды.

Деятельность специальных субъектов предупреждения преступлений непосредственно направлена на борьбу с преступностью, что находит отражение в нормативно-правовой базе, регламентирующей создание и функционирование соответствующих органов и их должностных лиц. К специальным субъектам относятся правоохранительные органы и должностные лица: сотрудники следствия, дознания, патрульно-постовой службы, участковые уполномоченные полиции, частные охранные предприятия и их сотрудники и т. д. Кроме того, общественные объединения и отдельные граждане также принимают участие в целенаправленной деятельности по предупреждению преступлений, например, общественные патрули.

Осуществление качественной профилактики как общими, так и специальными субъектами, возможно лишь путем непосредственной работы с гражданами, в частности, путем повышения их финансовой грамотности.

В России уровень финансовой грамотности особенно низок, что подтверждается многочисленными исследованиями, проведенными независимыми СМИ в 2018 году. Так, по данному показателю Российская Федерация занимает лишь девятое место среди стран Большой двадцатки.

Это связано, прежде всего, с наличием в современном законодательстве пробелов, отсутствием нормативно-правовой регламентации способов повышения финансовой грамотности населения. Это является основным препятствием развития финансовых рынков и способно привести к увеличению показателей мошенничества с использованием платежных систем. Именно поэтому финансовая грамотность играет огромную роль в профилактике вышеупомянутого вида преступлений. Следовательно, на сегодняшний день ключевой задачей проводимой государством экономической политики является разработка и внедрение программ по повышению финансовой грамотности среди населения. Это могут быть различные акции муниципального, регионального и федерального уровней, форумы, открытые лекции для подростков и людей среднего и старшего возраста.

Посредством проведения вышеупомянутых мероприятий можно донести до

населения информацию о правовых последствиях их невнимательности при использовании платежных систем. В качестве наглядных образцов в виде буклетов необходимо разработать рекомендации по снижению рисков попадания в сети мошенников. Соблюдение таких простых правил, как проверка url в адресной строке браузера, создание резервных копий ключей и паролей, не предоставление информации о номере и пин-коде банковской карте третьим лицам, установление лимита суточного снятия денежных средств с карты, внимательная проверка банкомата перед использованием будет способствовать сокращению числа преступлений по ст. 159.3 Уголовного кодекса Российской Федерации и улучшению уровня жизни населения.

Список использованной литературы

1. Алексеева Е.А., Абдулин Р.С. Криминология: общая часть: учебное пособие – Курган, 2019. – 148 с.
2. Аликперова Н.В. К вопросу об уровне финансовой грамотности российского населения // Материалы Международной научно-практической конференции «Доходы, расходы и сбережения населения России: тенденции и перспективы». 25 сентября 2014 г. - М., 2014. 221 с.
3. Еремина О.И. Финансовая грамотность населения и пути ее повышения // Современные проблемы и перспективы развития банковского сектора России. – 2017. – С. 179-181.
4. Однокоз В.Г. Мошенничество в сфере безналичных расчетов с использованием банковских карт // Молодой ученый. - 2017. - №1. - С. 242. – URL: https://moluch.ru/archive/135/37755/ (дата обращения 17.11.2019).
5. Теплова О.Д. Криминологические основы противодействия организованному мошенничеству: Монография / Теплова О.Д. - М.: РГУП, 2017. - 220 с.
6. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 04.11.2019) [Электронный ресурс] // СПС КонсультантПлюс: URL: http://www.consultant.ru/document/cons_doc_LAW_10699/