УДК 343.72

В. С. Голованова
курсант 36 взвода юридического факультета
Воронежского института МВД России

Научный руководитель:

Р. В. Колесников
доцент кафедры уголовного права и криминологии
Воронежского института МВД России,
кандидат юридических наук

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА КАК ОДИН ИЗ ВИДОВ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В связи с тем, что развитие не стоит на месте и XXI век по праву считается веком информационных технологий, в повседневную жизнь человека активно вошли, все больше используются и совершенствуются различные технологии. Главным преимуществом является то, что они способны облегчить жизнь человека, выполнять определенные действия при затратах на это минимального количества времени, позволяют дистанционно выполнять различные действия. Благодаря своим преимуществам данные технологии не только вошли в повседневную деятельность и жизнь человека, но и стали объектом для совершения преступлений. При этом стоит отметить, что совершение преступлений в информационной сфере набирает колоссальные масштабы.

В 2021 году в России зарегистрировано около 518 тыс. киберпреступлений, что на 1,4 % больше, чем годом ранее, но в 1,8 раза превосходит показатель 2019 года. В частности, количество заявлений о мошенничестве (хищение с обманом жертвы) выросло на 5,1 %, превысив 249 тыс. Управляющий RTM Group Евгений Царев рассказал «Коммерсанту», что рост количества результативных атак в 2021 году ускорился по сравнению с 2020 годом. Он составил 35 %. Это, по его словам, произошло в первую очередь за счет действий мошенников, в основном телефонных, а не хакеров [1].

Тенденцию увеличения данных преступлений можно объяснить тем, что наличные деньги как средства платежа активно выходят из оборота, поскольку сильно уступают средствам электронного платежа. Это обусловлено преимуществами совершения большинства платежных онлайн-операций, таких как получение заработной платы, оплата товаров и услуг, штрафов, налогов и многое другое. Помимо быстроты и простоты в использовании, электронные денежные

средства не обладают должной защитой, которая обеспечила бы им безопасность от вторжения и совершения преступлений.

В настоящее время ст. 159.3 Уголовного кодекса Российской Федерации предусматривает ответственность за мошенничество с использованием электронных средств платежа, но, к сожалению, по мнению ученых, не несет в себе какой-либо ясности об объеме преступных деяний, подпадающих под ее действие.

Одной из проблем граждан, из-за которой они часто становятся жертвами мошенничества, является их неосведомленность о том, какие методы и средства используют мошенники для того, чтобы совершить хищение денежных средств с их банковских карт и систем платежей. Злоумышленники совершают данное преступление путем обмана, входя людям в доверие, именно поэтому необходимо знать их приемы и места действий, чтобы избежать попытки завладения денежными средствами.

Места совершения мошенничества с банковскими картами могут быть различными. Рассмотрим некоторые из них. Например, на различных сайтах, где происходит продажа товаров и услуг, мошенники могут выступать как в роли продавцов, так и в роли покупателей. Если вы выступаете в качестве продавца, то мошенники находят такие пути обмана, как попросить у вас не только номер телефона и номер карты, по которому можно совершить платеж, но и код проверки подлинности карты. В этом случае стоит помнить, что для осуществления платежа достаточно только номера телефона и номера карты. В данном случае появляется угроза безопасности вашей банковской карты, поскольку благодаря тому, что мошенник будет знать необходимые данные, которые гарантировали ей защиту от посторонних лиц, у него появляется доступ к денежным средствам на вашем счете, которыми он сможет распорядиться. Похожая ситуация может случиться, если вы сами будете выступать в роли покупателя. В данном случае мошенник может попросить у вас предоплату и все данные карты, что грозит вам потерей денежных средств.

В социальных сетях или мессенджерах, когда ваш друг отправляет в социальной сети сообщение с просьбой дать ему взаймы денег или присылает ссылку на незнакомый сайт, стоит быть осторожнее, потому что, скорее всего, его страница была взломана мошенниками. Перейдя по данной ссылке, можно получить вирус, с помощью которого другому лицу станут известны данные о вас и ваших платежных системах.

Набирают популярность случаи, когда мошенники с других страниц предлагают работу с хорошим заработком, скидки на определенные товары и бренды, различные кредиты и другие продукты. Для получения предлагаемых услуг взамен они также могут требовать данные паспорта и вашей карты, что ни в коем случае нельзя делать для своей же безопасности.

Такая же схема действует с сообщениями, которые распространяются рассылками в электронной почте. Мошенники прибегают к различным способам заманивания своей жертвы. Они могут предлагать вам различные продукты, работу, говорить о том, что вы выиграли тот или иной приз и для того, чтобы его получить, необходимо лишь перейти по указанной ими ссылке и ввести необходимые данные. Чаще всего они делают это под видом иностранцев или от имени известных компаний или брендов. Как правило, если просто прочитать полученное сообщение, никаких тяжких последствий не бывает, но переходить по ссылке ни в коем случае не рекомендуется. Это может грозить вам вирусом, который будет контролировать то или иное средство, с которого был осуществлен переход по предоставленной мошенником ссылке.

Мошенники также используют сайты-двойники. Они создают свои сайты под видом уже существующих, делают для них такое же оформление и название, тем самым вводя пользователей в заблуждение, и используют это в своих корыстных целях. В качестве примера можно привести фишинговые сайты банков, которые злоумышленники используют для добычи персональных данных граждан, их счетов и карт. Работа сайта-двойника заключается в том, что при вводе той или иной информации на нем она сразу попадает в руки мошенников. На вашем смартфоне зловредные программы умеют маскироваться под мобильные банки и таиться в разных приложениях, которые вы скачиваете на телефон.

В настоящее время очень остро стоит вопрос о борьбе с мошенничеством с использованием электронных средств платежа. Для этого предлагаются различные меры совершенствования самой платежной системы, но, как показывает практика, также необходимо параллельно улучшать защиту данных банковских карт. Это связано с тем, что на практике мошенничество происходит из-за ненадежности методов идентификации пользователей.

Финансовая индустрия, которая ежегодно теряет от неправомерных действий мошенников большие деньги, пытается внедрить все более современные и продвинутые способы защиты банковских карт.

Сейчас в разных странах, в том числе и России, разрабатывается политика по усовершенствованию технологий идентификации клиентов и их банковских карт, которые будут более защищенными от мошенничеств. По предварительным разработкам они будут представлять собой мини-компьютеры с более широкой функциональной базой, чем до этого обладали банковские карты. Таким образом, технологии будут способствовать не только удобству и быстроте использования новых систем платежей, но и будут оснащены различными барьерами защиты данных от мошенников. Инновационные карты, внедрение которых позволит большинству российских банков решить проблему безопасности операций с пластиковыми картами (карта с биометрической защитой; карта

с датчиком сердцебиения; карта с дисплеем; карта «по требованию»; карта с меняющимся кодом безопасности) [2, с. 169].

Исходя из всего вышесказанного, можно сделать вывод о том, что для предотвращения мошенничества с банковскими картами и платежами на первоначальном этапе нужно реализовывать политику по информированию населения о том, какими способами и методами может осуществляться данный вид мошенничества и как им нужно действовать, чтобы не попасться на уловки злоумышленников. Помимо этого, необходимо разрабатывать новую систему защиты для банковских карт и счетов, что позволит гражданам удобно и спокойно распоряжаться своими платежными средствами без страха, что в определенный момент их могут похитить интернет-мошенники.

---

1. Число киберпреступлений в России [Электронный ресурс] // TADVISER. URL: https://www.tadviser.ru/a/593963 (дата обращения: 15.03.2023). Перейти к источнику Вернуться к статье

2. Третьякова Е. И. Способы совершения мошенничества с использованием электронных средств платежа // Изв. Тульс. гос. ун-та. Экон. и юрид. науки. 2020. № 1. С. 169–176. Вернуться к статье