

*Тастыгина М.В.,
кафедра «Уголовного права и процесса»
Северо – Восточный Федеральный университет
Юридический факультет
Студент 3 курс
Россия, г. Якутск*

ПРОБЛЕМА МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ КАРТ В РОССИИ

***Аннотация:** В статье раскрывается сущность состава мошенничества с использованием пластиковых карт. Раскрываются разновидности такого мошенничества. Перечислены способы самозащиты от злоумышленников.*

***Ключевые слова:** мошенничество, платежные карты, скимминг, вишинг, фишинг, траппинг, банкомат.*

***Annotation:** The article reveals the essence of fraud using plastic cards. The varieties of such fraud are disclosed. The methods of self-defense against intruders are listed.*

***Key words:** fraud, payment cards, skimming, vishing, phishing, trapping, ATM.*

На сегодняшний день информационные технологии приобрели актуальное значение в жизни каждого человека. Компьютеризация внедрилась во все сферы экономической, политической, социальной жизни. Не стала исключением и банковская сфера. В последние годы наблюдается тенденция увеличения количества людей, которые предпочитают безналичную форму расчета. В первую очередь, это объясняется удобством пользования пластиковой картой, которая дает возможность прямого доступа к личному счету, открытому в определенном банке. С развитием новых технологий, стало удобно использовать карты для оплаты интернет-покупок, снимать наличные денежные средства и пополнять счет через банкоматы. Основным достоинством использования

пластиковых карт является экономия времени при оплате товаров или услуг, а также потребителю нет необходимости держать при себе определенные суммы наличных средств.¹

Как свидетельствует статистика Банка России, в 2018 году впервые в России переводы с карты на карту опередили снятие наличных, тогда как общий объем безналичных операций в стране превзошел операции по снятию наличных дважды. Центральный банк РФ в 2018 году опубликовал статистику, в которой видно, что доля транзакций, совершенных при помощи банковских карт, составила около 80 % от числа всех операций, которые провели физические лица за прошлый год. Ежегодно увеличивается количество выпущенных карт, так, по состоянию на 01.01.2019 г. было выпущено порядка 272 608 млн. единиц, что превышает показатели прошлых лет на десятки млн. и является своего рода рекордным показателем за всю историю выпуска пластиковых карт в России. Все эти данные демонстрируют рост популярности безналичной формы оплаты в России. Но вместе с популярностью использования пластиковых карт в геометрической прогрессии растет и число мошеннических действий. Ежегодно мошенники изобретают все новые способы преступных действий с целью хищения денежных средств граждан.²

В наше время мошенничество - один из наиболее распространённых видов преступления в России. Согласно статистике на официальном сайте <https://мвд.рф>, на период за январь – сентябрь 2018 года в России всего зарегистрировано 1521,7 тыс. преступлений. Более половины всех зарегистрированных преступлений (52,5%) составляют хищения чужого имущества, совершённые путём кражи, мошенничества, грабежа, разбоя. Так, из них под статью «мошенничество» подпали 12,3 % преступлений, что является третьим по количеству после кражи и прочих преступлений.

1. ¹ Танасейчук Я. В. Мошенничество с использованием пластиковых карт// Право: современные тенденции: материалы V Междунар. науч. конф. (г. Краснодар, февраль 2018 г.). — Краснодар: Новация, 2018. — С. 57-62

2. ² Сайт Банка России [электронный ресурс] URL:https://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm

Мошенничество представляет собой вид хищения, являющийся сложным уголовно-правовым составом преступления, отличающимся от иных видов хищения объективной стороной, способами совершения преступления. Объективная сторона мошенничества формулируется как совершение хищения чужого имущества или приобретение права на него путем злоупотребления доверием или обмана. Данный вид преступления, как следует из объективной стороны преступления, совершается двумя способами. Так, злоупотребление доверием предполагает использование виновного заведомо ложных доверительных отношений с целью причинения ущерба пострадавшему и завладения чужим имуществом.³

Как и любой другой, данный состав преступления характеризуется особым предметом его совершения. Примечательно, что на сегодняшний день ведутся споры в теории уголовного права относительно определения предмета в указанном виде мошенничестве. Так, Скворцова С.А. считает, что предметом мошенничества с применением платежных карт являются денежные средства, а «банковская карта будет выполнять роль средства совершения преступления». В то же время в аналитическом обзоре от 18.12.2012 г. отмечено, что предмет рассматриваемого преступления - поддельная или принадлежащая другому лицу платежная карта. Предметом преступления признаются явления материального мира, по поводу которых или в связи с которыми совершается преступление, отсюда следует, что мнение, высказанное Скворцовой С.А., представляется наиболее рациональным.

Согласно ч. 1 ст. 159.3 УК РФ мошенничество с использованием платежных карт предполагает обязательный обман уполномоченного работника кредитной, торговой или иной организации. По смыслу содержания ч.1 ст. 159.3 УК РФ можно сделать вывод о том, что не может признаваться мошенничеством «хищение чужих денежных средств . . . , если выдача наличных денежных средств осуществляется посредством банкомата без участия уполномоченного работника

³ Дюсембина Д.Н., Зотина П.С. Анализ ситуации мошенничества с банковскими картами в России и за рубежом// Потенциал Российской экономики и инновационные пути его развития Омск, 12 апреля 2016 г. — с.308–312.

кредитной организации. Указанная формулировка правильна по-нашему мнению, т.к. обман невозможно совершить в отношении неодушевленного предмета - банкомата. Вместе с тем, следует отметить, что некоторые ученые, относят хищения, совершаемые посредством автоматизированных систем, к мошенничеству. При этом они руководствуются следующим. Банкомат состоит из двух частей: инженерной и сейфовой. В инженерной части находится компьютер с установленной операционной системой и прикладным программным обеспечением. Следовательно, банкомат можно признать компьютером, и виновный, вводя в него информацию, получает возможность завладеть чужим имуществом. И обман, в этом случае, учеными воспринимается как обман, направленный на деятельность кредитного учреждения, а техническое устройство является лишь связующим звеном.

Объективной стороной мошенничества может быть предусмотрено использование особых видов устройств, считывающих информацию с магнитных полос карт. Обычно это специально изготовленные для банкоматов клавиатуры, которыми накрывают существующие. При вводе держателем карты ПИН дополнительно установленное устройство считывает и записывает информацию на магнитной полосе. Таким образом, по словам Захарова А. у злоумышленников появляются данные необходимые для дальнейшего изготовления поддельной карты и ее использования в своих целях. Это деяние можно отнести к мошенничеству в сфере компьютерной информации, в то же время данное деяние совершено с использованием платежной карты.

Рассмотрим наиболее популярные виды мошеннических действий с использованием платежных карт в России. Одним из набирающих обороты видов преступлений среди мошенников является скимминг – похищение реквизитов платежной карты при помощи скиммера. Скиммер представляет собой устройство, снимающее с магнитной полосы данные карты, а ПИН-код получают при помощи мини-камеры. В итоге в распоряжении мошенников оказываются все данные, которые помогают реализовать денежные средства картой-клоном потерпевшего. Следующий вид мошенничества – фишинг –

представляет собой создание поддельного сайта определённого банка, который имитирует работу действующего. Данный вид мошенничества предполагает рассылку спам-сообщений и электронных писем клиентам для входа на поддельный сайт, где нужно указать данные о карте, включая номер и ПИН-код. Таким образом, граждане, переходя по ссылке, проходят на поддельный сайт и указывают на нем свои данные, которые впоследствии попадают к мошенникам. Наиболее распространенным видом фишинга являются поддельные интернет-магазины. Они привлекают своих жертв низкими ценами. Аналогом фишинга выступает такой вид мошенничества, как вишинг. Вишинг- средство совершения мошеннических действий при помощи телефона. Так, клиенту поступает звонок от «сотрудника» банка, который предупреждает его о попытке незаконного списания денежных средств со счета клиента и просит позвонить на указанный им номер. Соответственно, клиент, позвонив по данному номеру, попадает к подставному сотруднику банка, который просит указать данные платежной карты. Мошенничество с использованием банкомата называется траппинг – в банкомат устанавливается специальное задерживающее устройство, в результате вставленная в него платежная карта застревает. Злоумышленник, дождавшись, когда жертва едет в отделение банка, убирает задерживающее устройство, забирает карту и снимает оттуда денежные средства.

Таким образом, мы рассмотрели наиболее распространенные в России виды мошеннических действий с использованием платежных карт. Статья 159 Уголовного кодекса РФ гласит: «...Мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации». В статье 159 Уголовного кодекса РФ предусматриваются некоторые проблемы, связанные с её применением на практике, а также с пониманием состава преступления.⁴

⁴ «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ// «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.

С целью повышения эффективности борьбы с мошенничеством при помощи платежных карт, в России проводятся тренинги, семинары, которые направлены на решение проблемы по разработке механизма защиты платежных карт, банкоматов, а также расследований различных вариантов преступлений в сфере банковских преступлений. Для сохранения личной безопасности в процессе использования платежных карт, а также с целью сохранения денежных средств на счете, рекомендуется следовать правилам, минимизирующим риск пострадать от действий преступников. Во первых, перед использованием банкомата, необходимо его осмотреть на предмет обнаружения каких-либо необычных приспособлений. В случае их обнаружения, следует отказаться от использования такого банкомата. При вводе ПИН-кода необходимо прикрывать клавиатуру рукой, чтобы движений не было видно ни камерам, ни сзади стоящим людям. Нельзя сообщать данные своей карты ни полиции, ни оператору банка. При оказании помощи, сотрудники банка и его техническая поддержка, как правило, не спрашивают данные карты, кроме последних цифр платежной карты. Они обычно ограничиваются наводящими вопросами для установления личности клиента. Также не рекомендуется хранить все денежные средства на платежной карте. Лучше установить sms-оповещения на телефон, что позволит быть в курсе действий, происходящих с платежной картой, а также будет возможность вовремя заблокировать карту, в случае совершения не санкционированных списаний, и совершение иных преступных действий. Нельзя оплачивать покупки платежной картой в сомнительных интернет-магазинах. Тщательно проверять всю информацию, полученную от банка по электронной почте или телефону. Не следует переходить по ссылкам, указанным в письме, так как есть вероятность перехода на сайт-дубликат, разработанный мошенниками. Лучше набрать сайт самостоятельно. Следовательно, несмотря на возрастающий уровень преступной деятельности в банковской сфере, платежные карты набирают популярность среди граждан Российской Федерации. Банки, выпуская платежные карты, продолжают их наращивать объёмы и совершенствуют уровень защиты для того, чтобы

минимизировать мошеннические действия с использованием платежных карт. Пользователям карт следует быть бдительными и внимательным при использовании пластиковых карт, чтобы избежать участи стать жертвой мошенничества.⁵

По мнению большинства специалистов, главной задачей для предупреждения и выявления мошенничеств с использованием пластиковых карт на начальной стадии их совершения является обеспечение: а) сопровождения операций с пластиковыми картами в рамках проводимой банками платежной системы; б) безопасности операций с пластиковыми картами на национальном уровне; в) безопасности операций с пластиковыми картами в рамках конкретного банка; г) сотрудничества службы безопасности эмитентов и торговых организаций с правоохранительными органами.⁶

Использованные источники

1. Сайт Банка России [электронный ресурс]
URL:https://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm
2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ// «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.
3. Дюсембина Д.Н., Зотина П.С. Анализ ситуации мошенничества с банковскими картами в России и за рубежом// Потенциал Российской экономики и инновационные пути его развития Омск, 12 апреля 2016 г. — с.308–312.
4. Мусьял И.А. Мошенничество с использованием платежных карт// Проблемы правоохранительной деятельности.2017. № 1. — с. 147–151.
5. Танасейчук Я.В. Мошенничество с использованием пластиковых карт// Право: современные тенденции: материалы V Междунар. науч. конф. (г. Краснодар, февраль 2018 г.). — Краснодар: Новация, 2018. — С. 57-62.

5. ⁵ Мусьял И.А. Мошенничество с использованием платежных карт// Проблемы правоохранительной деятельности.2017. № 1. — с. 147–151.

6. ⁶ Танасейчук Я. В. Мошенничество с использованием пластиковых карт// Право: современные тенденции: материалы V Междунар. науч. конф. (г. Краснодар, февраль 2018 г.). — Краснодар: Новация, 2018. — С. 57-62