Карева Виктория Юрьевна
студентка
Уварова Анастасия Олеговна
студентка
Симонова Ольга Владимировна
старший преподаватель
ФГБОУ ВО «Ульяновский государственный
педагогический университет им. И.Н. Ульянова»
г. Ульяновск, Ульяновская область

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ КАРТ

Аннотация*: в приведенной статье исследуются актуальные проблемы, охватывающие тематику мошенничества с использованием платежных карт, приводятся примеры видов совершения подобных противоправных деяний. Приведены точки зрения экспертов, касающиеся особенностей толкования соответствующих норм и проблем квалификации специальных разновидностей мошенничества.*

Ключевые слова*: мошенничество с использованием платежных карт, электронные платежные карты, электронный расчет, мошенничество, статья 159, 3 УК РФ, бесконтактная оплата, банковская карта.*

В настоящее время особой популярностью пользуются электронные платёжные карты. Под этим понятием подразумевается средство безналичного расчёта за определённые товары или услуги. Использование карт обусловлено тем, что такой расчёт является наиболее практичным и удобным. Приобретая карты электронных платежей, многие люди ведут бизнес в сети Интернет, оплачивают услуги, совершают покупки и выполняют ряд других финансовых операций. Но, несмотря на столь существенные плюсы в использовании электронных платёжных карт, нельзя не отметить те недостатки, которые связаны с несанкционированными перечислениями денег между счетами владельцев. Говоря о данном факте, несомненно, каждый человек без исключения вспоминает о таком

понятии, как мошенничество. И тут же задаётся вопросом: «Как с ним бороться и какие меры предпринимает законодатель для устранения столь серьёзной проблемы?».

Уголовный Кодекс Российской Федерации от 13 июня1996 года №63-ФЗ (ред. от 01.04.2019) (далее по тексту – УК РФ) вводит новый состав преступления – «Мошенничество с использованием электронных средств платежа» (ст. 159.3 УК РФ). Ответственность за данный вид преступления подразумевает широкий диапазон санкций: от штрафа до лишения свободы. Представляется, что мошенничество с использованием платежных карт – это хищение чужого имущества, которое совершено с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты.

Достаточно большое количество видов мошенничества в настоящее время связано именно с банковскими картами. Распространён следующий вид:

СМС – мошенничество. Владельцу банковской карты поступает сообщение с информацией о том, что его карта заблокирована. Для того, чтобы восстановить доступ, пользователю говорят о том, что необходимо по указанному номеру совершить определённые действия. Мошенник, представляясь сотрудником банка, ловко выманивает всю нужную информацию.

В 2018 году появился новый вид мошенничества – запуск вирусной программы в банкоматах и терминалах. Суть заключается в том, что устройства выдачи денег заражаются специальным вирусом-трояном, который дает злоумышленникам возможность снять наличность из банкомата, введя на клавиатуре специальный код. Существует и несколько способов завладеть вашим электронным кошельком. В настоящее время появилось такое понятие, как брутфорс, то есть взлом электронного кошелька, с помощью подбора пароля. Мошенники, используя особые программы для взлома (чекеры) ловко подбирают пароль к кошельку пользователя.

Популярен и такой вид мошенничества, как взлом электронной почты, с последующим получением доступа к электронному кошельку. Злоумышленник, применив все необходимые средства, взламывает электронную почту, получает

личную информацию из писем пользователя. В дальнейшем с помощью системы восстановления доступа получает доступ к платежной системе.

С.В. Смолин, кандидат юридических наук, в журнале «Законность» рассуждал на тему использования мошенниками пассивной формы обмана при совершении преступлений с использованием платежных карт. Он утверждал, что существуют две противоположные позиции. Одни не поддерживают мнение о возможности использования пассивной формы обмана [8, с. 51]. Л.В. Боровых и Л.А. Корепанова считают, что владелец карты не обманывает сотрудника, хотя и умалчивает о своей личности [1, с. 82]. Н.В. Тимошин, а также С.М. Кочои утверждают, что при расчетах картами не считается обязательным факт оставления подписи в чеке или предъявление паспорта и других документов, удостоверяющих личность, достаточно вставить карту в соответствующее устройство [3, с. 106; 9, с. 12].

На сегодняшнее время актуально то, что граждане без чьей-либо помощи пользуются терминалами оплаты, для этого банковскую карту вставляют в банкомат, вводят пин-код и после того, как осуществилась оплата, забирают карту. Именно поэтому каждый человек может расплатиться любой картой, если известен пин-код. Однако существуют так называемые бесконтактные платежи. Это могут быть карты без пин-кода или платежи с помощью смартфона. В телефон вносятся все данные карты, и при взаимодействии смартфона и терминала осуществляется электронная оплата покупок. Таким образом, в результате вышесказанного увеличились случаи мошенничеств. Разумеется, платежные карты и бесконтактная оплата – это просто, легко и удобно. Но на наш взгляд, человек должен быть внимательным.

Особое волнение вызывает и то, что мошенничество с использованием электронных платежных карт, нередко носят организованный характер и в том числе именуются типом преступных промыслов организованных преступных групп [6, с. 59].

Криминологи отмечают «преступления в области компьютерной информации и хищение с использованием электронных средств считаются областью

повышенного внимания преступных сообществ, которые действуют как на национальном, так и транснациональном уровнях [7, с. 61].

Например, «По данным издательства Paypers, в феврале 2016 года в Великобритании группа неизвестных выставила на продажу различную финансовую информацию более чем о 100 000 жителей. Мошенники крадут банковские карты и продают их за 2 фунта стерлингов» [2, с. 310].

В Соединенных штатах количество поддельных платежных карт за последние годы возросла на 317%. Согласно опросам Unisys Security Insights, которые были опубликованы в 2015 году, около 60% жителей США находятся в страхе, они боятся, что их платежные карты попадут в руки к мошенникам.

В России борьба с мошенничеством заключается в том, что проводятся различные семинары, тренинги, обучения, которые направлены на защиту платежных карт, банкоматов.

С.О. Лукьянов акцентирует ряд особенностей в области увеличения защищенности расчетов с применением банковских карт и мероприятий, связанных с профилактикой мошенничества с применением платежных карт и их реквизитов. Согласно его суждению, следует использовать:

1. Защиту программных разработок – употребление экспертной системы предоставления авторизации с целью роста особых свойств обслуживания держателей платежных карт и избежание возможных ситуаций.

2. Защиту аппаратного устройства – техническое оснащение банкоматов и установка антискимминговых устройств для совершенствования механизма карт.

3. Правовую защиту – очень важно устанавливать строгие нормативно-правовые нормы, которые станут держать под контролем деятельность не только банковских учреждений, но и торгующих товаром точек, в которых будет предусмотрена ответственность сторон за несоблюдение правил обращения банковских карт.

4. Профилактическую защиту – к предоставленной группе следует отнести лимитирование по сумме транзакции, иными словами, ограничение суммы на

операцию в банкомате и покупку в торговой точке, и кроме того совершенствование финансовой и правовой грамотности людей в сфере обращения банковских карт [5, с. 117–118].

В. М. Кузин выделяет два способа улучшения защищенности банковских карт:

1. Замена незащищенных технологий в сфере разработки, создания банковских карт и контроля над операциями с их использованием, миграция в наиболее безвредные технологии.

2. Охрана имеющихся незащищенных технологий дополнительными мерами безопасности [4, с. 36].

Для того что бы оставаться в безопасности, необходимо следовать нескольким правилам:

1. Перед использованием банкомата необходимо его осмотреть. Если Вы обнаружили какие-либо приспособления, особенно на устройстве ввода, то лучше не использовать данный банкомат.

2. Правильнее пользоваться банкоматом, который будет находиться в отделении банка.

3. При вводе пин-кода нужно прикрывать клавиатуру рукой, чтобы движений не было видно сзади стоящим людям.

4. Нельзя никому сообщать данные своей карты.

5. Не нужно хранить все денежные средства на платежной карте.

6. Нельзя оплачивать платежной картой покупки в сомнительных интернет-магазинах.

7. Пользователи карт должны быть бдительными и внимательными для того, чтобы не стать жертвой преступной деятельности.

Вышеизложенное позволяет сделать вывод о том, что преступления в банковской сфере с каждым годом возрастают как в России, так и в зарубежных странах. Владельцам платежных карт необходимо быть внимательными и бдительными, чтобы не попасть в руки к мошенникам.

Список литературы

1. Боровых Л.В. Проблема квалификации хищения с использованием банковских карт / Л.В. Боровых, Л.А. Корепанова // Российский юридический журнал. – 2014. – №2. – С. 82–87.

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

3. Кочои С.М. Новые нормы о мошенничестве в УК РФ: особенности и отличия // Криминологический журнал Байкальского государственного университета экономики и права. – 2013. – №4. – С. 104–110.

4. Кузин М.В. Современные методы противодействия мошенничеству с банковскими картами // Безопасность информационных технологий. – 2012. – №3. – С. 35–37.

5. Лукьянов С.О. Мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник Тихоокеанского государственного технологического университета. – 2018. – №2. – С. 117–118.

6. Никитенко И.В. Координация преступных действий организованных групп: проблемы законодательства и правоприменительной практики / И.В. Никитенко, Т.В. Якушева // Вестник Дальневосточного юридического института МВД России. – 2017. – №2 (39). – С. 58–63.

7. Никитенко И.В. Организация преступного сообщества: проблемы квалификации / И.В. Никитенко, Т.В. Якушева // Уголовное право. – 2010. – №5. – С. 58–62.

8. Смолин С.В. Мошенничество с использованием платёжных карт // Законность. – 2016. – №1. – С. 49–51.

9. Тимошин Н.В. Новые нормы о мошенничестве в УК РФ: рекомендации по применению // Уголовный процесс». – 2013. – №1. – С. 10–15.