***УДК 336***

# МОШЕННИЧЕСТВО В СФЕРЕ ИСПОЛЬЗОВАНИЯ ПЛАСТИКОВЫХ КАРТ

**Сидорова Н.П., студентка 5 курса экономического факультета**
**Научный руководитель – Банникова Е. В.,**
**кандидат экономических наук, доцент**
**ФГБОУ ВО Ульяновский ГАУ**

***Ключевые слова:*** *мошенничество, скримминг, траппинг, банковская карта, фишинг.*

*В данной статье раскрывается состав мошенничества с использованием пластиковых карт. Рассматриваются разновидности такого мошенничества. Отдельное внимание уделено особенностям мошенничества в 2022 году.*

В последнее время банковские карты становятся неотъемлемой частью каждого человека. С их помощью возможна оплата в торговых и сервисных организациях, больницах и других общественных местах. Однако увеличение количества пластиковых карт у населения вызывает рост случаев мошенничества на рынке безналичных расчетов.

Помимо снятия средств и пополнения счета через банкомат пластиковыми банковскими картами можно совершать большое количество других операций, например, переводить денежные средства, оплачивать различные услуги и штрафы, кредиты и даже коммунальные платежи.

По данным Центробанка РФ, количество банковских карт, эмитированных кредитными организациями, ежегодно увеличивается примерно на 120 тыс. штук. Большинство граждан России используют пластиковые банковские карты: для получения пособий, зарплат, стипендий, пенсий и т.д. Соответственно любой держатель пластиковой банковской карты может стать жертвой мошенничества. С каждым годом количество преступлений данной категории растет, мошенники используют разные способы совершения преступления.

Несмотря на то, что банковские счета и платежные средства

(банковские карты) имеют достаточный уровень защиты, случаи кражи денежных средств продолжают поступать в криминальную статистику.

В настоящее время существует множество видов мошенничества с использованием пластиковых карт. Используются все доступные средства – телефон, сайты, онлайн-банкинг, мобильный банкинг и другие каналы. Рассмотрим самые распространенные из них:

1. По телефону. Этот вид мошенничества имеет множество вариаций, объединенных тем, что держателю карты звонят с неизвестного номера и под любым предлогом просят сообщить его данные.

2. Через СМС. Эта схема имеет много общего с предыдущим способом. Разница заключается в том, что ложная информация приходит в тексте СМС-сообщения. Рассылка осуществляется с незнакомого номера, но мошенники подписываются известной компанией.

3. Через мобильный банк. Услуга «Мобильный банк» позволяет совершать операции с помощью SMS-команд. Для перевода средств другому клиенту достаточно отправить сообщение на короткий номер банка с телефона, который привязан к карте.

Преступники не всегда преследуют цель узнать реквизиты карты. Самый простой способ незаконного обогащения – это убедить клиента в том, что он должен перевести деньги самостоятельно. Злоумышленники предлагают приобрести товары по выгодной цене и требуют перечисления предоплаты или полной суммы.

Некоторые мошенники действуют как фиктивные компании, предлагающие удаленную работу в интернете с хорошим заработком.

Распространённой схемой мошенников также является «помощь родным».

4. Скимминг. В банкомат устанавливается специальное оборудование – накладка на клавиатуру и скиммер (вставляется в картоприемник и позволяет считывать данные с магнитной полосы). Используя полученную информацию, мошенники делают дубликат карты и снимают с нее все средства.

5. Траппинг. Относительно новый вид мошенничества с банковскими картами, заключающийся в том, что преступники вставляют в картоприемник кусок пластика с прорезью по центру.

Клиент вставляет карту в банкомат, она попадает в прорезь и остается в автомате. Затем появляется злоумышленник, предположительно тоже сталкивавшийся с такой ситуацией, и советует ввести пин-код. Когда это не удается, клиент уходит, а злоумышленник извлекает карту с помощью заранее подготовленных инструментов.

6. Махинации с банковскими картами через интернет. Этот вид мошенничества называется фишингом. Мошенники создают поддельный сайт популярного интернет-магазина или интернет-банка, который выглядит как оригинал, но его URL – адрес отличается от реального на один символ. Для оплаты покупки или авторизации пользователь вводит конфиденциальные данные на фиктивной странице, которая попадает в руки злоумышленников.

7. Кража банковской карты. Некоторые преступники не хотят использовать изощрённые способы мошенничества, а предпочитают просто украсть карточку.

Геополитический кризис сыграл на руку мошенникам. В первые же дни после введения санкций против России и ЦБ РФ злоумышленники начали пытаться заработать на вводимых ограничениях. Еще один новый способ мошенничества – сбор денег на якобы гуманитарные нужды.

По данным ЦБ, в первом квартале 2022 года россияне переводили деньги мошенникам 258 097 раз, что на 8,5% больше, чем за аналогичный период прошлого года. При этом с января по март 2021 года зафиксировано 237 737 таких случаев.

Однако количество случаев вымогательства средств с помощью метода социальной инженерии сократилось до 52,2% с 56,2% в 2021 году.

Во втором квартале 2022 года мошенники провели банковские операции без согласия клиентов на общую сумму 2,85 млрд. рублей. Это на 11% меньше, чем за аналогичный период 2021 года (3,01 млрд. руб.). Количество зафиксированных сделок также уменьшилось: 211 263 за квартал (236 971 во втором квартале 2021 года). Доля социальной инженерии за год несколько снизилась – на ее долю пришлось 44,8% всех таких операций (годом ранее – 47%).

Больше всего таких операций совершается при оплате товаров и услуг через интернет – во втором квартале 2022 года их зафиксировали

139 950. На втором месте – дистанционное банковское обслуживание физлиц (37 272). Эти показатели ниже, чем в 2021 году. Однако количество мошеннических операций через банкоматы и платежные терминалы (32 396), дистанционное обслуживание юридических лиц (1 645) значительно увеличилось по сравнению с 2020 г.

Анализ отчетных инцидентов, связанных с информационной безопасностью при переводе денежных средств, показывает, что чаще всего для мошенничества злоумышленники использовали банкоматы, терминалы, импринтеры, сайты для оплаты товаров и услуг, а также системы дистанционного банковского обслуживания физических и юридических лиц.

Предотвращение мошенничества с банковскими картами – совместная задача государства и банковских учреждений, без которой невозможно дальнейшее развитие безналичных расчетов.

В России для повышения эффективности борьбы с данным видом мошенничества проводятся различные семинары, тренинги, направленные на решение задачи, связанной с разработкой механизма защиты платежных карт, банкоматов и исследованием различных вариаций преступлений в этой сфере. Для минимизации риска стать жертвой мошенничества с использованием платежных карт необходимо соблюдать правила основные безопасности.

**Библиографический список:**

1. Архипова, С.А. Государственный финансовый контроль: его сущность и значение / С.А. Архипова С.А. // Материалы VI Международной студенческой научной конференции «В мире научных открытий». – Ульяновск, 2022. – С. 4582-4587.

2. Михайлова, К.С. Осуществление контроля за движением денежных средств на предприятии / К.С. Михайлова // Материалы VI Международной студенческой научной конференции «В мире научных открытий». – Ульяновск, 2022. – С. 5037-5041.

3. Турыкина, В.А. Контроль и ревизия продажи алкогольной продукции / В.А. Турыкина // Материалы IV Международной студенческой научной конференции «В мире научных открытий». – Ульяновск, 2020. – С. 265-269.

4. Исаева, В.В. Как не стать жертвой карточных мошенников.

личный опыт / В.В. Исаева // Материалы IV Международной студенческой научной конференции «В мире научных открытий». – Ульяновск, 2020. – С. 287-290.

5. Банникова, Е.В. Внутренний аудит в системе экономической безопасности / Е.В. Банникова, О.И. Хамзина О.И., А.А. Навасардян // Материалы Национальной научно-практической конференции «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения». – Ульяновск, 20-21 июня 2019 г. – Ульяновск: УлГАУ, 2019. – С. 225-229.

## USE FRAUD PLASTIC CARDS

**Sidorova N.P.**

***Keywords:*** *fraud, skimming, trapping, bank card, phishing.*

*This article reveals the composition of fraud using plastic cards. Varieties of such fraud are considered. Special attention is paid to the features of fraud in 2022.*