УДК 336.01

РИСКИ МОШЕННИЧЕСТВА В СФЕРЕ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Головкова Е.А.

студент,

Вятский государственный университет,

Киров, Россия

Загребина А.А.

студент,

Вятский государственный университет,

Киров, Россия

Аннотация

В статье раскрыты понятия электронных денег и электронных платежей, основные способы кибермошенничества, также рассмотрены основные способы борьбы с мошенничеством в системе электронных платежей. Материалы статьи освещают вопросы основных положительных отличий использования электронного счета в сравнении с банковскими картами и данных о киберпреступлениях за 2020 год.

Ключевые слова: электронные деньги, пластиковые карты, электронные платежные услуги, безопасность, Интернет-технологии, банк, товары и услуги, электронный кошелек, кибербезопасность.

RISKS OF FRAUD IN THE SPHERE OF ELECTRONIC PAYMENTS

Golovkova E.A.

student,

Vyatka State University,

Kirov, Russia

Zagrebina A.A.
student,
Vyatka State University,
Kirov, Russia

Annotation
The article reveals the concepts of electronic money and electronic payments, the main methods of cyber fraud, and also discusses the main ways to combat fraud in the electronic payment system. The materials of the article highlight the main positive differences between the use of an electronic account in comparison with bank cards and cybercrime data for 2020.

Key words: electronic money, plastic cards, electronic payment services, security, Internet technologies, bank, goods and services, electronic wallet, cybersecurity.

Рынок современных платежных услуг начал формироваться примерно в 1990-х гг. Это произошло с появлением новых платежных средств: кредитных и дебетовых карт, развитием интернет технологий, появлением электронных денег, возможностью покупать товары и услуги посредством сети Интернет.[1]

Электронные деньги – современный механизм, позволяющий продавцам и покупателям обменивать товары и услуги на денежные средства через Интернет без личного контакта и посредников. Преимуществами использования электронных денег перед пластиковыми картами при использовании в сети являются:

- За перевод средств со помощью электронного кошелька, взимается гораздо меньшая комиссия, по сравнению с другими средствами перевода.

- Обезличенность данного платежного средства, оно позволяет покупателю (плательщику) оставаться конфиденциальным, так же, как и сам платеж.
- При создании электронного счета плательщик не несет никаких затрат.
- Электронные кошельки являются более защищенным средством по сравнению со счетами банковских пластиковых карт.

С целью минимизации рисков разработана схема электронных платежей посредством платежных систем с использованием дебетовых пластиковых карт в интернет-среде. Системы интернет-кредитования подобны классическим системам с использованием кредитных карт. Отличие в том, что все без исключения транзакции совершаются посредством сети-Интернет и по этой требуют дополнительной защищенности, а также аутентификации.[4]

Параметры банковской карты при оплате передаются в систему интернет-платежей с целью последующей авторизации либо посредством веб-сайта магазина, либо непосредственно через сервер платежной системы, что уменьшает возможность их получения третьими лицами. С целью избежания перехвата информации злоумышленниками в сети данные при передаче шифруются с использованием защищенных протоколов. Далее система интернет-платежей взаимодействует с традиционной платежной системой, отправляя запрос на авторизацию. Если банк-эмитент имеет онлайн-базу счетов, процессинговый орган отправляет ему запрос на авторизацию карты; если такой базы нет, то процессинговый центр сам хранит информацию о состоянии счетов держателей карт, стоп-листы и выполняет запросы на авторизацию. После подтверждения запроса через систему интернет-платежей результат авторизации передается в магазин, предоставляющий услугу или осуществляющий отгрузку товара, а процессинговый центр передает информацию о совершенной транзакции в расчетный банк.[2]

Начиная со времени пандемии 2020 года, быстрыми темпами начало развиваться кибермошенничество, представляющее собой активные действия в Интернет-пространстве путём обмана с целью получения выгоды. Преступления такого вида связаны прежде всего с хищением денежных средств, бонусов карт лояльности и др. физических и юридических лиц, используя личные данные. Кибермошенники используют возможности информационных технологий в преступных целях: создают дубликаты сайтов официальных ресурсов, взламывают аккаунты пользователей популярных сервисов и другое. [5]

В результате деятельности кибермошенников только в 2020 году:

1. Совершено около 170 тысяч краж с электронных кошельков и банковских счетов;
2. Жители РФ недосчитались на своих счетах 9,77 млрд рублей;
3. Общий ущерб от экономических преступлений, по данным МВД, составил 450 млрд руб.;
4. Только 14,6% средств, потерянных россиянами в результате действий злоумышленников, были возмещены банками своим клиентам;
5. С помощью терминалов и банкоматов у россиян было похищено более 740 млн рублей, клиенты смогли вернуть менее 10% от этой суммы;
6. Сумма хищений в результате кибератак на организации увеличилась на 46%, превысив 1 млрд руб.; количество транзакций, уменьшившись чуть более чем на треть, составило 3 млн.

Также особой популярностью у кибермошенников пользуются кредитные карты.

Мошенничество осуществляется несколькими способами: от подглядывания пин-кода до сложных хакерских атак. Самый примитивный механизм – кража пластикового носителя, если пин-код уже известен. Комбинацию легко подсмотреть у жертвы возле банкомата, далее остается незаметно завладеть картой.

Фишинг — это механизм, суть которого заключается в краже конфиденциальных данных пользователя. Чаще всего злоумышленники звонят, выдавая себя за сотрудника банка, сообщая о якобы незаконном списании или переводе денежных средств. Для отмены операции жертве необходимо назвать код из СМС или сообщить секретную комбинацию (код CVV на обороте).

Жертв таких действий несколько: физическое лицо, потерявшее средства, и банк, понесший репутационные риски.

С точки зрения закона, в случившемся виновен сам клиент, так как он сообщил третьим лицам информацию, которую должен хранить в тайне.

Выявление и предотвращение мошенничества в этом случае возможно только за счет повышения финансовой грамотности населения и разработки специальных моделей машинного обучения. Специалисты создают специальные модели и обучают их, но на практике это требует дорогостоящих ресурсов.

Более эффективный канал противодействия — работа с клиентами: обучение и разъяснение ключевых моментов информационной безопасности. В первую очередь в группе риска клиенты старшего возраста, которые отличаются особой доверчивостью. Всем следует помнить, что сотрудники банка не запрашивают одноразовые пароли из СМС или CVV-кодов.

Фарминг - разновидность мошенничества, при котором на устройство жертвы загружается вредоносный код. С его помощью подменяется информация об IP-адресах, после чего пользователь автоматически перенаправляется на поддельные сайты. Далее его просят ввести личную информацию, которая будет использована злоумышленниками. Фарминг нацелен на пользователей мобильного и онлайн-банкинга, а также платежных систем или сервисов обмена валюты.

В отличие от фишинга, от жертвы не требуется никаких дополнительных действий, перенаправление на сайты выполняется автоматически. Этот вид воровства практически отсутствует, так как фарминг работает только с малоизвестными финансовыми учреждениями.

Скимминг - этот способ обмана уже стал классикой, но сегодня он становится все менее распространенным по мере роста популярности чиповых карт. Для кражи денег злоумышленники используют специальные устройства, называемые скиммерами. Выпускаются в виде небольшой накладки на отверстие для приема карты в банкомате. Пока жертва снимает наличные или выполняет другие действия, скиммер копирует информацию с магнитной полосы карты. Продуманно сделанная накладка трудно различима даже профессионалу: она тонкая, почти незаметная, выполнена в той же цветовой гамме, что и сетевой банкомат. Помимо скиммера, мошенники используют миниатюрные камеры для слежки за пин-кодом.[3]

Платежная индустрия использует три основные технологии для защиты данных держателей карт в инфраструктуре и решениях для хранения: двухточечное шифрование (P2PE), шифрование в состоянии покоя и токенизация.

Для прибыльного и безопасного развития платежной системы необходимо устранить барьеры, препятствующие расширению российской национальной платежной системы.

Таким образом, с развитием электронных денег стало развиваться кибермошенничество. Для того, чтобы предотвратить себя от действий злоумышленников, необходимо повышать финансовую грамотность населения в области пользования электронными платежными средствами.

Библиографический список:

1. Авагян Г. Л. Деньги, кредит, банки: Учебное пособие / Г.Л. Авагян, Т.М. Ханина, Т.П. Носова. — М.: Магистр, НИЦ ИНФРА-М, 2019. — 416 с.
2. Белотелова Н. П., Белотелова Ж. С. Деньги. Кредит. Банки. — М.: Дашков и К, 2020. — 380 с.
3. Договоры банковского вклада и банковского счета. М.: Юрайт, 2020. 111 с.

4. Щербакова Н.В. Цифровые технологии в банковском секторе РФ: особенности и сопутствующие угрозы // Вестник Кемеровского государственного университета. Серия: Политические, социологические и экономические науки. 2021. Т. 6. № 1.
5. Мальцева С.М., Строганов Д.А., Кокорин А.Р., Куликова А.А К ВОПРОСУ О МЕТОДАХ ЗАЩИТЫ ОТ ФИНАНСОВОГО КИБЕРМОШЕННИЧЕСТВА // АНИ: экономика и управление. 2020. №2 (31). URL: https://cyberleninka.ru/article/n/k-voprosu-o-metodah-zaschity-ot-finansovogo-kibermoshennichestva (дата обращения: 26.12.2022).

Оригинальность 83%