УДК 336
DOI 10.51691/2500-3666_2022_5_13

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ «ЭЛЕКТРОННЫХ ДЕНЕГ» С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Годунова М.С.
студент кафедры современных технологий управления,
МИРЭА – Российский технологический университет (РТУ МИРЭА),
Москва, Россия

Печникова Е.Ю.
студент кафедры современных технологий управления,
МИРЭА – Российский технологический университет (РТУ МИРЭА),
Москва, Россия

Аннотация

Трудно представить современного человека, который не пользовался бы технологией электронных денег. Цель статьи заключается в рассмотрении электронных денег с точки зрения безопасности. Рассмотрены теоретические основы цифровой валюты, её виды и значение каждой категории. Выделены основные виды мошенничества, а также способы защиты своих сбережений. В результате исследования определена важность обеспечения безопасности электронных денег.

Ключевые слова: электронные деньги, безопасность, QIWI, мошенничество, онлайн.

MODERN TECHNOLOGIES OF «ELECTRONIC MONEY» FROM THE POINT OF VIEW OF INFORMATION SECURITY

Godunova M.S.
student Department of modern management technologies,
MIREA – Russian Technological University (RTU MIREA),
Moscow, Russia

Pechnikova E.Y.
student Department of modern management technologies,
MIREA – Russian Technological University (RTU MIREA),
Moscow, Russia

Abstract
It is difficult to imagine a modern person who would not use the technology of electronic money. The purpose of the article is to consider electronic money from the point of view of security. The theoretical foundations of digital currency, its types and the meaning of each category are considered. The main types of fraud are highlighted, as well as ways to protect your savings. As a result of the study, the importance of ensuring the security of electronic money was determined.

Keywords: electronic money, security, QIWI, fraud, online.

Вместе со стремительной цифровизацией всего мира неизбежным явлением стало возникновение электронных денег. На сегодняшний день сложно представить жизнь без возможности расплачиваться, не используя наличные средства. Существует немалое количество систем электронных денег, у каждой из которой свои отличительные черты. Необходимо разбираться в типах этих систем, чтобы понимать, как они функционируют и грамотно использовать. В силу развития и быстрого распространения электронных денег, важно уделить особое внимание безопасности и системе защиты пользователей [1].

Несмотря на то, что почти каждый человек сталкивался с данным понятием, как такового единого определения «электронных денег» еще нет. Поэтому выделим характеристики, присущие данному термину. Во-первых, в качестве места хранения подобных денег используется электронный носитель. Во-вторых, они принимаются к оплате в различных местах. В-третьих, они должны выпускаться эмитентом только в том случае, когда будут получены денежные средства в объеме, не меньшем, чем эмитируемая стоимость [7].

Системы электронных денег остаются актуальными в России по сей день. Банки и торговые предприятия вкладывают ресурсы в развитие цифровых возможностей, чтобы удовлетворять запросы общества. Несмотря на вводимые санкции против нашего государства, Россия не собирается отказываться от цифровой валюты и активно развивает свои системы. Например, Центральный Банк РФ в апреле 2022 года зарегистрировал платежную систему – Hello, представляющую из себя целый набор платежных сервисов и различных организаций, которые взаимодействуют согласно правилам платежной системы с целью реализации переводов денежных ресурсов [6].

Выделяют следующие формы электронных денег по виду технического устройства: на базе сетей и на базе смарт-карт.

Первая форма почти не имеет отличий от пластиковых карточек, здесь ключевую роль играют микрочипы. Примером могут послужить Mondex и Visa Cash.

В основе электронных денег на базе смарт-карт лежат программные системы, представленные в виде сетевого ресурса или программы. Эта форма защищается шифрованием и является наиболее защищенной. Примером являются Яндекс.Деньги, Вебмани и Киви. Существует множество видов электронных денег, для простоты понимания отразим характеристику наиболее популярных систем в таблице 1.

Таблица 1 – Характеристика различных систем электронных денег

Вид денег	**Характеристика**
Яндекс-деньги	Предоставляют возможность осуществления мгновенных платежей в пределах системы, а также управление кошельком напрямую с официального сайта. Очень популярны в России. Рубли – единственная валюта системы.
Webmoney	Нет ограничений, возможность осуществлять мгновенные переводы. Операции осуществляются по защищенным каналам.
QIWI	Используемые валюты: российские рубли, доллары, евро и казахские тенге.
PayPal	Возможность осуществления операций по всему миру. Предоставляют защищенное соединение для осуществления платежей. Пользуется популярностью среди иностранных работников.

Как и любая другая система, электронные деньги имеют свои преимущества и недостатки.

В качестве основных достоинств принято выделять следующее.

1. Благодаря использованию электронных денег не возникнет необходимость выдачи сдачи.

2. Государство не затрачивает ресурсы на печать и выпуск банкнот.

3. Нет зависимости между суммой средств и его весом – удобство в «переносе». Экономия времени и пространства.

4. Отсутствует необходимость пересчета денег – система делает это автоматически.

5. Сохраняемость. Их невозможно повредить, деньги не подлежат износу, так как находятся на электронном носителе.

6. Безопасное использование. Отсутствует возможность получить фальшивые деньги [9].

Однако помимо перечисленных достоинств, следует выделить ряд существенных недостатков электронных денег.

1. В случае порчи носителя электронных денег нет возможности их восстановления.

2. Специфика использования специальных инструментов обращения и хранения.

3. Острая зависимость от интернета.

4. В случае ослабленной защиты, украсть деньги становится очень просто.

5. Как правило, взимается комиссия за перевод денег с одной системы на другую.

6. Риск того, что мошенники отследят конфиденциальную информацию пользователя.

Безусловно, в современных условиях быстрое развитие систем электронных платежей упрощает жизнь человека. Однако финансовое мошенничество не стоит на месте, и аферисты придумывают все более изощренные способы воровства и схемы обмана. Вопрос обеспечения безопасного использования электронных денег является актуальным в наше время, поэтому стоит определить основные виды финансового мошенничества.

Под термином фрод сегодня понимают вид мошенничества в области IT, представляющий собой несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях связи. Карточным фродом или кардингом называют вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем [8]. С кардингом сталкиваются обычно люди, которые пренебрегают элементарными правилами безопасности, они доверчивы и невнимательны, например, при пополнении кошелька, предоставлении контента или доступа к играм, покупке электронных авиабилетов или билетов на концерт. Также стать жертвой кардинга можно, сообщив пароль или код из SMS людям, представляющимся сотрудниками банков, или переслав деньги человеку, который попал в «трудную жизненную ситуацию» [2].

Схем данного мошенничества множество, но выделяют два классических вида кардинга: фишинг и скимминг [5]. Поподробнее разберемся, что представляют собой данные махинации.

Фишинг (phishing от англ. fishing - рыбная ловля, закидывание удочки) - это вид интернет-мошенничества, заключающийся в получении данных карты непосредственно от ее держателя [4]. Способы получения информации, представляющей интерес для афериста, разнообразны. Это может быть и массовая рассылка электронных писем или SMS от имени банков, брендов, социальных сетей, и всплывающие окна на сайтах, и поддельные страницы известных веб-сайтов. Копии сайтов обычно внешне мало чем отличаются, поэтому в таких случаях важно обращать внимание на название ссылки, по которой необходимо перейти.

При вишинге (англ. vishing - от voice phishing) злоумышленники также выманивают конфиденциальную информацию владельца карты, однако посредством телефонного звонка, представляясь сотрудниками банка, покупателями товаров и так далее. Владелец карты должен понимать, что всегда можно перезвонить по официальному номеру банка с целью выяснения достоверной информации о текущем положении платежной карты, а также нужно помнить, что, сообщая персональные данные, он становится жертвой мошенничества [4].

Еще одним методом хищения электронных средств является скимминг. Скимминг (от англ. «to skim» - бегло прочитывать, скользить) - это копирование данных платежной карты с помощью специального инструмента (скиммера). Данные карты владельца считываются при ее вставлении в банкомат, также злоумышленники устанавливают мини-камеры или накладки на клавиатуру [4]. В связи с появлением бесконтактных способов оплаты скиммеры стали использовать новое оборудование для считывания данных с карт, так появился онлайн-скимминг. В практику этих аферистов входит проникновение на компьютеры сотрудников банков и проведение микротранзакций, позволяющих получать информацию о карте, в том числе и CVV-код [3].

Сегодня никто не может дать гарантию сохранности денежных средств, также отсутствуют универсальные правила безопасности в электронной среде. Мошенники подстраиваются под современные условия и придумывают все более хитрые способы выудить деньги, найдя лазейки даже к самым осторожным и предусмотрительным пользователям. Именно в силу того, что интернет является ненадежным средством хранения информации, очень важно обеспечить безопасность всех проводимых цифровых платежей. Для минимизации рисков финансовых потерь от мошеннических действий можно воспользоваться рядом советов и рекомендаций.

Во-первых, следует хранить PIN-код, логин, пароль, проверочные слова или специальные коды в безопасном месте, не сообщая их третьим лицам, и не стоит распространяться об одноразовых паролях из SMS. Во-вторых, при онлайн шопинге следить за использованием официальных сайтов и, оставляя реквизиты карты на сайте, нужно сверить веб-адрес с официальным названием сервиса. В-третьих, банкоматы нужно выбирать только те, которые стоят под камерами, в охраняемых местах. В-четвертых, рекомендуется тщательно изучать уведомления от банка и использовать отдельную карту для оплаты в интернете, что обезопасит от списывания всех средств со счета [4].

Таким образом, электронные средства расчетов представляют собой более удобный способ оплаты товаров и услуг. Уже можно сказать, что онлайновая оплата достигла значительных объемов, так как большинство пользователей использует данный вид платежей. Это объясняется бесспорным преимуществом электронных денег, выражающимся главным образом в сокращении временных и материальных затрат. Но, к сожалению, от распространения электронных способов оплаты не отстают и мошенники, использующие разные схемы хищения средств. Поэтому важно оставаться бдительным, чтобы не попасться на различного рода махинации.

Библиографический список:

1. Функционирование института электронных денег как отдельного механизма обеспечения экономической безопасности страны / С. Ю. Казанцева, Т. В. Сушкова, Ю. Г. Григоров, Л. Г. Алексанян // Вестник евразийской науки. – 2019. – Т. 11. – № 2. – С. 27.

2. Булахова В. Кардинг – что это такое в интернете и как это работает [Электронный ресурс]. — Режим доступа — URL: https://retireearly.ru/financial-literacy/carding (Дата обращения: 27.05.2022)

3. Решетникова М. Считать и украсть: как работает скимминг банковских карт [Электронный ресурс]. — Режим доступа — URL: https://trends.rbc.ru/trends/industry/612d019d9a79470c54677745 (Дата обращения: 27.05.2022)

4. Федосеева А. Кардинг, фишинг и скимминг: что это и как защитить свои средства? [Электронный ресурс]. — Режим доступа — URL: https://rb.ru/story/carding/ (Дата обращения: 27.05.2022)

5. Чернуха В. Кардинг – мошенничество с банковскими картами [Электронный ресурс]. — Режим доступа — URL: https://moneon.co/ru/blog/kartochnyi-frod-ugroza-dlia-bankovskoi-karty (Дата обращения: 26.05.2022)

6. Hello (платежная система) [Электронный ресурс]. — Режим доступа — URL: https://www.tadviser.ru/index.php/ (Дата обращения: 26.05.2022)

7. Виды электронных денег [Электронный ресурс]. — Режим доступа — URL: https://www.sravni.ru/enciklopediya/info/vidy-ehlektronnykh-deneg/ (Дата обращения: 26.05.2022)

8. Об электронных способах оплаты. Основные виды мошенничества [Электронный ресурс]. — Режим доступа — URL: http://73.rospotrebnadzor.ru/content/163/41364/ (Дата обращения: 26.05.2022)

9. Электронные деньги: виды, состояние, прогнозы [Электронный ресурс]. — Режим доступа — URL: https://kiosks.ru/index.php/ehlektronnye-dengi-vidy-sostoyanie-prognozy/ (Дата обращения: 27.05.2022)

Оригинальность 87%