DOI: 10.17117/na.2016.05.01.039

<http://ucom.ru/doc/na.2016.05.01.039.pdf>

Поступила (Received): 22.05.2016

Бичева Е.Е., Лебедева Е.В., Нефедова Л.М. Мошенничество в сфере электронных денег и электронных платежных систем

**Bicheva E.E., Lebedeva E.V., Nefedova L.M.
Fraud in the area of electronic money and
electronic payment systems**

В данной статье рассмотрено пользование электронными деньгами и электронными платежными системами в России, а так же степень безопасности проводимых в этой сфере операций. На основе анализа действия электронных денег и электронных платежных систем определены комплексы действий и мер, направленных на защиту средств, в соответствии с различными методами мошенничества

Ключевые слова: электронные деньги, электронные платежные системы, безопасность расчетов, мошенничество

This article discusses the use of electronic money and electronic payment systems in Russia, as well as the degree of security held in this area of operations. On the basis of the action of electronic money and electronic payment systems are defined by a combination of measures and to protect the funds in accordance with the different methods of fraud

Key words: electronic money, electronic payment systems, payment security, fraud

Бичева Елена Евгеньевна

Кандидат экономических наук, доцент
Воронежский государственный аграрный
университет им. императора Петра I
г. Воронеж, ул. Мичурина, 1

Bicheva Elena Evgenievna

Candidate of Economic Sciences, Associate Professor
Voronezh state agriculture university named Peter I
Voronezh, Michurina st., 1

Лебедева Екатерина Валерьевна

Студент
Воронежский государственный аграрный
университет им. императора Петра I
г. Воронеж, ул. Мичурина, 1

Lebedeva Ekaterina Valerievna

Student
Voronezh state agriculture university named Peter I
Voronezh, Michurina st., 1

Нефедова Лилия Михайловна

Студент
Воронежский государственный аграрный
университет им. императора Петра I
г. Воронеж, ул. Мичурина, 1

Nefedova Lily Mikhailovna

Student
Voronezh state agriculture university named Peter I
Voronezh, Michurina st., 1

В современном мире достижения научно-технического прогресса дают возможность совершать покупки, платежи не выходя из дома. Многие думают, что электронные деньги – это пластиковые карты, с помощью которых можно расплатиться в магазинах, гостиницах, на транспорте, купить билеты и т.д. В

действительности такие пластиковые карточки, как Visa, MasterCard, Maestro, не относятся к электронным денежным средствам, а представляют собой лишь средство доступа к счету в банке, который выпустил данную карту.

Электронные деньги – форма денежных средств, которая представляет денежные обязательства эмитента в электронном виде, находящиеся в распоряжении пользователя на электронном носителе. К их преимуществам относят легкость и быстроту расчетов, портативность, снижение человеческого фактора, и т.д.

Так что же оплачивается пользователями с помощью электронных денег? Владельцы электронных кошельков регулярно платят с их помощью за телекоммуникационные услуги, оплачивают электронными деньгами покупки в интернет-магазинах и товары по каталогам, онлайн-игры, бытовые платежи, погашают кредиты и многое другое.

Рис. 1. Рейтинг использования электронных платежных систем

Из рис.1 видно, как растет популярность платежных систем. Это данные исследований e-Finance User Index 2015 агентства Marksw Webb Rank & Report. Для пользователей главным критерием выбора платежной системы является «доверие» к нему, где безопасность является ключевой статьей.

Рассмотрим с этой стороны приведенные выше электронные платежные системы, используемые в России:

WebMoney – самая популярная система. Позволяет заводить неограниченное количество кошельков в самых распространенных валютах, в том числе валютах стран бывшего СССР (Белоруссия, Казахстан, Украина), долларах США, ЕВРО и золоте.

Яндекс кошелёк – платёжная система, принадлежащая популярному в России поисковику и серверу бесплатной почты. Доступно два вида интерфейса – кошелёк на сайте или в компьютере.

Visa QIWI Walle – это электронный кошелек, основанный на предоплаченном счете Visa, который может быть привязан к виртуальной или пластиковой предоплаченной карте Visa.

PayPal – самая популярная платёжная система в Европе. Является одной из самых простых в проведении платежа – нужна электронная почта получателя. Платежи поддерживаются подавляющим большинством англоязычных сервисов.

Деньги @mail.ru – это электронная платежная система, разработанная порталом mail.ru. Можно осуществлять различные коммунальные платежи, заносить деньги на мобильный счёт или оплачивать интернет и онлайн-игры.

Во всех этих системах существует несколько методов защиты:

1. Пароли (дополняются другими мерами защиты, о которых пойдет речь ниже).

2. Файлы ключей.

При регистрации кошелька пользователь получает файл, где хранятся «ключи» от этого кошелька, без которого, даже зная пароль, злоумышленник не сможет открыть кошелек.

3. Экранная клавиатура.

С одной стороны – снижает безопасность, так как кто-то другой может подсмотреть введенный контрольный код; с другой – экранная клавиатура защищает от кейлоггеров (клавиатурных шпионов).

4. Контрольная фраза.

Использование контрольной фразы борется с фишингом – массовой рассылкой писем пользователям с просьбой зайти на определенную страницу и ввести там свой пароль.

5. Блокировка счета.

Если пользователю стало известно, что кто-то узнал или украл его пароль, была утеряна пластиковая карта и др. В таком случае посредством звонка, SMS либо другим способом пользователь блокирует свой счет.

Несмотря на все методы борьбы с мошенничеством в электронных платежных системах, часто происходят взломы и «уводы» средств от владельцев. Самыми используемыми схемами мошенничества являются:

– Фальшивые письма и фишинговые сайты. Основная их цель – заставить получателя перейти по ссылке на поддельный (фишинговый) сайт, где крадутся учетные данные его электронного кошелька. Такие письма маскируют под официальное письмо платежной системы получателя. При переходе по ссылке в письме происходит попадание на поддельную страницу, сходную со страницей платежной системы, где при вводе учетных данных профиля осуществляется передача логина и пароля мошенникам.

– «Волшебные кошельки» и другие пирамиды. На каком-либо форуме помещается сообщение, в котором содержится список электронных кошельков (3-7 штук) и настоятельно рекомендуется отправить \$ 1 на каждый из них. Далее предлагается разместить это сообщение на более чем 200 форумах, где в списке кошельков вместо последнего необходимо поставить свой номер. Затем приводится подробный расчет, как за несколько месяцев на электронный кошелек попадет многократно умноженная сумма. Главная цель и итог – незаконный увод денег.

– Генераторы. Предлагается программное обеспечение, которое, якобы, позволит увеличить сумму в кошельке в несколько раз без уплаты взносов. После установки такой программы происходит потеря всех средств, которые находились в кошельке.

– Компьютерный шантаж. Этот тип происходит в результате посещения сайта, который заражен вредоносным программным обеспечением. Пользователь включает свой компьютер и видит окно со следующим содержанием: «Не пытайтесь убрать программу с вашего компьютера, так как можете его повредить. Чтобы возобновить его работу, отправьте SMS **** со следующим содержанием ***** два раза, и мы вышлем вам код доступа для разблокировки системы». Очевидно, что при отправке SMS произойдет только списание существенной суммы.

– Поддельные обменные пункты. Продавцы утверждают, что с их помощью можно обменять WMZ на WMR (или наоборот) по выгодному курсу и без уплаты процентов. Никакого обмена не происходит: мошенники указывают, что на сайте проводятся технические работы и требуется время на осуществление обмена. Но в итоге – жертва остается ни с чем.

Для безопасности всех проводимых расчетов через электронные платежные системы, нужно соблюдать такие меры предосторожности как:

1. Элементарные средства предосторожности.

К примеру, не следует сообщать никому свои пароли и коды – ни устно, ни по email, ни в ответной SMS, даже если кто-то представился сотрудником банка. Внимательно относитесь к публикуемой информации, не оставляйте важные данные в соц. сетях.

2. Использование уникальных паролей

Вы можете повысить безопасность своих учётных записей, используя для каждой из них уникальные сложные пароли.

3. Использование одноразовых паролей

Преимущество одноразового пароля по сравнению со статическим состоит в том, что пароль невозможно использовать повторно. Таким образом, злоумышленник, перехвативший данные из успешной сессии аутентификации, не может использовать скопированный пароль для получения доступа к защищаемой информационной системе.

4. Выбирайте сервис электронной почты с хорошей репутацией (лучше всего с двухэтапной авторизацией).

Защита электронных денег начинается с обеспечения безопасности e-mail. Лучше заводить отдельный электронный почтовый ящик. Лучше регистрировать их в надежных почтовых сервисах Gmail и Яндекс. Считается, что почта от Mail.ru не слишком надежна, потому ее лучше вообще не использовать.

5. Проверяйте, кто отправил Вам электронное письмо.

Обязательно смотрите на адрес отправителя, если получили письмо с запросом персональной информации, так как сообщения часто похожи на официальные обращения компаний.

В настоящее время электронные платежные системы и электронные деньги динамично развиваются, поэтому риски, связанные с мошенничеством в сфере электронных денег, полностью исключить невозможно. Поэтому следует применять средства и инструменты для их уменьшения не только самим электронным платежным системам, но и их пользователям.

Список используемых источников:

1. Лямин Л., Пятиизбянцев Н. Мошенничество в платежной сфере // Бизнес энциклопедия. 2016.
2. Комаров А. Электронные деньги: преимущества и недостатки // Финансовая газета. Региональный выпуск. 2008. №8 (февраль).
3. Лаврушина О. Деньги, кредит, банки. 2014.
4. Кочергин Д.А. Электронные деньги. 2011.
5. Звонова Е.А., Топчий В.Д. Деньги, кредит, банки. 2016.

© 2016, Бичева Е.Е., Лебедева Е.В., Нefeldова Л.М.
Мошенничество в сфере электронных денег и
электронных платежных систем

© 2016, Bicheva E.E., Lebedeva E.V., Nefedova L.M.
Fraud in the area of electronic money and electronic
payment systems