УДК 33 **DOI: 10.34670/AR.2020.91.1.050**

Мировой подход к защите электронных денег и диверсификация рисков

Ермаков Николай Сергеевич

Аспирант,
Российский экономический университет им. Плеханова,
115093, Российская Федерация, Москва, Стремянный переулок, 36,
e-mail: nikolay.ermakov1@gmail.com

Галкина Елизавета Алексеевна

Магистр,
Финансовый университет при Правительстве Российской Федерации,
125167, Российская Федерация, Москва, Ленинградский пр-т., 49,
e-mail: eagalkinabs@gmail.com

Аннотация

В статье проанализированы основные подходы к защите и электронных денежных средств в процессе диверсификации существующих рисков безопасности. Выделены основные авторские позиции известных отечественных и зарубежных ученых по данной проблеме, указаны их наработки и предложения по повышению безопасности операций с электронными деньгами. Изучены основные положения определения сущности электронных денег, их классификации и возможности применения, позиция стран ЕС в вопросе эмиссии электронных денежных средств и их защите на государственном и негосударственном уровне. Проанализированы основные достижения в сфере безопасности электронных денег, связанные с именем Д. ли Чаума, изучены основные средства защиты – криптографические протоколы, анонимные цифровые подписи, и проч. Автором выделены наиболее распространенные в мире на сегодняшний день виды мошенничества и риски в сфере операций с электронными денежными средствами, исследованы их опасности и способы предотвращения. Проанализированные основные способы защиты электронных денег, применяемые сегодня наиболее известными и распространенными платежными системами, провайдерами и сервисами, включающие парольную защиту, применение возможностей экранной клавиатуры и мыши, использование специальных кодовых фраз, блокировки счета. Наконец, выделены особенности безопасности и защиты электронных денежных средств наиболее распространенной дебетовой электронной платежной системы в мире – PayPal. Приведены мнения специалистов и высказана авторская позиция по вопросу диверсификации операционных рисков в процессе проведения финансовых операций.

Для цитирования в научных исследованиях

Ермаков Н.С., Галкина Е.А. Мировой подход к защите электронных денег и диверсификация рисков // Экономика: вчера, сегодня, завтра. 2020. Том 10. № 1А. С. 443-451. DOI: 10.34670/AR.2020.91.1.050

Ключевые слова

Электронные деньги, защита, риски, платежная система, криптовалюта, эмитент, безопасность.

Введение

Современная мировая финансовая система сегодня не может обойтись без электронных денежных систем. Они прочно вошли в обиход практически каждого человека и активно применяются для всех видов финансовых расчетов в виртуальном пространстве сети Интернет, а также для конвертации денег и проведения денежных переводов. Удобства применения электронных денег, минимальная комиссия и быстрый доступ обеспечили им огромную популярность и распространение, а внедрение интернет-банкинга, электронных кошельков, различных платежных карт и устройств для работы с ними могут вытеснить, по прогнозам специалистов, обращение обычных денег уже через пару десятилетий.

При этом одной из главных характеристик электронных денег является их безопасность, ведь в отличие от обычной валюты электронным денежным средствам свойственно серьезное внутреннее противоречие – с одной стороны, они являются полноправным средством платежей всех видов, а с другой – обязательствами эмитента, которые необходимо выполнить в традиционных деньгах. Центробанки национальных финансовых систем сегодня в большинстве своем не проводят эмиссию электронных денег, однако устанавливают определенные правила и согласовывают нормы их распространения и обращения ввиду опасения неконтролируемой эмиссии, опасения использования для отмывания денег и финансирования терроризма, а также в различных мошеннических схемах [Electronic Fund Transfers, www].

Именно защита электронных денег от несанкционированного эмитентом доступа к ним, подделки, взлома или кражи средств с электронных кошельков сегодня выходит на первый план. Возникающие в процессе использования электронных денежных средств операционные риски в результате сбоев системы, незаконной деятельности интернет-мошенников, хакеров приводят к серьезным финансовым потерям. Поэтому особую важность сегодня приобретают способы, инструменты и виды защиты электронных денег на мировых финансовых рынках, опыт которых можно использовать в отечественной финансовой системе, что и объясняет актуальность данного исследования

Цель статьи заключается в анализе мирового опыта защиты электронных денег в условиях диверсификации существующих рисков.

Основное содержание

Исследованиями в сфере регулирования и защиты электронных денег за рубежом занимались целый ряд известных финансовых аналитиков, специалистов в сфере кибербезопасности и т.д.: Д. Чаум, А. Липис, Б. Норман, М. Тарази, Т. Кубота, Б. Норман, И. Портела, С. Лили и проч.

Так, М. Тарази указывает, что существенный рост влияния электронных виртуальных валют и денежных систем, особенно в странах так называемого «третьего мира», создает предпосылки для распространения многочисленных нарушений защиты средств клиентов на электронных счетах и виртуальных кошельках. Исследователь приводит пример платежной системы M-Pesa,

работающей на базе мобильного оператора Safaricom в Кении, Танзании и Афганистане, ЮАР, Индии, Египте и других развивающихся странах и сумевшей за короткий срок завевать большой сегмент рынка электронных валют и платежных систем в мире. Однако из-за низкой защищенности бесфилиального банкинга системы M-Pesa на протяжении 2010-2015 гг. было совершено более 20 тыс. краж приватных данных пользователей системы, отчего более 25 тыс. человек понесли убытки на сумму около 40 млн. дол. США. Как итог, отмечает М. Тарази, поддерживающая сервис M-Pesa компания Vodafone была вынуждена не только отменить кооперацию с институтом микрофинансирования Faulu, но и создать отдельную службу безопасности для системы, вложив в защиту M-Pesa более 200 млн. дол. США [Tarazi, www].

В свою очередь, Т. Кубота, известный японский эксперт в сфере виртуальных валют и электронных платежных систем, проанализировав основные подходы к нормативной защите электронных денег в Японии, США, Великобритании, Индии, Малайзии, Сингапуре и других странах, пришел к выводу о необходимости создания трансграничных международных институций, которые занимались исключительно вопросами финансовой кибербезопасности. В сотрудничестве с группой ученых японских университетов Васеда и Аиши исследователь Т. Кубота высказывает мнение о существенном повышении рисков в процессе проведения операций с электронными деньгами, резком увеличении кибрпреступности в данной сфере и, как следствие – больших убытках и падении доверия к существующим системам электронных платежей, виртуальным валютам и электронным деньгам. Ученый также предлагает ряд мер, призванных значительно повысить уровень защиты финансовых операций в виртуальном пространстве в общем и самих электронных денег, в частности [Kubota, 2007, 18].

Большой вклад в разработку мер защиты цифровых валют и платежных систем внесли европейские ученые. В частности, группой специалистов под руководством Б. Нормана были разработали основы защиты электронных денег клиентов и общей безопасности, которые вошли в Директиву ЕС (2006/2004/ЕС) о гармонизации трансграничных операций, регламентирующей порядок сотрудничества между национальными правовыми системами в сфере защиты прав потребителей, в том числе электронных денег [Norman and others, 2009]. Среди последних авторских наработок в данной сфере отметим работу С. Лили «Защита клиентов в сфере электронных денег: мобильные деньги», в которой автор анализирует последние разработки систем кибербезопасности в плане защиты электронных денег в странах европейского Союза, в частности Германии, Франции, Голландии, странах Скандинавии и проч.

Среди отечественных ученых, занимающихся разработкой проблемы защиты электронных денег, отметим А.Н. Богомолова, Ю.А. Колесникова, Д.А. Кочергина, П. Равенкова, В.В. Хмырова и проч., а также экспертов в сфере информационной безопасности В.Л. Достова, Д. Макарского, А.С. Шкарупеловой и т.д. Например, П. Равенков, анализируя международный опыт регулирования в сфере применения электронных денег, указывает на резкое возрастание числа киберпреступлений, связанных с кражей электронных денег, взломом электронных кошельков, использования приватных электронных счетов для отмывания денег и проч. Ученый отмечает, что для России можно перенять опыт внедрения мер в сфере защиты электронных денег США, Сингапуре, Австралии, странах Еврозоны и т.д. [Ревенков, www].

Известный специалист в сфере кибербезопасности Д. Макарский указывает на наиболее распространенные в странах ближнего зарубежья и ЕС методы взлома электронных кошельков, счетов, файлов ключей. По мнению аналитика, основными способами эффективной защиты виртуальных средств и счетов, применяемых в мире и внедряемых сегодня в России, стоит назвать контрольные экранные коды, контрольные фразы, использование последних

обновляемых антивирусных программ и т.д. [Макарский, www].

В. Достов, оценивая возникающие в процессе пользования электронными денежными средствами риски, обращает внимание на операционные риски в процессе обращения электронных денег в развитых странах мира, особенно при операциях с криптовалютами. Ученый указывает на существующие мошеннические схемы с финансовыми пирамидами, недобросовестными ресурсами по обмене валют в онлайн-режиме и проч. [Достов, Шуст, 2013].

Исследуя актуальные вопросы защиты электронных денег за рубежом, необходимо сначала определить понятие и сущность электронных денег. Сегодня данный термин имеет достаточно много значений, поскольку постоянно совершенствуется и дополняется. Например, в статье 3 Федерального закона «О национальной платежной системе» электронные денежные средства определяются как «…средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счёта (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа…» [Федеральный закон «О национальной платежной системе», 2011].

В странах Европейского Союза электронными деньгами принято считать такие финансовые обязательства эмитента, которые в электронном виде находятся на определенном электронном носителе пользователя и соответствуют таким критериям:

– фиксация и хранение на определенном электронном носителе;

– выпуск денег эмитентом в не меньшем объёме, чем эмитированная денежная стоимость, при получении денежных средств от иных лиц;

– прием электронных денег как средства платежа иными организациями, кроме эмитента [Christen, Lyman, Rosenberg, 2003].

Среди всех разновидностей электронных денег принято разграничивать их на базе смарт-карт и на базе сетей. Также как смарт-картовые, так и сетевые электронные денежные средства подразделяются на фиатные, или фидуциарные (принятые и регулируемые государством), например, отечественные Яндекс.деньги, африканская M-Pesa, американская PayPal, гонконгская «Октопус» и проч.), и нефиатные, или негосударственные – WebMoney, QIWI, EasyPay т.д. В Европе не относятся к электронным денежным средствам, согласно позиции Европейского центрального банка, средства доступа к личному или корпоративному банковскому счету – традиционные банковские карты (причем как магнитные, так и микропроцессорные), интернет-банкинг, одноцелевые карты (топливные, подарочные, телефонные и др.) [Колесников, 2015, 187].

В процессе применения и защиты электронных денежных средств остро встает вопрос возможности их эмиссии и наличия эмитента, то есть институции, которая имеет право осуществления эмиссии тех или иных электронных денег. Поскольку с данным вопросом тесно связана проблема безопасности электронных денежных средств, в мире ее решению уделяется очень большое внимание. К примеру, в странах Европейского Союза, кроме ЕЦБ, эмиссию электронных денег имеют право осуществлять ELMI – Институты электронных денег. В Гонконге, например, для осуществления эмиссии финансовая организация должна иметь статус депозитной компании и получить соответствующую лицензию. Индия, Мексика, Нигерия, Сингапур, Тайвань, Украина и еще целый ряд развивающихся стран мира разрешают проводить эмиссию электронных денег только государственным банкам. В нашей стране такими

эмитентами, кроме банков, могут быть и НКО (небанковские кредитные организации), имеющие право и соответствующие лицензии эмиссировать виртуальные деньги.

Справедливо заметим, что вопросы защиты электронных денег стали активно разрабатываться с самого начала их внедрения на мировых финансовых рынках. Впервые методику криптографической защиты электронных денежных средств предложил известный американский программист и криптограф Д. ли Чаум. В числе его разработок: средства анонимности электронных денег ecash, внедрение криптографических протоколов, которые созданная им компания DigiCash стала активно внедрять в практику. Также в соавторстве с Х. ван Антверпеном Чаум ввел в практику понятие индивидуальной и групповой цифровой подписи, предложил идею анонимного общения в процессе проведения финансовых операций в Интернете с помощью механизма смешанных сетей, которые сегодня стали основой для создания анонимных инструментов просмотра веб-страниц с финансовой информацией. Кроме того, ученый предложил новый тип анонимной корпоративной финансовой связи DC-Nets для решения проблем безопасности межкорпоративных финансовых операций с электронной валютой на базе программного инструмента Dissent [Шкарупелова, Трунина, 2012].

Впоследствии идеи Чаума стали определяющими для обеспечения безопасности финансовых операций с электронными денежными средствами. Так называемая «слепая» цифровая подпись, или blind signature (когда пользователь, подписывающий информацию о электронных деньгах, видит только необходимую ему часть, однако она заверяет всю информацию целиком) активно используется фактически во всех электронных платежных системах и криптовалютах в мире.

Сегодня защита электронных денежных средств в мире является необычайно востребованной. Постоянно появляются новые способы и виды мошенничества, способы взлома электронных счетов, виртуальных кошельков, кражи средств. Среди наиболее распространенных способов мошенничества в данной сфере стоит отметить:

1) фишинг – основанный на получении e-mail-писем от якобы авторитетной финансовой или торговой организации с просьбой обновления актуальной финансовой информации либо ее передачи под каким-либо предлогом – участия в акции, выигрыше денег, скидках при покупках, получения фиктивного наследства и т.д. Мошенники как можно точнее копируют интернет-ресурсы настоящей организации и от ее имени якобы предлагают свои услуги;

2) скимминг – применение злоумышленниками специальных устройств, которые могут скачать или считать информацию со счета или кошелька пользователя. Это могут быть хакерские программы, скиммеры (специальные приборы для считывания информации) и др.;

3) генераторы – предложения программного обеспечения якобы для майнинга криптовалюты, увеличения счета на виртуальных кошельках, а также способов «защиты» электронных средств; при их применении деньги «перекачиваются» на счет злоумышленников;

4) компьютерный шантаж – после, как правило посещения «зараженного» вирусом сайта на рабочем столе высвечивается информация приблизительно такого типа «…Не пытайтесь убрать программу с вашего компьютера, так как можете его повредить. Чтобы возобновить его работу, отправьте SMS **** со следующем содержанием ******** два раза, и мы вышлем вам код доступа для разблокировки системы…». Наиболее часто, по статистике, данная схема мошенничества характерна для стран СНГ и ближнего зарубежья;

5) поддельные сайты с «обменом валют», майнингом, оплатой услуг и т.п. без уплаты процентов, по очень выгодному курсу или иными заманчивыми предложениями; после обращения на данный сайт и введения своих реквизитов счетов сайт блокируется, может

появиться надпись о проведении «профилактических» работ и проч. [Кочергин, 2005, 29].

Основными средствами защиты электронных денежных средств сегодня определяются:

1. Применение паролей, кодов, платежных PIN-кодов и проч. Многие платежные системы и криптовалюты требуют для входа в личный кабинет, виртуальный кошелек код или пароль, иногда несколько, часто применяются обновления через e-mail или мобильный телефон. Некоторые системы (например, WebMoney, Payeer, Skrill (Moneybookers) и т.д.) также могут требовать отдельные файлы ключей. Однако большинство специалистов в сфере киберзащиты отмечают недостаточность уровня защищенности паролями и кодами, поэтому рекомендуют применять также и иные способы защиты.

2. Применение экранной клавиатуры для защиты от вредоносных троянских программ, вирусов, червей. В частности, используемая в Беларуси платежная система EasyPay использует ввод необходимых символов на экране монитора, защищая таким образом данные от клавиатурных шпионов, проникающих в компьютер через считывание специального лог-файла. Существует также комбинированный метод такой защиты с применением экранной клавиатуры и мыши – в частности, он используется в британской экосистеме электронных трансакций Zapp, голландской системе онлайн-банкинга iDEAL, китайской системе электронных платежей Alipay, привязанной к интернет-магазину Alibaba, и проч.

3. Использование специальной фразы или набора слов. Данный метод защиты электронных средств применяется для защиты от фишинга и пресекает попытки мошенничества со стороны злоумышленников, так как после открытия операционной страницы любого сервиса должна появиться контрольная фраза. Если ее нет, имеет место попытка мошенничества.

4. Блокировка счета или кошелька, которая применяется практически во всех видах электронных денежных средств в том случае, если все остальные способы не в состоянии обеспечить безопасность и пользователь уже стал жертвой кражи данных, средств, взлома аккаунта и т.д. Команда блокировки отправляется через звонок или отправку SMS на определенный номер. Данная мера является крайне, но она обеспечивает наивысшую степень защиты [Основные способы защиты электронных денег, www].

В настоящее время защита электронных денежных средств и диверсификация существующих операционных, нормативных, пользовательских рисков в мире являются чрезвычайно важными и актуальными. Однако наибольшим видом риска в процессе защиты электронных денежных средств является человеческий фактор, который делает уязвимой любую, даже самую совершенную систему защиты. Диверсификация таких рисков сегодня является важнейшей задачей как государственных регуляторов электронных денежных систем, так и в первую очередь органов и служб безопасности платежных систем, провайдеров и проч.

В качестве примера рассмотрим методы защиты в системе PayPal, являющейся сегодня одной из крупнейших электронных платежных систем в мире (более 200 млн. пользователей, 202 страны мира, сотрудничество с 25 национальными валютами). Она была создана в США как подразделение компании eBay, но с 2015 года выступающая как самостоятельный контрагент на финансовом рынке [Risk management for electronic banking and electronic money activities, www].

Данная платежная система обеспечивает безопасность своих пользователей через шифрование каждой операции с электронными деньгами на основе технологии SSL, контроль всех операций в реальном времени, гарантию возврата средств при условии соответствия требованиям Программы безопасности PayPal и проч. Система также возмещает нанесенный пользователю ущерб в случае несанкционированного денежного перевода по его счету (если

данная ситуация была допущена не по вине пользователя).

Однако, по мнению специалистов, обычные пользователи могут быть слабо защищены в данной системе, так как защита именно виртуального кошелька или карты в PayPal идет по стандартной схеме – логин и пароль. Поэтому они советуют с целью диверсификации операционных рисков использовать при проведении операций иные дебетовые карты с переводом средств перед непосредственным снятием денег, покупкой, оплатой услуг и т.д.

Заключение

Таким образом, сегодня вопросы защиты электронных денег и диверсификации рисков безопасности проведения различных операций с ними играют важнейшую роль в системе виртуальных финансов. Практически во всех странах мира действуют свои нормы и правила регулирования операций с электронными денежными средствами, а операторы и провайдеры платежных систем и криптовалют стараются в максимальной мере нивелировать риски кражи средств и личных данных пользователей, взлома платежных аккаунтов, виртуальных кошельков. Но наряду с методами и способами защиты предотвращать риски незаконных операций с электронными средствами обязаны и сами пользователи, постоянно отслеживая свои счета, следя за паролями, кодами, попытками взлома, проверяя проводимые операции и т.п.

Библиография

1. Достов В.Л., Шуст П.М. Виртуальные валюты и криптовалюты: новые возможности или новые риски? // Финансовая безопасность. 2013. №3. С. 61-64.
2. Достов В.Л., Кузнецов В.А., Шуст П.М. Электронные деньги как инструмент оптимизации платежного оборота (точка зрения) // Деньги и кредит. 2013. № 12. С.7-13.
3. Колесников Ю.А. Понятие электронных денег по законодательству России и зарубежных стран // Пробелы в российском законодательстве. 2015. № 2. С. 187-191.
4. Кочергин Д.А. Интерпретация электронных денег и оценка их влияния на денежно-кредитную систему // Финансы и кредит. 2005. №13(181). С. 29-39.
5. Макарский Д. Способы защиты электронных денег. URL: http://www.nestor.minsk.by/sr/2007/12/sr71214.html (дата обращения: 20.01.2020).
6. Основные способы защиты электронных денег. URL: https://allchangers.ru/faq/osnovnye-sposoby-zacshity-elektronnyh-deneg.html (дата обращения: 12.01.2020).
7. Ревенков П. Международный опыт регулирования в области применения электронных денег // Библиотека маркетолога. URL: https://www.marketing.spb.ru/mr/it/AML-CFT.html (дата обращения: 9.12.2019).
8. Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ // Собрание законодательства РФ. 04.07.2011. № 27. ст. 3872.
9. Шкарупелова А.С., Трунина В.Ф. Проблемы безопасности испозования электронных денег // Экономика и современный менеджмент: теория и практика: сб. ст. по матер. IX междунар. науч.-практ. конф. Новосибирск: СибАК, 2012.
10. Christen R., Lyman T. and Rosenberg R. Guiding Principles on Regulation and Supervision of Microfinance. Consensus Guidelines. Washington, D.C.: CGAP. 2003.
11. Electronic Fund Transfers, Regulation E; Docket No. R-1343 Federal Reserve System. URL: http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20081218a4.pdf (Accessed 24/01/2020).
12. Kubota T. Cyberlaw for Global E-business: Finance, Payments and Dispute Resolution. Waseda University, Japan. 2007. 318 p.
13. Norman B, Brierley P., Gibbard P., Mason A., Meldrum A . Risk-based methodology for payment systems oversight // Financial stability paper, 2009. № 6. P.1-13.
14. Risk management for electronic banking and electronic money activities. URL: http://www.bis.org/publ/bcbsc215.pdf/ (Accessed 15/12/2019).
15. Tarazi M. Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds. URL: https://www.cgap.org/sites/default/files/CGAP-Focus-Note-Nonbank-E-Money-Issuers-Regulatory-Approaches-to-Protecting-Customer-Funds-Jul-2010.pdf (Accessed 28/12/2019).

The global approach to the protection of e-money and risk diversification

Nikolai S. Ermakov

Postgraduate,
Plekhanov Russian University of Economics,
115093, 36, Stremyanny lane, Moscow, Russian Federation;
e-mail: nikolay.ermakov1@gmail.com

Elizaveta A. Galkina

Master,
Financial University under the Government of the Russian Federation
125167, 49, Leningradsky prospect, Moscow, Russian Federation;
e-mail: eagalkinabs@gmail.com

Abstract

The article analyzes the main approaches to the protection of e-money in the process of diversification of existing security risks. The main author's positions of well-known domestic and foreign scientists on this problem are highlighted, their developments and suggestions for improving the security of operations with electronic money are indicated. The main provisions of the definition of the essence of electronic money, their classification and application, the position of the EU countries in the issue of e-money emission and their protection at the state and non-state level are studied. The main achievements in the field of electronic money security related to the name of D. Li Chaum are analyzed, the main means of protection are studied – cryptographic protocols, anonymous digital signatures, and so on. The author identifies the most common types of fraud in the world today and risks in the field of operations with electronic money, examines their dangers and methods of prevention. The main ways of protecting electronic money that are used today by the most well-known and widespread payment systems, providers and services, including password protection, the use of on-screen keyboard and mouse capabilities, the use of special code phrases, and account blocking, are analyzed. Finally, the features of security and protection of electronic funds of the most common debit electronic payment system in the world – PayPal-are highlighted. The opinions of experts are given and the author's position on the issue of diversification of operational risks in the process of financial transactions is expressed.

For citation

Ermakov N.S., Galkina E.A. (2020) Mirovoi podkhod k zashchite elektronnykh deneg i diversifikatsiya riskov [The global approach to the protection of e-money and risk diversification]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 10 (1A), pp. 443-451. DOI: 10.34670/AR.2020.91.1.050

Keywords

Electronic money, protection, risks, payment system, cryptocurrency, Issuer, security.

Referenses

1. Dostov V.L., SHust P.M. (2013) Virtual'nye valyuty i kriptovalyuty: novye vozmozhnosti ili novye riski? [Virtual currencies and cryptocurrencies: new opportunities or new risks?] // Finansovaya bezopasnost' [Financial safety], 3, 61-64.
2. Dostov V.L., Kuznecov V.A., SHust P.M. (2013) Elektronnye den'gi kak instrument optimizacii platezhnogo oborota (tochka zreniya) [Electronic money as a tool for optimizing payment turnover (point of view)] // Den'gi i kredit [Money and credit], 12, 7-13.
3. Kolesnikov YU.A. (2015) Ponyatie elektronnyh deneg po zakonodatel'stvu Rossii i zarubezhnyh stran [The concept of electronic money under the legislation of Russia and foreign countries] // Probely v rossijskom zakonodatel'stve [Gaps in Russian legislation], 2, 187-191.
4. Kochergin D.A. (2005) Interpretaciya elektronnyh deneg i ocenka ih vliyaniya na denezhno-kreditnuyu sistemu [Interpretation of electronic money and assessment of its impact on the monetary system] // Finansy i kredit [Finance and credit], 13(181), 29-39.
5. Makarskij D. Sposoby zashchity elektronnyh deneg [Ways to protect electronic money]. URL: https://allchangers.ru/faq/osnovnye-sposoby-zacshity-elektronnyh-deneg.html (Accessed 20/01/2020).
6. Osnovnye sposoby zashchity elektronnyh deneg [Main ways to protect electronic money]. URL: https://allchangers.ru/faq/osnovnye-sposoby-zacshity-elektronnyh-deneg.html (Accessed 12/01/2020).
7. Revenkov P. Mezhdunarodnyj opyt regulirovaniya v oblasti primeneniya elektronnyh deneg [International regulatory experience in the use of electronic money] // Biblioteka marketologa [Marketer's Library]. URL: https://www.marketing.spb.ru/mr/it/AML-CFT.html (Accessed 9/12/2020).
8. Federal Law "On the National Payment System" dated 06/27/2011 No. 161-ФЗ // Collection of legislation of the Russian Federation. 07/04/2011. No. 27. Article 3872.
9. Shkarupelova A.S., Trunina V.F. (2012) Problemy bezopasnosti ispozovaniya elektronnyh deneg [Problems of security of using electronic money] // Ekonomika i sovremennyj menedzhment: teoriya i praktika: sb. st. po mater. IX mezhdunar. nauch.-prakt. konf [Economics and modern management: theory and practice: sat. St. on mater. IX Intern. science.-prakt. conf]. Novosibirsk.
10. Christen R., Lyman T. and Rosenberg R. (2003) Guiding Principles on Regulation and Supervision of Microfinance. Consensus Guidelines. Washington.
11. Electronic Fund Transfers, Regulation E; Docket No. R-1343 Federal Reserve System. URL: http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20081218a4.pdf (Accessed 24/01/2020).
12. Kubota T. (2007) Cyberlaw for Global E-business: Finance, Payments and Dispute Resolution. Waseda University, Japan.
13. Norman B, Brierley P., Gibbard P., Mason A., Meldrum A. (2009) Risk-based methodology for payment systems oversight // Financial stability paper, 6, 1-13.
14. Risk management for electronic banking and electronic money activities. URL: http://www.bis.org/publ/bcbsc215.pdf/ (Accessed 15/12/2019).
15. Tarazi M. Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds. URL: https://www.cgap.org/sites/default/files/CGAP-Focus-Note-Nonbank-E-Money-Issuers-Regulatory-Approaches-to-Protecting-Customer-Funds-Jul-2010.pdf (Accessed 28/12/2019).