

ЭЛЕКТРОННЫЕ ДЕНЬГИ: ВОЗМОЖНОСТИ ДЛЯ БЫСТРЫХ ПЛАТЕЖЕЙ И РИСКИ ИХ ИСПОЛЬЗОВАНИЯ В ПРОТИВОПРАВНЫХ ЦЕЛЯХ

А. А. Коваль

Российский центр компетенций и анализа стандартов ОЭСР РАНХиГС
при Президенте Российской Федерации, Москва, Россия

М. Ю. Кузьменков

Клуб «Россия – ОЭСР» ВАВТ Минэкономразвития России, Москва, Россия

Электронные денежные средства широко используются в трансграничных коммерческих отношениях. Они повышают скорость и снижают стоимость платежей для бизнеса. Вместе с тем электронные деньги могут быть использованы для отмывания денежных средств, полученных преступным путем, и финансирования терроризма. Государства – члены ФАТФ распространяют положения законодательства о противодействии легализации преступных доходов в отношении эмитентов электронных денег. Страны также подчеркивают, что особый риск для легализации преступных доходов представляют анонимные деньги и предоплаченные карты. Поэтому многие государства устанавливают в национальном законодательстве меры, которые обеспечивают реализацию риск-ориентированного подхода, направленного на минимизацию рисков отмывания денежных средств и финансирования терроризма. Например, в Европейском союзе в настоящее время разрабатываются поправки к директиве, направленные на устранение рисков использования электронных денег и предоплаченных карт для легализации преступных доходов. Авторами предложены меры по совершенствованию законодательства о противодействии отмыванию денежных средств и финансированию терроризма для минимизации соответствующих рисков в ходе использования электронных денег. Вместе с тем отмечается необходимость создания условий для расширения возможностей применения удаленной идентификации, как это предусмотрено программой «Цифровая экономика Российской Федерации».

Ключевые слова: отмывание денежных средств, электронные деньги, предоплаченные карты, ФАТФ.

E-MONEY: OPPORTUNITIES FOR QUICK PAYMENTS AND RISKS OF THEIR USE FOR ILLEGAL PURPOSES

Aleksandra A. Koval

Russian Center of Competences and Analysis of Standards of OECD of a RANEPa
under the President of the Russian Federation, Moscow, Russia

Mihail Yu. Kuzmenkov

Russia OECD VAVT Club of the Ministry of Economic Development
of the Russian Federation, Moscow, Russia

E-money is widely used in cross-border commercial relations. It can increase the speed and cut cost of payments for business. At the same time e-money can be used for laundering funds gained by criminal ways and for terrorism financing. FATF member-states use provisions of the legislation about fighting criminal incomes' legalization in respect to e-money issuers. These countries also underline that special risk for criminal incomes' legalization can be caused by anonymous money and pre-paid cards. Therefore, many countries fix in their national laws measures that ensure realization of risk-oriented approach directed at minimizing risks of money laundering and terrorism financing. For example, the EU develops amendments to the directive aiming at elimination of risks dealing with use of e-money and pre-paid cards for legalizing criminal incomes. The authors propose measures aimed at improvement of legislation about fighting money laundering and terrorism financing to minimize respective risks in

using e-money. At the same time the necessity to develop conditions for extending possibilities of remote identification was pointed out, as it was envisaged by the program 'Digital Economics of the Russian Federation'.

Keywords: money laundering, e-money, pre-paid cards, FATF.

Стремительное развитие Интернета в 1990-х гг. предопределило рост трансграничной электронной коммерции, успешное функционирование которой напрямую зависит от скорости и надежности проведения трансграничных платежей. Изменение бизнес-моделей в условиях электронной коммерции требовало появления новых способов осуществления платежей. Наряду с традиционными банковскими расчетами широкое распространение получили расчеты с использованием электронных денег, которые снижают транзакционные издержки, исключая из системы взаимоотношений банки со сложными системами корреспондентских отношений. Международный банк расчетов еще в 1996 г. отметил огромный потенциал электронных денег в упрощении и удешевлении расчетов с использованием электронных денег между продавцами и потребителями. За последние 20 лет электронные деньги стали широко использоваться по всему миру. По данным Европейского центрального банка за 2016 г., объем электронных денег, выпущенных в Европейском союзе, составил 10,6 млрд евро¹.

В России комплексное регулирование электронных денежных средств появилось относительно недавно по сравнению с Европейским союзом, где первая директива, регулирующая эмиссию электронных денег, была принята еще в 2000 г. Нормативная база в отношении использования электронных денежных средств сформировалась с принятием в 2011 г. Федерального закона «О национальной платежной системе», который заложил правовые основы для использования электронных денежных средств в расчетах между физическими лицами и между компаниями и физическими лицами (сегмент B2C). Закон опре-

делил понятие электронного средства платежа и ввел требования по их использованию в зависимости от степени анонимности. Электронные средства платежа были разделены на персонифицированные и неперсонифицированные. Именно в отношении последних и возникает наибольшее количество вопросов ввиду возможных рисков использования таких электронных средств платежа для целей легализации преступных доходов и финансирования терроризма. За ограничение возможностей использования неперсонифицированных средств выступает российское подразделение финансовой разведки Росфинмониторинг. Вместе с тем План мероприятий по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации» предусматривает необходимость увеличения доступности финансовых услуг посредством:

- сохранения возможности снятия остатка электронных денежных средств в наличной форме с неперсонифицированных электронных средств платежа в случае использования предоплаченной карты клиентом – физическим лицом, прошедшим упрощенную идентификацию;
- увеличения лимита операций, совершаемых клиентом, который прошел упрощенную идентификацию;
- обеспечения возможности переводов между корпоративными электронными средствами платежа (расчеты в сегменте B2B).

Электронные деньги создают огромные возможности для удобных трансграничных платежей, но также создают и дополнительные риски с точки зрения возможности их использования в противоправных целях – для легализации преступных доходов и финансирования терроризма. Для минимизации таких рисков страны предусматривают распространение норм законодательства о противодействии отмыва-

¹ URL: <http://sdw.ecb.europa.eu/reports.do?node=1000003509> (дата обращения: 02.03.2018).

нию денежных средств, полученных преступным путем, и финансированию терроризма в отношении эмитентов электронных денег. Соответствующие положения нашли свое отражение в законах о борьбе с легализацией преступных доходов Великобритании, Эстонии, Австралии, Японии и др.

Ключевым вопросом обеспечения безопасности операций с использованием электронных денег является идентификация их владельцев. Обязанность операторов электронных денежных средств (эмитентов электронных денег) идентифицировать клиентов основывается на стандартах Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), участницей которой является и Россия. В соответствии с Рекомендацией 10 ФАТФ странам следует требовать от финансовых учреждений проведения процедур должной осмотрительности в отношении клиентов. Это предполагает идентификацию и проверку личности клиента; идентификацию бенефициарного владельца; понимание цели деловых отношений; постоянный мониторинг этих отношений¹.

С точки зрения ФАТФ новые платежные продукты и сервисы, в том числе электронные средства платежа, выполняют функции, аналогичные функциям счетов, и должны рассматриваться в соответствии с Рекомендацией 10. В Руководстве ФАТФ «Риск-ориентированный подход к предоплаченным картам, мобильным платежам и системам платежей в Интернете» 2013 г. отмечается, что несмотря на то, что странам следует требовать от финансовых учреждений применять каждую из этих мер должной осмотрительности, степень применения таких мер должна определяться на основе риск-ориентированного подхода².

В отношении новых платежных продуктов и услуг, которые выполняют функции,

аналогичные функциям счетов, требования Рекомендации 10 заключаются в том, что страны не должны разрешать финансовым учреждениям сохранять анонимные счета или счета с явно вымышленными именами. Данная Рекомендация ФАТФ находит свое отражение в национальном законодательстве стран-участниц. Например, статья 135 Закона «О борьбе с отмыванием денег и финансированием терроризма» Австралии 2006 г. устанавливает, что предоставление или получение определенной услуги, используя ложное имя клиента или его анонимность, будет являться преступлением.

При осуществлении мер противодействия легализации преступных доходов и финансированию терроризма с учетом риск-ориентированного подхода страны могли бы рассмотреть возможность упрощения мер должной осмотрительности, когда новые платежные продукты являются продуктами с более низким уровнем риска. Так, например, законодательство Великобритании допускает применение процедуры дью-дилидженс в отношении электронных денег. Это означает, что эмитент электронных денег продолжает соблюдать требования дью-дилидженс, однако может скорректировать масштабы, сроки или тип принимаемых им мер, которые достаточны, чтобы подтвердить то, что деловые отношения или сделки представляют низкую степень риска отмывания денежных средств и финансирования терроризма.

В любом случае эмитент соответствующего платежного средства должен осуществлять достаточный контроль за своими деловыми отношениями с пользователями электронных денег, чтобы он мог выявлять любые необычные или подозрительные операции. При этом ФАТФ отмечает, что использование пороговых значений является важным инструментом для применения процедур должной осмотрительности в отношении клиентов, использующих новые платежные продукты и услуги. Пороговые значения могут использоваться в качестве

¹ URL: <http://www.fedsfm.ru/content/files/documents/fatf/рекомендации%20фатф.pdf> (дата обращения: 02.03.2018).

² URL: http://www.eurasiangroup.org/ru/news/typ_buh.pdf (дата обращения: 02.03.2018).

эффективного смягчающего фактора риска для конкретного продукта и, следовательно, в качестве меры, позволяющей применять упрощенные процедуры должной осмотрительности в отношении клиентов.

ФАТФ подчеркивает, что пороговые значения могут отличаться в странах. Кроме того, в строго определенных обстоятельствах доказанного низкого риска отмывания денежных средств, полученных преступным путем, и финансирования терроризма страны могут рассмотреть возможность исключения определенных новых платежных продуктов и услуг из проведения процедур должной осмотрительности в отношении клиентов (например, когда платежные продукты имеют строго ограниченную сферу применения и были пополнены со счета, владелец которого должным образом был идентифицирован). В таких обстоятельствах особенно низкий порог может быть полезен для обеспечения дополнительной защиты.

Опыт ЕС показывает, что усиливаются меры по ограничению сферы анонимного использования электронных денежных средств. Рынок анонимных prepaid карт составляет 2% от числа prepaid карт, выпущенных в Европейской экономической зоне (ЕЕА), или около 2 млн карт. В Директиве ЕС о противодействии использованию финансовой системы для целей отмывания денег и финансирования терроризма 2015 г.¹ допускается, что страны – члены Европейского союза в национальном законодательстве на основе риск-ориентированного подхода могут разрешить финансовым учреждениям не применять определенные меры должной осмотрительности в отношении электронных денег, когда выполняются все следующие условия для снижения риска:

- платежный инструмент имеет максимальный лимит ежемесячных платежей в размере 250 евро, который может использоваться только в этом государстве-члене;

- максимальная сумма, хранящаяся в электронном виде, не превышает 250 евро;

- платежный инструмент используется исключительно для покупки товаров или услуг;

- платежный инструмент не может финансироваться за счет анонимных электронных денег;

- эмитент осуществляет достаточный контроль за транзакциями или деловыми отношениями, чтобы обеспечить обнаружение необычных или подозрительных транзакций.

Таким образом, в ЕС также строго ограничена возможность использования анонимных электронных денежных средств.

Особое внимание в настоящее время уделяется использованию prepaid карт. В отчете Управления по финансовому регулированию и надзору Великобритании «Платежные услуги и электронные деньги: наш подход» prepaid карты определяются как вид электронных денег, которые могут быть использованы для оплаты товаров в розничной торговле, или виртуальные кошельки, которые могут быть использованы для оплаты товаров или услуг в Интернете.

Государства стремятся урегулировать отношения, связанные с выпуском и использованием prepaid карт, поскольку они характеризуются высоким риском. Это предполагает определение круга субъектов, которые могут выпускать такие карты, и распространение на них законодательства по противодействию отмыванию преступных доходов. Согласно Закону Японии «О платежных системах» 2009 г., ни одно лицо не может заниматься бизнесом по выпуску prepaid платежных инструментов для стороннего бизнеса, если это лицо не является корпорацией, зарегистрированной премьер-министром.

Вопрос сокращения возможностей использования анонимных prepaid карт – один из ключевых в рамках разработки поправок к Директиве ЕС. Это связано в том числе с тем, что prepaid

¹ URL: [http://www.cbr.ru/today/anti_legalization/fatf/Directive%20\(rus\)%202015_849.pdf](http://www.cbr.ru/today/anti_legalization/fatf/Directive%20(rus)%202015_849.pdf) (дата обращения: 02.03.2018).

карты использовались преступниками в ходе подготовки нападений на Париж в ноябре 2015 г. для оплаты гостиничных номеров и аренды машин. В отчете ФАТФ «Возникшие риски финансирования терроризма» 2015 г. отмечается, что предоплаченные карты заменяют дорожные чеки как способ перемещения денег через границы. Такие карты могут быть пополнены внутри страны наличными или не подпадающими под регулирование электронными методами (например, с анонимных электронных кошельков) и незаметно вывезены за границу. По прибытии в страну высокого риска финансирования терроризма средства затем конвертируются обратно в наличные средства через банкоматы, ограничиваясь только лимитами снятия денежных средств с банкоматов. Даже в отношении предоплаченных карт, по которым применялись процедуры должной осмотрительности, правоохранительные органы (в США и в Европе) столкнулись с злоупотреблением в связи с их использованием: незаконный оборот наркотиков, торговля людьми, проституция, уклонение от уплаты налогов с использованием предлагаемой анонимности по некоторым из этих карт¹.

Разработанные поправки к Директиве ЕС предполагают, что государства-члены будут иметь возможность разрешать анонимное использование электронных денежных продуктов только в двух ситуациях: когда клиенты используют свой предоплаченный инструмент (например, предоплаченные карты) непосредственно в магазине с учетом максимальной суммы транзакции в размере 150 евро; когда клиенты осуществляют онлайн-транзакцию с предоплаченной картой в пределах 50 евро. Представители ЕС отмечают, что социальное удобство, предлагаемое предоплаченными картами, не обязательно должно приравниваться к анонимности.

В США основными эмитентами предоплаченных карт являются банки, на которых распространяется Программа

идентификации клиентов (CIP), установленная в Patriot Act². Она требует от банка получения информации, чтобы сформировать разумное представление в отношении личности каждого клиента, включая, как минимум, имя, дату рождения, адрес и ИНН. В руководстве Совета управляющих Федеральной резервной системы США уточнено применение правила CIP: выпуск предоплаченной карты общего назначения американским банком создает формальные банковские отношения, что эквивалентно открытию счета. Это предполагает устранение анонимности с 1 доллара.

Таким образом, стандарты ФАТФ и практика стран – членов организации свидетельствуют о том, что использование послаблений в отношении применения требования идентификации является допустимым только в строго определенных в законе случаях в отношении новых платежных продуктов и сервисов, характеризующихся низким риском. Установленные в России лимиты в отношении общей суммы переводимых электронных денежных средств с использованием одного неперсонифицированного электронного средства в течение календарного месяца в несколько раз превышают максимально допустимые суммы, установленные в ЕС (в России эта сумма составляет 40 тыс. рублей). С учетом риск-ориентированного подхода представляется возможным сохранить возможность использования анонимных (неперсонифицированных) электронных средств платежа, снизив лимит в отношении общей суммы переводимых электронных денежных средств с использованием одного неперсонифицированного электронного средства в течение календарного месяца и определив, что пополнение таких электронных средств платежа возможно только в тех случаях, когда была проведена идентификация.

Проект закона «О внесении изменений в статьи 7 и 10 ФЗ "О национальной платежной системе" (в части совершенствования

¹ URL: <http://base.garant.ru/71279458/> (дата обращения: 02.03.2018).

² URL: <https://www.home.barclays/content/dam/barclayspublic/docs/Utilities/usa-patriot-act-client>

ния контроля за платежами, осуществляемыми с использованием неперсонифицированных электронных средств платежа)» устраняет возможность снятия наличных с неперсонифицированных предоплаченных карт, в том числе в отношении лиц, прошедших упрощенную идентификацию. Ограничение возможностей использования предоплаченных карт для снятия наличных не противоречит логике ФАТФ, предполагающей риск-ориентированный подход к использованию новых платежных продуктов и сервисов, в случае, когда речь идет именно об анонимных картах (когда не была проведена идентификация).

В свою очередь законопроект распространяет свое действие на неперсонифицированные электронные средства платежа – как на случаи непроведения иденти-

фикации физического лица, так на случаи их упрощенной идентификации. Это не будет способствовать решению задач Плана мероприятий по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации» в части унификации требований по идентификации, расширению возможностей и способов идентификации, совершенствования правил доступа к государственным информационным системам для организаций, обязанных проводить идентификацию, и развития удаленной идентификации. Представляется, что ограничение снятия наличных в отношении предоплаченных карт должно применяться только в случаях, когда не была проведена идентификация.

Список литературы

1. *Всяких М. В., Нестерова Н. С.* Современные платежные системы коммерческого банка // Концепт. – 2015. – № 8. – С. 1–7.
2. *Гладкова С. Б., Лебедева М. Е.* Актуальные проблемы коммерческих банков при выполнении функций ПОД/ФТ // Известия Санкт-Петербургского государственного экономического университета. – 2016. – № 2. – С. 41–45.
3. *Гладкова С. Б., Гулько А. А.* Еще раз о проблемах реализации кредитными организациями требований в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма // Финансы и кредит. – 2013. – № 42.
4. *Карпунин В. И.* Виртуальный проект для виртуальной экономики: о Crypto currency и не только // Вестник Российского экономического университета имени Г. В. Плеханова. – 2018. – № 3 (99). – С. 33–49.
5. *Марамыгин М. С., Прокофьева Е. Н., Маркова А. А.* Экономическая природа и проблемы использования виртуальных денег (криптовалют) // Известия УрГЭУ. – 2015. – № 2 (58). – С. 37–43.
6. *Мусалаева С. А.* Электронные деньги и платежные системы // Проблемы современной экономики. – 2010. – № 4 (36). – С. 206–208.
7. *Филиппов Д. И.* Финансовые инновации в процессе трансформации цифровой экономики // Вестник Российского экономического университета имени Г. В. Плеханова. – 2018. – № 3 (99). – С. 58–71.

References

1. *Vsyakih M. V., Nesterova N. S.* Sovremennye platezhnye sistemy kommercheskogo banka [Today's Payment Systems of the Commercial Bank]. *Koncept* [Concept], 2015, No. 8, pp. 1–7. (In Russ.).
2. *Gladkova S. B., Lebedeva M. E.* Aktual'nye problemy kommercheskih bankov pri vypolnenii funkciy POD/FT [Acute Problems of Commercial Banks in Fulfilling POD/FT

Functions]. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta* [Izvestiys of the St. Petersburg State Economics University], 2016, No. 2, pp. 41–45. (In Russ.).

3. Gladkova S. B., Gul'ko A. A. Eshche raz o problemah realizacii kreditnymi organizatsiyami trebovaniy v sfere protivodeystviya legalizacii (otmyvaniyu) dohodov, poluchennyh prestupnym putem, i finansirovaniyu terrorizma [About Problems of Credit Organizations' Fulfillment of Requirements in the Sphere of Fighting Income Laundering Gained by Criminal Ways and Terrorism Financing]. *Finansy i kredit* [Finance and Credit], 2013, No. 42. (In Russ.).

4. Karpunin V. I. Virtual'nyy proekt dlya virtual'noy ekonomiki: o Crypto currency i ne tol'ko [Virtual Project for Virtual Economy: About Crypto Currency and Other Issues]. *Vestnik Rossiyskogo ekonomicheskogo universiteta imeni G. V. Plekhanova* [Vestnik of the Plekhanov Russian University of Economics], 2018, No. 3 (99), pp. 33–49. (In Russ.).

5. Maramygin M. S., Prokof'eva E. N., Markova A. A. Ekonomicheskaya priroda i problemy ispol'zovaniya virtual'nyh deneg (kriptovalyut) [Economic Nature and Problems of Using Virtual Money (Crypto-currencies)]. *Izvestiya UrGEU* [Izvestiya of the Urals State Economics University], 2015, No. 2 (58), pp. 37–43. (In Russ.).

6. Musalaeva S. A. Elektronnye den'gi i platezhnye sistemy [E-Money and Payment Systems]. *Problemy sovremennoy ekonomiki* [Issues of Modern Economics], 2010, No. 4 (36), pp. 206–208. (In Russ.).

7. Filippov D. I. Finansovye innovacii v processe transformacii cifrovoy ekonomiki [Finance Innovation in the Process of Digital Economy Transformation]. *Vestnik Rossiyskogo ekonomicheskogo universiteta imeni G. V. Plekhanova* [Vestnik of the Plekhanov Russian University of Economics], 2018, No. 3 (99), pp. 58–71. (In Russ.).

Сведения об авторах

Александра Александровна Коваль
научный сотрудник Центра Россия – ОЭСР.
Адрес: Российский центр компетенций
и анализа стандартов ОЭСР ФГБОУ ВО
«Российская академия народного хозяйства
и государственной службы при Президенте
Российской Федерации», 119571, Москва,
проспект Вернадского, д. 82, стр. 1.
E-mail: chil57@mail.ru

Михаил Юрьевич Кузьменков
научный сотрудник
Клуба «Россия-ОЭСР» ВАВТ
Минэкономразвития России.
Адрес: Клуб «Россия – ОЭСР» ВАВТ
Минэкономразвития России,
119285, Москва,
ул. Пудовкина, д. 4А.
E-mail: kuzmenkov.m.u@yandex.ru

Information about the authors

Aleksandra A. Koval
Researcher of the Russia – OECD Center
(RANEPA).
Address: Russian Center of competence
and anaiysis of OECD standards
of RANEPA, 1 building, 82 Vernadsky Avenue,
Moscow, 119571,
Russian Federation.
E-mail: chil57@mail.ru

Mihail Yu. Kuzmenkov
Researcher of the Russia – OECD Club RFTA
of the Ministry of Economic Development
of the Russian Federation.
Address: Russia OECD VAVT Club
of the Ministry of Economic Development
of the Russian Federation, 4A Pudovkina Str.,
Moscow, 119285, Russian Federation.
E-mail: kuzmenkov.m.u@yandex.ru