УДК 336.7:347.73

# МОЖЛИВОСТІ ДЛЯ ВІДМИВАННЯ ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ, АБО ФІНАНСУВАННЯ ТЕРОРИЗМУ ЗА ДОПОМОГОЮ ЕЛЕКТРОННИХ ГРОШЕЙ

# POSSIBILITIES FOR THE LAUNDERING INCOMES CRIMINALLY OBTAINED OR TERRORISM FINANCING THROUGH ELECTRONIC MONEY

**Тетяна Анатоліївна МЕДВІДЬ**
*к. е. н., головний спеціаліст Департаменту фінансового моніторингу Національного банку України*

**Tetiana A. MEDVID**
*Candidate of Economics, Chief Specialist of Financial Monitoring Department of the National Bank of Ukraine*

*Анотація. У статті наведено показники популярності використання електронних грошей. Розраховано кількість жертв кіберзлочинності залежно від показників світового ВВП, ВВП України та ВВП Сербії. Визначено шляхи можливості легалізації коштів, отриманих злочинним шляхом за допомогою електронних грошей. Досліджено анонімність певних дій щодо використання електронних грошей при проведенні банківських операцій.*

*Summary. The popularity of electronic money is indicated by the author of the article. Number of victims of cybercrime are estimated, depending on the of world GDP, Ukraine's GDP and Serbia's GDP performance. The ways of the possibility of legalization of proceeds of crime by means of electronic money are determined. The anonymity of certain actions according to use of electronic money in the course of banking operations is investigated.*

***Ключові слова:*** *електронні гроші, банківські карти, електронні гаманці, відмивання коштів, фінансування тероризму, легалізація коштів.*
***Key words:*** *electronic money, bank cards, electronic wallets, money laundering, terrorism financing, funds legalization.*

**Постановка проблеми.** Згідно з даними компанії КіПіЕмДжі (KPMG) в 2011 році налічувалося близько 2 млрд користувачів Інтернет і більше 5 млрд мобільних підключень по всьому світу. Щодня, відсилаються близько 294 млрд електронних листів і 5 млрд електронних повідомлень [1].

За даними Дата Інсайт (Data Insight) [2], популярність електронних грошей в Інтернеті вже вище банківських карт. Якщо виникає необхідність здійснити платіж он-лайн, 30% респондентів вибирають платежі з електронних гаманців, 26% розплачуються кредитними картами, і лише 9% здійснюють платежі через Інтернет-банкінг. При цьому 8% людей активно використовують в Інтернеті і банківську карту, і електронний гаманець.

При цьому, за даними компанії Norton у 2011 році 431 млн осіб по всьому світу стали жертвами кібер-злочинності, а загальна сума втрат у результаті склала близько 114 млрд дол США (Близько 0,14% від світового ВВП; близько 35% від ВВП України, або 144,3% від ВВП Сербії).

Усвідомлення феномену електронних грошей в Європі на офіційному рівні відбулося в 1994 році. Після аналізу нових технологічних схем, а саме наперед оплачених карток багатоцільового використання, центральні банки Європейського Союзу дійшли до фундаментального висновку: у разі поширення подібних продуктів, з боку центральних банків є необхідним постійний моніторинг відповідних систем, обмін інформацією та ухвалення політичних рішень з метою збереження цілісності платіжної системи.

Хоча єдиного підходу до визначення поняття «електронні гроші» насьогодні не існує, проте найчастіше можна натрапити на таке тлумачення: електронні гроші – одиниці вартості,

які зберігаються на електронному пристрої, приймаються як засіб платежу іншими, ніж емітент, особами і є грошовим зобов'язанням емітента.

**Аналіз останніх досліджень і публікацій.** Останніми роками все більшого поширення набуває практика здійснення розрахунків з використанням електронних грошей. Сьогодні можна продавати та купувати товари, переказувати кошти за допомогою таких систем як WebMoney, «Яндекс. Деньги», RBK Money, E-Gold, LiqPay, Z-Payment, Paypal, Liberty Reserve, ePassporte, Moneybookers тощо. Ця проблема мала відображення у роботах таких вітчизняних та зарубіжних науковців – Коваленко В. В., Дмитрова С. О., Бережного О. М., Ляміна Л. В., Кошовець О. Б., Ганічева Н. А. З одного боку, розвиток ринку електронних грошей є логічним наслідком еволюції інформаційних технологій. З іншого – їх широке застосування приховує значний ризик їх використання для проведення нелегальних фінансових операцій, ухилення від оподаткування та фінансового моніторингу.

**Мета статті** – окреслити шляхи розширення використання електронних грошей як одного з важелів у боротьбі в сфері відмивання коштів, отриманих злочинним шляхом, або фінансування тероризму.

**Обґрунтування отриманих наукових результатів.** Групою з розробки фінансових заходів з відмиванням коштів (ФАТФ) було виявлено три основні типології, пов'язаних з незаконним використанням нових способів платежів для цілей відмивання грошей та фінансування тероризму [3]:

1) Вкладення грошей третіми особами (включаючи фіктивних та підставних осіб);

2) Використання безособового характеру рахунків для використання нових способів платежів;

3) Провайдери послуг нових способів платежів або їхні співробітники, які є співучасниками злочинних схем.

У процесі легалізації коштів, отриманих злочинним шляхом, електронним грошам властива дихотомія, адже вони одночасно можуть бути як:

– інструмент генерації нелегальних грошових потоків (об'єкт предикатного злочину);

– інструмент трансформації нелегального капіталу в законну форму (інструмент злочину – процесу легалізації).

Таким чином, питання способів введення і виведення цих коштів в/із системи є вкрай важливим (див. табл. 1).

Крім способів введення/виведення електронні гроші мають низку й інших властивостей, які роблять їх вразливими для відмивання коштів, отриманих злочинним шляхом, та фінансування тероризму, зокрема:

– анонімність клієнтів;

– деперсоніфікованість електронних грошей;

– можливість здійснення транскордонних переказів;

– висока швидкість платежів та їх низька вартість;

– відсутність єдиних міжнародних стандартів і неврегульованість питань національного законодавства тощо.

При цьому основні можливості легалізації коштів, отриманих злочинним шляхом за допомогою електронних грошей полягають у:

– швидкому, дешевому проведенні трансакції і легкості обходу обмежень, зокрема за сумами платежів;

– організації та проведення нелегальної

*Таблиця 1*

*Способи введення/виведення електронних грошей*

| **Персоніфіковані способи** | **Можливість того, що про фінансову операцію у разі виникнення підозр буде повідомлено ПФР1** | **Деперсоніфіковані способи** | **Можливість того, що про фінансову операцію у разі виникнення підозр буде повідомлено ПФР** |
|---|---|---|---|
| Банківською картою | + | Через термінали з внесення готівки | - |
| Банківським / поштовим переказом | + | За допомогою передплаченої карти | - |
| За готівку через банківське відділення | + / – 2 | За допомогою спеціального обмінного пункту | - |
| За допомогою Інтернет-банкінгу | + | За допомогою інших електронних грошей | - |

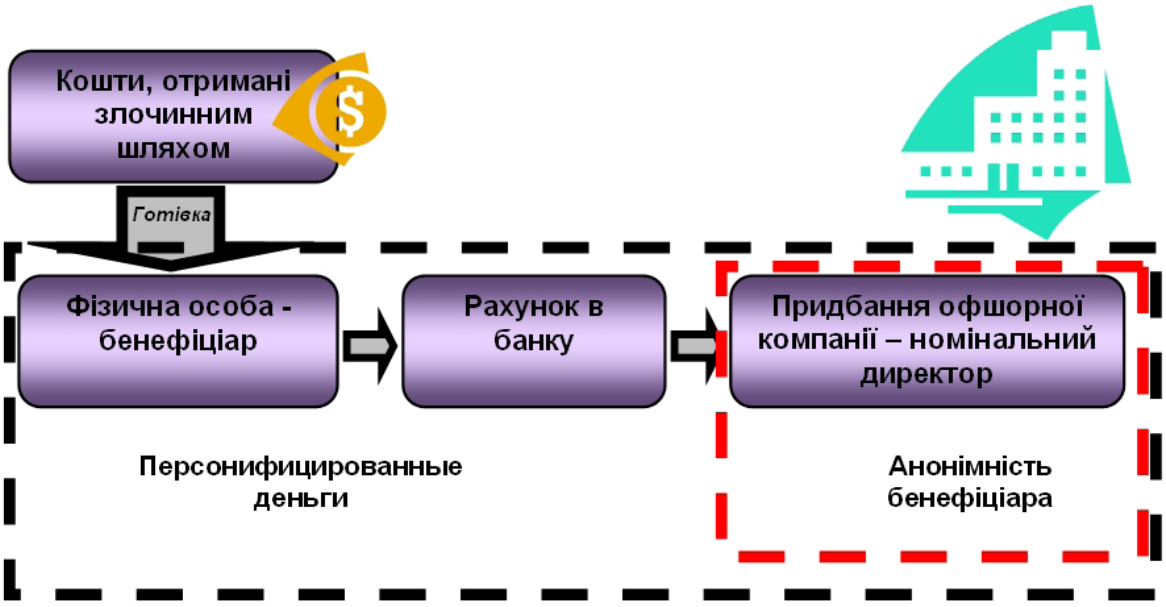


*Рис. 1. Придбання офшорної компанії з використанням банківського рахунку*

діяльності в/за допомогою мережі Інтернет (шахрайство, хакерство, порноіндустрія, торгівля зброєю і наркотиками тощо), доходи від якої надходять за допомогою платежів в електронних грошах;

– ухиленні від сплати податків;

– приховуванні слідів трансакції (послідовного ряду трансакцій).;

– використанні третіх осіб;

– можливості деперсоніфікованого введення/виведення готівки;

– «обхід» банківської системи, яку жорстко регулюють з питань легалізації коштів, отриманих злочинним шляхом, та фінансування тероризму;

– неврегульованості законодавства;

– труднощах збору доказової бази;

– труднощах міжнародного співробітництва;

– легкості фізичного переміщення передплачених карт (карт для поповнення рахунку тощо).

Дещо детальніше пропонуємо дослідити те, яким чином за допомогою електронних грошей можна не лише забезпечити анонімність певних

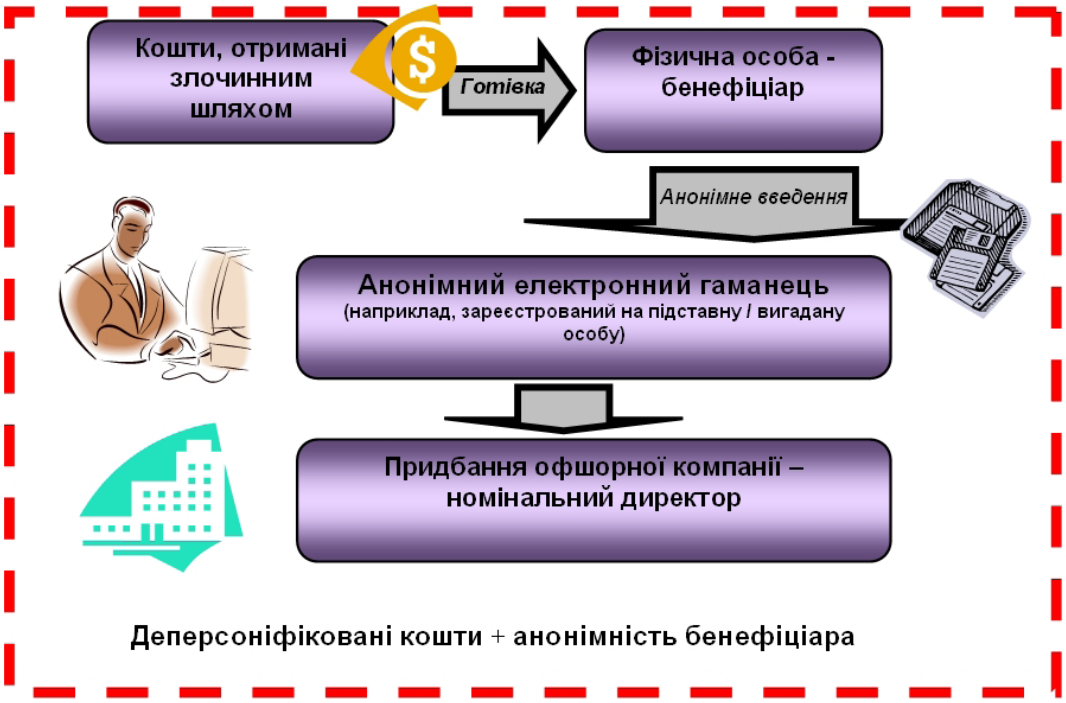


*Рис. 2. Придбання офшорної компанії з використанням електронних грошей*

дій, а й поглибити той рівень анонімності, що досягають зазвичай при проведенні операції, наприклад, з придбання офшорної компанії за допомогою традиційних засобів – банківського переказу (див. рис. 1 та 2).

Слід зважати, що готова офшорна компанія може виступати не тільки як суб'єкт господарювання, а й ставати засновником/учасником інших компаній та установ, зокрема банків, що робить не можливим виявити реальних контролерів таких утворень. Навіть більше, в разі проведення розслідування буде вкрай важко довести приналежність певних коштів, або визначити причетність певних осіб до дій таких офшорних компаній.

Тим паче, варто відмітити те, що інкорпорацію офшорної компанії зазвичай здійснюють за індивідуальними замовленнями з урахуванням інвестиційних потреб клієнта.

Створення і реєстрацію офшорної компанії можуть проводити як самі засновники, так і місцеві та міжнародні юридичні фірми за довіреністю.

У першому випадку потрібна особиста участь всіх засновників-акціонерів у складанні, оформленні і представленні засновницьких і реєстраційних документів до місцевого реєстру компаній, наймі персоналу, оренді юридичної адреси, встановленні засобів зв'язку і виборі приміщення для проектованої компанії, встановленні необхідних контактів з місцевою адміністрацією тощо. Дуже рідко засновникам вдається з першої спроби зареєструвати свою компанію без юридичних неузгодженостей, повернення документів і втрати часу.

У другому випадку засновникам достатньо після внесення певного авансу юридичній фірмі повідомити необхідний мінімум інформації про себе і компанію, яку створюють, і чекати реєстраційного свідоцтва. Більшість інвесторів вважають за краще користуватися послугами юридичних фірм, оскільки в такому випадку створення і реєстрація обходиться без ускладнень, і не вимагає особистого виїзду засновників в країну реєстрації компанії.

Практично в усіх офшорних центрах розроблено типову документацію, зокрема й стандартні засновницький договір, статут та інші засновницькі документи і форми, а якщо час дозволяє, то засновникам достатньо замовити юридичній фірмі офшорну компанію, яку, залежно від офшорної юрисдикції, буде створено протягом декількох днів або тижнів. Замовлену компанію створять і в тому випадку, якщо у засновників є особливі нестандартні побажання щодо її назви, засновницького договору, статуту, при цьому врахування таких побажань вимагає додаткових узгоджень, експертиз і витрат. У цьому випадку ймовірні випадки повернення реєстраційних документів для уточнення, переоформлення і обґрунтовування, оскільки особливі побажання можуть і не співпадати з нормами місцевого офшорного режиму.

У динамічному офшорному бізнесі час цінують дуже високо, і в певних випадках має попит у підприємців експрес-реєстрація офшорної компанії. Більшість місцевих і міжнародних юридичних фірм можуть задовольнити цей особливий попит, пропонуючи клієнтам компанії, які були створені заздалегідь, з блискавичною перереєстрацією їх на нового власника протягом одного дня і навіть однієї години.

Можливість експрес-реєстрації забезпечується наявністю типових засновницьких і реєстраційних документів і форм, чітким режимом реєстрації, готовністю юридичних контор заради зручності клієнтів йти на додаткові трудові і фінансові витрати і завдяки співпраці місцевої адміністрації з юридичними фірмами. Якщо місцевий реєстратор компаній не наполягає на подальшій перевірці ділової репутації засновників, то юридичні фірми можуть заздалегідь заснувати і зареєструвати необхідну кількість офшорних компаній на ім'я своїх службовців з перспективою їх надшвидкісного продажу майбутнім клієнтам. У цьому випадку службовці юридичних фірм виступають в ролі засновників, директорів і секретарів готових компаній, реєстраційні документи яких в очікуванні покупця поступають на полицю (звідси і назва «компанія на полиці»).

Після отримання заявки і передоплати від клієнта юридична фірма оформлює купівлю-продаж готової компанії спеціальним актом про перехід її акцій у власність клієнта і протоколом зборів акціонерів про відставку акціонерів і директорів першого складу, і вступ в права нових акціонерів та директорів готової компанії. Після відповідного повідомлення реєстратора компаній продаж готової компанії новому власнику стає фактом, що відбувся.

Реєструючи готові компанії заздалегідь, до їх продажу майбутнім клієнтам, юридичні фірми кредитують клієнтів по заснуванню і реєстрації цих компаній і на період до їх реалізації «заморожують» свої кошти. Якщо готові компанії не продано до настання термінів сплати річного збору (а це максимум 1 рік), то в цьому випадку юридичні фірми повинні самі сплатити цей збір за «компанії на полиці», що знаходяться в їх власності. Нарешті, юридичні компанії несуть певну моральну відповідальність за можливі

непристойні вчинки зареєстрованих ними, а потім проданих новим власникам, готових компаній перед місцевою адміністрацією.

Для компенсації вищезазначених витрат юридичних фірм готові компанії продають за цінами вище, ніж ціни компаній на 15–20 %, які створюють на замовлення, а клієнти вважають цю ціну резонною і обґрунтованою – за економію часу, надійність, наочність і якісне оформлення засновницьких і реєстраційних документів готових компаній.

Готові компанії – це переважно нові компанії, що ще не почали проводити комерційні операції і тому що не накопичили ніяких зобов'язань перед третіми особами. Вони в буквальному розумінні законсервовані «на полиці», а точніше, в сейфах юридичних фірм в очікуванні своїх нових господарів. Проте в розпорядження юридичних контор деколи повертають раніше продані готові компанії, від яких їх нові власники з тих або інших причин відмовилися. Такі вже «вживані» готові компанії можуть мати найнесподіваніші, зокрема й боргові зобов'язання, які можуть бути пред'явлені до виконання новим власникам компаній.

Однією з переваг готових компаній, яку засновники схильні враховувати, є та обставина, що попередня реєстрація на ім'я місцевих юридичних фірм, по суті, позбавляє засновників обов'язкової перевірки їх ділової репутації з боку місцевої адміністрації офшорних центрів, а юридичні фірми таку перевірку своєї клієнтури зазвичай не здійснюють.

Таким чином, забезпечення анонімності при проведенні фінансових операцій за допомогою електронних грошей може спровокувати значні ризики щодо відмивання коштів, отриманих злочинним шляхом, або фінансування тероризму. Підтвердженням цієї тези також є історія діяльності відомої системи І-голд (e-gold).

Платіжна система e-gold розпочала свою роботу в 1996 р. Компанію було зареєстровано в офшорній зоні – на Бермудах, але всі трансакції проводилися в Мельбурні, Австралія. З початку роботи системи e-gold її оборот склав більше 90 млн транзакцій. Фізичний обсяг перекладеного допомогою системи золотого еквівалента перевищив 2,2 тони. Платіжна система e-gold мала більше 5 млн користувацьких акаунтів з 165 держав світу. Щоденний оборот в системі доходив до 5 млн дол США.

При цьому:

– існувала можливість відкриття рахунку та проведення транзакції без перевірки інформації про користувачів;

– персонал не мав можливості контролювати сотні тисяч акаунтів користувачів;

– можливе просте переміщення грошей між рахунками e-gold угоду користувача e-gold явно не забороняло застосування системи в злочинних цілях і тощо.

Тому, систему e-gold активно застосовували у злочинній діяльності, зокрема для бізнесу, що експлуатує дітей, бізнесу, пов'язаного з фінансовими пірамідами, шахрайством з кредитними картами і розкраданням персональних даних.

Платіжна система e-gold привернула до себе увагу контролюючих органів ще в 2004 р. А в кінці липня 2008 р., під тиском влади США, система e-gold, фактично, перестала функціонувати як платіжний інструмент.

Реєстрацію нових клієнтських акаунтів призупинено на невизначений час, обмін e-gold на інші електронні валюти заборонено.

Порівняльний аналіз 65 рахунків з найбільшими оборотами в системі станом на січень 2008 року виявив, що більше 70% з них використовувалися для ведення кримінального бізнесу.

При цьому, керівництво та засновників компанії покарано. Нині сайт e-gold зберігає свою працездатність, хоча реєстрацію нових акаунтів тимчасово було припинено на невизначений термін, а доступ до раніше відкритих акаунтів проводиться після введення персонального ідентифікатора платника податків (Tax ID).

Кожен користувач платіжної системи e-gold тепер повинен представити системі документ, що підтверджує його особу (обов'язково з фотографією) та адресу проживання (наприклад, квитанції оплати комунальних послуг). Також фахівці e-gold зробили географічний аналіз кримінальної активності користувачів, в результаті чого було вирішено тимчасово обмежити такий «географічний» ризик. Для цього обрали такий шлях: ввели обмеження на розмір грошових операцій, які відрізняються для жителів різних країн. Всього встановлено 4 категорії країн. Для мешканців держав вищої категорії, таких як США, Франція, Німеччина тощо (всього в цьому списку 30 країн), дозволено проводити вхідні та вихідні операції в розмірі 3000 дол США на місяць. Для основної маси інших держав ця сума становить 1000 дол США. Для користувачів з країн третьої категорії обидва ліміти становлять 0 дол США, що фактично означає неможливість використання свого рахунку в системі e-gold. І з громадянами Північної Кореї, Куби та Ірану e-gold працювати поки не збирається взагалі [5].

Як відомо, фінансування тероризму суттєво відрізняється від процесів відмивання коштів,

отриманих злочинним шляхом, оскільки джерела коштів можуть мати як нелегальне, так і цілком законне походження, а обсяги фінансування тероризму зазвичай є незначними (декілька тисяч доларів).

Саме тому, слід поглянути на електронні гроші крізь призму ризику їх використання для фінансування тероризму. Як засвідчує практика таким ризиком не слід нехтувати.

22 липня 2011 жертвами подвійного теракту в Норвегії стали 77 осіб. Мати підозрюваного у скоєнні цього теракту, Андерса Брейвіка, зізналася на допиті в тому, що допомогла синові легалізувати близько 400 000 норвезьких крон. Поліція встановила, що в 2003 і 2006 роках на рахунках Брейвіка за кордоном перебувало близько 3,6 мільйонів крон. У той час він займався продажем підроблених атестатів через Інтернет. Покупці фальшивих атестатів оплачували документи через PayPal, e-gold або переводили кошти на банківський рахунок Брейвіка в Латвії. Потім Брейвік знімав готівку в банкоматах м. Осло за допомогою іноземних кредитних карток [2].

**Висновки.** Таким чином, з огляду на постійне розширення використання електронних грошей насьогодні стоїть низка завдань у сфері боротьби з відмиванням коштів, отриманих злочинним шляхом, або фінансуванням тероризму:

1. Визначення співвідношення вартості впровадження/посилення заходів запобігання та протидії легалізації коштів, отриманих злочинним шляхом, фінансуванням тероризму та обсягів ринку, рентабельності проектів, пов'язаних з електронними грошима.

2. Необхідність розширення переліку суб'єктів первинного фінансового моніторингу (наприклад, включення мобільних операторів, агентів з обміну електронних грошей).

3. Проведення перевірки клієнтів і можливостей застосування спрощеної методики залежно від суми платежу електронними грошима.

4. Визначення основних інструментів та необхідних масштабів застосування ризик-орієнтованого підходу щодо операцій з електронними грошима.

5. Створення адекватної нормативної та методологічної бази щодо операцій з електронними грошима.

*1. ПФР – підрозділ фінансової розвідки. В Україні – Державна служба фінансового моніторингу України (прим. автора).*

*2. Залежно від законодавства окремої юрисдикції. У низці країн (наприклад, США, Австралії тощо) про всі готівкові операції понад визначену суму повідомляється ПФР; у інших країнах (Росія, Україна тощо) при проведенні фінансової операції з готівкою без відкриття рахунку понад визначену суму здійснюється ідентифікація особи, яка її проводить.*

*3. Феномен тероризму: сучасні форми, економічні аспекти та основні шляхи запобігання / О. М. Бережний, Т. А. Медвідь. — Вісник НБУ. — листопад 2011. — С. 24–31.*

*Список використаних джерел*

1. Кошовец О. Б., Ганичев Н. А. Долгосрочные перспективы развития российского информационно-коммуникационного комплекса / О. Б. Кошовец, Н. А. Ганичев // Проблемы прогнозирования. — 2011г. — №6.

2. Мати Брейвіка зізналась, що відмивала гроші для сина [Електроний ресурс]. — Режим доступу : http://news.finance.ua/ua/~/1/0/all/2012/04/01/274706/

3. Новые способы платежей. Рабочая группа по типологиям. Итоговый проект документа (30 сентября 2010 года) 18 октября 2010 года, Штаб-квартира ОЭСР, Париж, Франция.

4. Офіційний сайт DATA Insight. [Електроний ресурс]. — Режим доступу : http://www.datainsight.ru/.

5. Офційний сайт e-gold. [Електроний ресурс]. — Режим доступу : http://www.e-gold.com/.