

УДК 336.71.078.3

*Кобилянська Л. М., Хвалінський С. О., Осипчук М. Д.***СВІТОВА ПРАКТИКА ВІДМИВАННЯ ДОХОДІВ: СУЧАСНІ МЕТОДИ ТА ТЕНДЕНЦІЇ**

*Розглянуто сучасні методи відмивання доходів і виокремлено низку заходів щодо запобігання та протидії відмиванню коштів у світовому масштабі. Окреслено способи легалізації доходів, одержаних злочинним шляхом, через ринки золота, незаконне втручання в роботу телекомунікаційних та інформаційних мереж, туристичний і гральний бізнес.*

Ключові слова: злочинні доходи, ринки дорогоцінних металів, золоті депозити, кіберзлочин, кібератака, турагентство, гральний бізнес.

Необхідність зменшення впливу тіньового сектору економіки, що ставить під загрозу фінансову безпеку кожної держави, детермінує актуальність дослідження проблеми протидії легалізації злочинних доходів. Нині відмивання коштів набуло глобального характеру: за оцінками МВФ їх сукупний щорічний обсяг становить 2–5 % світового валового продукту [1].

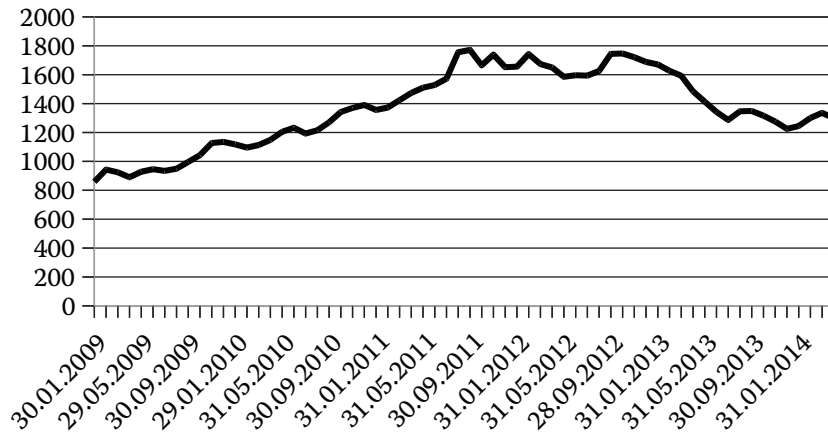
Дослідженню питання легалізації (відмивання) доходів, одержаних злочинним шляхом, та ефективності протидії цьому явищу приділяли увагу такі вітчизняні й зарубіжні вчені, як Є. Абрамов, Ю. Блащук, П. Біленчук, В. Голубев, С. Гуржій, О. Дзюблюк, В. Єгорова, О. Києвець, П. Кверк, І. Мекзенцева, В. Михальський, А. Суєтін, В. Танзі, В. Фадеєв, Л. Чиж та ін. Утім, у зв'язку з появою нових методів легалізації доходів, сучасна практика їх відмивання потребує аналізу.

Метою статті є з'ясування нинішніх способів легалізації (відмивання) доходів, одержаних злочинним шляхом, що сприятиме виявленню основних ознак проведення ризикових операцій, а також слугуватиме базою для визначення у подальших дослідженнях головних заходів із запобігання та протидії відмиванню коштів та фінансуванню тероризму.

Одним із методів, що активно використовується, є операції на ринку дорогоцінних металів. Ринок золота дає змогу інвестування коштів у ліквідний товар, що має високу внутрішню вартість, конвертованість і потенційну анонімність при здійсненні переказів і переміщень. Дорогоцінні метали є універсальним еквівалентом добробуту, важливим елементом фінансової системи та джерелом інвестицій. Золото зберігає вартість, незважаючи на форму, приміром, у вигляді зливків чи готових прикрас (зауважимо, що в останніх до вартості золота додається художня цінність). Таким чином, його часто застосовують як засіб, що дає змогу полегшувати переміщення матеріальних цінностей. Враховуючи посилення наглядового тиску на банки в контексті протидії відмиванню доходів, у найближчій перспективі можна очікувати переливання брудних грошей із банківського сектору на ринок золота.

© Кобилянська Л. М., Хвалінський С. О., Осипчук М. Д., 2014

Світові банківські резерви золота станом на травень 2014 р. дорівнювали 31 820,3 т [2]. П'ятирічна динаміка ціни на золото наведена на рисунку. Протягом цього періоду його ціна варіювалась у межах від 919,5 дол. США за тройську унцію (січень 2009 р.) до 1813,5 дол. США (серпень 2011 р.). З березня 2013 р. вона коливається в межах 1192–1394,8 дол. США. Згідно з даними Всесвітньої ради золота (World Gold Council), станом на початок червня 2014 р. ціна золота дорівнювала 1247,5 дол. США за тройську унцію [2].



Рисунк. Динаміка ціни на золото, дол. США/тройську унцію

Складено за розрахунками автора на підставі: Gold Price in a Range of Currencies since December 1978 [Електронний ресурс]. – Режим доступу: <https://www.gold.org/research/gold-price-range-currencies-december-1978-xlsx-version>.

Золото часто є джерелом нелегальних доходів, які відмиваються (через контрабанду чи нелегальну торгівлю), а також засобом відмивання (через відкриту купівлю за кошти сумнівного походження). Більшість випадків відмивання із залученням золота пов'язані з нелегальною торгівлею наркотиками, організованою злочинною діяльністю та нелегальною торгівлею товарами; воно також активно використовується терористичними угрупованнями, що порушує проблему фінансування золотом терористичної діяльності.

Загалом є чотири види незаконних операцій, пов'язаних із золотом:

- 1) легалізація брудних коштів шляхом купівлі золота;
- 2) виготовлення фальшивих накладних на золото, що використовуються або для приховування руху коштів між суб'єктами схеми відмивання (імітація продажу без реального руху золота), або для пояснення походження нелегального золота (викраденого чи завезеного контрабандним шляхом);
- 3) ухилення від сплати високих ставок ПДВ у країні видобутку золота: останнє купується у країнах із низькою ставкою ПДВ і експортується до країни походження з метою перепродажу та отримання прибутку;
- 4) контрабанда золота, зокрема в країнах, де операції з ним обмежені чи заборонені.

Розглядаючи конкретні схеми відмивання коштів, насамперед слід виокремити "золотий" торговельний бум у Туреччині 2011–2013 рр. У 2011 р. країна

експортувала золото в грошовому еквіваленті обсягом 1,5 млрд дол. США, а імпортувала – на 6,2 млрд дол. США; у 2012 р. експорт зріс до 13,3 млрд дол. США, а імпорт – до 7,6 млрд, сягнувши в 2013 р. 16 млрд дол. США [4]. Причина цієї динаміки полягає в такому. Відповідно до санкцій, запроваджених США, у розрахунках за газ з Іраном було заборонено використання іноземної валюти. Тому Туреччина розраховувалася з Іраном турецькими лірами, за які Іран у подальшому купував золото в Туреччині, що мало вигляд експорту останнього. У зв'язку з відсутністю у Туреччині потрібної кількості золота вона купувала його у Швейцарії. Таким чином, іранський газ був оплачений на 15 млрд дол. США. Реалізація цієї схеми призвела до підвищення зовнішньоторговельного дефіциту в 2013 р. на 18,7 % порівняно з 2012 р. – до 99,85 млрд дол. США, що спричинено зростанням ціни золота на 150 % протягом 2013 р. [5]. Торговельні операції з Іраном проходили через ОАЕ. Схему контролював іранський бізнесмен, банком-посередником був турецький Halkbank. Для забезпечення зручності транспортування золота і вирішення поточних питань “куратор” обладок за допомогою хабарів заручився підтримкою генерального директора Halkbank, міністра економіки Туреччини і двох його синів – міністра закордонних справ Туреччини і міністра ЄС [4].

Частиною цієї схеми було залучення на ринок золота, що перебувало у приватній власності громадян (*under-the-pillow gold*), в обсязі близько 5 тис. т загальною вартістю 300 млрд дол. США. Також банкам було дозволено тримати 30 % обов'язкових резервів на рахунках центрального банку в золоті, що розширювало кредитні можливості за рахунок вивільнених коштів і, таким чином, стимулювало їх до залучення золотих депозитів [6]. Величина останніх, що у 2010 р. становила 2 млрд лір, зросла у 2013 р. до майже 22 млрд лір, тобто на 990 %, а їх частка у загальному обсязі депозитів – з 0,3 до 2,5 % відповідно. Під час приймання золота на депозит банками не порушувалося питання про його походження, що стало передумовою відмивання брудних грошей. До “золотої лихоманки” долучилися не лише звичайні громадяни, а й низка компаній та іноземних інвесторів. Таким чином, золоті запаси ЦБ Туреччини в 2013 р. зросли до 21 млрд дол. США (519,7 т), а загальні резерви – до 135 млрд дол. США [7]. Така схема дала змогу відмити через банки, зокрема Halkbank, близько 85 млрд євро [4]. Як результат, за упущення в забезпеченні протидії відмиванню коштів та фінансуванню тероризму FATF досі ставить Туреччину на один рівень з Індонезією, Пакистаном, Сирією, Єменом, Ефіопією, Еквадором та Нігерією [8].

Відмивання грошей на ринку золота поширене і в інших країнах. Так, в Іспанії у лютому 2014 р. внаслідок спецоперації, спрямованої на протидію відмиванню коштів на ринку цінних металів, у торговців ними було вилучено 6,5 т золота і срібла та 1,7 млн євро готівкою [9].

Для відмивання грошей за допомогою золота часто застосовуються так звані паралельні банківські схеми, зокрема система “хавала-хунді-фей квіан” (*hawala-hundi-fej qian*), поширена в Південній Азії, що базується на довірі й тісних ділових контактах, а золото вважається переданим без фізичного переміщення. Застосування цієї схеми є економічно вигіднішим і не гальмується бюрократичними процедурами, на відміну від руху коштів через офіційні

банківські системи. Такий спосіб відмивання активно поширюється на інші регіони. Центром системи “хавала-хунді-фей квіан” є країни Перської затоки – саме через них відбувається “рух” золота [10].

В Україні ринок благородних металів перебуває у стані зародження, тому використовується найпростіший вид нелегальних операцій – легалізація брудних коштів шляхом купівлі дорогоцінних металів. Як приклад можна навести два випадки. Згідно з даними Департаменту фінансових розслідувань Державної служби фінансового моніторингу України, особою (державним службовцем керівної ланки) здійснювалися фінансові операції на суму понад 4 млн грн [11]. Проте сума проведених фінансових операцій не відповідала сумі офіційно задекларованих доходів. За рахунок зазначених коштів особою було погашено раніше взятий банківський кредит, розміщено депозити у банківських установах, придбано золото у вигляді банківського металу. В іншому випадку фізичною особою за готівку було куплено та внесено на банківські рахунки 495,6 тройської унції золота (6,7 млн грн) та 1454,1 тройської унції срібла (0,5 млн грн). Джерелом походження коштів, спрямованих на купівлю дорогоцінних металів, було вказано надходження від батьків, які декларували незначні доходи [11]. Вочевидь, операції з дорогоцінними металами здійснювалися за кошти сумнівного походження.

Посилення інформатизації спричинило появу нових способів викрадення й відмивання коштів із використанням сучасних комунікаційних технологій. Комп’ютерні технології, значно спрощуючи організаційні, виробничі, управлінські процеси і полегшуючи зберігання, обмін та передавання інформації, водночас генерують новий вид злочинної діяльності – комп’ютерну кіберзлочинність. До найпоширеніших видів кіберзлочинів можна віднести викрадення конфіденційної інформації (секретних технологій та інноваційних розробок), коштів з рахунків юридичних чи фізичних осіб із подальшим відмиванням, ухилення від сплати податків, оприлюднення інформації з особистих сайтів, атаку державних сайтів будь-якого рівня, а також одержання доступу до клієнтських баз корпорацій та фінансових установ.

Інформація чи гроші викрадаються через мережу Інтернет, що надає додаткові можливості для переказу коштів із рахунків фізичних або юридичних осіб на рахунки зловмисників, насамперед за допомогою вірусних програм для зчитування паролів і конфіденційної інформації. Віруси, вражаючи комп’ютерні системи, копіюють паролі, ключі, зберігають скріншоти, пов’язані з фінансовою чи іншою важливою інформацією, та передають дані кіберзлочинцям. Небезпечним винаходом є програми, здатні впливати на роботу та спричиняти збій у функціонуванні стратегічних об’єктів, телекомунікаційних мереж чи банківської інфраструктури. Збитків завдають так звані DDoS-атаки, що здійснюються за допомогою ботнетів та блокують сервіси дистанційного банківського обслуговування.

Істотно зросли обсяги торгівлі шпигунськими та вірусними програмами в інтернеті, а також продаж клієнтських баз та викраденої інформації. Так, у грудні 2013 р. відбулося втручання в роботу мережі роздрібної торгівлі Target (США), внаслідок чого викрадено дані 40 млн кредитних карт і 70 млн облі-

кових записів користувачів, що згодом з'явилися на сайтах підпільних ринків продажу інформації [12].

Є велика кількість видів шахрайств у віртуальному просторі з платіжними картками для банкоматів (фішинг, фармінг, трешинг, вішинг, смішинг, скімінг, шиммінг, траппінг, фантом) чи створення карток-копій, що завдають масштабних економічних збитків. Згідно з розрахунками Центру стратегічних і міжнародних досліджень (США) та компанії McAfee, щорічні втрати світової економіки від кіберзлочинів варіюються в межах від 300 млрд до 1 трлн дол. США і становлять 0,4–1,4 % світового ВВП [13].

Значно спрощується проведення операцій із відмивання коштів організованими кримінальними угрупованнями завдяки створенню фіктивних інтернет-аукціонів та електронних магазинів, туристичних агентств, інвестиційних банків, а також злочинним махінаціям із банківськими кредитами, розсилці спаму, азартним он-лайн іграм, викупу та реєстрації доменів (кіберсквотинг), крадіжці послуг (фоундфрейкінг, рефайлінг) [14]. Створення он-лайн банків та можливість здійснення електронних платежів і транскордонний характер мережевих операцій надають безліч можливостей приховування руху злочинних доходів. Глобальний формат телекомунікаційних і комп'ютерних мереж, цілодобовий доступ до електронних рахунків, висока швидкість здійснення трансакцій, їх анонімність і широкі можливості зловживань конфіденційними даними (доменами, паролями, адресами, іменами) надзвичайно розширюють межі злочинної діяльності.

Кіберзлочини здійснюються за рахунок інноваційних підходів та проведення високоінтелектуальних операцій, застосування нестандартних рішень і урізноманітнення методів. Організація злочинних груп є високоструктурованою та вирізняється вузькою спеціалізацією ролей і обов'язків. Водночас складнішим та витонченішим стає доступ до інформації, що реалізується на підпільних ринках.

Дані оператора зв'язку Deutsche Telekom (Німеччина) засвідчили, що за кількістю кібератак лідерами є США, Китай, країни Латинської Америки й Центральної та Східної Європи, тоді як Росія посідає чільне місце з точки зору якості вчинення телекомунікаційних правопорушень. Україна входить до десяти країн світу, з території яких здійснюється найбільша кількість кібератак. Зокрема, у січні 2014 р. з її території було здійснено 52 009 кібератак, у лютому 2014 р. – 110 132, у березні – 111 730 [15]. До того ж у різноманітних віртуальних сферах діяльності працюють окремі етнічні групи, що свідчить про сформовану спеціалізацію хакерських угруповань. Так, в'єтнамські групи здебільшого віддають перевагу електронній комерції, тоді як вихідці з країн Східної Європи вчиняють злочини проти фінансових інститутів. Китайські хакери переважно зосереджені на IP-технологіях.

Нині констатується тенденція посилення ролі туристичного бізнесу в схемах відмивання коштів і фінансування тероризму. Найчастіше інструментами легалізації злочинних доходів є туристичні агентства, готелі, а також грально-розважальні заклади. У 2013 р. було викрито співробітників підрозділу світової фармацевтичної корпорації GlaxoSmithKline (GSK) у Китаї, яким, починаючи з 2007 р., у вигляді оплати участі лікарів у конференціях перека-

зано на рахунки 700 китайських туристичних агентств близько 3 млрд юанів (489 млн дол. США). Насправді кошти витрачалися на хабарі лікарям та чиновникам, подарунки, розваги тощо з метою налагодження каналів збуту та впливу на процес ціноутворення. Таким чином, GSK та турагентства були кримінальними партнерами (лідер – GSK). Відмивання здійснювалося через організацію фіктивних конференцій, а кошти, витрачені на хабарі лікарям та чиновникам, закладалися у вартість продукції та становили близько 20–30 % вартості вироблених у Китаї препаратів.

Аналогічна схема застосовувалася іншими міжнародними фармацевтичними компаніями. З турфірмою Shanghai Linjiang, задіяною в інциденті з GSK, співпрацювали такі потужні міжнародні компанії, як Sanofi (Франція), Novartis (Швейцарія), Merck (США) і Roche (Швейцарія), що стало підставою для початку розслідування, яке триває й донині. Під слідством перебувають й інші туристичні агентства, котрі, як і Shanghai Linjiang, отримали величезний дохід, здійснивши кілька фактичних бронювань [16].

Такий спосіб відмивання практикується у багатьох країнах. За оцінками Федеральної служби фінансового моніторингу Російської Федерації (РФ), у 2012 р. у вигляді здійснення оплати за неіснуючі тури з країни було виведено 19 млрд руб. [17]. Потік коштів, що виводяться з РФ за кордон, перманентно зростає – приблизно на 6 % щороку. Найпоширенішими схемами є зарубіжні платежі за фіктивні товари й послуги, зокрема у сфері туризму. За даними Асоціації туроператорів Росії, кожен двадцятий долар, сплачений турагентствам, одержаний злочинним шляхом та легалізується за їх допомогою [17].

У березні 2014 р. Службою з попередження і боротьби з відмивання коштів при Національному центрі боротьби з корупцією (НЦБК) разом із прокуратурою по боротьбі з корупцією і компетентними органами США виявлено схему шахрайства, яку практикувала програма міжнародного обміну “Work & Travel” у Молдові. У 2010–2013 рр. громадяни Молдови, які скористалися послугами місцевого представництва програми, переказали на рахунки офшорної компанії понад 6 млн дол. США, що завдало збитків державному бюджету на 15 млн леїв [18].

Наявна практика відмивання коштів через туристичні агентства з метою фінансування тероризму. Громадянин США палестинського походження (штат Флорида, США) зробив спробу перерахування через турагентство Arabian Horizon Travel and Tourism (штат Мічиган, США) коштів на суму 53 тис. дол. США до Ємену. Також йому пред’явлено підозру щодо нелегального переказу 83,5 тис. дол. США до банку West Bank у Палестині та Люксембурзі [19].

У відмиванні злочинних доходів часто задіюють гральний бізнес. Індустрія азартних ігор потребує посиленої уваги, оскільки, будучи законною (у межах певної території), дає змогу компонувати легальний та нелегальний капітал. Ця галузь віддає перевагу використанню готівкових коштів, забезпечуючи анонімність клієнтам. Зокрема, казино пропонують низку фінансових послуг (надання кредитів, сейфів, продаж чеків і переказ коштів), а факт депонування значних сум готівкових коштів не привертає уваги.

З огляду на це слід відзначити намір РФ створити ігрову зону в анексованому Криму [20]. Законопроект “Про внесення змін у статтю 9 Федерального

закону “Про державне регулювання діяльності з організації й проведення азартних ігор та про внесення змін у деякі законодавчі акти Російської Федерації” від 21.04.2014 № 503797-6 (у частині створення ігрової зони на території Республіки Крим) було прийнято у першому читанні 10 червня 2014 р. На нашу думку, такий проект має незначні шанси на реалізацію у найближчій перспективі, оскільки відповідно до законопроекту з федерального бюджету РФ додаткових бюджетних асигнувань на створення такої зони не передбачено, з боку Криму інвестиції (які, за попередніми оцінками, мають становити щонайменше 1,5 млрд дол. США) наразі нереальні, а надходження іноземного капіталу також неможливе через економічні санкції та обмеження з боку Заходу на економічну діяльність в анексованому Криму.

Досвід створення та функціонування ігрових зон у Росії є негативним. Гральний бізнес дозволено в чотирьох таких зонах, з яких фактично здійснює діяльність протягом семи років лише одна (“Азов-Сіті”, Краснодарський край) та досі є неприбутковою. Аналіз діяльності ігрових зон Рахункової палати РФ за перші чотири роки функціонування (2007–2010 рр.) свідчить, що механізм їх створення не забезпечив очікуваного економічного ефекту: при обсязі витрачених бюджетних коштів 1,4 млрд руб. податкові надходження були на рівні 98,7 млн руб. (у 14 разів менше) [21]. Тому плани створення ігрової зони в Криму видаються сумнівними у зв'язку з відсутністю необхідних інвестиційних ресурсів у регіоні, а також попереднім негативним досвідом. При цьому цілком імовірно, що остання буде локальною зоною для відмивання коштів та посилення злочинних тенденцій, зокрема проституції та наркобізнесу.

Легалізація доходів, одержаних злочинним шляхом, та фінансування тероризму набувають глобального характеру. Спостерігається тенденція до диверсифікації інструментів та схем відмивання доходів, що потребує перманентного моніторингу й дослідження з метою ефективної протидії та боротьби з цим явищем. З огляду на посилення наглядного тиску на банки в контексті протидії відмиванню доходів ймовірно переливання брудних грошей із банківського сектору в інші сфери, зокрема на ринок золота, у туристичний та гральний бізнес, активізація кіберзлочинності. Ці тенденції актуалізують потребу розроблення нових методів протидії відмиванню коштів у вказаних сферах.

Повністю унеможливити залучення золота до операцій із відмивання доходів надзвичайно складно, але обмежити його використання шляхом упровадження суворої перевірки джерел коштів на його придбання цілком реально. Ефективність протидії кіберзлочинам у міжнародному форматі зумовлена необхідністю координації зусиль із залученням значних фінансових, технічних, комунікаційних та організаційних резервів. Новітні системи мережевого захисту фінансових установ та організацій, роз'яснювальна робота серед клієнтів у питаннях збереження конфіденційності інформації та персональних даних, обмеження анонімності користувачів у мережі Інтернет та під час проведення банківських операцій он-лайн сприятиме зниженню кількості кіберзлочинів та створенню перешкод подальшому відмиванню незаконно отриманих доходів. З метою запобігання легалізації протиправно одержаних

капіталів і фінансуванню тероризму в сфері туристичного бізнесу доцільно посилити контроль за фінансовими операціями туристичних компаній, здійснювати ретельнішу перевірку іноземних контрагентів щодо достовірності укладених договорів, а також проводити моніторинг компаній, котрі отримують значний дохід, здійснюючи невелику кількість бронювань. Запропоновані рекомендації стосовно протидії легалізації коштів за допомогою розглянутих методів дадуть змогу зменшити масштаб тіньового сектору економіки та підвищити рівень фінансово-економічної безпеки держави.

### Список використаних джерел

1. Money-Laundering and Globalization [Електронний ресурс]. – Режим доступу: <https://www.unodc.org/unodc/en/money-laundering/globalization.html>.
2. World Official Gold Holdings, International Financial Statistics // World Gold Council. – May 2014 [Електронний ресурс]. – Режим доступу: [http://www.gold.org/download/private/World\\_Official\\_Gold\\_Holdings\\_as\\_of\\_May2014\\_IFS.pdf](http://www.gold.org/download/private/World_Official_Gold_Holdings_as_of_May2014_IFS.pdf).
3. Gold Price in a Range of Currencies since December 1978 [Електронний ресурс]. – Режим доступу: <https://www.gold.org/research/gold-price-range-currencies-december-1978-xlsx-version>.
4. Record Gold Import Hits Turkey's Trade Balance / Daily News [Електронний ресурс]. – Режим доступу: <http://www.hurriyetdailynews.com/record-gold-import-hits-turkeys-trade-balance.aspx?PageID=238&NID=61826&NewsCatID=344>.
5. Foreign Trade Statistics [Електронний ресурс]. – Режим доступу: [http://www.turkstat.gov.tr/PreTablo.do?alt\\_id=1046](http://www.turkstat.gov.tr/PreTablo.do?alt_id=1046).
6. Ash A. Why Experts are Praising Turkey's Gold Policy / A. Ash // Business Insider [Електронний ресурс]. – Режим доступу: <http://www.businessinsider.com/how-the-central-bank-of-turkey-uses-gold-2013-1>.
7. Gold Demand Trends (2013) // World Gold Council [Електронний ресурс]. – Режим доступу: [http://www.gold.org/sites/default/files/GDT\\_Q4\\_2013.pdf](http://www.gold.org/sites/default/files/GDT_Q4_2013.pdf).
8. FATF Public Statement – 14 February 2014 [Електронний ресурс]. – Режим доступу: <http://www.fatf-gafi.org/countries/s-t/turkey/documents/public-statement-feb-2014.html>.
9. Spain Raids Gold Dealers suspected of Money-Laundering [Електронний ресурс]. – Режим доступу: <http://www.globalpost.com/dispatch/news/afp/140212/spain-raids-gold-dealers-suspected-money-laundering>.
10. Moulette P. Money-Laundering: staying Ahead of the latest Trends / P. Moulette [Електронний ресурс]. – Режим доступу: [http://www.oecdobserver.org/news/archivestory.php/aid/244/Money\\_laundering:\\_staying\\_ahead\\_of\\_the\\_latest\\_trends.html](http://www.oecdobserver.org/news/archivestory.php/aid/244/Money_laundering:_staying_ahead_of_the_latest_trends.html).
11. Актуальні методи і способи легалізації (відмивання) доходів, одержаних злочинним шляхом, та фінансування тероризму [Електронний ресурс]. – Режим доступу: [http://www.nssmc.gov.ua/user\\_files/content/792/1361363780.pdf](http://www.nssmc.gov.ua/user_files/content/792/1361363780.pdf).
12. Markets for Cybercrime Tools and Stolen Data [Електронний ресурс]. – Режим доступу: [http://www.rand.org/content/dam/rand/pubs/research\\_reports/RR600/RR610/RAND\\_RR610.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf).
13. The Economic Impact of Cybercrime and Cyber Espionage. Report // Center for Strategic and International Studies, July 2013 [Електронний ресурс]. – Режим доступу: [http://csis.org/files/publication/60396rpt\\_cybercrime-cost\\_0713\\_ph4\\_0.pdf](http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf).
14. Структура кіберзлочинності [Електронний ресурс]. – Режим доступу: <http://cybercop.in.ua/index.php/naukovi-statti/80-naukovi-statti/202-struktura-kiber-zlochinnosti>.



15. Overview of Current Cyber Attacks // Top 15 of Source Countries [Електронний ресурс]. – Режим доступу: <http://www.sicherheitstacho.eu/?lang=en>.
16. Barboza D. Glaxo Used Travel Firms for Bribery, China Says / D. Barboza (July 15, 2013) [Електронний ресурс]. – Режим доступу: [http://www.nytimes.com/2013/07/16/business/global/glaxo-used-travel-firms-in-bribery-china-says.html?\\_r=1&](http://www.nytimes.com/2013/07/16/business/global/glaxo-used-travel-firms-in-bribery-china-says.html?_r=1&).
17. Зыкова Т. Под видом оплаты турслуг за рубеж в 2012 году выведено 19 млрд рублей / Т. Зыкова [Електронний ресурс]. – Режим доступу: <http://www.fedsfm.ru/press/media-review/420>.
18. A Brand New “Work & Travel” Scheme: Money-Laundering of 6 Million Dollars and MDL 15 Million Damage to the State [Електронний ресурс]. – Режим доступу: <http://www.cna.md/en/evenimente/brand-new-work-travel-scheme-money-laundering-6-million-dollars-and-mdl-15-million-damage>.
19. Schlusel D. Religion of Laundering Money Orders Through Travel Agencies to Terrorists in Yemen / D. Schlusel [Електронний ресурс]. – Режим доступу: <http://www.debbieschlusel.com/3196/religion-of-laundering-money-orders-through-travel-agencies-to-terrorists-in-yemen-update-travel-agency-named-under-investigation-for-terrorism-but-not-indicted-why-money-went-to-palestinian-t>.
20. О внесении изменений в статью 9 Федерального закона “О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации”: проект закону Російської Федерації від 21.04.2014 № 503797-6 [Електронний ресурс]. – Режим доступу: [http://asozd2c.duma.gov.ru/addwork/scans.nsf/ID/7C1E5D159428AE3F43257CC10027A531/\\$FILE/503797-6.PDF?OpenElement](http://asozd2c.duma.gov.ru/addwork/scans.nsf/ID/7C1E5D159428AE3F43257CC10027A531/$FILE/503797-6.PDF?OpenElement).
21. Отчет о результатах контрольного мероприятия “Проверка расходов государственных средств на создание игорных зон за 2007–2010 годы, а также оценка эффективности их функционирования” (совместно с контрольно-счетными органами субъектов Российской Федерации) // Бюллетень Счетной палаты. – 2012. – № 6. – С. 56–57.

*Стаття надійшла до редакції  
10 червня 2014 року*