ISSN (Print) 2307-6968, ISSN (Online) 2663-2209
Вчені записки Університету «КРОК» №3 (59), 2020

Розділ 8. Економічна безпека держави та суб'єктів господарської діяльності

УДК 351:343.326
DOI: 10.31732/2663-2209-2020-59-236-242

ФІНАНСУВАННЯ ТЕРОРИЗМУ: НОВІ ВИКЛИКИ ТА ЗАГРОЗИ ДЕРЖАВНІЙ БЕЗПЕЦІ, НАПРЯМИ УДОСКОНАЛЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ

Грабчук О.В.[1], Супрунова І.В.[2]

[1] асистент кафедри права та правоохоронної діяльності, Державний університет «Житомирська політехніка», м. Житомир, вул. Чуднівська, 103, 10005, Україна, тел.: (067)-994-23-34, e-mail: crimcase08@gmail.com, ORCID: https://orcid.org/0000-0001-8066-6547

[2] к.е.н., доцент, доцент кафедри економічної безпеки, публічного управління та адміністрування, Державний університет «Житомирська політехніка», м. Житомир, вул. Чуднівська, 103, 10005, Україна, тел.: (067)-708-33-21, e-mail: suprunova13s@gmail.com, ORCID: https://orcid.org/0000-0001-5484-6421

TERRORISM FINANCING: NEW CHALLENGES AND THREATS TO STATE SECURITY, DIRECTIONS FOR IMPROVING PUBLIC ADMINISTRATION

Hrabchuk O.[1], Suprunova I.[2]

[1] assistant professor of law and law enforcement activities department, State University «Zhytomyr Polytechnic», Zhytomyr, st. Chudnivska, 103, 10005, Ukraine, tel.: (067)-994-23-34, e-mail: crimcase08@gmail.com, ORCID: https://orcid.org/0000-0001-8066-6547

[2] Ph.D. (Economics), associate professor, associate professor of economic security, public administration and management department, State University «Zhytomyr Polytechnic», Zhytomyr, st. Chudnivska, 103, 10005, Ukraine, tel.: (067)-708-33-21, e-mail.: suprunova13s@gmail.com, ORCID: https://orcid.org/0000-0001-5484-6421

Анотація. *Під впливом сучасних інформаційно-комп'ютерних технологій розширюються способи фінансування тероризму. Встановлено, що для розробки дієвих заходів та інструментів виявлення нових загроз необхідне ґрунтовне вивчення таких схем та способів. Метою дослідження є розкриття особливостей DarkNet, криптовалюти та їх впливу на державну безпеку, що стане основою для удосконалення державного управління протидією фінансуванню тероризму. В статті розкрито напрями використання DarkNet для терористичних цілей. Особливу увагу приділено фінансуванню тероризму через DarkNet з використанням в якості платіжного засобу криптовалюти. Охарактеризовано криптовалюту та її переваги з двох сторін – як сучасний платіжний засіб (відсутність комісії за здійснення переказів між країнами; обмежений обсяг випуску; доступність в будь-який момент часу) та як інструмент відмивання грошей, джерело фінансування тероризму (відсутність регулювання емісії; анонімність; недостатній рівень безпеки збереження; складність контролю переказів). Враховуючи наведені переваги та їх вплив на економіку, держава визначає статус криптовалюти на своїй території. Наведені приклади використання криптовалюти в світі з метою фінансування тероризму. Встановлено, що для України, як лідера в світі за використанням цифрової валюти, необхідне чітке закріплення її правового статусу та встановлення обмежувальних правових норм для протидії несприятливим явищам. Це дозволить врегулювати її використання в господарській діяльності та створить умови для боротьби правоохоронних органів із залученням цифрових валют в злочинній діяльності. Обґрунтована нагальна потреба у розробці нових методів та заходів для відстеження та аналізу використання терористами DarkNet. Частина заходів повинна бути пов'язана з пошуком програмного забезпечення, що дозволить покращити каталогізацію глибоких веб-сайтів.*

Ключові слова: *державне управління; фінансування тероризму; крипто валюта; цифрова валюта; DarkNet.*
Формули: 0; рис.: 2; табл.: 0; бібл.: 10.

Annotation. *Modern information and computer technologies are expanding the ways of financing terrorism. It is established that the development of effective measures and means of identifying new threats requires a careful study of such schemes and methods. The aim of the study is to reveal the features of DarkNet, cryptocurrencies and their impact on national security, which will be the basis for improving public administration in the fight against terrorist financing.*

The article reveals the directions of using DarkNet for terrorist purposes. Particular attention is paid to the financing of terrorism through DarkNet using cryptocurrency as a means of payment. Cryptocurrency and its benefits are described in two ways - as a modern means of payment (no commission for transfers between countries; limited issue; availability at any time) and as a tool for money laundering, a source of terrorist financing (lack of regulation; anonymity; insufficient security). storage, the complexity of transmission management). Given the above advantages and their impact on the economy, the state determines the status of cryptocurrency in its territory. Examples of the use of cryptocurrency in the world to finance terrorism are given. It is established that Ukraine, as a world leader in the use of digital currency, needs a clear consolidation of its legal status and the establishment of restrictive legal norms to combat adverse events. This will regulate its use in economic activities and create conditions for law enforcement agencies to combat the involvement of digital currencies in criminal activities. There is an urgent need to develop new methods and measures to track and analyze the use of DarkNet by terrorists. Some activities need to be related to finding software that will improve the cataloging of deep websites.

Key words: *public administration; terrorist financing; cryptocurrency; digital currency; DarkNet.*
Formulas: 0; fig.: 2; tabl.: 0; bibl.: 10.

Постановка проблеми. Боротьба з тероризмом як в Україні, так і в більшості країн світу, не втрачає своєї актуальності. Її важливим напрямом є протидія фінансуванню, яке є підґрунтям для виникнення та продовження функціонування явища тероризму. Дослідження даного питання проводитися не один рік, вагомими є розробки науковців та дії різноманітних установ і органів як на міжнародному, так і на державному рівнях.

Проте слід враховувати той факт, що існуюча на сучасному етапі достатньо велика кількість способів фінансування тероризму під впливом розвитку інформаційно-комп'ютерних технологій постійно розширюється та удосконалюється. Поряд із традиційними способами з'являються нові, які базуються на доступності інтернету, стрімкому поширенню соціальних мереж. Крім того, навіть дієві, професійні механізми боротьби з фінансуванням тероризму необхідно модифікувати у зв'язку з появою нових загроз, впровадженням сучасних цифрових технологій.

Таким чином, удосконалення державного регулювання в сфері протидії фінансуванню тероризму можливе тільки за умови чіткого розкриття його теоретичних засад з врахуванням сучасних тенденцій розвитку економіки та цифрових технологій.

Аналіз останніх досліджень і публікацій. Розкриття особливостей використання інформаційно-комп'ютерних технологій для фінансування тероризму піднімалося Віліч В., Старцевим Г. Проблемні питання обігу криптовалюти як з правової, так економічної точок зору розглядалося в працях таких науковців, як Деревянко Б., Леськів С., Мірецька Е., Омельчук Л., Пашко Д. Проте незважаючи на інтерес до криптовалюти, розкриття її особливостей, характеристик з позиції державного управління протидією фінансування тероризму практично не здійснювалося.

Формулювання цілей статті. Мета дослідження полягає в розкритті особливостей DarkNet та криптовалюти та їх впливу на державну безпеку, що стане основою для удосконалення державного управління протидією фінансуванню тероризму. Методологічну основу дослідження склали емпіричні побудови, аналіз та синтез, системний підхід.

Виклад основного матеріалу дослідження. В епоху інформаційних технологій тероризм набуває значно ширшого наповнення. Його можна розглядати як звичайний тероризм, в якому класична зброя використовується для знищення ресурсів та людей у фізичному сенсі; як технотероризм, коли класичні боєприпаси використовуються для руйнування інфраструктури та заподіяння шкоди в кіберпросторі; і як кібертероризм, де нові інструменти (шкідливе програмне забезпечення, електромагнітна зброя) використовуються для знищення та модифікації даних у кіберпросторі [1].

Кіберпростір дозволяє значно полегшити доступ більшої кількості людей до пропаганди терористичних організацій та незаконної діяльності.

За таких умов особливу небезпеку з точки зору фінансування тероризму несе технологія DarkNet. Для характеристики даної прихованої мережі, з'єднання якої встановлюються тільки між довіреними пірами з використанням нестандартних протоколів та портів, використовуються також такі поняття, як «темна мережа», «чорний інтернет», «прихована мережа», «темний веб» тощо. Ця технологія недостатньо досліджена і в наукових працях та на практиці зустрічаються випадки, коли дане поняття ототожнюється з Deep Web, Deep Net. Зрозуміло, що більша частина інформації в Інтернеті прихована далеко на сайтах, і стандартні пошукові системи не можуть отримати доступ до неї. Саме тому, не дивлячись на певну схожість щодо відсутності індексації стандартними пошуковими системами, ці технології є різними.

Можливості Інтернету використовуються терористичними угрупованнями вже понад двадцять років. Проте наявні характеристики видимого Інтернету (Surface Web) не забезпечують анонімності (тобто не передбачають відсутності стеження) для злочинців, тим самим стимулюють до пошуку інших більш сприятливих для них способів.

DarkNet, з однієї сторони, спрямований на забезпечення недоторканності особистого життя та захисту від політичних репресій, а з іншої – приховує в собі низку небезпечних цілей. Зокрема, з його використанням відбуваються злочини в сфері інформаційних технологій, незаконне розповсюдження файлів, захищених авторськими правами та фінансується тероризм. DarkNet є дуже популярним місцем для різного роду незаконної діяльності, зокрема для продажу нелегальної зброї і вибухових речовин.

Для терористичних цілей DarkNet може використовуватися за такими напрямами:

- для зв'язку, радикалізації та планування терористичних атак (використання видимого Інтернету прискорило темпи усунення екстремістів);
- для вербування (більшою мірою для надання подальших вказівок);
- для пропаганди;
- для використання віртуальних валют.

Саме останній напрям викликає найбільше занепокоєння. Криптовалюта часто використовується для платежів, пов'язаних з незаконною торгівлею, відмиванням грошей злочинними угрупуваннями та фінансуванням терористичних операцій.

В той же час використання такого інструменту, як криптовалюта (зустрічаються і інші поняття для позначення даного інструменту, зокрема віртуальна валюта, цифрова валюта тощо) в комерційних операціях в Інтернеті набуває все більшої популярності. Це, в свою чергу, зумовлює залучення нових технології для здійснення злочинів.

Протягом останніх років терористичні угруповання диверсифікують свої джерела фінансування. Один з напрямів такої диверсифікації є збір коштів в Інтернеті, як за допомогою традиційних платформ внесків в Інтернеті та соціальних мережах, так і за допомогою криптовалют.

Так, яскравим прикладом використання криптовалюти для фінансування тероризму є спеціально створена палестинською групою «Аль-Кассам» інфраструктура збору коштів для бойовиків. Збройне відділення ХАМАС розпочало проект на початку 2019 року, використовуючи криптовалюту для збору коштів, які потім були виділені на покриття витрат на джихад проти Ізраїлю. Поширення інформації про групу та розкриття інструкцій щодо підтримки її діяльності криптовалютами відбувалося через соціальні мережі, зокрема Twitter [2].

Є також приклади дієвих заходів в боротьбі з організованою криптовалютною злочинністю, спрямованою на фінансування тероризму. Так, в 2020 р. французькими правоохоронними органами за звинуваченням у створенні «цілої архітектури мережі фінансування тероризму» з використанням криптовалюти затримано осіб, що

керували діяльністю злочинної групи в північно-західному регіоні Сирії з 2013 р. [3].

Використання криптовалюти терористичними угрупуваннями обумовлено такими її перевагами, як анонімність та відсутність складних процедур обміну. Саме тому ставлення до криптовалюти сьогодні двояке (рис. 1).

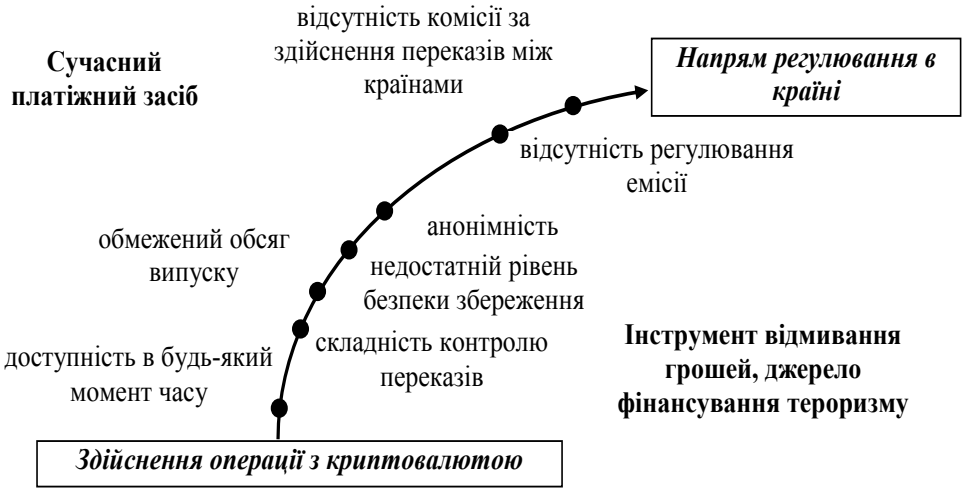

Рис. 1. Оцінка операцій з криптовалютою для визначення статусу її визнання в країні
Джерело: розробка автора

З однієї сторони віртуальна валюта є сучасним платіжним засобом, який здатний у майбутньому здійснити революційний вплив на традиційну систему розрахунків. Її вже на сучасному етапі охоче використовуються в діяльності «стартапів». Українська біржа стала першою в світі площадкою, де торгуються деривативи Bitcoin. Зростаючий інтерес до криптовалюти підтверджується і показниками. Так, в 2017 р. Україна входила в ТОП-10 країн світу за кількістю користувачів Bitcoin [4], а в 2020 р. наша країна вже входила в ТОП-3 за спільнотою блокчейн-розробників та посіла перше місце в рейтингу використання криптовалюти (рис. 2).

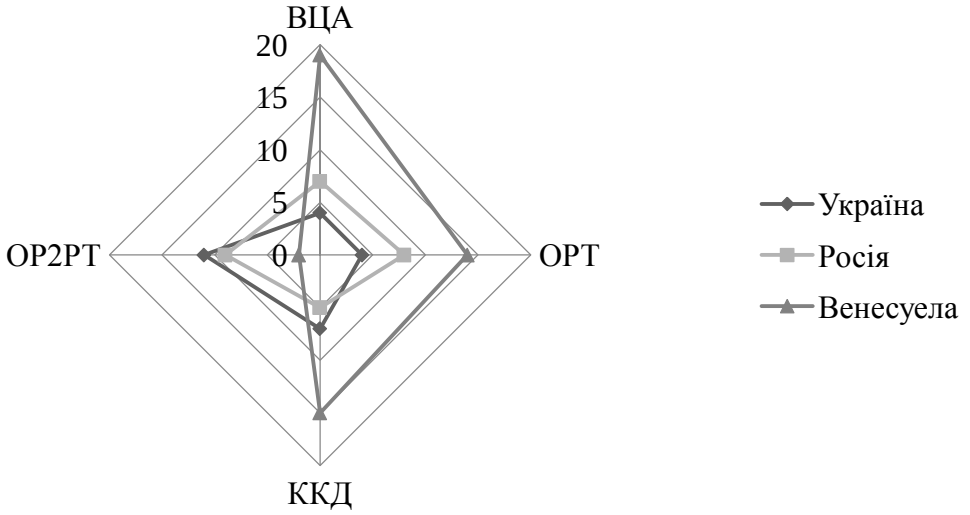

Рис. 2. Критерії розрахунку індексу застосування цифрових активів в Україні, Росії та Венесуелі
Джерело: представлено на основі звіту аналітичної компанії Chainalysis [5]
Умовні позначення:

ВЦА – вартість цифрових активів, що пересилаються, в розрахунку на душу населення
ОРТ – обсяг роздрібних транзакцій (на суму менше 10000 дол. США), розрахований за паритетом купівельної спроможності на душу населення
ККД – кількість криптовалютних депозитів, зважених за кількістю користувачів Інтернету
ОР2РТ – обсяг Р2Р транзакцій, розрахований за паритетом купівельної спроможності на душу населення та кількістю користувачів Інтернет

Україна, як і Росія, отримала високі значення за всіма критеріями, що включаються до Глобального індексу прийняття криптографічних даних. Для Венесуели всі критерії мали середнє значення за винятком обсягу Р2Р транзакцій, за яким країна посіла друге місце та яке фактично і дозволило піднятися їй в рейтингу.

Таким чином, беззаперечним є факт наявності на території України криптовалюти, проте її основна маса знаходиться в так званій «сірій» зоні. Така ситуація цілком зрозуміла, адже офіційного правового статусу на території нашої країни у неї немає.

З іншої сторони швидкість та анонімність онлайн-платежів обґрунтовують її використання в незаконній сфері – відмивання грошей, придбання зброї та інших незаконних товарів і послуг (дитяча порнографія, вибухівка). Це, в свою чергу, створює загрози державі та вимагає розробки механізмів державного управління в сфері протидії фінансуванню тероризму, зокрема, обумовлює необхідність запровадження обмежувальних правових норм для протидії несприятливим явищам.

Слід враховувати, що протягом останніх років сфера загроз, які виходять від тероризму, значно розширилася. Як справедливо зазначає Г.В. Старцєв, «до неї стали включати загрози соціального та політичного характеру, зокрема загрози територіальної цілісності країни» [6]. Тому питання вибору та впровадження дієвих заходів держави, спрямованих на своєчасне виявлення та усунення можливостей використання криптовалюти для фінансування тероризму особливо актуальне.

Зарубіжні країни по-різному підходять до питань оцінки впливу криптовалюти на економічний розвиток – від повного заперечення або навіть розгляду її як загрози до визнання її фактором економічного зростання. Відповідно різняться і позиції щодо правового регулювання обігу криптовалюти – від невизнання до його розробки. В той же час ігнорування криптовалюти на державному рівні не вирішить проблем та не усуне загроз, які вона в собі приховує.

На сучасному етапі не існує розроблених механізмів захисту від негативного впливу криптовалюти на державну безпеку. Невизначеність правового статусу криптовалюти призводить до труднощів у процесі оподаткування та взаємодії з контролюючими органами. Сплачуючи кошти за віртуальну валюту, суб'єкти отримують актив, для якого немає правил як щодо його оподаткування, так і відображення в бухгалтерському обліку. Саме тому погоджуємося з Е. Мірецькою в тому, що визнання криптовалюти «…дозволить визначити правову базу для її функціонування та отримати від цього вигоди через податкову систему, але також обмежить її використання в … злочинній діяльності як у процесах легалізації коштів, тобто відмивання грошей, так і, наприклад, у процесах фінансування тероризму» [7].

Узагальнюючи праці науковців [8; 9; 10], до особливих питань, пов'язаних з операціями з криптовалютою, які потрібно вирішити на сучасному етапі слід віднести: визначення правового режиму інструменту криптовалюти; правового статусу «ферм криптовалюти»; правового режиму операцій із майнінгу (видобування) криптовалюти; обґрунтування легітимації чи заборони обігу криптовалюти; оподаткування операцій із криптовалютою у випадку їх легітимації. Як бачимо, практично всі проблемні питання, пов'язані з окресленням місця криптовалюти на законодавчому рівні, а це, в свою чергу, дозволить не тільки

врегулювати її використання в господарській діяльності, але й створить умови для боротьби правоохоронних органів з залученням цифрових валют в злочинній діяльності.

Враховуючи значні ризики, які в собі несе криптовалюта щодо фінансування тероризму, необхідним є проведення ґрунтовного дослідження питань державного управління протидією фінансування тероризму, розробки системи економіко-правових заходів, що дозволили б вирішити проблеми, пов'язані з обігом криптовалюти.

Висновки. Враховуючи стрімкий розвиток інформаційно-комп'ютерних технологій, обґрунтована необхідність удосконалення державного управління протидією фінансуванню тероризму. Постійне удосконалення підходів до використання терористами DarkNet створює нові перепони для урядів, установ, спеціалізованих органів в боротьбі з тероризмом. Фінансування тероризму через DarkNet з використанням в якості платіжного засобу криптовалюти на сьогоднішній день становить реальну загрозу світовій спільноті. Адже контроль операцій з використанням криптовалюти є досить складним процесом, що зумовлено відсутністю емісійного центру, анонімністю технологій блокчейн. А враховуючи розвиток сучасних цифрових технологій, вважаємо, що протягом найближчих років правовий статус та умови функціонування ринку криптовалюти зазнають значних змін. Тому питання розробки правового забезпечення операцій з криптовалютою є актуальним особливо щодо обґрунтування механізмів державного управління в сфері протидії фінансуванню тероризму в контексті забезпечення державної безпеки. Необхідним є удосконалення законодавства в сфері протидії легалізації (відмивання) доходів, одержаних злочинним шляхом та фінансуванню тероризму в напрямі врахування використання цифрових валют для здійснення цих злочинів.

Обґрунтована нагальна потреба у розробці нових методів та заходів для відстеження та аналізу використання терористами DarkNet. Частина заходів повинна бути пов'язана з пошуком програмного забезпечення, що дозволить покращити каталогізацію глибоких веб-сайтів. Проте потребують також зміни і діючі нормативно-правові документи. Отже, назріла необхідність системного аналізу та вдосконалення законодавства, а також розробки спеціальних програмних засобів з метою ефективної протидії новим викликам і загрозам у сфері фінансування тероризму.

Література:

1. Vilić V. Dark web, cyber terrorism and cyber warfare: dark side of the cyberspace. *Balkan Social Science Review*. 2017. Vol. 10. P. 7-25. URL: https://www.researchgate.net/publication/324720749_DARK_WEB_CYBER_TERRORISM_AND_CYBER_WARFARE_DARK_SIDE_OF_THE_CYBERSPACE

2. Jesteś z nami? Rzuć bitcoina. Kryptowaluty sfinansują działalność ekstremistów. 19 lutego 2020. URL: https://www.cyberdefence24.pl/jestes-z-nami-rzuc-bitcoina-kryptowaluty-sfinansuja-dzialalnosc-ekstremistow.

3. Kryptowaluty źródłem finansowania terroryzmu. Areszt dla 29 osób. 30 września 2020. URL: https://www.cyberdefence24.pl/kryptowaluty-zrodlem-finansowania-terroryzmu-areszt-dla-29-osob.

4. Правовое регулирование криптовалютного бизнеса. Февраль 2017 г. URL: https://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin-Businesses-Regulation.pdf.

5. The 2020 Global Crypto Adoption Index: Cryptocurrency is a Global Phenomenon. URL: https://blog.chainalysis.com/reports/2020-global-cryptocurrency-adoption-index-2020.

6. Старцев Г.В. Экономические и правовые механизмы по противодействию террористическим угрозам. *МИР (Модернизация. Инновации. Развитие).* 2010. № 4. С. 128-131.

7. Mirecka E. Kryptowaluty a problematyka stabilności finansowej i gospodarczej. *Zeszyty Naukowe Uniwersytetu Szczecińskiego Finanse Rynki Finansowe Ubezpieczenia*. 2018. Vol. 2 (92), S. 281-289. DOI : https://doi.org/10.18276/frfu.2018.92-24.

8. Деревянко Б. В. Ризики здійснення операцій з криптовалютою (біткойнами) громадян і суб'єктів господарювання України. *Форум права.* 2017. № 3. С. 33–39. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2017_3_8.

9. Леськів С. Кримінально-правові аспекти визначення статусу криптовалюти в Україні: вітчизняний та зарубіжний досвід.

Підприємництво, господарство і право. 2019. № 9. С. 199-203. DOI : https://doi.org/10.32849/2663-5313/2019.9.33.

10. Пашко Д. В, Омельчук Л. В. Потреба визначення статусу криптовалют в Україні: економічні та кримінальні процесуальні аспекти. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2018. Вип. 1-2 (10-11). С. 173-179.

References:

1. Vilić, V. (2017), "Dark web, cyber terrorism and cyber warfare: dark side of the cyberspace", *Balkan Social Science Review*, vol. 10, pp. 7-25, retrieved from : https://www.researchgate.net/publication/324720749_DARK_WEB_CYBER_TERRORISM_AND_CYBER_WARFARE_DARK_SIDE_OF_THE_CYBERSPACE.

2. Jesteś z nami? Rzuć bitcoina. Kryptowaluty sfinansują działalność ekstremistów (2020), retrieved from : https://www.cyberdefence24.pl/jestes-z-nami-rzuc-bitcoina-kryptowaluty-sfinansuja-dzialalnosc-ekstremistow.

3. Kryptowaluty źródłem finansowania terroryzmu. Areszt dla 29 osób (2020), retrieved from : https://www.cyberdefence24.pl/kryptowaluty-zrodlem-finansowania-terroryzmu-areszt-dla-29-osob.

4. Legal regulation of the cryptocurrency business (2017), retrieved from: https://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin-Businesses-Regulation.pdf.

5. The 2020 Global Crypto Adoption Index: Cryptocurrency is a Global Phenomenon (2020), retrieved from: https://blog.chainalysis.com/reports/2020-global-cryptocurrency-adoption-index-2020

6. Startcev, G. V. (2010), "Economic and legal mechanisms to counter terrorist threats", *MIR (Modernizatciia. Innovatcii. Razvitie)*, № 4, pp. 128-131.

7. Mirecka, E. (2018), "Cryptocurrencies and the issues of financial and economic stability", *Zeszyty Naukowe Uniwersytetu Szczecińskiego Finanse Rynki Finansowe Ubezpieczenia*, vol. 92, pp. 281–289. DOI : https://doi.org/10.18276/frfu.2018.92-24.

8. Derevianko, B. V. (2017), " Risks of transactions with cryptocurrency (bitcoins) of citizens and business entities of Ukraine", *Forum prava*, № 3, pp. 33–39, retrieved from: http://nbuv.gov.ua/UJRN/FP_index.htm_2017_3_8

9. Leskiv, S. (2019), "Criminal law aspects of determining the status of cryptocurrency in Ukraine: domestic and foreign experience", *Pidpryiemnytstvo, hospodarstvo i pravo*, № 9, pp. 199-203. DOI : https://doi.org/10.32849/2663-5313/2019.9.33.

10. Pashko, D.V, Omelchuk, L.V. (2018), "The need to determine the status of cryptocurrencies in Ukraine: economic and criminal procedural aspects", *Mizhnarodnyi yurydychnyi visnyk: aktualni problemy suchasnosti (teoriia ta praktyka)*, № 1-2 (10-11), pp. 173-179.

Стаття надійшла до редакції 17.10.2020 р.