Legal Horizons

Journal homepage: https://legalhorizons.com.ua/en
***Legal Horizons*, 14(2), 105-110**

UDC 343.37(075.8)
DOI: 10.21272/legalhorizons.2021.i14.p105

Criminological Aspects of Combatting Money Laundering in Cyberspace

Mykhailo O. Dumchykov*, Olha S. Bondarenko

Sumy State University
40007, 2 Rymskyi-Korsakov Str., Sumy, Ukraine

Article's History:

Submitted: 15.03.2021
Revised: 02.05.2021
Accepted: 04.06.2021

Abstract

This study investigates the criminological counteraction to cyber-legalisation of corrupt income. The study emphasised that the number of Internet users in Ukraine has increased over the last decade, and the level of cybercrime has increased along with it. The spread of computer viruses, fraud, theft of funds from bank accounts or e-wallets, personal and commercial information, and violations of computer systems are far from a complete list of cybercrimes, as their number and variety only increase. It was found that, in contrast to "classic" money laundering through the use of the banking system, cyber-legalisation of income is based on the use of various types of transactions: from bank transfers, replenishment, or withdrawal of cash to the use of digital currency. The authors described the methods used by criminals upon money laundering in the field of cybercrime. The main areas of improvement of methods of ensuring the counteraction to and prevention of legalisation of the profits connected with crime in cyberspace include amendments to the Criminal Code of Ukraine concerning introduction of new articles; recognition of computer and digital data as evidence for the prompt investigation of cybercrime; larger-scale introduction of electronic-digital signature, which will positively affect the protection of funds and valuable information. Particular attention was also paid to the importance of the introduction of certain safeguards by banking institutions to prevent criminal acts in case of certain dubious financial transactions: notifying customers of each transaction that was concluded using their account; implementation of mandatory two-factor authentication; introduction of a "black list" of accounts (IP addresses) of fraudsters to automatically block transactions, etc. The authors concluded that cybercrime is the latest form of socially dangerous acts, which carries great threats, but, unlike the usual theft and fraud, it is constantly improving along with technology, which, in turn, complicates the prevention and counteraction to illegal actions

Keywords: cybercrime, corruption, financial transactions, prevention of money laundering, cyber-legalisation

Suggested Citation:

Dumchykov, M.O., & Bondarenko, O.S. (2021). Criminological aspects of combatting money laundering in cyberspace. *Legal Horizons*, 14(2), 105-110.

*Corresponding author

Кримінологічні аспекти протидії легалізації корупційних доходів в кіберпросторі

Михайло Олександрович Думчиков, Ольга Сергіївна Бондаренко
Сумський державний університет
40007, вул. Римського-Корсакова, 2, м. Суми, Україна

Анотація

Стаття присвячена темі кримінологічної протидії кіберлегалізації корупційних доходів. У статті наголошено на тому, що за останнє десятиліття в Україні зросла кількість користувачів мережі Інтернет, паралельно з цим зріс і рівень кіберзлочинності. Поширення комп'ютерних вірусів, шахрайство, викрадення коштів з банківських рахунків або електронних гаманців, особистої та комерційної інформації та порушення правил роботи комп'ютерних систем далеко є не повним переліком кіберзлочинів, оскільки з кожним днем їх кількість та різноманіття тільки збільшується. З'ясовано, що на відміну від «класичного» відмивання доходів, що отримані злочинним шляхом за допомогою використання банківської системи, кіберлегалізація доходів заснована на використанні різних типів транзакцій: від банківських переказів, поповнення або зняття готівки до використання цифрової валюти. Охарактеризовано методи, які використовуються злочинцями у процесі відмивання корупційних доходів, одержаних у сфері кіберзлочинності. Названо основні напрями вдосконалення методів забезпечення у сфері протидії та попередження легалізації прибутків, пов'язаних зі злочинністю у кіберпросторі: внесення змін до Кримінального кодексу України щодо запровадження нових статей; визнання комп'ютерних і цифрових даних у якості доказів задля оперативного розслідування кіберзлочинів; більш масштабне впровадження електронно-цифрового підпису, що позитивно вплине на захист коштів, цінної інформації. Також особлива увага звертається на важливість впровадження банківськими установами певних запобіжників, коли виникає певні сумнівні фінансові транзакції, з метою запобігання злочинним діянням: повідомлення клієнтів про кожну транзакцію, що була проведена з його рахунком; здійснення обов'язкової двофакторної автентифікації; введення «чорного списку» рахунків (IP-адрес) шахраїв для автоматичного блокування операцій тощо. Зроблено висновок, що кіберзлочинність є новітньою формою суспільно-небезпечних діянь, що несе великі загрози, але, на відміну від звичайних крадіжок і шахрайства, вона постійно вдосконалюється разом з технологіями, що, зі свого боку, ускладнює попередження та протидію незаконним діям

Ключові слова: кіберзлочини, корупція, фінансові транзакції, попередження легалізації прибутків, кіберлегалізація

Постановка проблеми

Майбутнє кожної країни світу у багатьох аспектах залежить від економіки. А для того, щоб забезпечити легальне існування та розвиток цієї сфери потрібно уникати або запобігати злочинам, а також не шкодити окремим особам, організаціям, установам, підприємствам або країнам в економічних питаннях. За останнє десятиліття в Україні зросла кількість користувачів мережі Інтернет, паралельно з цим зріс і рівень кіберзлочинності. На сьогодні персональний комп'ютер, телефон або інший гаджет з доступом до мережі Інтернет є звичайністю, яка необхідна для того, щоб забезпечити себе доступом до великої кількості інформації, передачі різноманітних документів, файлів і будь-яких даних, здатність проводити банківські операції, торгівлю, грошові транзакції тощо. Одними з основних проблем в Україні є тіньова економіка та кіберзлочинність. Це і заважає подальшому розвитку нашої країни у всебічних напрямах, зокрема й на міжнародній арені, оскільки через подібні проблеми ми лишаємося іноземних інвестицій, можливих вигідних ринкових відносин тощо.

Поширення комп'ютерних вірусів, шахрайство, викрадення коштів з банківських рахунків або електронних гаманців, особистої та комерційної інформації та порушення правил роботи комп'ютерних систем далеко є не повним переліком кіберзлочинів, оскільки з кожним днем їх кількість і різноманіття тільки збільшується. На відміну від «класичного» відмивання доходів, що були отримані злочинним шляхом, за допомогою використання банківської системи, кіберлегалізація доходів, заснована на використанні різних типів транзакцій, від банківських переказів, поповнення або зняття готівки до використання цифрової валюти.

Розкриття та відстеження злочинних фінансових ланцюгів є складним завданням для правоохоронних органів, оскільки заплутані схеми є справжнім викликом, а для цього потрібні кваліфіковані спеціалісти у кібербезпеці, належне програмне та

технічне забезпечення, що зможе допомогти якісно та ефективно протидіяти кіберлегалізації доходів. Аналіз становлення та розвитку економічної та кіберсфери, їх проблеми та шляхи удосконалення, на сьогодні заслуговують особливої уваги.

Аналіз останніх досліджень і публікацій

Науковим вивченням питання кіберзлочинності та пов'язаною з нею легалізацією доходів та інших подібних економічних суспільно-небезпечних діянь у сфері комп'ютерних інформаційних технологій займались такі вчені, як-от: Ю.М. Коломієць та Г.М. Симонова [1], Ю.А. Лісік, М.В. Грайворонський [2], С.С. Чернявський, В.А. Некрасов, А.В. Титко [3] та ін. Окремі питання кіберзлочинності розглядали у своїх наукових працях українські вчені О.С. Бондаренко та Д.А. Рєпін [4], М.Ю. Яцишин [5], М.О. Кравцова, О.М. Литвинов [6], С.О. Гнатюк [7], а також такі зарубіжні дослідники: С. Вронка [8], О.Є. Акінбовал, Н.Е. Клінгельхофер, М.Ф. Зеріхун [9], Маскун, Ахмад, Насвар, Х. Ассідік, А. Сяфіра, М. Напанг, М. Хендрапаті [10], Г. Урбас [11] та багато інших.

Мета статті

Метою статті є визначення основних напрямів розвитку кіберзлочинності та тінізації економіки, а також з'ясування спільних проблем, які перешкоджають оперативно протидіяти, запобігти або навіть мінімізувати скоєння подібних злочинів.

Виклад основного матеріалу

Відмивання доходів, одержаних злочинним шляхом вимагає від злочинців оперативної та ефективної їх легалізації. Легалізація доходів, отриманих злочинним шляхом є досить глобальною проблемою, тому її потрібно вирішувати на міжнародному рівні для того, щоб спільними зусиллями досягти поставлених цілей. Наразі такі заходи проводяться, наприклад, міжнародними організаціями для боротьби з корупцією, організованою злочинністю, легалізацією незаконно отриманих коштів і прийняття міжнародних стандартів, нормативних і рекомендаційних документів в галузі протидії тіньовій економіці.

Завдання детінізації економіки України є актуальними в умовах сучасних геополітичних викликів, євроінтеграційних процесів. Окреслені напрями протидії тінізації економіки формують підґрунтя для подальшого розроблення комплексного плану детінізації економіки та бюджетної сфери. Детінізація економіки України вимагає здійснення досліджень, формування комплексної стратегії протидії у співпраці із зарубіжними партнерами, насамперед з метою використання їхнього позитивного досвіду в цій сфері [3].

Беручи до уваги статистичні дані Генеральної прокуратури України за період січень-жовтень 2019 року[1] було виявлено 5820 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, але водночас тільки 390 проваджень було закрито за ч. 1 п. 1, 2, 4, 6 ст. 284 КПК України[2].

Відповідно до відомостей щодо протидії легалізації доходів за 2018 рік, передбачених ст. 209 ККУ було встановлено суму легалізованих коштів і майна у розмірі 295 460 071 грн (не враховуючи кримінальних правопорушень, пов'язаних з приватизацією) і було накладено арешт на майно на суму 22 680 000 грн і 742 грн було вилучено[3]. Отже, стає цілком прозорим стан протидії легалізації доходів та кіберзлочинності в Україні.

Тому автори статті дотримуються думки, що кіберзлочинність відіграє досить впливову роль у тіньовій економіці. У сучасних умовах кіберзлочинність стає одним із найнебезпечніших суспільно-економічних явищ глобального характеру, яке турбує весь цивілізований світ. В Україні до певного часу економічні та правові науки особливо не переймалися дослідженнями проблем комп'ютерної злочинності. Воно й зрозуміло: рівень життя, соціально-економічного розвитку та комп'ютеризації ще років десять тому не давали приводу для занепокоєння. Однак сьогодні, коли, кількість споживачів Інтернету в нашій країні та по всьому світу збільшуються з кожною секундою, питання захисту інформаційних систем як у технологічному, так і в правовому аспекті є невідкладним.

Більш того, враховуючи специфіку кіберзлочинності – організатори та виконавці кіберзлочинних схем є переважно освіченими, технічно грамотними та підготовленими особами, відповідно методи, які вони використовують для легалізації отриманих коштів, можуть також бути досить складними та нетиповими [1].

На сучасному етапі існують такі спеціалізовані міжнародні угоди, які спрямовано на боротьбу з кіберзлочинами: Конвенція Ради Європи «Про кіберзлочинність» від 23.11.2001[4], спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону

[1]Єдиний звіт про кримінальні правопорушення по державі за січень-жовтень 2019 року. URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=113897&libid=100820&c=edit&_c=fo (дата звернення: 17.04.2021).

[2]Кримінальний процесуальний кодекс України від 13 квітня 2012 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 14.04.2021).

[3]Звіт про протидію легалізації доходів, одержаних злочинним шляхом за 12 місяці 2018 року. URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=113652&libid=100820&c=edit&_c=fo (дата звернення: 10.04.2021).

[4]Конвенція Ради Європи від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 11.04.2021).

(проект по створенню потенціалу та політики в галузі інформаційних технологій, регулювання і законодавчої бази для тихоокеанських острівних країн ICB4PAC від 26.11.2009[1]) тощо. Хоча ці угоди були направлені на окремі регіони світу, деякі з них вплинули і на своїх «сусідів», а також продемонстрували іншим країнам гідний приклад, який, на думку авторів статті, необхідно якомога швидше перейняти. У законодавстві України відсутній термін «кіберзлочинність», хоча 07.09.2005 ВРУ було ратифіковано Конвенцію «Про кіберзлочинність» від 23.11.2001[2], що демонструє певні починання у цій сфері.

Міжнародне співробітництво з іноземними країнами є одним із невідкладних засобів боротьби зі злочинністю, зокрема враховуючи й кіберзлочинність: починаючи від законодавчої бази, що буде правильно та більш масштабно регулювати відносини у сфері інформаційних технологій, закінчуючи співробітництвом відповідних органів, що пов'язані з кіберзлочинністю, оскільки основною метою детінізації економіки є суттєве зниження рівня тінізації, шляхом створення сприятливих умов для залучення тіньових капіталів, збільшення економічної спроможності, збільшення національного багатства держави та інших показників. Це зі свого боку призведе до приросту залучених іноземних інвестицій, і відповідно реалізації цих інвестицій на благо економічного життя держави. Реінвестування цих ресурсів у новостворювані сфери виробництва та соціальну інфраструктуру необхідне для покращення рівня життя населення, зміцнення економічної безпеки держави та збільшення приросту доходів до бюджету.

Практика міжнародного співробітництва досить широко застосовується в Україні, у вигляді двосторонніх угод: Договір між Україною і Республікою Польща про правову допомогу та правові відносини у цивільних і кримінальних справах[3]; Договір між Україною та Канадою про взаємодопомогу у кримінальних справах[4], а також багатосторонніх договорів: Конвенція про правову допомогу і правові відносини в цивільних, сімейних і кримінальних справах[5]; Конвенція Ради Європи про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, та про фінансування тероризму[6]; Кримінальна конвенція про боротьбу з корупцією[7], а також відомчих договорів, що укладені Генеральною прокуратурою України: Угода про правову допомогу та співробітництво між Генеральною прокуратурою України і Генеральною прокуратурою Литовської Республіки[8]; Меморандум про співробітництво між Генеральною прокуратурою України і Прокуратурою Республіки Болгарія[9]. Проте, незважаючи на актуальність сфери кіберзлочинності та кіберлегалізації доходів, це питання майже не обговорюється [12].

Методи, які використовуються злочинцями у процесі відмивання доходів, одержаних у сфері кіберзлочинності, є досить різноманітними:

– використання чужих рахунків, реквізити яких були викрадені або втрачені;

– залучення «дропів» – це особи, які є безпосередніми помічниками у вчиненні злочину, у такий спосіб як зняття готівки з різних банкоматів, оскільки готівкові кошти майже неможливо відслідкувати (поза межами платіжних, банківських систем) або переказ коштів між рахунками, що дозволяє заплутати ланцюг переказів, і в такий спосіб залишитися непокараним.

– як правило, цей ланцюг переривається використанням готівкових операцій згаданим вище способом, після якого можливе використання традиційної платіжної системи, якщо в ній інтегровані онлайн-платежі або інші онлайн-послуги, тоді гроші можуть бути швидко переведені в електронні, а

[1]Проект по створенню потенціалу та політики в галузі інформаційних технологій, регулювання і законодавчої бази для тихоокеанських острівних країн (ICB4PAC) від 26 листопада 2009 р. URL: https://mjcs.gov.vu/images/2015_DWA/Child_Desk/ICB4PAC_Vanuatu_COP_Assessment_Final.pdf (дата звернення: 18.04.2021).

[2]Конвенція Ради Європи від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 11.04.2021).

[3]Договір між Україною і Республікою Польща про правову допомогу та правові відносини у цивільних і кримінальних справах від 24 травня 1993 р. https://zakon.rada.gov.ua/laws/show/616_174#Text (дата звернення: 18.04.2021).

[4]Договір між Україною та Канадою про взаємодопомогу у кримінальних справах від 23 вересня 1996 р. URL: https://zakon.rada.gov.ua/laws/show/124_003#Text (дата звернення: 20.04.2021).

[5]Конвенція про правову допомогу і правові відносини у цивільних, сімейних і кримінальних справах від 10 листопада 1994 р. URL: https://zakon.rada.gov.ua/laws/show/997_009#Text (дата звернення: 25.04.2021).

[6]Конвенція Ради Європи про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, та про фінансування тероризму. URL: https://zakon.rada.gov.ua/laws/show/994_948#Text (дата звернення: 20.04.2021).

[7]Кримінальна конвенція про боротьбу з корупцією (ETS 173) від 27 січня 1999 р. URL: https://zakon.rada.gov.ua/laws/show/994_101#Text (дата звернення: 22.04.2021).

[8]Угода про правову допомогу та співробітництво між Генеральною прокуратурою України і Генеральною прокуратурою Литовської Республіки від 08 грудня 1992 р. URL: https://zakon.rada.gov.ua/laws/show/440_008#Text (дата звернення: 19.04.2021).

[9]Меморандум про співробітництво між Генеральною прокуратурою України і Прокуратурою Республіки Болгарія від 1 червня 2001 р. URL: https://old.gp.gov.ua/ua/file_downloader.html?_m=fslib&_t=fsfile&_c=download&file_id=84334 (дата звернення: 20.04.2021).

згодом їх можна практично анонімно перевести на рахунок іноземної держави.

– купівля електронних грошей, криптовалюти, що ускладнить розслідування подібних злочинів;

– використання платіжних онлайн-систем та електронних гаманців;

– використання доходів, отриманих за допомогою кіберзлочинності, шляхом придбання різноманітних товарів або послуг для подальшого їх збуту й отримання готівки (оплата послуг у мережі Інтернет, товарів в інтернет-магазинах, надання або повернення фінансових позик, купівля комп'ютерних ігор, програмного забезпечення тощо).

Частина доходів, здобутих злочинним шляхом, використовується для придбання нового обладнання та розробки більш ефективних вірусних програм для обходу безпеки.

Характерними ознаками таких видів злочину є:

I. Анонімність (електронний гаманець можна створити лише за допомогою електронної пошти або номеру телефону, що дає можливість створити безліч таких гаманців, і при цьому буде складно ідентифікувати злочинця).

II. Простота вчинення злочину (дистанційне вчинення злочинного діяння, цілодобова доступність до електронних платіжних систем).

III. Рентабельність (кіберлегалізація доходів є безперечно дуже вигідним і прибутковим злочином, що є однією з причин його популярності).

IV. Відсутність ефективного запобігання та протидії кіберзлочинності (невизначеність поняття «кіберзлочин» у законодавстві України, що, як наслідок, виключає постійне та дієве регулювання цієї сфери) [4].

V. Стає цілком зрозуміло, що подібний розвиток інформаційних технологій тягне за собою й швидкий розвиток кіберзлочинності, тому потрібно удосконалити методи попередження та протидії економічній злочинності у кіберпросторі. Ефективна протидія кіберзлочинності має пов'язувати у собі сукупність законодавчих, організаційних, технічних та інформаційних заходів. Наразі в Україні залишаються невирішеними багато питань у галузі протидії кіберзлочинності. По-перше, це відсутність офіційного визначення терміну «кіберзлочинність». На думку авторів, вирішення цієї проблеми надасть значний поштовх до попередження та запобігання легалізації доходів, отриманих завдяки кіберзлочинності. Удосконалення методів забезпечення у сфері протидії та попередження легалізації прибутків, пов'язаних зі злочинністю у кіберпросторі, можливе за допомогою такого:

– внесення змін до Кримінального кодексу України щодо запровадження нових статей, які пов'язані саме з кібер-легалізацією доходів, та кіберзлочинністю в цілому (створити нову статтю, взявши за основу 2 статті: 209, 361 ККУ «Кіберлегалізація доходів», оскільки відмивання коштів здійснюється за допомогою електронно-обчислюваних машин (комп'ютерів), автоматизованих систем тощо).

– визнання комп'ютерних та цифрових даних у якості доказів задля оперативного розслідування кіберзлочинів;

– більш масштабне впровадження електронно-цифрового підпису, що позитивно вплине на захист коштів, цінної інформації (оскільки такий спосіб дасть змогу ідентифікувати підписувача і в разі неправомірних діянь, запобігти та протидіяти їм).

По-друге, банківськими установами мають бути впровадженні певні запобіжники, коли виникає певні сумнівні фінансові транзакції, з метою запобігання злочинним діянням:

– повідомлення клієнтів про кожну транзакцію, що була проведена з його рахунком;

– здійснення обов'язкової двофакторної автентифікації, що буде слугувати як додатковий рівень захисту, який гарантує, що доступ до вашої електронної, банківської інформації маєте тільки ви;

– введення «чорного списку» рахунків (IP-адрес) шахраїв для автоматичного блокування операцій;

– спроба входу до платіжної системи, або до рахунку за допомогою старих паролів, ключів, пін-кодів;

– спроба входу з нового IP-адресу на сайт банку або електронної платіжної системи, наприклад іншої країни тощо;

– значна кількість переказувань коштів протягом невеликого проміжку часу;

– здійснення операцій за втраченими документами осіб або їх платіжних реквізитів, що є найбільш поширеним на сьогодні;

– надходження грошових потоків на рахунки фізичних осіб із наступним зняттям через банкомати в день їх зарахування;

– міжнародні перекази, що отримуються з-за кордону або відправляються за кордон;

– іноді злочинці можуть вказувати досить сумнівні призначення платежу, зазвичай, при зарахуванні коштів з-за кордону, наприклад, виграш в казино, продаж веб-сайтів або Інтернет-магазинів тощо[1].

Висновки

На основі викладеного вище матеріалу можна прийти висновку, що кіберзлочинність є новітньою формою суспільно-небезпечних діянь, що несе великі загрози, але, на відміну від звичайних крадіжок і шахрайства, вона постійно вдосконалюється разом з технологіями, що, зі свого боку, ускладнює попередження та протидію незаконним діям. Рівень кібербезпеки в Україні не на високому рівні, а тому автори статті впевнені, що нехтувати такою важливою складовою як інтернет-простір не потрібно,

[1]Звіт про протидію легалізації доходів, одержаних злочинним шляхом за 12 місяці 2018 року. URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=113652&libid=100820&c=edit&_c=fo (дата звернення: 10.04.2021).

оскільки в передових країнах світу цей напрям є пріоритетним у внутрішній і зовнішній політиці країни. Але комплексна боротьба з цією проблемою вимагає спільних зусиль держави, громадян, міжнародного співробітництва та відповідного дієвого законодавства.

Список використаних джерел

[1] Коломієць Ю.М., Симонова Г.М. Легалізація доходів, одержаних у сфері кіберзлочинності. *Кібербезпека в Україні: правові та організаційні питання:* матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 17 листопада 2017 р.). Одеса: Одеський державний університет внутрішніх справ, 2017. С. 100–101.

[2] Лісік Ю.А., Грайворонський М.В. Архітектура аналітичної системи для виявлення шахрайських транзакцій. *XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»* (м. Київ, 25-27 травня 2017 р.). Київ: ВПІ ВПК «ПОЛІТЕХНІКА», 2017. С. 151–154.

[3] Тіньова економіка в Україні: стан, тенденції, шляхи подолання: аналіт. огляд / [упоряд.: С.С. Чернявський, В.А. Некрасов, А.В. Титко та ін.]. Київ: Національна академія внутрішніх справ, 2017. 152 с.

[4] Бондаренко О.С., Рєпін Д.А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право.* 2018. № 1. С. 246–248.

[5] Яцишин М.Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права.* 2018. № 53(5). С. 92-99. doi: 10.5281/zenodo.2009191.

[6] Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні. Харків: Панов, 2016. 210 с.

[7] Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації.* 2013. Т. 19, № 2. С. 118–129.

[8] Wronka C. "Cyber-laundering": The change of money laundering in the digital age. *Journal of Money Laundering Control*. 2021. doi: 10.1108/JMLC-04-2021-0035.

[9] Akinbowale O.E., Klingelhöfer H.E., Zerihun M.F. Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*. 2020. No. 27(3). P. 945–958.

[10] Maskun, Achmad, Naswar, Assidiq H., Syafira A., Napang, M., & Hendrapati, M. Qualifying cyber crime as a crime of aggression in international law. *Journal of East Asia and International Law*. 2020. Vol. 13, No. 2. P. 397–418. doi: 10.14330/jeail.2020.13.2.08.

[11] Urbas G. Legal perspectives on cybercrime. In *Research Handbook on Transnational Crime* (pp. 316–326). London: Edward Elgar Publishing Ltd, 2019. 544 p.

[12] Маланчук П.М., Кандиба Ю.О. Міжнародне співробітництво під час кримінального провадження. *Правові горизонти.* 2017. № 3(16). С. 71–76.

References

[1] Kolomiets, Y.M., & Simonova, G.M. (2017). Legalization of proceeds from cybercrime. In *Cybersecurity in Ukraine: Legal and organizational issues: Materials of the All-Ukrainian scientific-practical conference* (pp. 100-101). Odesa: Odessa State University of Internal Affairs.

[2] Lisik, Y.A., & Graivoronsky, M.V. (2017). Analytical system architecture for fraudulent transaction detection. In *Theoretical and applied problems of physics, mathematics and computer science: XV All-Ukrainian scientific-practical conference of students, graduate students and young scientists* (pp. 151-154). Kyiv: VPI VPK «POLYTECHNICS».

[3] Chernyavskyi, S.S., Nekrasov, V.A., & Tytko, A.V. (2017). *Shadow economy in Ukraine: State, trends, ways of overcome: Analytical review.* Kyiv: National Academy of Internal Affairs.

[4] Bondarenko, O.S., & Repin, D.A. (2018). Cybercrime in Ukraine: Causes, signs and countermeasures. *Comparative and Analytical Law*, 1, 246-248.

[5] Yatsyshyn, M.Y. (2018). Criminalization of cybercrime in international law: Comparative analysis. *Forum Prava*, 53(5), 92-99. doi: 10.5281/zenodo.2009191.

[6] Kravtsova, M.O., & Litvinov, O.M. (2016). *Prevention of cybercrime in Ukraine.* Kharkiv: Panov.

[7] Gnatyuk, S.O. (2013). Cyberterrorism: Development history, current trends & countermeasures. *Ukrainian Scientific Journal of Information Security*, 19(2), 118-129.

[8] Wronka, C. (2021). "Cyber-laundering": The change of money laundering in the digital age. *Journal of Money Laundering Control*. doi: 10.1108/JMLC-04-2021-0035.

[9] Akinbowale, O.E., Klingelhöfer, H.E., & Zerihun, M.F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, 27(3), 945-958.

[10] Maskun, Achmad, Naswar, Assidiq, H., Syafira, A., Napang, M., & Hendrapati, M. (2020). Qualifying cyber crime as a crime of aggression in international law. *Journal of East Asia and International Law,* 13(2), 397-418. doi: 10.14330/jeail.2020.13.2.08

[11] Urbas, G. (2019). Legal perspectives on cybercrime. In *Research Handbook on Transnational Crime* (pp. 316-326). London: Edward Elgar Publishing Ltd.

[12] Malanchuk, P.M., & Kandyba, Yu.O. (2017). International cooperation during criminal proceeding. *Legal Horizons*, 3(16), 71-76.