

ISSN 2307-5740
DOI: 10.31891/2307-5740

Науковий журнал

ВІСНИК

**Хмельницького
національного
університету**

Економічні науки

2019, № 6, Том 2

Scientific journal

HERALD

of Khmelnytskyi National University

Economic sciences

2019, Issue 6, Part 2

Хмельницький 2020

ВІСНИК
Хмельницького національного університету

Затверджений як фахове видання (перереєстрація), група «Б»
Наказ МОН 28.12.2019 №1643

Засновано в липні 1997 р.

Виходить 6 разів на рік

Хмельницький, 2019, № 6, Том 2 (276)

**Засновник і видавець: Хмельницький національний університет
(до 2005 р. — Технологічний університет Поділля, м. Хмельницький)**

Наукова бібліотека України ім. В.І. Вернадського http://nbuv.gov.ua/j-tit/Vchnu_ekon

Журнал включено до наукометричних баз:

Index Copernicus <http://jml2012.indexcopernicus.com/i++++i+++p4539,3.html>
Google Scholar <http://scholar.google.com.ua/citations?hl=uk&user=nDupjDAAAAAJ>
РИНЦ http://elibrary.ru/title_about.asp?id=37652

Головний редактор **Войнарченко М. П.**, д. е. н., професор, заслужений діяч науки і техніки України, член-кореспондент Національної академії наук України, проректор з науково-педагогічної та наукової роботи, перший проректор Хмельницького національного університету

Заступник головного редактора. **Нижник В. М.**, д. е. н., професор, заслужений діяч науки і техніки України, проректор з науково-педагогічної роботи
Голова редакційної колегії
серії «Економічні науки» **Хмельницького національного університету**

Відповідальний секретар **Кравчик Ю. В.**, к. е. н., начальник відділу інтелектуальної власності та трансферу технологій Хмельницького національного університету

Ч л е н и р е д к о л е г і ї с е р і ї « Е к о н о м і ч н і н а у к и »

Войнарченко М. П., д. е. н.; **Альошин О. Б.**, д. е. н.; **Асаул А. М.**, д. е. н. (Російська Федерація); **Васильківський Д. М.**, д. е. н.; **Вівчар О. І.**, д. е. н.; **Ведерников М. Д.**, д. е. н.; **Вишковська Зофія**, д. е. н. (Польща); **Геєць В. М.**, д. е. н.; **Гончар О. І.**, д. е. н.; **Григорук П. М.**, д. е. н.; **Джалагонія Давід**, проф. (Грузія); **Диха М. В.**, д. е. н.; **Дудко В. М.**, д. е. н. (Російська Федерація); **Журба І. Є.**, д. е. н.; **Завгородня Т. П.**, д. е. н.; **Замазій О. В.**, д. е. н.; **Євдокимов В. В.**, д. е. н.; **Йохна М. А.**, д. е. н.; **Кравчик Ю. В.**, к. е. н.; **Ковальчук С. В.**, д. е. н.; **Кулинич Р. О.**, д. е. н.; **Лук'янова В. В.**, д. е. н.; **Ляшенко О. М.**, д. е. н.; **Любохинець Л. С.**, к. е. н.; **Матюх С. А.**, к. е. н.; **Мікула Н. А.**, д. е. н.; **Микитенко В. В.**, д. е. н.; **Мороз О. В.**, д. е. н.; **Нижник В. М.**, д. е. н.; **Олуйко В. М.**, д. н. держ. упр.; **Орлов О. О.**, д. е. н.; **Рудніченко Є. М.**, д. е. н.; **Савіна Г. Г.**, д. е. н.; **Семикіна М. В.**, д. е. н.; **Скоробогата Л. В.**, к. е. н.; **Стадник В. В.**, д. е. н.; **Тельнов А. С.**, д. е. н.; **Ткаченко І. С.**, д. е. н.; **Троїковські Тадеуш**, к. е. н. (Польща); **Тюріна Н. М.**, к. е. н.; **Філіппова С. В.**, д. е. н.; **Хрущ Н. А.**, д. е. н.; **Церуйова Тетяна**, д. е. н. (Словакія); **Череп А. В.**, д. е. н.; **Чорна Л. О.**, д. е. н.

Технічний редактор **Кравчик Ю. В.**, к. е. н.
Редактор-коректор **Броженко В. О.**

Рекомендовано до друку рішенням Вченої ради Хмельницького національного університету,
протокол № 5 від 27.12.2019

Адреса редакції: **Україна, 29016, м. Хмельницький, вул. Інститутська, 11, Хмельницький національний університет редакція журналу "Вісник Хмельницького національного університету" (0382) 67-51-08**
e-mail: **visnyk.khnu@gmail.com**
web: **<http://journals.khnu.km.ua/vestnik>
http://lib.khnu.km.ua/visnyk_tup.htm**

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 9721 від 29 березня 2005 року (перереєстрація)

© Хмельницький національний університет, 2020
© Редакція журналу "Вісник Хмельницького національного університету", 2020

УДК 303.642.023: 004.056

DOI: 10.31891/2307-5740-2019-276-6(2)-253-259

ЗОЛКОВЕР А.О.

Київський національний університет технологій та дизайну

КУЗЬМЕНКО О. В., КУШНЕРЬОВ О. С., КОЙБІЧУК В.В.

Сумський державний університет

БІБЛІОМЕТРИЧНИЙ АНАЛІЗ ДОСЛІДЖЕНЬ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ЦИФРОВІЗАЦІЇ ФІНАНСОВОГО СЕКТОРУ ЕКОНОМІКИ ДЕРЖАВИ

Розвиток інформаційних технологій змінює всі усталені процеси функціонування як економіки в цілому, так і фінансового сектору зокрема. У той же час, цифровізація фінансового сектору створила сприятливі умови для розвитку кіберзлочинності, так здійснення фінансових злочинів перейшло з реального у віртуальний простір та зосередилось на викраданні інформації про банківські рахунки й банківські карти, зломи паролів, шахрайство з банкоматами та інше. У статті проведено бібліометричний аналіз наукових публікацій, присвячених проблемі кіберзлочинності в умовах цифровізації фінансового сектору економіки України. В результаті побудови графіків динаміки публікацій бази даних Scopus встановлено зростаючі тенденції публікативної активності науковців в сфері кіберзлочинності. Найвищу активність у вирішенні проблем пов'язаних з кіберзлочинами проявляють науковці США та Великобританії, як передових країн в сфері електронної комерції.

Ключові слова: бібліометричний аналіз, фінансовий сектор, кіберзлочини, інформаційні технології, Scopus.

ZOLKOVER A.

Kyiv National University of Technologies and Design

KUZMENKO O., KUSHNEROV O., KOIBICHUK V.

Sumy State University

BIBLIOMETRIC ANALYSIS OF CYBERCRIME RESEARCH IN THE CONTEXT OF DIGITALIZATION OF THE FINANCIAL SECTOR OF THE NATIONAL ECONOMY

The development of information technology changes the long-standing processes of functioning of both the economy in general and the financial sector in particular. Automation of business processes of financial institutions and digitalization of products of financial intermediaries create new conditions for the implementation of economic activities of all economic agents. Meanwhile, the digitalization of the financial sector has created favorable conditions for the development of cybercrime. Thus, financial crimes moved from the real to the virtual space and focused on the theft of information about bank accounts and bank cards, password cracking, ATM fraud, etc. The purpose of this article is to conduct a bibliometric analysis of scientific publications that deal with the issue of cybercrime in the context of digitalization of the financial sector of the Ukrainian economy. The research was carried out based on publications indexed in the Scopus database during the last 7 years. The plotting of the dynamics of publications in the Scopus database showed an increase in the general trend of publication activity in the field of cybercrime and the field of its interaction with the financial sector. The histogram of the geography of studies dealing with the issue of cybercrime in the context of digitalization of the financial sector of the economy showed the highest activity in solving the problem by scientists from the USA and Great Britain, which are leaders in the field of e-commerce. The bibliometric map of keywords of publications, built using the VOSviewer software, allowed identifying 7 clusters representing the areas of research: computer security, analysis of large databases, digital data storage, artificial intelligence, e-commerce, digital and mobile forensics. The results obtained can be used to identify the most potential areas for the spread of cybercrimes in the digital financial space, as well as tools to counter these types of crimes in Ukraine.

Keywords: bibliometric analysis, financial sector, cybercrime, information technology, Scopus.

Постановка проблеми. Випереджаючий розвиток інформаційних технологій в останні роки змусив суб'єктів ринку фінансових послуг кардинально змінити власну діяльність, максимально автоматизував бізнес-процеси та спрямував продаж послуг та продуктів у віртуальну площину. Все більше грошових платежів здійснюється у безготівковій формі за допомогою мобільного або Інтернет-банкінгу із будь-якого місця та у будь-який час. Це спричиняє активний розвиток Інтернет-торгівлі та розвитку інших віртуальних послуг. Окремо необхідно сказати про становлення електронних грошей, які ще більше розширюють можливість суб'єктів господарювання реалізовувати фінансові транзакції в кіберпростір.

В той же час, розвиток електронної комерції активізував новий вид шахрайства – кіберзлочини, які пов'язані з на викраданням інформації про банківські рахунки й банківські карти, зломи паролів, шахрайство з банкоматами та інше. Дані види злочинів призводять до значних втрат не тільки конкретних фінансових установ або клієнтів, але й економічній безпеці держави в цілому, оскільки отримані незаконно фінансові ресурси спрямовуються злочинцями на інші більш масштабні правопорушення.

Вище розглянута ситуація зумовлює необхідність у створенні ефективної системи кібрезахисту та інформаційної безпеки, що б дозволило захистити населення, суб'єктів господарювання та державу від значних фінансових, матеріальних та репутаційних втрат. Встановлена проблема, безумовно, заслуговує на увагу вітчизняних та закордонних науковців, що повинно реалізовуватись у численних наукових статтях та аналітичних звітах теоретико-методичного й практичного характеру. Проте розвиток даної тематики та її подальша формалізація у наукових працях повинна носити концептуальний, інтернаціональний та

високоякісний характер, про що може свідчити оприлюднення отриманих результатів у журналах, що індексуються міжнародними базами даних Scopus та Web of Science. Проте справедливо зауважити, що особливої практичної цінності набувають статті присвячені аналізу взаємозв'язку кіберзлочинності, фінансового сектора та економічної безпеки. Це пов'язано із тим, що наслідки кіберзлочинів синергетично поширюються на клієнтів фінансових установ, безпосередньо, фінансових посередників, а також державу в рамках акумулювання майбутніх загроз та недоотримання поточних відрахувань до бюджету. Саме тому дана стаття є актуальною, а визначена мета на часі.

Аналіз останніх досліджень і публікацій. Досліджуючи науковий доробок українських та закордонних науковців щодо кіберзлочинності та ролі інструментів протидії даним видам злочинів з метою забезпечення інформаційної й економічної безпеки держави зауважимо, що вітчизняні дослідники спочатку концентрували свою увагу на правовому визначенні категорії «кіберзлочинність» та його кримінологічній характеристиці [0, 0, 0, 0, 0, 0]. В останні роки (2018-2019 рр.) вітчизняні науковці почали розглядати економічні аспекти кіберзлочинів [0], механізм їх реалізації в цифровому просторі [0] та інструменти протидії даним видам правопорушень [0, 0, 0]. Закордонні науковці, в свою чергу, поряд з дослідженням загальних характеристик кіберзлочинів [0, 0, 0, 0] значну увагу приділяють й конкретним механізмам здійснення кіберзлочинів [0, 0], їх впливу на інформаційну безпеку країни [0], факторам, що стимулюють розвиток даного явища [0], особливостям прогнозування майбутнього розвитку кіберзлочинності [0], відношенням соціуму до даних видів правопорушень та їх обізнаності в цій проблематиці [0], а також можливостям захисту суспільства та економіки від кіберзлочинів [0].

Аналіз досліджень вітчизняних та закордонних науковців щодо досліджень кіберзлочинності в умовах цифровізації фінансового сектору економіки держави дозволяє зробити висновок про початковий етап наукового пошуку українських вчених відносно цього питання. Саме тому міжнародний досвід вирішення проблеми кіберзлочинності в сучасних умовах розвитку фінансового сектору є необхідним тригером майбутнього розвитку наукових напрямів в даній сфері.

Мета статті полягає у проведенні бібліометричного аналізу наукових публікацій міжнародної бази даних Scopus, присвячених дослідженню кіберзлочинності в умовах цифровізації фінансового сектору економіки держави.

Виклад основного матеріалу. Глобалізація фінансових ринків та інтернаціоналізація економічних відносин спричинили зменшення розривів між часом поширення новітніх розробок в різних країнах. Так, впровадження фінансових інновацій в центральному підрозділі глобальної компанії майже відразу поширюється на її структурні підрозділи. Ці явища спричиняють інтенсифікацію розвитку як позитивних, так і негативних процесів у фінансовому секторі національних економік. Паралельно з розвитком реальних фінансових процесів повинна розвиватись й наукова думка, а також практичні науково-методичні розробки в цій тематиці. Проте, наукові дослідження, так само як й інтернаціональні фінансові продукти, повинні носити міжнародний характер. Розвиток сучасної економічної науки неможливий в межах ізольованої території окремої країни. Виходячи з цього, основою бібліометричного аналізу виступила міжнародна база даних наукових публікацій Scopus. В нашому випадку, база даних Scopus дозволяє ідентифікувати різні вектори дослідження кіберзлочинності в умовах цифровізації фінансового сектору економіки держави.

Переходячи безпосередньо до результатів бібліометричного аналізу значимих наукових публікацій за 2012-2019 рр. було сформовано мапу взаємозв'язків поняття «кіберзлочинність» з іншими науковими категоріями. Інструментарієм реалізації даного етапу виступив VOSviewer. Це дозволило виділити 7 груп, які на рисунку узагальнені за допомогою бірюзового, фіолетового, червоного, сірого, блакитного, рожевого та коричневого кольорів (рисунок 1). Необхідно зазначити, що більшому розміру прямокутника відповідає більша частота згадування категорії, яка в ньому зазначена, як ключового поняття у взаємозв'язку з категорією «кіберзлочинність».

Проводячи більш детальний аналіз результатів змістовно-контекстуального блоку бібліометричного аналізу зауважимо, що основний масив наукових досліджень сконцентрований на ідентифікації взаємозв'язків між кіберзлочинністю та цифровою криміналістикою й протидією інформаційних злочинів (бірюзова група), мобільною криміналістикою (фіолетова група), штучним інтелектом й системами навчання (червона група), аналізом великих баз даних (синя група), електронною комерцією (сіра група), комп'ютерною безпекою й інтернетом (коричнева група), а також ж цифровим зберіганням даних (рожева група).

Між ідентифікованими групами є перетини, а саме: від ефективності організації процесу цифрової криміналістики збільшується рівень розкриття злочинів та обсяг доказової бази, а результативна система протидії інформаційним злочинам є дієвим превентивним інструментом даних видів злочинів. Штучний інтелект й аналіз великих баз даних є стимулом, як для ефективної боротьби з кіберзлочинами, оскільки допомагає правоохоронним органам у пошуку злочинців в мережі Інтернет, так й для злочинців, оскільки допомагає проаналізувати систему захисту різних внутрішніх систем установ та організацій. Інтернет – є ареалом діяльності кіберзлочинців, електронна комерція – є сферою реалізації кіберзлочинів, а цифрове зберігання даних основою для їх реалізації.

На основі розміру прямокутника, що описує рень впливовості явища у дослідженні аспектів кіберзлочинності засвідчив, що основоположними категоріями у дослідженні кіберзлочинності в умовах

рамки ідентифікації кіберзлочинців в Інтернеті, оскільки на початкових етапах необхідно було чітко зрозуміти, що саме трактувати, як кіберзлочини. На рубежі 2014–2017 рр. зацікавленість дослідників була прикута до цифрового зберігання даних та хмарних технологій, як новітніх технологій, як дали можливість кіберзлочинцям значно розширити можливості власної діяльності. У 2018–2019 рр. центральне місце починають займати системи навчання та алгоритмізація, як найбільш сучасні методи оптимізації бід-яких процесів діяльності населення.

Логічним продовженням часового бібліометричного аналізу досліджень з питань кіберзлочинності є його просторова складова (рис. 3). На основі даних зображених на рисунку 3, справедливо виділити сім основних світових центри дослідження наданої проблеми. Так, безумовно, країною лідером дослідження кіберзлочинності в умовах цифровізації фінансового сектору є США, не менш значимою державою є Великобританія, до якої в групу також поали Австрія, Італія, Норвегія, Україна. Іншими значно меншими групами країн є Австралія й Китай, Індія й Тайвань, Канада, Іспанія й Португалія, Індонезія, а також Південна Африка, Чилі й Швейцарія.

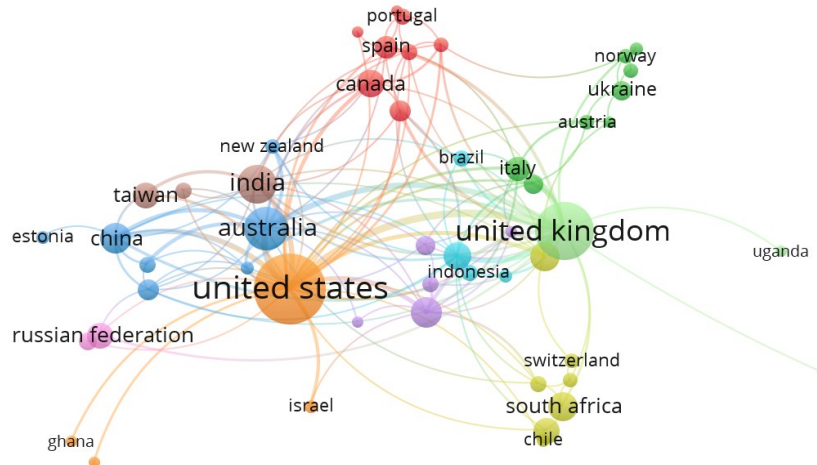


Рис. 3. Територіальне розгалуження наукової бібліографії поняття «cybercrime» (кіберзлочинність) за останні роки з застосуванням програми VOSViewerv.1.6.10

Одним з завершальних етапів бібліографічного аналізу є дослідження галузевої приналежності проаналізованих публікацій. Так, на основі рисунку 4, зазначимо, що переважна більшість наукових публікацій за тематикою кіберзлочинність зустрічається у комп'ютерних науках (30%) та у галузі соціальних наук (37,88%), практично така ж кількість емпіричних досліджень реалізована у сфері економіки, економетрики та фінансів (29,79%). Разом з тим, вагома частка публікацій з релевантною тематикою стосуються бізнесу, менеджменту та обліку (24%). Значний обсяг досліджень присвячених проблематиці кіберзлочинності спостерігається в інженерії (15%). Цікавий нам, економічний напрямок, акумулює в собі тільки 10% від усіх наукових досліджень присвячених кіберзлочинності. В усіх інших галузях частка наукових досліджень присвячених кіберзлочинності не перевищує 6%. В свою чергу необхідно зазначити, що досліджувана категорія є складною та багатогранною, що обумовлює наявність міждисциплінарного характеру її дослідження. Підтвердженням даної гіпотези є рисунок 4, де зображено перетин понять кіберзлочинності та фінансовий сектор.

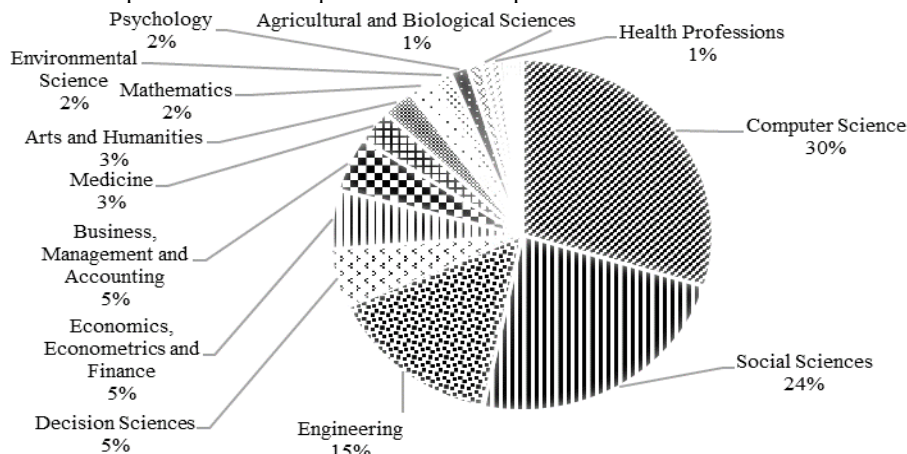


Рис. 4. Структурна галузевої приналежності наукових публікацій з питань «cybercrime» (кіберзлочинність) у базі даних Scopus за 2012-2019 рр.

7. Fighting against cybercrime : problems and prospects in Ukraine and the world / A. Borko, V. Nehodchenko, O. Volobuieva, I. Kharaberiush // *Business Laws and Legal Rights: Research and Practice*. – 2019. – Volume 22. – Special Issue 2. – P. 1–5.
8. Fishing as a cybercrime in the internet banking system: Economic and legal aspects / O. Ilchenko, V. Chumak, S. Kuzmenko, O. Shelukhin, A. Dobrovinskiy // *Journal of Legal, Ethical and Regulatory*. – 2019. – Issues, 22. – Special Issue 2. – 6 p.
9. Follert F. On the dealing with cybercriminals: economic considerations for a current problem / F. Follert // *List Forum fur Wirtschafts- und Finanzpolitik*. – 2019. – № 45 (1). – P. 27–33.
10. Jerome Orji U. An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states / U. Jerome Orji // *Computer Law and Security Review*. – 2019. – Volume 35 (6). – art. № 105330.
11. Mechanism of legal regulation of fight against cybercrime in Ukraine / Serkevych, I., Yevkhutych, I., Hazdayka-Vasylyshyn, I., Sozanskiy, T., Pasyeka, O. // *Journal of Legal, Ethical and Regulatory Issues*. – 2019. – № 22 (6). – P. 1–6.
12. Ozdamli F. Knowledge levels and attitudes toward cybercrimes of adolescents in Northern Cyprus / F. Ozdamli, E. Ercag // *TEM Journal*. – № 8 (4). – P. 1345–1350.
13. Park J. The economics of cybercrime: The role of broadband and socioeconomic status / J. Park, D. Cho, J. Lee, B. Lee // *ACM Transactions on Management Information Systems*. – 2019. – Volume 10 (4). – art. № 13.
14. Peculiarities of the legal control of cryptocurrency circulation in Ukraine / S. Drobyazko, R. Blahuta, V. Gurkovskiy, Y. Marchenko, L. Shevchenko // *Journal of Legal, Ethical and Regulatory Issues*. – 2019. – № 22 (6). – P. 1–6.
15. Vanni D. Are we any good at protecting our societies and economies from the threat of economic crime and misconduct? : A look at the Italian system / D. Vanni // *Journal of Financial Crime*. – 2019. – № 26 (4). – P. 1006–1013.
16. Yeoh P. Artificial intelligence: accelerator or panacea for financial crime? / P. Yeoh // *Journal of Financial Crime*. – 2019. – № 26 (2). – P. 634–646.
17. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінальноправове дослідження) : моногр. / Азаров Д. С. – К. : Атіка, 2007. – 304 с.
18. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» і «кіберзлочинність» / В. М. Бутузов // *Інформаційна безпека людини, суспільства, держави*. – 2010. – № 1(3). – С. 16-18.
19. Гвоздецька М. О. Кримінологічна характеристика кіберзлочинності: сучасний стан, структура та специфіка вивчення. Матеріали всеукраїнської науково-практичної конференції, м. Кропивницький, 23-25 листопада 2016 р. С. 52–53
20. Марков В. В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації / В. В. Марков // *Південноукраїнський правничий часопис*. – 2013. – № 1. – С. 112-115.
21. Никифорчук Д. Й. Характеристика кіберзлочинів, що вчиняються з метою отримання незаконних доходів / Д. Й. Никифорчук, Є. В. Лизогубенко // *9 Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.)*. – Донецьк : Донец. юрид. ін-т, 2013. – С. 43-45.
22. Шеломенцев В. П. Організована кіберзлочинність: до визначення поняття / В. П. Шеломенцев // *Боротьба з організ. злочинністю і корупцією (теорія і практика) : наук.-практ. журн. ; МНДЦ при РНБО України*. – 2009. – № 21. – С. 314–322.

References

1. A systematic approach toward description and classification of cyber crime incidents / G.C. Babu, A. S. Hanuman, J. S. Kiran, B. S. Babu // *International Journal of Recent Technology and Engineering*. 2019 – № 7 (6). – P. 1886–1889.
2. Actual situation of computer crime in the credit and financial sphere of Ukraine (modern aspects) / O. Kofanova, Y. Tereshchenko, R. Kutsyi, N. Morhun, O. Gushchyn // *Banks and Bank Systems*. – 2019. – № 14 (1). – P. 172–180.
3. Almazkyzy K. The essence and content of cybercrime in modern times / K. Almazkyzy, Y. N. Esteusizov // *Journal of Advanced Research in Law and Economics*. – 2018. – № 9 (3). – P. 834–841.
4. Broadhead S. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments / S. Broadhead // *Computer Law and Security Review*. 2018. – № 34 (6). – P. 1180–1196.
5. Corbet S., Gurdgiev C. What the hack: Systematic risk contagion from cyber events / S. Corbet, C. Gurdgiev // *International Review of Financial Analysis*. – 2019. – Volume 65. – art. № 101386.
6. Deepalakshmi R. Prediction of cybercrime by using euclidean voronoi on persons arrested under cybercrime / R. Deepalakshmi // *International Journal of Recent Technology and Engineering*. – 2019. – № 8 (3). – P. 8739–8741.
7. Fighting against cybercrime : problems and prospects in Ukraine and the world / A. Borko, V. Nehodchenko, O. Volobuieva, I. Kharaberiush // *Business Laws and Legal Rights: Research and Practice*. – 2019. – Volume 22. – Special Issue 2. – P. 1–5.
8. Fishing as a cybercrime in the internet banking system: Economic and legal aspects / O. Ilchenko, V. Chumak, S. Kuzmenko, O. Shelukhin, A. Dobrovinskiy // *Journal of Legal, Ethical and Regulatory*. – 2019. – Issues, 22. – Special Issue 2. – 6 p.
9. Follert F. On the dealing with cybercriminals: economic considerations for a current problem / F. Follert // *List Forum fur Wirtschafts- und Finanzpolitik*. – 2019. – № 45 (1). – P. 27–33.
10. Jerome Orji U. An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states / U. Jerome Orji // *Computer Law and Security Review*. – 2019. – Volume 35 (6). – art. № 105330.
11. Mechanism of legal regulation of fight against cybercrime in Ukraine / Serkevych, I., Yevkhutych, I., Hazdayka-Vasylyshyn, I., Sozanskiy, T., Pasyeka, O. // *Journal of Legal, Ethical and Regulatory Issues*. – 2019. – № 22 (6). – P. 1–6.

12. Ozdamli F. Knowledge levels and attitudes toward cybercrimes of adolescents in Northern Cyprus / F. Ozdamli, E. Ercag // TEM Journal. – № 8 (4). – P. 1345–1350.
13. Park J. The economics of cybercrime: The role of broadband and socioeconomic status / J. Park, D. Cho, J. Lee, B. Lee // ACM Transactions on Management Information Systems. – 2019. – Volume 10 (4). – art. № 13.
14. Peculiarities of the legal control of cryptocurrency circulation in Ukraine / S. Drobnyazko, R. Blahuta, V. Gurkovskiy, Y. Marchenko, L. Shevchenko // Journal of Legal, Ethical and Regulatory Issues. – 2019. – № 22 (6). – P. 1–6.
15. Vanni D. Are we any good at protecting our societies and economies from the threat of economic crime and misconduct? : A look at the Italian system / D. Vanni // Journal of Financial Crime. – 2019. – № 26 (4). – P. 1006–1013.
16. Yeoh P. Artificial intelligence: accelerator or panacea for financial crime? / P. Yeoh // Journal of Financial Crime. – 2019. – № 26 (2). – P. 634–646.
17. Azarov D. S. Zlochyny u sferi kompiuternoï informatsii (kryminalnopravove doslidzhennia) : monohr. / Azarov D. S. – K. : Atika, 2007. – 304 s.
18. Butuzov V. M. Spivvidnoshennia poniat «kompiuterna zlochynnist» i «kiberzlochynnist» / V. M. Butuzov // Informatsiina bezpeka liudyny, suspilstva, derzhavy. – 2010. – № 1(3). – S. 16-18.
19. Hvozdetzka M. O. Kryminolohichna kharakterystyka kiberzlochynnosti: suchasnyi stan, struktura ta spetsyfika vyvchennia. Materialy vseukrainskoi naukovo-praktychnoi konferentsii, m. Kropyvnytskyi, 23-25 lystopada 2016 r. S. 52–53
20. Markov V. V. Pro mekhanizmy skoiennia zlochyniv u kiberprostorii ta osoblyvosti yikh kvalifikatsii / V. V. Markov // Pivdenoukrainskyi pravnychi chasopys. – 2013. – № 1. – S. 112-115.
21. Nykyforchuk D. Y. Kharakterystyka kiberzlochyniv, shcho vchyniautsia z metoiu otrymannia nezakonnykh dokhodiv / D. Y. Nykyforchuk, Ye. V. Lyzohubenko // 9 Borotba z internet-zlochynnistiu : materialy mizhnar. nauk.-prakt. konf. (Donetsk, 12–13 cherv. 2013 r.). – Donetsk : Donets. yuryd. in-t, 2013. – S. 43-45.
22. Shelomentsev V. P. Orhanizovana kiberzlochynnist: do vyznachennia poniattia / V. P. Shelomentsev // Borotba z orhaniz. zlochynnistiu i koruptsiieiu (teoriia i praktyka) : nauk.-prakt. zhurn. ; MNDT pry RNBO Ukrainy. – 2009. – № 21. – S. 314–322.

Рецензія / Peer review: 11.10.2019

Надрукована / Printed: 02.01.2020