DOI: http://www.doi.org/10.21272/legalhorizons.2019.i16.p:55

АКТУАЛЬНІ ПИТАННЯ ЩОДО ПРОТИДІЇ КІБЕРЗАГРОЗАМ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ[2]

Мельник Вадим Іванович,
кандидат юридичних наук,
викладач кафедри адміністративного,
господарського права та фінансово-економічної безпеки,
Навчально-науковий інститут права,
Сумський державний університет

Кіяшко Юрій Михайлович,
викладач кафедри адміністративного,
господарського права та фінансово-економічної безпеки,
Навчально-науковий інститут права,
Сумський державний університет

Бондаренко Максим Олександрович,
Навчально-науковий інститут права,
Сумський державний університет

Стаття присвячена дослідженню проблематики визначення основних наявних загроз у кіберпросторі наслідки від дії яких негативно впливатимуть на прийнятне, із точки ефективності, функціонування фінансової складової економічної безпеки держави. А також питанню виявлення найбільш суттєвих недоліків нормативно-правового регулювання в окресленій сфері з метою пропонування шляхів їх ефективного вирішення.

За для забезпечення всебічності та повноти дослідження проаналізовано поняття «фінансова безпека» і «кіберзагроза», розглянуто характеристику видів останньої. З'ясовано, що фінансова безпека держави слугує основою для економічної безпеки країни та визначає реальні можливості останньої у питанні забезпечення інших видів безпеки. Встановлено та обґрунтовано, що, станом на сьогодення, кіберзагрози являють собою один із суттєвих і постійно еволюціонуючих деструктивних чинників, здатних дестабілізувати фінансову систему України. Зокрема, надведено ряд нещодавніх конкретних прикладів, коли національна фінансова система «потерпала» від наслідків дії кібер-атак (вірусні програми «Petya», «NotPetya», «WannaCry», протиправна діяльність угрупування «Carbanak» та ін.).

Наголошено, що для ефективної протидії цьому виду загроз має існувати сприятливе правове середовище, максимально адаптоване до сучасних реалій у кіберпросторі. Акцентовано увагу на необхідності своєчасної та адекватної реакції від законодавчого органу та інших

[2] Робота виконана в проекті 0118U003582

компетентних інституцій на появу таких нових протиправних діянь.

Проаналізовано існуюче чинне нормативно-правове забезпечення щодо протидії загрозам у кіберпросторі. Встановлено, що існуюче політико-правове становище, об'єктивно, не дозволяє говорити про ефективну протидію всім кіберзагрозам, та, відповідно, комплексне забезпечення фінансової складової економічної безпеки держави.

У цьому аспекті виявлено й розглянуто основні недоліки правого регулювання досліджуваної сфери відносин, а також запропоновано шляхи їх дієвого вирішення. Наголошено, що якнайскоріше врегулювання окреслених авторами проблемних питань сприятиме нормальному функціонуванню всіх структурних елементів фінансової безпеки України. Припущено, що це слугуватиме сталому економічному розвитку держави та забезпеченню соціально-економічного благополуччя її населення.

Ключові слова: фінансова безпека держави, економічна безпека держави, інтернет-мережа, кібератака, кібербезпека, кіберзлочинність, кіберпростір.

Melnik V. I., Kiiashko Yu. M., Bondarenko M. O. Topical issues of counteracting cyber threats in the context of ensuring financial security of the state. The article is devoted to the research of the problem of determining the main existing threats in cyberspace, which have a negative influence on the adoption, in terms of efficiency, of the functioning of the financial component of the economic security of the state. As well as refuting the identification of the most important shortcomings of regulatory regulation in certain areas in order to suggest ways to effectively address them.

For the purpose of ensuring the comprehensiveness and completeness of the research, the concepts of "financial security" and "cyber threats" have been analyzed, the characteristics of the latter are considered. It is revealed that financial security of the state serves as the basis for economic security of the country and determines the real possibilities of the latter in the issue of securing other types of security. It is established and grounded that, as of today, cyber threats represent one of the essential and constantly evolving destructive factors that can destabilize the financial system of Ukraine. In particular, a number of recent concrete examples were given when the national financial system "suffered" from the effects of cyber-attacks (viral programs "Petya", "NotPetya", "WannaCry", illegal activities of the "Carbanak" group, etc.).

It is stressed that in order to effectively counteract this kind of threats, there should be a favorable legal environment that is maximally adapted to the current realities in cyberspace. The emphasis is placed on the need for a timely and adequate response from the legislature and other competent institutions to the emergence of such new offenses.

The existing regulatory and legal framework for dealing with threats in cyberspace has been analyzed. It is established that the existing political and legal situation, objectively, does not allow speaking about effective counteraction to all cyber threats, and, accordingly, comprehensive provision of financial component of economic security of the state.

In this aspect, the main shortcomings of the right regulation of the studied sphere of relations were identified and considered, as well as the ways of their effective solution were proposed. It was emphasized that as soon as possible the resolution of the problem issues outlined by the authors would contribute to the normal functioning of all structural elements of Ukraine's financial security. It is supposed that it will serve the sustainable economic development of the state and ensure the social and economic well-being of its population.

Keywords: financial security of the state, economic security of the state, internet network, cyber attack, cyber security, cybercrime, cyber space.

Вступ. Обрання проєвропейського вектору розвитку держави вимагає існування сприятливої обстановки для функціонування національної економіки – одного з ключових факторів для успішного впровадження необхідних реформ. Передумовою для такого становища є належне функціонування всіх сфер і ланок фінансової безпеки держави – важливого елементу економічної безпеки України. З огляду на це важливим завданням держави є забезпечення фінансової безпеки, в тому числі шляхом дієвої протидії наявним та латентним загрозам.

Постановка проблеми. В умовах динамічного розвитку інформаційно-комунікаційних технологій (далі – ІКТ) та їх стрімкого впровадження у різні сфери фінансової діяльності держави виникає об'єктивна потреба в створенні дієвої системи захисту фінансової безпеки України у мережі Інтернет. Результати одного з нещодавніх експериментів, проведеного групою експертів із кібербезпеки продемонстрували фактичну уразливість перед кіберзагрозами значної кількості державних установ (підприємств), у тому числі й критично важливих об'єктів інфраструктури [1]. Безумовно, що об'єктом деструктивних кібер-діянь може стати й певна сфера публічної фінансової діяльності, внаслідок чого, потенційно, державі можуть бути завдані колосальні збитки та, ймовірно, виникне потреба в використанні коштів платників податків для усунення негативних наслідків та відновлення бажаного стану речей. У свою чергу це може суттєво позначитися на здатності забезпечення ефективного функціонування всіх сфер і ланок економічної системи та гальмуватиме її подальший розвиток.

Тому, не виникає сумніву, що існуючий стан правового забезпечення в окресленій сфері вимагає особливої уваги, зважаючи на постійне збільшення методів вчинення таких дій, транснаціоналізацію кіберзлочинності, а також необхідності слідування міжнародному трендові щодо уніфікації стандартів із протидії правопорушенням у кіберпросторі. Адже, нинішнє становище, в короткостроковій перспективі, неодмінно деструктивно вплине на прийнятне, із точки зору дотримання законності й ефективності, функціонування фінансової складової економічної безпеки держави. З огляду на все це стає очевидно, що, на сьогоднішній день, вказане питання є вкрай актуальним і потребує вивчення та змістовного дослідження.

Аналіз останніх досліджень і публікацій. Різні аспекти питання щодо протидії кіберзагрозам були об'єктом наукового інтересу таких дослідників, як І. В. Березовської, І. В. Діордіци, А. Г. Волова, Д. В. Дубова, О. В. Кубишкіна, О. В. Логінова В. Ю. Лук'янчикова, Р. В. Лук'янчука, О. В. Манжай, Ю. Є. Максименка, А. В. Мовчан, М. А. Ожевана, Ю. Ю. Орлова, В. В. Петрова, А. Л. Татузова, В. В. Шемчука та ін. Вплив кіберзагроз на різні економічні відносини, зокрема й фінансові аналізувалися багатьма науковцями. Серед яких доцільно виокремити окремі публікації О. В. Гайдука, В. О. Голубєва, С. В. Кавуна, О. В. Ставицького, І. В. Чекунова, А. Ю Шинкаренка й ін. У той же час питання щодо протидії кіберзагрозам залишається дискусійним і потребує окремої уваги.

Постановка завдання. За результатами аналізу наявного нормативно-правового забезпечення тих відносин у кіберпросторі наслідки від яких можуть впливати на певну сферу фінансової діяльності держави з'ясувати проблемні питання та запропонувати шляхи їх ефективного вирішення.

Виклад основного матеріалу. У відповідності до п. 5 Методичних рекомендацій щодо розрахунку рівня економічної безпеки України, затвердженої наказом Міністерства економічного розвитку і торгівлі України від 29.10.2013 № 1277 [2] фінансова безпека являє собою стан фінансової системи країни, за якого створюються необхідні фінансові умови для стабільного соціально-економічного розвитку країни, забезпечується її стійкість до фінансових шоків та дисбалансів, створюються умови для збереження цілісності та єдності фінансової системи країни [2]. Вона є елементом економічної безпеки [2] і відграє особливу роль щодо питання її ефективного функціонування. При цьому, сама економічна безпека, на думку І. І. Яремко, «… є матеріальною основою національної суверенності, що визначає реальні можливості у забезпеченні інших видів безпеки. Тобто економічна безпека – це підґрунтя для функціонування всіх інших її елементів, що входять у цю систему (військової, технічної, продовольчої, екологічної)» [3, с. 75]. Тому, очевидно, що існування комплексу сприятливих умов для належного функціонування фінансової безпеки держави є одним із ключових факторів для існування та стабільного розвитку держави, здатної ефективно провадити економічну політику у відповідності до інтересів українського народу. Адже, дієва та оперативна протидія як латентним, так і явним всім її загрозам – запорука економічної стабільності в державі.

Безпосередньо акцентуючи увагу на питанні щодо протидії загрозам у кіберпросторі вважаємо за доцільне, для повноти й всебічності дослідження, звернути увагу на сутність поняття «кіберзагроза» за для чіткого усвідомлення значення такої дефініції і відмежування від інших її подібних. У цьому аспекті доцільно зазначити, що вказаний термін знайшов власне відображення у національній правовій площині. Так, відповідно до ч. 6 ст. 1 ЗУ «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [4] кіберзагрозою вважаються наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [4]. Як бачимо законодавець визнав, що вказана проблема є вкрай важливою для України та, відповідно, поступово формує правовий інструментарій для

виявлення й реальної протидії цьому різновиду загроз. У той же час варто розуміти, що досліджувана сфера є однією з найменливіших на сучасному етапі і вимагає своєчасної та адекватної реакції від законодавчого органу та інших компетентних інституцій.

Слід наголосити, що попри власну відносну, порівняно з більшістю інших загроз, новизну в наукових колах уже пропонуються диференціації їх видів. Наприклад, М. В. Грайворонський стверджує, що кіберзагрози варто поділяти на такі види: 1) таргетовані атаки. В залежності від цілей, можна виділити дві протилежні тактики атак на комп'ютерні системи. Перший варіант – застосувати для атаки програмне забезпечення (вірус, троянський кінь), маючи на меті компрометацію якомога більшої кількості систем. Другий варіант – проводити атаку прицільно (звідки й назва «таргетовані», тобто націлені), для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів (як правило, посадових осіб високого рангу або їхніх помічників, науковців, взагалі людей, які мають справу з особливо цінною інформацією); 2) кібертероризм (вплив на системи керування). Те, що власне і називають кібертерроризмом – можливість впливу через комп'ютерну мережу (зокрема, Інтернет) на системи керування транспортом, промисловими об'єктами, будинками та будь-якими технологічними процесами. ІКТ надають терористам кілька інструментів: застосування комп'ютерних мереж для керування, координації дій і підготовки терактів; можливість терористам напряму звертатись до широкого кола людей, використовуючи сервіси сучасного Інтернету; потенційно будь-який технологічний процес, яким керує цифрова система керування (або SCADA), може стати об'єктом атаки кібертерористів; 3) кібервійни. Stuxnet – це є прообраз кіберзброї для ведення кібервійни, використовується для здійснення диверсій або відключення систем (наприклад, комплексів протиповітряної чи протиракетної оборони); 4) хактивізм. Зловживання інформацією у соціальних мережах (вплив на суспільство). Деякі хакерські угруповання ставлять за мету видобування конфіденційної (іноді таємної) інформації і розкриття її шляхом розміщення в Інтернет-мережі у вільному доступі. Як правило, йдеться про викриття таємних операцій, змов, корупції та інших дій на рівні урядів чи окремих політичних сил, які суперечать закону, принципам демократії й іншим загальнолюдським цінностям; 5) атаки на банківські системи (викрадення грошей). Чим ширше у банківській сфері застосовуються інформаційно-комунікаційні технології, тим більше можливостей для махінацій у цій сфері. Дуже поширеними є фішинг, викрадення і використання атрибутів платіжних карток, а також застосування дуже складного і досконалого шкідливого програмного забезпечення для втручання в роботу систем клієнт-банк; 6) атаки на електронний уряд. «Електронний уряд» – інформаційно-комунікаційна система, або об'єднання інформаційно-комунікаційних систем, що автоматизує інформаційну взаємодію органів державної влади та органів місцевого самоврядування з громадянами та суб'єктами господарювання із метою підвищення ефективності надання державних послуг. Атаки на електронний уряд можуть зашкодити функціонуванню такої системи, а у країнах з низьким рівнем впровадження ІКТ – підірвати довіру до демократичних перетворень і технічного прогресу; 7) апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання [5, с. 17]. Зважаючи на такий широкий спектр загроз у кіберпросторі, а також об'єкти їх руйнівного впливу вкотре доводиться той факт, що імовірні наслідки від здійснення цих протиправних дій можуть суттєво негативно відобразитися на нормальному функціонуванні фінансової безпеки України.

Необхідно вказати, що за даними «Kaspersky Lab», 90% від усіх кібератак припадає на масові загрози, зазвичай вони ефективно блокуються антивірусними сервісами. 9,9% складають цільові атаки. З цього відсоткового співвідношення лише 0,1% становить новація нашого століття – кібер-зброя [6]. Проте результати від її вмілого використання, як відомо, мають негативні наслідки для всіх країн.

Із приводу здійснення масових та відчутних для економіки держави кібератак на юридичних осіб і громадян, на території України потрібно відзначити такі дії, що розпочалися 14 квітня 2017 року, причиною яких стало оновлення програми «M.E.Doc» [7], що використовувалась у більшості установ та організацій для подання звітності або обміну внутрішньої кореспонденції [8]. Під цієї час процедури виник «бекдор», тобто можливість віддаленого доступу до комп'ютеру в обхід підтвердження особи-власника (автентифікації) [9]. Цей, так званий «бекдор» залишився поза увагою відповідальних осіб, які мали б виправити помилки програми. Тож ним скористалися кіберзлочинці для досягнення власних протиправних цілей.

Також серед нещодавніх значимих кібератак доцільно виділити поширення вірусу «WannaCry», протиправного діяння, вчиненого 12 травня 2017 року [10], який вражав операційні системи

Microsoft Windows внаслідок шифрування файлів [11]. В результаті здійснення якого у Великобританії почалися перебої в функціонуванні системи охорони здоров'я, у ФРН це негативно відобразилося на роботі залізничної компанії «Deutsche Bahn». Дія цієї загрози також позначилася на діяльності різних організацій, зокрема таких як міжнародна служба доставки «FedEx Corporation», телекомунікаційна компанія «Telefonica SA», в Іспанії, «Altice Portugal», в Португалії та багатьох інших [12]. Внаслідок дії цього вірусу ставалися перебої в роботі юридичних осіб-резидентів України.

Безумовно, що в такому контексті не можливо не звернути увагу й на наслідки дії так званого вірусу «Petya», який згодом еволюціонував у «NotPetya». Як повідомляє «The Talos Blog», близько 80% українських підприємств постраждали від зазначеної хакерської атаки [13], що була визнана Адміністрацією Президента США найбільшою в історії [14].

Вказана атака була цілеспрямована, зокрема й на дестабілізацію роботи інформаційних систем багатьох значимих об'єктів державної та приватної форм власності. Зокрема, мова йде про Національний банк України, Міністерство внутрішніх справ України, Секретаріат Кабінету міністрів, Державну фіскальну службу України, «Нову пошту», «Укртелеком», «Ощадбанк», «Київенерго», «WOG», «Київстар», «Епіцентр» та багато інших [15]. Також ця кібератака вразила й роботу сайту Чорнобильської атомної електростанції, внаслідок чого певний час повноцінно не працювали системи радіаційного моніторингу [16]. За виняткових обставин, таке становище могло призвести до необхідності виділення значних фінансових витрат з державного бюджету. В цілому ж у результаті здійснення цих атак, за підрахунками організації «Громадянська кібероборона», сумарні збитки сягнули біля 10 млрд. грн [17].

Також не доцільно оминати увагою питання кібератак здійснених на об'єкти критичної інфраструктури в Україні. До прикладу, напад хакерів на «Прикарпаттяобленерго» [18] можна вважати одним із перших випадків, коли за допомогою кібератаки на деякий час було припинено електропостачання.

Окрім масових таких атак, хакери подекуди реалізують свої злочинні амбіції через скімінг [19], тобто створення накладок на банкоматах, що зчитують дані пластикової картки клієнта банку. Так, «знявши» кошти в одному місці, згодом можна отримати смс-повідомлення про аналогічну фінансову операцію з того самого рахунку у іншому місці планети [20].

Серед цільових атак на фінансову систему країн, слід виділити діяльність організованого злочинного угрупування (далі – ОЗУ) «Carbanak» [21]. Внаслідок протиправних дій у кіберпросторі цього угрупування банківські системи багатьох держав, в тому числі й України, зазнали суттєвих фінансових збитків. Сума отриманих коштів, за повідомленням «The Bell» склала 1,2 млрд. дол. [22]. Безумовно, в фінансових системах практично усіх цих держав, у результаті вчинення такого виду протиправних дій виникали дисбаланси, що створювало перешкоди для їх бажаного функціонування.

Загалом же не виникає сумніву, що перешкоди в діяльності згаданих юридичних осіб, насамперед банківських, а також контролюючих установ негативно впливатимуть на нормальне функціонування фінансової складової економічної безпеки країни. Адже, нерідко виникатимуть передумови для появи різних фінансових ризиків що, безумовно, перешкоджатиме належній фінансовій діяльності держави.

Вочевидь, що для реальної протидії цим загрозам, як уже зазначалось, має існувати сприятливе правове середовище, адаптоване до сучасних реалій у кіберпросторі. Адже, як слушно зазначають М. М. Присяжнюк та Є. І. Цифра, «активність з боку провідних держав світу в кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах у кіберпросторі, обумовлюють необхідність вироблення рекомендацій щодо короткострокових та довгострокових пріоритетів трансформації вітчизняного безпекового сектора» [23, с. 65]. Доводиться констатувати, що вітчизняне нормативно-правове забезпечення цієї сфери, попри певні суттєві позитивні «зрушення» все ж вимагає постійної та особливої уваги. Це пояснюється частим виникненням і розвитком нових методів здійснення протиправних діянь в інтернет-мережі, а також вже хронічно запізнілим реагуванням національних компетентних інституцій у питанні розробки та активного впровадження нових ефективних механізмів протидії цим загрозам.

Сучасне правове забезпечення щодо протидії кіберзагрозам складають відповідні положення Конституції України від 28.06.1996 № 254к/96-ВР [24], Конвенція про кіберзлочинність від 23.11.2001 [25], ряд окремих норм Кримінального кодексу України від 05.04.2001 № 2341-III [26], закони України «Про національну безпеку України» від 21.06.2018 № 2469-VIII [27], «Про основні засади забезпечення кібербезпеки

України» від 05.10.2017 № 2163-VIII [4], Стратегія національної безпеки України затверджена Указом ПУ від 26.05.2015 № 287/2015 [28], Стратегія кібербезпеки України, затверджена Указом ПУ від 15.03.2016 № 96/2016 [29], Воєнна доктрина України, затверджена Указом ПУ від 24.09.2015 № 555/2015 [30] й ін. Слід також вказати, що важлива роль у цьому аспекті відводиться нормам іншого чинного законодавства, які наділять уповноважені державні органи компетенцією на реалізацію державної політики в аналізованій сфері.

Проте, варто зазначити, що дія перелічених нормативно-правових актів і їх дотримання не вирішує питання ефективної протидії всім кіберзагрозам, та, відповідно, комплексного забезпечення фінансової складової економічної безпеки держави. Тому, зупинимося на деяких проблемних питаннях із метою визначення недоліків правового регулювання у конкретній сфері відносин й, відповідно, пропонування шляхів їх вирішення.

Зокрема однією з багатьох важливих проблем, особливо в умовах активної транснаціоналізації кіберзлочинності залишається питання наявності різних підходів щодо правового врегулювання конкретних відносин у законодавчих базах різних держав. Попри декларування рекомендації в Конвенції про кіберзлочинність від 23.11.2001 [25] щодо першочергової необхідності спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, між іншим, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва [25] все ж правове регулювання тієї чи іншої держави різниться, що часто негативно впливає на ефективну протидію кіберзагрозам. Тому, констатуємо, що на сьогоднішній день у повній мірі не вирішене питання існування уніфікованих підходів стосовно правового врегулювання відносин в інтернет-мережі, як між державами-учасниками названого документу, так із іншими суб'єктами міжнародного права.

Наприклад, у ході розслідування вже згадуваної нами кібер-атаки «WannaCry» стало відомим, що суб'єктами цього злочину було угрупування, учасники якого перебували на території Корейської Народно-Демократичної Республіки [31]. Встановлена обставина унеможливила проведення слідчих дій та, відповідно, відносно імовірних правопорушників не були вжиті легально допустимі й обґрунтовані заходи державного примусу.

Тому, ми переконані, що вирішення вказаного питання має принципово важливе значення, оскільки уніфікація міжнародно-правових стандартів стосовно протидії кіберзагрозам надасть змогу ефективно запобігати цим діянням у майбутньому. Це, зокрема має реалізовуватися шляхом розробки та прийняття (затвердження) відповідних правових актів, проведення спільних тренінгів, операцій з виявлення і протидії кіберзлочинності, екстрадиції правопорушників, консультацій (обговорень) за участю науковців, фахівців, представників компетентних структур та інших форм міжнародного й міждержавного співробітництва. Тому, очевидно, що Україна як постійний учасник міжнародного діалогу має брати активну участь у різних спільних заходах, присвячених питанням протидії кіберзагрозам. Переконані, що це консолідує наявні зусилля під час виявляння та запобігання, насамперед транснаціональній кіберзлочинності.

Зосереджуючи увагу на основних проблемних аспектах вітчизняного нормативно-правового регулювання сфери кіберпростору слід зупинитися на такому питанні, як непоодинокі випадки неможливості встановлення осіб-правопорушників, які вчиняють протиправні дії в інтернет мережі. Нині, децентралізована структура кіберпростору дозволяє створювати інтернет-сайти з купівлі-продажу речей вилучених із цивільного обороту, або ж оборотоздатність яких обмежена. При цьому можуть виникати, згадані нами, ситуації, за яких, із точки зору законодавства однієї держави такі дії є правомірними, а з позиції вітчизняного – порушують ті чи інші норми. Так чи інакше мова йде про можливі випадки, за яких порушується санкціоновані державою вимоги. Безумовно, це становище може призвести до дестабілізації обстановки в державі, що негативно вплине на фінансову діяльність останньої.

З огляду на це складне питання та усвідомлення можливих наслідків від здійснення розглянутих протиправних діянь убачається за доцільне посилити міжнародну співпрацю, у частині активної протидії правопорушенням в інтернет-мережі. Важливим напрямом у межах такого співробітництва має стати консультування між компетентними органами з питань законодавчого регулювання відносин в цій сфері, а також активне впровадження новітніх методів протидії кіберзагрозам.

Слід також зазначити, що створення Департаменту кіберполіції в структурі Національної поліції України у 2015 році було позитивним кроком для ефективного вирішення питання щодо притягнення до кримінальної відповідальності в зазначених правопорушеннях. Так за 2018 рік, співробітниками Департаменту кіберполіції розслідувалося 11 131 кримінальне провадження, з яких 1 139 у сфері протиправного контенту, 3 607 у сфері електронної комерції, 3 697

у сфері платіжних систем, 2 688 у сфері кібербезпеки. Крім того, у 2018 році співробітниками департаменту кіберполіції було підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного секторів. Серед них – представники міжнародних кампаній у сфері інформаційної безпеки та ІТ-компанії, а також поліцією Австралії, Сінгапуру, Катару та ще ряду країн. Крім того, налагоджено ефективну взаємодію з найвідомішими світовими соціальними мережами [32].

Для забезпечення фінансової складової економічної безпеки важливим є не лише захист від зовнішніх атак, а й дієві методи оподаткування. Це, зокрема сприятиме ефективному функціонуванню однієї з її складових – безпеки податкової.

Варто наголосити, що специфіка інтернет-мережі та її особливе «місцезнаходження» є причиною появи складнощів з оподаткування, зокрема мова йде про відносини у сфері електронної комерції. Нині, в мережі існує багато сайтів-сервісів, що дозволяють створити свої онлайн-магазини [33] без належної реєстрації як суб'єкта господарської діяльності. Важливим є момент фактичної відсутності державних кордонів, тож міжнародний інтернет-магазин може провадити свою діяльність на території України при цьому відраховуючи податкові платежі до відповідного бюджету іншої держави, чи не сплачуючи їх взагалі.

На нашу думку вбачається за доцільне наділити компетенцією Державну податкову службу України щодо виявлення правопорушників у цій сфері. В подальшому такі відомості мають надаватися підрозділам податкової міліції, які уповноважені здійснювати досудове розслідування податкових злочинів. Також, за для успішної реалізації поставленої мети слід створити окремий підрозділ у структурі ДПС ключовим завданням якого має бути моніторинг злочинних дій та пошук сайтів-порушників податкового законодавства.

Для ефективної діяльності податкових структур в інтернет-середовищі, вважаємо за доцільне створити єдину базу даних, до якої будуть вноситися дані про сайти-правопорушники. Доступ до такої бази слід надати всім провідним державним інституціям, які мають протидіяти кіберзагрозам (Департаменту кіберполіції Національної поліції України, Державній службі спеціального зв'язку та захисту інформації України, Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, податковим структурам, Державній службі України з питань безпечності харчових продуктів та захисту споживачів та ін.). Ці суб'єкти здійснюючи моніторинг кіберпростору, відповідно до власних завдань та функцій повинні наповнювати єдину базу даних сайтів-правопорушників, що сприятиме дієвій протидії цьому виду загроз. Також у перспективі це сприятиме нормальному функціонуванню всіх структурних елементів фінансової безпеки України.

Висновки. За результатами проведеного дослідження слід відзначити, що в сучасних складних політичних, правових та економічних умовах, пов'язаних із активною інформатизацією всіх сфер правовідносин виникає об'єктивна потреба у створенні дієвої системи захисту фінансової безпеки держави в кіберпросторі. Адже, як показує практика наслідки від здійснення кібератак можуть нести певні реальні та суттєві ризики для нормального функціонування вітчизняної фінансової системи – базової передумови для економічного розвитку держави та соціально-економічного благополуччя її населення. Особливо гостро ця проблема постала перед Україною, яка при значній помітній фінансовій нестабільності стала об'єктом частих кібератак. Нинішнє нормативно-правове регулювання досліджуваної сфери залишається недосконалим і вимагає законодавчого реагування, що має сприяти належному функціонуванню фінансової складової економічної безпеки держави, створюючи додаткові передумови для її подальшого розвитку.

Література:

1. После Petya. С любого комьютера можно хакнуть пол-Украины. URL : https://tech.liga.net/technology/article/posle-petya-s-lyubogo-komyutera-mojno-haknut-pol-ukrainy.

2. Методичні рекомендації щодо розрахунку рівня економічної безпеки України : Наказ Міністерства економічного розвитку і торгівлі України від 29.10.2013 р. № 1277. URL : https://zakon.rada.gov.ua/rada/show/v1277731-13 (дата звернення: 28.05.2019).

3. Яремко І. І. Економічна безпека як складова національної безпеки держави. Інтегроване стратегічне управління: проблеми адміністрування, економічної безпеки та проектної діяльності : тези доповідей першої міжвузівської науково-практичної конференції, 24–26 квітня 2013 р., Львів, 2013. С. 74–75.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.05.2019).

5. Грайворонський, М. В. Сучасні підходи до забезпечення кібернетичної безпеки. Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». Київ, 2015. С. 10–17.

6. Mitnick K. Ghost in the Wires: My Adventures As the World's Most Wanted Hacker 2011. URL : https://www.amazon.com/Ghost-Wires-Adventures-Worlds-Wanted/dp/0316037729 (дата звернення: 28.05.2019).

7. Petya ransomware eats your hard drives. URL : https://www.kaspersky.com/blog/petya-ransomware/11715/ (дата звернення: 28.05.2019).

8. Ransom.Petya. URL : https://www.symantec.com/security-center/writeup/2016-032913-4222-99 (дата звернення: 28.05.2019).

9. Cherepanov A. Analysis of TeleBots' cunning backdoor. URL : https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ (дата звернення: 28.05.2019).

10. Масштабна хакерська атака вивела з ладу десятки тисяч комп'ютерів по всьому світу. URL : https://ua.112.ua/svit/masshtabna-khakerska-ataka-vyvela-z-ladu-desiatky-tysiach-kompiuteriv-po-vsomu-svitu-389508.html (дата звернення: 29.05.2019).

11. WannaCry ransomware that infected Telefonica and NHS hospitals is spreading aggressively, with over 50,000 attacks so far today. URL : https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today (дата звернення: 29.05.2019).

12. Глобальна кібер-атака: все, що слід знати про «найбільшу в історії програму-шантажиста». URL : https://zik.ua/news/2017/05/16/globalna_kiberataka_vse_shcho_slid_znaty_pro_naybilshu_1097119 (дата звернення: 29.05.2019).

13. The MeDoc Connection. URL : https://blog.talosintelligence.com/2017/07/the-medoc-connection.html (дата звернення: 29.05.2019).

14. Statement from the Press Secretary. URL : https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (дата звернення: 29.05.2019).

15. В Україні десятки компаній та установ атакував комп'ютерний вірус. URL : https://hromadske.ua/posts/ukrposhtu-ukrenerho-ta-banky-atakuvav-podibnyi-do-wannacry-virus (дата звернення: 29.05.2019).

16. Комп'ютерний вірус атакував ЧАЕС – не працює сайт станції. URL : https://hromadske.ua/posts/kompiuternyi-virus-atakuvav-chaes-ne-pratsiuiut-servera-ta-sait-stantsii (дата звернення: 29.05.2019).

17. Через атаку вірусу Petya Україна за півгодини втратила 10 млрд гривень – експерт. URL : https://ukr.segodnya.ua/economics/enews/iz-za-ataki-virusa-petya-ukraina-za-polchasa-poteryala-10-mlrd-griven-ekspert-1069181.html (дата звернення: 29.05.2019).

18. Хакери атакували українські обленерго. URL : https://techtoday.in.ua/news/xakeri-atakuvali-ukrayinski-oblenergo-56163.html (дата звернення: 29.05.2019).

19. Как защититься от скимминга:что нужно знать, чтобы не стать жертвой мошенников. URL : https://journal.tinkoff.ru/skimming/ (дата звернення: 30.05.2019).

20. Голованов В. Невидимые скиммеры: новое слово в мошенничестве с кредитками. URL : https://habr.com/ru/post/363839/ (дата звернення: 30.05.2019).

21. Катана из Аликанте. Как удалось раскрыть крупнейшее цифровое ограбление в истории. URL : https://thebell.io/katana-iz-alikante-kak-udalos-raskryt-krupnejshee-tsifrovoe-ograblenie-v-istorii/ (дата звернення: 30.05.2019).

22. Голованов В. Невидимые скиммеры: новое слово в мошенничестве с кредитками. URL : https://habr.com/ru/post/363839/ (дата звернення: 30.05.2019).

23. Присяжнюк М. М., Цифра Є. І. Особливості забезпечення кібербезпеки. Реєстрація, зберігання і обробка даних, 2017. Т. 19. № 2. С. 61–68.

24. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL : https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 30.05.2019).

25. Конвенція про кіберзлочинність : Міжнародний документ від 23.11.2001 р. URL : https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 30.05.2019).

26. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 30.05.2019).

27. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 30.05.2019).

28. Стратегія національної безпеки України : Указ Президента України від 26.05.2015 р. № 287/2015. URL : https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 30.05.2019).

29. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016. URL : https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 30.05.2019).

30. Воєнна доктрина України : Указ Президента України від 24.09.2015 р. № 555/2015. URL : https://zakon.rada.gov.ua/laws/show/555/2015 (дата звернення: 30.05.2019).

31. Lazarus Under The Hood/kaspersky.lab. URL : https://securelist.com/lazarus-under-the-hood/77908/ (дата звернення: 30.05.2019).

32. Підсумки 2018 року в цифрах. URL : https://cyberpolice.gov.ua/results/2018/ (дата звернення: 30.05.2019).

33. Wix: создай свой сайт бесплатно. URL : https://ru.wix.com/ (дата звернення: 30.05.2019).