Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2023. № 10.

DOI: http://doi.org/10.32702/2307-2105.2023.10.38
УДК 336.71

Є. Ю. Мордань,
к. е. н., доцент, доцент кафедри фінансових технологій і підприємництва,
Сумський державний університет, м. Суми
ORCID ID: https://orcid.org/0000-0002-3942-1262
В. В. Бардакова,
студентка кафедри фінансових технологій і підприємництва,
Сумський державний університет, м. Суми
ORCID ID: https://orcid.org/0009-0001-3367-8163
Л. В. Сокол,
студентка кафедри фінансових технологій і підприємництва,
Сумський державний університет, м. Суми
ORCID ID: https://orcid.org/0009-0000-9842-6752

УДОСКОНАЛЕННЯ ВІТЧИЗНЯНОЇ СИСТЕМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА КІБЕРШАХРАЙСТВУ НА ОСНОВІ ВПРОВАДЖЕННЯ МІЖНАРОДНОГО ДОСВІДУ

Ye. Mordan,
PhD in Economics, Associate Professor,
Senior Lecturer of the Department of Financial Technologies and Entrepreneurship, Sumy State University, Sumy
V. Bardakova,
Student of the Department of Financial Technologies and Entrepreneurship, Sumy State University, Sumy
L. Sokol,
Student of the Department of Financial Technologies and Entrepreneurship, Sumy State University, Sumy

IMPROVEMENT OF THE NATIONAL SYSTEM OF COMBATING CYBERCRIME AND CYBERFRAUD BASED ON THE IMPLEMENTATION OF INTERNATIONAL EXPERIENCE

На основі аналізу існуючих трактувань сутності поняття кіберзлочин сформоване його авторське визначення, під яким варто розуміти сукупність правопорушень, які вчиняються у віртуальному просторі з використанням комп'ютерних систем та мереж, а також інших технологічних засобів для отримання незаконного доступу до інформації, шахрайства, розповсюдження шкідливого програмного забезпечення та інших дій, що завдають збитків. Сформовано класифікацію кіберзлочинів залежно від мотивів їх вчинення. Визначено, що під час повномасштабної війни в Україні кількість кіберзлочинів значно зросла, особливо активізувалося платіжне шахрайство. Розглянуто вітчизняну систему протидії кіберзлочинам та кібершахрайству, яка базується на засадах виявлення, попередження та стримування. Визначено, що міжнародна співпраця та міжнародне право відіграють важливу роль у подоланні кіберзлочинності, яка має вже давно транснаціональний характер. Вивчено досвід провідних країн світу в боротьбі з кіберзлочинністю і можливість імплементації кращих практик в удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству. Запропоновано шляхи удосконалення цієї системи на основі міжнародного досвіду США та Франції.

On the basis of the analysis of existing interpretations of the essence of the concept of cybercrime, its author's definition was formed, which should be understood as a set of offenses committed in virtual space using computer systems and networks, as well as other technological means for obtaining illegal access to information, fraud, spreading harmful software and other damaging actions. A classification of cybercrimes has been formed depending on the motives for their commission (cyberfraud for the purpose of making money, cyberespionage, the distribution of malicious software, cyberterrorism, etc.). It was determined that during the full-scale war in Ukraine, the number of cybercrimes increased significantly, especially payment fraud. The domestic system of combating cybercrimes and cyberfraud is considered, which is based on the principles of

detection and prevention of cybercrimes, their deterrence and cyberresistance. It was determined that international cooperation and international law play an important role in overcoming cybercrime, which has long been transnational in nature. The experience of the world's leading countries in the fight against cybercrime and the possibility of implementing best practices in improving the domestic system of countering cybercrime and cyberfraud have been studied. Ways to improve this system are proposed based on the international experience of the USA and France. It is suggested that when building a national cyber defense system, it is worth taking into account the experience of the United States regarding the complex and cohesive interaction of various government structures, with a clear division of powers in the field of cyberspace protection, their cooperation with the private sector, the population and international partners, and the experience of France in establishing the requirement to authorize web authors -sites. It was determined that the current state of legal support for the fight against cybercrime in Ukraine needs to be improved by making changes and additions to a number of normative legal acts, taking into account international experience.

Ключові слова: *кібершахрайства, кіберзлочинність, міжнародний досвід, система протидії, кібербезпека, фішинг, правопорушення, кіберстійкість.*

Keywords: *cyberfraud, cybercrime, international experience, counteraction system, cybersecurity, phishing, offences, cyber resilience.*

Постановка проблеми у загальному вигляді та її зв’язок із важливими науковими чи практичними завданнями. В сучасних реаліях існування суспільства інформаційні технології створюють багато можливостей для його прогресивного розвитку в різних сферах життя. Окрім позитивних аспектів, інформаційні технології також провокують появу нових ризиків, пов’язаних із зростання та поширення кіберзлочинів та кібершахрайств. Кіберзлочинність є наслідком швидкого розвитку цифрових

технологій та поширення Інтернету. Сама природа Інтернету надає зловмисникам багато можливостей для вчинення комп'ютерних злочинів на принципах віддаленості, анонімності та складності виявлення. Кіберзлочинність стала серйозною загрозою для бізнесу, урядових органів, індивідуальних користувачів та суспільства загалом. Органи правопорядку, компанії з кібербезпеки та міжнародні організації спільно працюють над тим, щоб протидіяти цьому виду злочинності, але динамічний розвиток технологій вимагає постійного оновлення заходів безпеки. Тому, удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству на основі міжнародного досвіду є важливим завданням в умовах зростаючої загрози кібератак.

Аналіз останніх досліджень і публікацій дав змогу виявити, що поняття кіберзлочину є відносно новим, але прогресивним явищем. Дослідженням питань щодо розкриття сутності понять кіберзлочину та кібершахрайста, характеристики основних видів кіберзлочинів, дослідження зарубіжного досвіту в боротьбі з кібершахрайством та його імплементація в національне правове поле, займалися наступні науковці: Бельський Ю.[3], Боженко В. [4], Болгов В. [5], Бутузов В. [6], Буяджа С. [7], Лугіна Н. [11], Петровський О. [12], Савчук Н. [16], Копатін О. [10], Чинник П. [17].

Незважаючи на численні публікації з проблем функціонування вітчизняної системи протидії кіберзлочинам, у науковій літературі недостатньо представлені розробки, що розкривають дане питання. Тому слід провести детальний аналіз та дослідити міжнародний досвід та можливості впровадження його в Україні.

Метою статті є аналіз та дослідження вітчизняної системи протидії кіберзлочинності та кібершахрайству, виявлення проблем та способів вдосконалення цієї системи на основі впровадження міжнародного досвіду.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів.

На відміну від традиційних видів злочинів, таких як вбивство чи крадіжка, історія яких сягає століть, кіберзлочинність є дуже молодим явищем, яке виникло та еволюціонувало з розвитком глобальної мережі Інтернет. Поняття «кіберзлочинність» вперше з'явилося в американській, а потім і іншій зарубіжній літературі на початку шістдесятих років минулого століття і визначалося як порушення прав та інтересів інших осіб у зв'язку з автоматизованими системами обробки даних. Поняття комп'ютерної злочинності як сукупності кримінальних правопорушень включає всі види кримінальних правопорушень, вчинених у сфері інформації та телекомунікацій, де інформація, джерела інформації, інформаційні технології можуть бути об'єктом кримінальних правопорушень, засобом злочину. Детальний аналіз трактувань сутності поняття кіберзлочини вітчизняними науковцями та законодавчою базою [3, 5, 13, 10], дає можливість сформувати авторське визначення цього поняття. Так, під кіберзлочинністю, ми розуміємо, сукупність правопорушень, які вчиняються у віртуальному просторі з використанням комп'ютерних систем та мереж, а також інших технологічних засобів для отримання незаконного доступу до інформації, шахрайства, розповсюдження шкідливого програмного забезпечення та інших дій, що завдають збитків.

Український вчений В. Бутузов [6] обґрунтовує думку, що комп'ютерні злочини та кіберзлочини являють собою різні види злочинів у сфері високих інформаційних технологій, класифікація яких відбувається за такими ознаками:

 ознакою віднесення певних злочинів у сфері високих інформаційних технологій до комп'ютерних є знаряддя вчинення злочину – комп'ютерна техніка;

 ознакою віднесення злочинів у сфері високих інформаційних технологій до кіберзлочинів є специфічне середовище вчинення злочинів – кіберпростір (середовище комп'ютерних систем та мереж).

На його думку, тільки діяння із цього переліку можуть бути віднесені до кіберзлочинів.

Вважаємо, що залежно від мотивів вчинення кіберзлочинів, їх можна класифікувати за такими категоріями:

– кібершахрайство з метою заробітку: отримання чи крадіжка конфіденційної інформації з метою незаконного збагачення, злам паролів і отримання доступу до управління банківськими рахунками; шантаж щодо розкриття особистої інформації з метою отримання фінансової вигоди; шахрайські схеми щодо псевдоінвестицій, продажу фіктивних товарів чи послуг, добровільного переведення коштів громадянами на банківські рахунки шахраїв використовуючи різноманітні тактики тощо;

– кібершпигунство: використання програм шпигунів для отримання комерційних, політичних, військових та інших даних з метою набуття переваг в політичних, військових або економічних аспектах;

– поширення шкідливого програмного забезпечення: розробка та розповсюдження вірусного програмного забезпечення, яке наносить шкоду інформаційним системам, зокрема знищує дані чи встановлює контроль над ними;

– кібертероризм: нанесення шкоди комп’ютерним системам, що керують соціально важливу інфраструктуру (енергетична, фінансова, транспортна тощо) створюючи загрозу для громадської безпеки;

– інші злочини.

Найчастіше, вчинені кіберзлочити можуть включати декілька мотивів одночасно, тому всі види злочинів тісно пов’язані між собою.

Кіберзлочинність передбачає методи збору інформації, а збитки, які вона завдає, визначаються якістю інформації. Сучасне суспільство не може обійтися без електронних посередників і цифрових методів зберігання та обробки даних, тому кіберзлочинність є основною загрозою для існування та контролю публічних систем.

Однією з головних проблем аналізованих видів злочинів є низький рівень їх розслідуваності, що зумовлено відсутністю спеціальної експертизи, оскільки в умовах стрімкого розвитку інформаційних технологій методика криміналістичного дослідження цих об'єктів потребує постійного оновлення. Операційні системи, формати даних, протоколи та середовище передачі даних, а також технічне обладнання, яке забезпечує процеси передачі та обробки даних, змінюються щороку. Також постійно змінюється та розвивається й сам вид злочину – кібершахрайство.

Досить розповсюдженими зараз є шахрайські дії з використання електронних пристрої, що дозволяють зчитувати необхідні дані з клавіатури банкоматів або платіжних карток; підробки платіжних карток із використанням викрадених даних; встановлення в банкоматах технічних засобів, які дозволяють знімати гроші або платіжні картки; телефонного шахрайства (злочинці видають себе за банківських службовців з метою отримання необхідної інформації).

За даними дослідницького центру Finances online за 2022 рік [1] до числа найбільш поширених кіберзлочинів у світі відносять: фішинг (38 %), вторгнення в мережу (32 %), використання програм-шпигунів (20 %), а також злочинне використання викраденого або загубленого мобільного пристрою (10 %), у тому числі перевипуск його Sim карти, що фактично надає віддалений доступ до смартфону та усіх його додатків.

У 2022 році Департаментом кіберполіції порушено приблизно 5 тис. кримінальних правопорушень, повідомлено про підозру 1 тис. особам за вчинення 2,3 тис. кримінальних правопорушень, затримано понад 100 кіберзлочинців, задокументовано та притягнуто до відповідальності 10 хакерів. До суду з обвинувальними актами скеровано 2,7 тис. кримінальних правопорушень за обвинуваченням 840 осіб. Протягом року до підрозділу надійшло 70 тис. звернень громадян, з яких через форму «Зворотного зв'язку» Департаменту– 62,8 тис. звернень [9].

Під час повномасштабної війни в Україні значно активізувалося платіжне шахрайство. Найпоширенішим видом є фейкова соціальна допомога, яка надається державою або міжнародними організаціями громадянам України, які постраждали від війни. У 2022 році НБУ виявив близько 4 500 джерел шахрайства, тоді як у 2021 році їх було значно менше [15]. Як наслідок, Національний банк запровадив заходи для запобігання роботі шкідливих веб-сайтів. Їх реалізація сприятиме посиленню кібербезпеки фінансової системи, захисту громадян України від шахраїв, а також зменшенню кількості фішингових атак та загального обсягу фінансового шахрайства в майбутньому. Як наслідок, шахраї користуються зайнятістю правоохоронців, щоб уникнути покарання, і планують використовувати нові, більш інноваційні та технологічні методи для повторення більш тяжких злочинів.

Визначивши основні види кіберзлочинів, можна стверджувати, що існуюча система протидії кіберзлочинам в Україні повинна приділяти особливу увагу наступному:

1) розкриття, усунення/послаблення та нейтралізації причин кіберзлочинів проти власності;

2) усунення ситуацій, які безпосередньо спонукають або провокують вчинення злочинів проти власності в кіберпросторі;

3) виявлення осіб з підвищеним кримінальним ризиком та зниження цього ризику;

4) нагляд над тими особами, поведінка яких може свідчити про реальну можливість вчинення комп'ютерних злочинів проти власності, а також розробка методів їх запобігання та виправлення.

Безперечно, боротьба з кіберзлочинністю має стати одним із головних завдань правоохоронних органів. Враховуючи те, що цей вид злочинності вважається транснаціональним, країни світу повинні посилювати міжнародну співпрацю в цій сфері.

У Законі України «Про основні засади забезпечення кібербезпеки України» [13] визначено основних суб'єктів національної системи кібербезпеки та описано їх основні завдання. Таким суб'єктами є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.

Також, відповідно до затвердженої Стратегії [14] подальший розвиток національної системи кібербезпеки повинен базуватися на засадах виявлення та попередження кіберзлочинів, їх стримуванні та кіберпротистоянні. Важливим є забезпечення кіберстійкості через здатність усіх учасників кібербезпеки своєчасно розпізнавати загрози кібербезпеці, створювати захист, розгортати інструменти для виявлення кібератак, відповідним чином реагувати та швидко відновлювати стабільну роботу під час і після кібератаки.

Тому, одним із пріоритетних орієнтирів у системі кібербезпеки має стати досвід провідних країн світу, які вже досягли досить серйозних результатів у сфері інформаційної безпеки. У зв'язку з цим виникає нагальна потреба у розвитку міжнародного співробітництва та реалізації різнобічного інформаційного обміну.

З початку 1990-х років, численні міжнародні організації акцентували увагу на необхідності розробки та ухвалення міжнародних юридичних інструментів для подолання кіберзлочинності. Саме інформаційна безпека є важливою складовою національної безпеки, і може бути як інструментом безпеки, так і загрозою чи небезпекою. Кіберзлочинці швидко освоюють нові технології, адаптують нові методи атак і співпрацюють один з одним. По всьому світу діють міжнародні злочинні угруповання, які можуть координувати складні атаки за лічені хвилини. Тому для правоохоронних органів важливо бути в курсі нових технологій, розуміти, які можливості вони надають злочинцям і як їх можна використовувати для боротьби з

кіберзлочинністю. Враховуючи швидкозмінний характер кіберзлочинності, важливо мати платформу для обміну інформацією та координації дій, щоб правоохоронні органи могли швидко реагувати на нові загрози.

Усі міжнародні організації визнають загрозу і транснаціональний характер кіберзлочинності, обмеженість одностороннього підходу до проблеми і необхідність міжнародного співробітництва як у прийнятті необхідних технічних заходів, так і в розвитку міжнародного права. Так, ОЕСР, Рада Європи, Європейський Союз, ООН та Інтерпол відіграють важливу роль у координації міжнародних зусиль і розвитку міжнародного співробітництва у боротьбі з високотехнологічною злочинністю. Зокрема, Міжнародна організація кримінальної поліції (Інтерпол) (International Criminal Police Organization (ICPO, Interpol)) розслідує широкий спектр кіберзлочинів, включаючи афери та шахрайські дії в Інтернеті, кібератаки тощо. Також Інтерпол допомагає правоохоронним структурам інших держав з цифровою криміналістикою. У складі Інтерполу є Центр кіберсинтезу. Центр кіберсинтезу об’єднує кіберекспертів із правоохоронних органів та промисловості, щоб зібрати та проаналізувати всю наявну інформацію про злочинну діяльність в кіберпросторі та надати країнам цілісну, діючу розвідку [17].

На даному етапі деякі міжнародні угоди (наприклад, Конвенція Ради Європи про кіберзлочинність, Резолюція Ради Європейського Союзу, спільний проект Європейського Союзу-Міжнародного союзу електрозв'язку та держав Тихоокеанського регіону (проект ICB4PAC), проект Організації Об'єднаних Націй з удосконалення законодавства щодо боротьби з кіберзлочинністю в африканських країнах (проект ЕСКЗА)) за своєю природою не є глобальними міжнародними інструментами, але деякі з них мають вплив далеко за межами регіону, в якому вони були прийняті.

Цікавим є досвід провідних країн світу в боротьбу з кіберзлочинністю і можливість імплементації кращих практик в удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству.

Сполучені Штати Америки одні із перших почали розробку та провадження організаційної та правової системи для регулювання таких правопорушень. Одним із ключових положень Національної стратегії національної безпеки США, прийнятої у 2015 році, є положення про необхідність захисту від кібератак у кіберпросторі. Велика увага приділяється безпеці громадян, захисту їх прав та інтересів, оскільки країна активно працює над боротьбою з такими негативними явищами, як злочини в кіберпросторі, зокрема кібершахрайство. США можна назвати головною мішенню кібершахраїв, тому досвід країни є дуже корисним для розробки правових інструментів боротьби з цим явищем. Незважаючи на все вищезазначене, США значною мірою використовують метод саморегулювання Інтернету, а тому законодавство в цій сфері представлено різноманітними нормативно-правовими актами.

Провідну роль у забезпечення безпеки США в он-лайн просторі відіграє Міністерство національної безпеки США (Department of Homeland Security, DHS). Воно зосереджується на розробці та впровадженні стратегій, політик і заходів, що мають на меті протидію кіберзлочинності та забезпечення стійкості країни перед кіберзагрозами.

У структурі DHS є Секретна служба США (U.S. Secret Service) та Імміграційна та митна служба США (U.S. Immigration and Customs Enforcement,ICE), які мають спеціальні відділи, що займаються боротьбою з кіберзлочинністю. Відділ кіберрозвідки Секретної служби США зосереджений на виявленні та пошуку міжнародних кіберзлочинців, пов’язаних з кібервторгненнями, банківським шахрайством, витоком даних та іншими комп’ютерними злочинами. Також, Секретна служба має у своєму підпорядкуванні Національний інститут комп’ютерної криміналістики, який провадить освітні послуги у сфері кіберобізнаності для федеральних, державних та міжнародних правоохоронних органів. Центр розслідування кіберзлочинів Імміграційної та митної служби США надає комп’ютерні

технічні послуги для підтримки внутрішніх і міжнародних розслідувань кіберзлочинів [2].

У США активну боротьбу з кіберзлочинністю веде Федеральне бюро розслідувань (ФБР), (Federal Bureau of Investigation, FBI). Воно здійснює заходи з попередження та розслідування широкого спектру кіберзлочинів, таких як: вторгнення до комп'ютерних систем та мереж; вимагання через кіберпростір (шифрування ваших даних без вашого відома та вимагання викупу за їх розкодування); крадіжка особистої інформації та інше. У 2021 році ФБР отримало рекордну кількість скарг на кіберзлочини, понад 840 тис., потенційні збитки яких перевищили 6,9 мільярда доларів. Крім того, у 2022 році спостерігалося збільшення кількості атак програм-вимагачів з боку транснаціональних злочинців, які загрожують призвести до перебоїв у роботі критично важливих сервісів у всьому світі.

США допомагає розбудовувати потенціал у сфері кібербезпеки за кордоном на основі двосторонніх договорів з іншими країнами. Це дозволяє обмінюватися досвідом у боротьбі з кіберзлочинністю. Зокрема, у 2022 році підписано Меморандум про співробітництво між Державною службою спеціального зв'язку та захисту інформації України та Агентством з кібербезпеки та захисту інфраструктури США (CISA). У рамках Меморандуму реалізується ряд спільних ініціатив з обміну даних щодо ризиків та інцидентів з кібербезпеки, обміну найкращими практиками у сфері співробітництва «держава–приватний бізнес», проведення командно-штабних навчань та впровадження практик із захисту критичної інфраструктури.

Варто зазначити, що у США функціонує система обов'язкового сповіщення компаній та організацій про кібератаки та кіберінциденти. Це сприяє швидкій реакції та координації заходів для обмеження поширення шкоди.

Значний акцент також робиться на підвищення кіберграмотності громадян та співробітників компаній. Програми навчання та освітні

ініціативи розроблені з метою поширення знань про основні принципи кібербезпеки, визнання потенційних загроз та засобів їх запобігання.

Крім того, урядові агентства співпрацюють з приватними секторами та міжнародними партнерами, обмінюючися інформацією та кращими практиками у боротьбі з кіберзлочинами та кібершахрайством.

Всі ці складові утворюють цілісну систему протидії кібершахрайству в США, яка сприяє ефективному забезпеченню кібербезпеки та зменшенню ризику кіберзлочинів.

З 2013 року в Європейському Союзі існує Європейський центр боротьби з кіберзлочинністю (European Cybercrime Centre – EC3). Мета його діяльності це співпраця та координація роботи держав-членів ЄС та міжнародних партнерів, обмін кращими практиками у боротьбу з кіберзлочинністю; створення більш безпечного онлайн-середовища в Європі та за її межами. Щорічно EC3 публікує звіт щодо Оцінки загроз організованої злочинності в Інтернеті (Internet Organised Crime Threat Assessment – IOCTA) в якому міститься опис найбільш поширених видів кіберзлочинів у поточному році, визначаються прогнозні тенденції їх розвитку та надаються рекомендації з боротьби проти кіберзлочинності. Також, в ЄС значна увага приділяється проблематиці раннього виявлення й оперативного реагування на кіберінциденти та кібератаки проти електронних інформаційних ресурсів.

Окрім вивчення досвіду Європейського співтовариства в цілому, цікавим є аналіз правової системи боротьби з кіберзлочинністю у Франції, яка однією з перших серед країн-членів ЄС вжила заходів щодо посилення ролі держави в регулюванні кіберпростору. Наразі французьке законодавство виділяє наступні види кіберзлочинів:

1) суспільно небезпечні діяння, пов'язані з незаконним тиражуванням комп'ютерного програмного забезпечення, незаконним втручанням в автоматизовані системи обробки даних, вторгненням на сайти, створенням і розповсюдженням шкідливих програм тощо;

2) поширення сайтів, пов'язаних з: дитячою порнографією, збутом наркотиків, терористичною спрямованості, замахом на приватне життя, інструкціями по експлуатації вибухових речовин, реклами в шахрайських цілях [7].

Цей досвід є актуальним для практики в Україні, оскільки поняття кіберзлочинності фундаментально не осмислене та не сформульоване. Важливим також є чітке розмежування злочинів з точки зору їх впливу та негативних наслідків на соціальні процеси в країні. Якщо перша форма кіберзлочинів за французькою класифікацією адекватно врегульована в Україні Розділом XVI Кримінального кодексу України, то досвід регулювання другої форми заслуговує на детальний аналіз.

Варто також згадати французький закон про обов'язкову реєстрацію власників веб-сайтів та кримінальну відповідальність хостинг-провайдерів, які надають хостинг ідентифікованим користувачам. Ще одним цікавим аспектом цього законодавства є обов'язок провайдерів розкривати інформацію про авторів веб-сайтів потенційним третім особам, що тягне за собою кримінальну відповідальність. Цей вид відповідальності також передбачений за неповну або невірну інформацію, надану авторами французьких веб-сайтів, а також для провайдерів послуг, які надають серверне місце ідентифікованим користувачам. Крім того, провайдер несе відповідальність за будь-який веб-сайт, авторство якого не встановлено, з можливим покаранням у вигляді шестимісячного відключення від Інтернету. Будь-яка державна діяльність, спрямована на створення контролю над громадянами, за своєю суттю є негативною, проте це є вимущений крок у сфері боротьби з кіберзлочинністю. Однак, зважаючи на останні тенденції розвитку удосконалення національного законодавства в частині запровадження відповідальності за порушення правил кібернагляду рано чи пізно постане на порядку денному. У зв'язку з цим буде корисно проаналізувати досвід більш розвинених країн, і французьке законодавство є одним із пріоритетних для вивчення в цьому контексті.

У сфері активної боротьби з кіберзлочинністю 14 лютого 2008 року була прийнята Французька стратегія боротьби з кіберзлочинністю, спрямована на співпрацю з приватними компаніями (постачальниками IT та телекомунікаційних послуг) та правоохоронними органами з метою обміну інформацією та об'єднання зусиль у боротьбі з кіберзлочинністю. Отже, особливостями правового регулювання боротьби з кіберзлочинністю у Франції є:

1) істотна роль держав в регулюванні суспільних відносин в Інтернеті;

2) контроль за користувачами шляхом встановлення вимоги до авторизації авторів веб-сайтів;

3) налагодження співпраці правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз;

4) наявність двостороннього діалогу з громадянами та належне роз'яснення їх прав і обов'язків як користувачів Інтернету;

5) встановлення курсу на вільне співробітництво з іншими державами шляхом надання доступу до власних кібермереж в разі вчинення на території Франції кіберзлочинів [7].

Майже всі виокремлені особливості можуть бути застосовані до сучасних українських реалій. Таким чином, аналіз нормативно-правової бази боротьби з кіберзлочинністю у Франції дозволяє виділити наступні шляхи застосування позитивного досвіду в Україні:

- встановлення вимоги авторизації авторів веб-сайтів;
- налагодження співпраці правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз;
- налагодження двостороннього діалогу з громадянами.

Висновки. Загроза кіберзлочинності є дуже серйозною проблемою сьогодення, яка проявляється у незаконному доступі до даних, шахрайстві, витоку конфіденційної інформації, атак на комп'ютерні системи та інші порушення, що наносять шкоду окремим особам, організаціям та державі. Ця загроза має значний потенціал завдати серйозних збитків технологічним

структурам, економіці, державній безпеці та конфіденційності особистих даних. Оскільки сучасне суспільство не може обійтися без електронних носіїв інформації та цифрових способів їх зберігання та обробки, кіберзлочинність є однією з найбільших загроз для існування та регулювання суспільних процесів.

Аналіз міжнародного досвіду по боротьбі з кіберзлочинністю, на прикладі США та Франції, засвідчив необхідність удосконалення сучасного правового та організаційного забезпечення боротьби з кіберзлочинністю в кіберпросторі України. При розбудові національної системи кіберзахисту варто враховувати досвід США щодо комплексної та згуртованої взаємодії різних державних структур, з чітким розподілом повноважень у сфері забезпечення захисту кіберпростору, їх співпрацю: з приватним сектором, інформуючи останніх про можливі кібератаки; з населенням щодо створення освітніх платформ, навчальних програм для підвищення обізнаності громадян щодо існуючих видів кібершахрайств та способів їх попередження; з міжнародними партнерами через обмін інформацією та отримання найкращих практик у боротьбі з кіберзлочинами та кібершахрайством.

Франція є гарним прикладом для позитивних змін, які Україна може винести з цього досвіду. По-перше, порівняно з іншими країнами ЄС, Франція більш жорстко підійшла до встановлення контролю в кіберпросторі, зокрема через встановлення вимоги авторизації авторів веб-сайтів. По-друге, Франція є взірцем налагодження двосторонніх відносин на рівні «держава-держава», «держава-громадянин» та «держава-приватний сектор економіки», зокрема через налагодження співпраці правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз та налагодження двостороннього діалогу з громадянами.

Таким чином, сучасний стан правового забезпечення боротьби з кіберзлочинністю в України потребує вдосконалення, шляхом внесення змін та доповнень до низки нормативно-правових актів, враховуючи міжнародний досвід. Активна співпраця з міжнародними структурами по боротьбі з

кіберзлочинністю пришвидшить процеси вдосконалення кіберзахисту країни та побудови ефективної організаційної структури щодо боротьби з кіберзлочинністю.

Робота виконана в рамках держбюджетних науково-дослідних робіт 0121U100467 «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України».

Література

1. 119 Impressive Cybersecurity Statistics: 2023 Data & Market Analysis. *FinancesOnline Research Center*. URL: https://financesonline.com/cybersecurity-statistics/ (дата звернення: 22.08.2023).

2. Combatting Cyber Crime. *Офіційний вебпортал Агентство з кібербезпеки та захисту інфраструктури США (CISA).* URL: https://www.cisa.gov/combatting-cyber-crime (дата звернення: 22.08.2023).

3. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник.* 2014. №6. С. 414–418.

4. Боженко В.В., Койбічук В.В., Габенко М.М. Вплив кібершахрайств на фінансову систему на прикладі країн Євросоюзу. *Вісник СумДУ. Серія Економіка.* 2021. № 2. С. 47–52.

5. Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. К.: Національна академія прокуратури України, 2015. 202 с.

6. Бутузов В.М. Протидія комп'ютерній злочинності в Україні. Київ: КИТ, 2010. 148 с.

7. Буяджа С. Позитивний досвід правового регулювання боротьби з кіберзлочинністю в країнах ЄС. *European political and law discourse.* Volume 4, Issue 4, 2017, p. 41-46.

8. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. *Юрист&Закон*. 2020. №12. URL:

https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення: 20.08.2023).

9. Звіт про результати роботи Департаменту кіберполіції у 2022 році / *Офіційний вебпортал кіберполіції України* URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/ (дата звернення: 22.08.2023).

10. Копатіна О., Скулишина Є. Словник термінів з кібербезпеки. К.: Аванпост- Прим, 2012. 214 с.

11. Лугіна Н., Лучук А. Оптимізація правового регулювання боротьби з кібершахрайством: зарубіжний досвід і його значущість в українській практиці. *Юридичний науковий електронний журнал.* 2021. № 1. С. 238–241.

12. Петровський О.М., Лівчук С.Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Young Scientist.* 2019. № 12.1 (76.1). С. 55-59.

13. Про основні засади забезпечення кібербезпеки України. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 22.08.2023).

14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.21 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 22.08.2023).

15. Протидія кібершахрайству у фінансовій сфері, лютий 2023 року. *Офіційний вебпортал НБУ*. URL: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori (дата звернення: 22.08.2023).

16. Савчук Н. В. Світовий досвід державного регулювання ринку інтернет-послуг. *Формування ринкових відносин в Україні.* 2012. № 4. С. 24–28.

17. Чинник П. А. Світовий досвід боротьби з кіберзлочинністю. *Збірник матеріалів Міжнародної науково-практичної конференції Кіберзлочинність та торгівля людьми (27 травня 2020 року, м. Харків).*

Харківський національний університет внутрішніх справ. Харків, 2020. С. 221–223.

References

1. FinancesOnline Research Center (2023), “119 Impressive Cybersecurity Statistics: 2023 Data & Market Analysis”, available at: https://financesonline.com/cybersecurity-statistics/ (Accessed 22 August 2023).

2. The official site of the US Cybersecurity and Infrastructure Security Agency (CISA) (2023), “Combatting Cyber Crime”, available at: https://www.cisa.gov/combatting-cyber-crime (Accessed 22 August 2023).

3. Belsky, Y. (2014), “On the definition of the concept of cybercrime”, *Yurydychnyi Visnyk, vol.* 6, pp. 414–418.

4. Bozhenko, V.V. Koybichuk, V.V. and Habenko M.M. (2021), “The impact of cyberfraud on the financial system on the example of the countries of the European Union”, *Visnyk SumDU. Seriya Ekonomika,* vol. 2, pp. 47–52.

5. Bolhov, V. Gadion, N. and Gladun, O. (2015), *Orhanizatsijno-pravove zabezpechennia protydii kryminal'nym pravoporushenniam, scho vchyniaiut'sia z vykorystanniam informatsijnykh tekhnolohij* [Organisational and legal support for combating criminal offences committed with the use of information technology], Natsional'na akademiia prokuratury Ukrainy, Kyiv, Ukraine.

6. Butuzov, V.M. (2010), *Protudiia compiuternoi zlochinnosti v Ukraini* [Counteraction to computer crime in Ukraine], KYT, Kyiv, Ukraine.

7. Buiadzha, S. (2017), “Positive experience of legal regulation of the fight against cybercrime in EU countries”, *European political and law discourse,* vol. 4, Issue 4, p. 41–46.

8. Gazizova, Yu. (2020), “Cybercrime in Ukraine. The era of digital technologies is the era of new crimes”, *Yuryst&Zakon,* vol. 12, available at: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (Accessed 20 August 2023).

9. The official site of the Cyber Police of Ukraine (2022), “Report on the results of the work of the Cyber Police Department in 2022”, available at:

https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/ (Accessed 22 August 2023).

10. Kopatin, O. And Skulyshyn, E. (2012), *Slovnuk terminiv z ciberbezpeku* [Dictionary of Cybersecurity Terms], Avanpost-Prim, Kyiv, Ukraine.

11. Luhina, N. and Luchuk, A. (2021), "Optimization of legal regulation of the fight against cyberfraud: foreign experience and its significance in Ukrainian practice", *Juridical scientific and electronic journal*, vol 1, p. 238–241.

12. Petrovskyi, O.M. and Livchuk, S.Y. (2019), "Problems of combating cybercrime: international experience and Ukrainian realities", *Young Scientist*, vol. 12.1 (76.1), p. 55-59.

13. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2163-19 (Accessed 22 August 2023).

14. President of Ukraine (2021), Decree "On the decision of the National Security and Defence Council of Ukraine of 14 May 2021 "On the Cybersecurity Strategy of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text (Accessed 22 August 2023).

15. The official site of the National Bank of Ukraine (2023) "Combating cyberfraud in the financial sphere, February 2023", available at: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori (Accessed 22 August 2023).

16. Savchuk, N. V. (2012), "World experience of state regulation of the Internet services market", *Formation of market relations in Ukraine*, vol. 4, p. 24–28.

17. Chynnyk, P.A. (2020), "World experience in the fight against cybercrime", *Zbirnyk materialiv Mizhnarodnoi naukovo-praktychnoi konferentsii. Kiberzlochynnist' ta torhivlia liud'my* [Collection of materials of the International Scientific and Practical Conference. Cybercrime and human trafficking], Kharkiv National University of Internal Affairs, Kharkiv, Ukraine, pp. 221–223.

Стаття надійшла до редакції 09.10.2023 р.