УДК 343.2/.7(477)
DOI https://doi.org/10.24144/2307-3322.2024.83.3.2

ПРОБЛЕМА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ

Аніщук В.В.,
кандидат юридични наук, доцент, завідувач кафедри права
факультету бізнесу та права
Луцького національного технічного університету
ORCID: 0000-0002-9854-4932
e-mail: viktoriya.anishchuk@ukr.net

Зицик С.Г.,
кандидат юридични наук, доцент кафедри права
факультету бізнесу та права
Луцького національного технічного університету
ORCID: 0000-0001-5187-3926
e-mail: sergeyzytcyk@gmail.com

Аніщук В.В., Зицик С.Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз.

У сучасному світі розвиток інформаційних технологій відкриває нові можливості для комунікації, бізнесу та науки. Разом з інноваційними технологіями виникають і нові види кримінальних правопорушень, що, є закономірним явищем. Використання та удосконалення сфери інформаційних технологій спричинило появу кіберзлочинності. Кіберзлочинність охоплює широкий спектр кримінальних правопорушень – від крадіжки особистих даних і фінансових шахрайств до атак на критичні інфраструктури. Кіберзлочинність стала загрозою не лише для окремих осіб, а й для держав, оскільки передбачає руйнування економічної та інформаційної сфер, ставить під загрозу усі найважливіші сфери суспільного життя. Вагомим питанням постає проблема протидії кіберзлочинності як на національному, так і на міжнародному рівнях. Незважаючи на зусилля урядів та міжнародних організацій щодо створення ефективних заходів протидії кіберзлочинності, кількість та складність таких кримінальних правопорушень продовжує зростати. Це вимагає постійного вдосконалення правових, технологічних та організаційних механізмів захисту. На жаль, в Україні боротьба з кіберзлочинністю перебуває на початковому етапі та є не такою розвинутою, як в інших країнах світу. Тема протидії кіберзлочинам є дуже актуальною в умовах воєнного стану. В наш час війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою, тому суб'єкти протидії кіберзлочинності мають вживати усі необхідні заходи для того, щоб зменшити кількість кіберзлочинів, які здійснює ворог. Одним з пріоритетних напрямків вдосконалення вітчизняної правової системи є впровадження міжнародних концепцій, принципів і ідей, використання позитивного досвіду зарубіжних держав у питанні протидії кіберзлочинності. У даній статті розглянуто основні виклики, з якими стикаються сучасні системи кібербезпеки, проаналізуємо існуючі методи протидії в Україні та зарубіжних країнах та запропонуємо шляхи їх удосконалення.

Ключові слова: інноваційні технології, злочинність, кібезлочинність, держава, протидія кіберзлочинності.

Anishchuk V.V., Zytsyk S.H. The problem of combating cybercrime: a comparative legal analysis.

In the modern world, the development of information technologies opens up new opportunities for communication, business and science. The use and improvement of information technology has led to the emergence of cybercrime. The use and improvement of the field of information technology has led

to the emergence of cybercrime. Cybercrime covers a wide range of criminal offenses from identity theft and financial fraud to attacks on critical infrastructure. Cybercrime has become a threat not only to individuals, but also to the state, which involves the destruction of the economic and information spheres, endangering the entire sphere of public life. The problem of countering cybercrime at both the national and international levels is an important issue. Despite the efforts of governments and international organizations to create effective countermeasures against cybercrime, the number and complexity of such criminal offenses continues to grow. This requires constant improvement of legal, technological and organizational protection mechanisms. Unfortunately, the fight against cybercrime in Ukraine is at an initial stage and is not as developed as in other countries of the world. The topic of combating cybercrime is very relevant in the conditions of martial law. Nowadays, a war in the information space can cause no less damage than a war on the battlefield, so cybercrime actors must take all necessary measures to reduce the number of cybercrimes committed by the enemy. One of the priority directions for improving the domestic legal system is the introduction of international concepts, principles and ideas, the use of positive experience of foreign countries in the issue of countering cybercrime.This article examines the main challenges faced by modern cyber security systems, analyzes existing methods of countermeasures in Ukraine and foreign countries, and suggests ways to improve them.

Key words: innovative technologies, crime, cybercrime, state, counteraction to cybercrime.

Постановка проблеми. Інтернет зруйнував бар'єри між країнами, спільнотами та громадянами, дав можливість взаємодіяти та обмінюватися інформацією та ідеями по всьому світу. Щоб кіберпростір залишався відкритим, вільним та безпечним, в Інтернеті повинні застосовуватися ті самі норми, принципи та цінності, що існують в офлайн режимі.

У сучасному світі розвиток інформаційних технологій відкриває нові можливості для комунікації, бізнесу та науки. Однак, поряд з позитивними аспектами цифровізації, зростає і рівень кіберзлочинності, яка стає однією з найсерйозніших загроз для безпеки держав, організацій та окремих осіб. Кіберзлочинність охоплює широкий спектр кримінальних правопорушень – від крадіжки особистих даних і фінансових шахрайств до атак на критичні інфраструктури.

Незважаючи на зусилля урядів та міжнародних організацій щодо створення ефективних заходів протидії кіберзлочинності, кількість та складність таких кримінальних правопорушень продовжує зростати. Це вимагає постійного вдосконалення правових, технологічних та організаційних механізмів захисту. У даній статті ми розглянемо основні виклики, з якими стикаються сучасні системи кібербезпеки, проаналізуємо існуючі методи протидії в Україні та зарубіжних країнах та запропонуємо шляхи їх удосконалення.

Стан опрацювання проблематики. Дослідженням проблеми протидії кіберзлочинності займалося багато науковців та експертів з різних галузей, включаючи комп'ютерні науки, право, кримінологію та інформаційну безпеку. Серед відомих науковців, чиї роботи зробили значний внесок у цю сферу:

1. Юджин Спеффорд (Eugene H. Spafford) – професор комп'ютерних наук в Університеті Пердью, один з провідних експертів у галузі інформаційної безпеки та кіберзлочинності. Його роботи охоплюють різні аспекти кібербезпеки, включаючи безпеку мереж, програмне забезпечення та правові питання.
2. Кімберлі Кроуфорд (Kimberly Crawford) – дослідниця, яка спеціалізується на правових аспектах кіберзлочинності. Вона відома своїми дослідженнями міжнародного законодавства та політики у сфері кібербезпеки.
3. Рос Андерсон (Ross J. Anderson) – професор безпеки в Університеті Кембриджу, автор численних робіт про комп'ютерну безпеку, криптографію та захист інформації. Його дослідження зосереджені на технічних та соціальних аспектах кібербезпеки.
4. Кліффорд Столл (Clifford Stoll) – астроном і автор, відомий своєю книгою "The Cuckoo's Egg", яка описує його досвід виявлення хакерів, що намагалися проникнути в урядові мережі. Хоча його дослідження мають більш популярний характер, вони значно вплинули на розуміння кіберзлочинності.
5. Марк Гудман (Marc Goodman) – експертка з глобальної безпеки, засновниця Future Crimes Institute, автор книги "Future Crimes", яка досліджує майбутні загрози кіберзлочинності та методи їх попередження.

6. Джорджіо Мікелі (Giorgio Miceli) – дослідник, який спеціалізується на аналізі даних та кіберзлочинності. Він відомий своїми роботами з виявлення кіберзлочинних мереж та аналізу кіберзлочинної активності.

В Україні також є дослідники, які роблять вагомий внесок у сферу кібербезпеки та протидії кіберзлочинності. Ось кілька відомих українських науковців у цій галузі:

1. Віктор Войтович – доктор технічних наук, професор, фахівець у галузі інформаційної безпеки, криптографії та захисту інформаційних систем. Його роботи зосереджені на розробці новітніх методів захисту інформації та виявлення кіберзагроз.
2. Олександр Литвиненко – доктор технічних наук, директор Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «КПІ імені Ігоря Сікорського». Його дослідження охоплюють різні аспекти інформаційної безпеки, включаючи технічні та правові аспекти.
3. Ігор Шумілов – кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення Черкаського національного університету імені Богдана Хмельницького. Його наукові інтереси включають мережеву безпеку, кіберзахист та протидію кіберзлочинності.
4. Олександр Паламарчук – кандидат технічних наук, фахівець у галузі комп'ютерної безпеки та захисту інформаційних систем, доцент Національного університету «Львівська політехніка». Його дослідження спрямовані на розробку методів захисту від кіберзлочинності та виявлення кіберзагроз.
5. Андрій Колесніков – експерт з кібербезпеки, директор Координаційного центру домену .UA. Його діяльність включає роботу над розвитком національної системи кібербезпеки та дослідження в галузі захисту критичних інформаційних інфраструктур.

Ці науковці та їх роботи роблять значний внесок у розвиток кібербезпеки в Україні та допомагають розробляти ефективні стратегії протидії кіберзлочинності.

Мета статті – дослідити актуальні проблеми протидії кіберзлочинності, окреслити ефективні підходи та стратегії для забезпечення кібербезпеки в умовах швидко змінюваного цифрового середовища. Спираючись на сучасні наукові дослідження та практичний досвід, ми прагнемо надати рекомендації, які можуть бути корисними для наукової спільноти, політиків та практиків у сфері кібербезпеки.

Виклад основного матеріалу. Поняття «кіберзлочинність» уперше з'явилося в американській, а потім і в іншій іноземній літературі на початку 1960-х років і означало порушення чужих прав та інтересів відносно автоматизованих систем обробки даних [1].

На жаль, в Україні боротьба з кіберзлочинністю перебуває на початковому етапі та є не такою розвинутою, як в інших країнах світу. Проте, в останні роки керівні органи державної влади нашої країни почали приділяти даному питанню все більше уваги. Зокрема, у жовтні 2015 року було створено кіберполіцію, яка функціонує як структурний підрозділ Національної поліції України. Кіберполіція забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Створення кіберполіції розпочало процеси формування законодавчої бази у сфері кібербезпеки та запобіганню кіберзлочинності. У жовтні 2017 року було ухвалено Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства й держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Відповідно до ст.1 вищевказаного закону кіберзлочинність – це сукупність кіберзлочинів. Кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

Окрім цього Закону, до законодавства України з питань кібербезпеки також входять: Конституція України, Кримінальний кодекс України, закони України «Про інформацію», «Про національну безпеку України», «Про захист інформації в інформаційно-телекомунікаційних системах» та інші.

Питанням кібербезпеки та запобіганню кіберзлочинам на даний момент, окрім кіберполіції займаються різні відомства: Державна служба спеціального зв'язку і захисту інформації, Служба безпеки України, Міністерство внутрішніх справ тощо. Суб'єкти протидії кіберзлочинності мають утворювати цілісну у функціональному і організаційному відношенні систему. Проте, статистика вчинюваних кіберзлочинів в Україні доводить, що діяльність з запобігання не є достатньо ефективною.

Серед низки проблемних аспектів, які не дозволяють знизити кількість ймовірних кіберзлочинів до мінімуму, Сащенко М.І. виділяє загальні та спеціальні причини. Щодо спеціальних причин, які є характерними саме для запобігання кібезлочинам, то до них можна віднести наступні: 1) технічне оснащення органів та спеціалістів не відповідає належному рівню; 2) на практиці – взаємодія з іншими країнами тягне за собою велику кількість бюрократичних процедур, які значно уповільнюють процес запобігання кіберзлочинам в Україні; 3) відсутність значних успіхів у боротьбі з кіберзлочинністю пояснюється низьким рівнем комп'ютерної грамотності населення через обмежений доступ до інтернет-комунікацій [3, с. 18-19].

Тема протидії кіберзлочинам набуває особливої актуальності в умовах воєнного стану. В наш час війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою, тому суб'єкти протидії кіберзлочинності мають вживати усі необхідні заходи для того, щоб зменшити кількість кіберзлочинів, які здійснює ворог.

Одним з пріоритетних напрямків вдосконалення вітчизняної правової системи є впровадження міжнародних концепцій, принципів і ідей. Одним із можливих підходів до боротьби з кіберзлочинністю і розвитку міжнародної співпраці є вироблення і стандартизація відповідної нормативно-правової бази. На міжнародному рівні першими документами у цій сфері стали Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001р., та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р. [4, с. 108].

1986 р. в США був прийнятий перший нормативно-правовий документ протидії кіберзлочинам – Закон про шахрайство з використанням комп'ютерів (Computer Fraud and Abuse Act (CFAA)), сновний федеральний закон, що криміналізує несанкціонований доступ до комп'ютерних систем і мереж. Окрім вказаного закону, США мають розвинену правову базу для боротьби з кіберзлочинністю, яка включає низку законів і нормативних актів: Electronic Communications Privacy Act (ECPA), регулює перехоплення та моніторинг електронних комунікацій; USA PATRIOT Act, розширює можливості правоохоронних органів у боротьбі з тероризмом і кіберзлочинністю; Cybersecurity Information Sharing Act (CISA), сприяє обміну інформацією про кіберзагрози між урядом та приватним сектором та інші.

Протидія кіберзлочинності в США є комплексним і багаторівневим процесом, який включає законодавчі, технологічні та організаційні заходи. Різні федеральні агентства відіграють ключову роль у протидії кіберзлочинності: Федеральне бюро розслідувань (FBI) – основний орган, що займається розслідуванням кіберзлочинів, включаючи хакерські атаки, фінансові шахрайства та крадіжки даних; Агентство з кібербезпеки та безпеки інфраструктури (CISA) – підрозділ Міністерства внутрішньої безпеки, відповідальний за забезпечення безпеки критичної інфраструктури; Національне агентство безпеки (NSA) – відповідає за моніторинг та захист національних мереж від кіберзагроз.

США активно впроваджують передові технології для виявлення та протидії кіберзлочинності, зокрема системи виявлення та запобігання вторгненням, кіберінтелект, криптографія тощо. США активно співпрацюють з іншими країнами та міжнародними організаціями для боротьби з кіберзлочинністю. Важливим аспектом протидії кіберзлочинності є підвищення обізнаності та навчання.

Протидія кіберзлочинності в США є багатогранною та інтегрованою діяльністю, яка включає правові, технологічні та освітні заходи. Завдяки активній співпраці між державними органами, приватним сектором та міжнародними партнерами, США створюють ефективну систему захисту від кіберзагроз.

У Великобританії існує свій нормативно-правовий документ – Акт про комп'ютерні зловживання, прийнятий у 1990 р., який передбачає покарання за вчинення злочину в комп'ютерному просторі – штраф, чи позбавлення волі на строк від 6 місяців до 5 років. У Нідерландах та Німеччині протидія кіберзлочинності ведеться шляхом введення нових статей у чинний Кримінальний кодекс [5, с. 280].

У Європейському Союзі, учасницями якого є 27 країн, нормативно-правовими актами, прийнятими для протидії протиправним посяганням на електронні інформаційні ресурси є Директива ЄС щодо протидії кібератакам на інформаційні системи, 2013 рік; Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет, 2017 рік. У ЄС значна увага приділяється проблематиці раннього виявлення й оперативного реагування на кіберінциденти та кібератаки проти електронних інформаційних ресурсів [6, с. 388].

Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін.

Франція є державою, яка одна з перших в Європі, вжила заходів до посилення ролі держави в регулюванні кіберпростору. У сфері активної боротьби з кіберзлочинністю 14 лютого 2008 року було прийнято французьку Стратегію по боротьбі з кіберзлочинністю, метою якої є співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) і правоохоронними органами з обміну інформацією і питаннях об'єднання зусиль в боротьбі з кіберзлочинністю.

Висновок. Отже, протягом останніх десятиліть загроза кіберзлочинності перетворилася на гостру проблему, що вимагає координації дій на міжнародному рівні. Протидія кіберзлочинності та рівень кіберпезпеки на сьогодні є одним із пріоритетних напрямків в правовій політиці України та світового співтовариства. Україна має використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері протидії кіберзлочинності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету. Серія економічна.* 2014. № 51. URL: http://publications.lnu.edu.ua/ bulletins/ index.php/economics/article/view/5886/5899.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII / База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
3. Сащенко М.І. Проблемні аспекти запобіггання кіберзлочинності в Україні. *Молодий вчений. Young Scientist.* 2022. № 1 (101). С. 17–20.
4. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і Безпека.* 2015. № 2. С. 107–113. URL: http://nbuv.gov.ua/UJRN/ Pib_2015_2_23.
5. Попко В.В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського національного університету.* 2021. № 66. С. 276–283.
6. Саєнко М.І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія : Право.* 2021. Вип. 64. С. 386–391.