ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 3 (13), 2024
УДК 343.3/.7:004.056.5(477)
DOI 10.31732/2708-339X-2024-13-A18

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ: ПРАВОВІ ПРОБЛЕМИ ТА ШЛЯХИ ЇХ РОЗВ'ЯЗАННЯ

Француз А.Й.,
Герой України, Заслужений юрист України,
доктор юридичних наук, професор
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: anatoliyfj@krok.edu.ua
ORCID: https://orcid.org/0000-0003-2861-1252

Шепеля А.М.,
здобувачка вищої освіти ОКР «Магістр»,
спеціальності «Право»,
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: inter_students@krok.edu.ua

CURRENT ISSUES OF COMBATING CYBERCRIME IN UKRAINE: LEGAL PROBLEMS AND WAYS TO SOLVE THEM

Frantsuz A.Yo.,
Hero of Ukraine, Honored Lawyer of Ukraine,
Doctor of Legal Sciences, Professor,
Head of the Department of State and Legal Disciplines of «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: AnatoliyFJ@krok.edu.ua
ORCID: https://orcid.org/0000-0003-2861-1252

Shepelia A.M.,
graduate of the Master's degree of
«KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: inter_students@krok.edu.ua

***Анотація**. Сучасний світ є доволі динамічним явищем, що призводить до інтенсифікації не лише можливостей, але й потенційних загроз. Інноваційні технології відкривають нові горизонти для розвитку бізнесу, освіти та культури, значно полегшуючи комунікацію та доступ до інформації. Водночас вони створюють сприятливі умови для кіберзлочинців, діяльність яких стає все більш різноманітною та складною.*

Кіберзлочинність охоплює широкий спектр кримінальних правопорушень: від крадіжки особистих даних і фінансових шахрайств до атак на критичні інфраструктури. Загрози кіберзлочинності стосуються не лише окремих осіб, які можуть втратити заощадження чи особисті дані, але й корпорацій, що можуть зіткнутися з порушенням операційної діяльності, втратою клієнтської бази та репутації, а також держав, де такі дії здатні спричинити значні економічні втрати, компрометацію національної безпеки, порушення конфіденційності критично важливої інформації та дестабілізацію системи державного управління, яка є основою суспільного порядку і розвитку.

У зв'язку з цим існує нагальна потреба вдосконалення нормативно-правової бази, яка має відповідати сучасним викликам цифрового світу, забезпечувати ефективне переслідування кіберзлочинців та створювати умови для міжнародної співпраці у сфері кібербезпеки. Також необхідно підвищувати рівень освіти у цій галузі, впроваджуючи навчальні програми з кібербезпеки у школах, університетах і професійних закладах, а також організовуючи регулярні тренінги для працівників державних установ, бізнесу та широкого загалу. Розвиток технологій захисту інформації, включаючи використання штучного інтелекту, блокчейн-технологій та удосконалення шифрувальних систем, має стати пріоритетом для наукових досліджень та інновацій.

Ці заходи є критично важливими, оскільки кіберзлочинність постійно еволюціонує, стаючи дедалі складнішою, технічно витонченішою та непередбачуваною, і від ефективності нашої реакції на нові виклики, а також

своєчасного впровадження превентивних дій, залежить не лише безпека окремих громадян, бізнесу чи установ, але й стабільність держави.

У статті акцентується увага на необхідності комплексного підходу до протидії викликамкібербезпеки, що уможливлює створення сприятливого інформаційного середовища.

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

Формул*: 0, рис.: 0, табл.: 0, бібл.: 11.*

Abstract*.The modern world is a highly dynamic phenomenon, leading to an intensification not only of opportunities but also of potential threats. Innovative technologies open new horizons for the development of business, education, and culture, significantly simplifying communication and access to information. At the same time, they create favorable conditions for cybercriminals, whose activities are becoming increasingly diverse and complex.*

Cybercrime encompasses a wide range of criminal offenses: from theft of personal data and financial fraud to attacks on critical infrastructure. The threats posed by cybercrime affect not only individuals, who may lose their savings or personal data, but also corporations, which may face operational disruptions, loss of client bases, and reputational damage. Furthermore, states are vulnerable to such actions, which can result in significant economic losses, compromise of national security, breaches of confidentiality of critical information, and destabilization of governance systems, which are fundamental to societal order and development.

In this context, there is an urgent need to improve the legal framework to address the challenges of the digital world, ensure effective prosecution of cybercriminals, and create conditions for international cooperation in the field of cybersecurity. It is also essential to enhance education in this area by introducing cybersecurity programs in schools, universities, and vocational institutions, as well as organizing regular training for employees of government institutions, businesses, and the general public. The development of information protection technologies, including the use of artificial intelligence, blockchain technologies, and improved encryption systems, should be prioritized in scientific research and innovation.

These measures are critically important because cybercrime is continuously evolving, becoming increasingly sophisticated, technically advanced, and unpredictable. The security of individuals, businesses, and institutions, as well as the stability of states, depends on the effectiveness of our response to emerging challenges and the timely implementation of preventive actions.

The article emphasizes the need for a comprehensive approach to countering cybersecurity challenges, enabling the creation of a favorable informational environment.

Keywords*: innovative technologies, crime, cybercrime, state, countering cybercrime.*

Formulas*: 0, fig.: 0, tabl.: 0, bibl.: 11.*

Постановка проблеми. Кіберзлочинність є однією з найбільших загроз сучасного інформаційного суспільства. Україна, як решта країн, зіштовхнулася з численними викликами у цій сфері. Поява новітніх технологій, інтенсифікація ролі Інтернету та глобалізація інформаційних систем сприяють розвитку різноманітних форм злочинності вимагає термінового реагування на правовому рівні. Такі трансформації детермінують адаптацію нормативно-правової бази та розробки ефективних механізмів протидії, що створять сприятливі безпечні умови для держави та для кожного її громадянина зокрема. За умов перманентного розвитку технологій важливо не лише визнати існуючі проблеми, а й проактивно вживати заходів для їх вирішення.

Аналіз останніх досліджень і публікацій здійснено на основі національних та міжнародних джерел, таких як закони України щодо кібербезпеки, європейські директиви, матеріали від кіберполіції, а також статті та аналітичні дані про кібератаки та заходи боротьби з кіберзлочинністю.

Не вирішені раніше проблеми загальної частини. Система кібербезпеки України включає суттєві прогалини в законодавстві, неузгодженість нормативно-правових актів, слабку міжвідомчу координацію та недостатню кваліфікацію персоналу, що не дозволяє ефективно реагувати на кіберзагрози.

Формулювання цілей статті. Виявлення ключових правових прогалин у сфері протидії кіберзлочинності в Україні та їх вплив на ефективність боротьби з кіберзлочинами.

Розробка рекомендацій щодо вдосконалення законодавчих ініціатив в Україні, орієнтуючись на європейський досвід. У результаті дана стаття має на меті не лише науковий аналіз, але й створення практичних рекомендацій, що можуть бути інтегровані задля інтенсифікації ефективності протидії кіберзлочинності як на національному, так і на європейському рівнях.

Виклад основного матеріалу. У сучасному світі кіберзлочинність грає роль

однієї з найбільших загроз для інформаційної безпеки як окремих країн, так і міжнародного співтовариства в цілому. Цей вид злочинності охоплює широкий спектр правопорушень, пов'язаних з використанням комп'ютерних технологій та мереж, включно, але не обмежуючись, кібератаками, шахрайством в Інтернеті, фішингом, розподіленими атаками типу «відмова в обслуговуванні» (DDoS) та викраденням особистих даних. Актуальність питання протидії кіберзлочинності зумовлена не лише зростанням кількості таких злочинів, але й їхнім впливом на економічну, соціальну та політичну стабільність країн.

Кіберзлочини можна дефініювати як злочини, що посягають на інформаційні системи та дані, завдаючи шкоди особам, організаціям і державам. Вони часто вимагають високого рівня технічних знань і можуть здійснюватися як окремими злочинцями, так і організованими групами, що використовують міжнародні зв'язки для укриття своїх дій. Це підкреслює необхідність міжнародної співпраці в боротьбі з кіберзлочинністю, оскільки правопорушники часто діють поза межами юрисдикції однієї країни.

Кіберзлочинність в Україні сьогодні є серйозною загрозою безпеці як окремих громадян, так і цілої держави. Як показує практика, нині одним із найпоширеніших видів кіберзлочинів є шахрайство в Інтернеті. Згідно даних, оприлюднених на офіційному сайті Кіберполіції Украни, протягом 2021 року до кіберполіції надійшло понад 48 тисяч звернень, що стосуються інтернет-шахрайства. Крім того, начальник відділу протидії різновидам онлайн-шахрайств Департаменту кіберполіції, Іван зауважив, що станом впродовж 2021 року було викрито та припинено діяльність 422 онлайн-аферистів, які фігурують у 2025 кримінальних провадженнях щодо вчинення шахрайств, пов'язаних з продажем товарів на популярних онлайн-маркетплейсах. Злочинна схема передбачала, що жертви замовляли й оплачували певну продукцію, але не отримували її [5].

Варто зазначити, що різкий ріст цін на Bitcoin та іншу криптовалюту наприкінці минулого року спричинив незначне збільшення кількості криптомайнерів. Це сталося вперше з жовтня 2018 року. За умови подальшого зростання попиту на криптовалюту такі шкідливі програми, фішинг та шахрайство з цифровою валютою знову наберуть популярності. Крім того, у 2020 році помітно зросла кількість цілеспрямованих атак програм-вимагачів, які вимагають платежі у криптовалюті, впливаючи цим самим на її ціну [9].

Поширеним видом кіберзлочинів є кібератаки. Так, 23 грудня 2015 року була здійснена так звана атака на «Прикарпаття обленерго», внаслідок якої було знеструмлено протягом кількох годин близько 30 підстанцій, і 230 тис. споживачів. Даного роду напад був реалізований завдяки зловмисному програмному забезпеченню, що деформувало роботу системи управління [10].

Іншою доволі серйозною актуальною проблемою є крадіжка особистих даних. Так, у червні 2017 року, відбулася масова кібератака з використанням вірусу, який спочатку був названий Petya. A, а згодом його ознаменували NotPetya. Вірус здійснював блокування комп'ютерних систем компаній, вимагаючи за розблокування 300 доларів у біткоїнах. Відповідно до даних Національного банку України, тоді кібернападу зазнала третина вітчизняних банківських установ, уряд, низка регіональних енергетичних організацій, логістична компанія «Нова пошта», редакції великих медіахолдингів та інші підприємства. Служба безпеки України повідомила, що зараження комп'ютерних систем розпочалося напередодні Дня Конституції України через використання шкідливого бухгалтерського програмного забезпечення та реалізовувалося в декілька етапів [7].

Неабиякого розмаху сьогодні набувають і випадки крадіжки інтелектуальної власності. Прикладом можуть слугувати ситуації викрадення комерційних таємниць компаній через зломи їхніх інформаційних систем, включно з технологіями та виробничими, що процесами, що мали місце у 2020 та демонструють різноманіття форм кіберзлочинності в Україні і підкреслюють важливість підвищення рівня кібербезпеки та обізнаності населення про загрози в цифровому середовищі [8].

У відповідь на ці виклики питання кіберзлочинності в Україні регулюється через низку законодавчих актів, міжнародних угод

і організаційних структур. Засадничим законодавчим актом у даній галузі є Кримінальний кодекс України, який містить статті, що визначають відповідальність за різні види кіберзлочинів, такі як несанкціонований доступ до інформаційних систем, зловживання даними та комп'ютерні шахрайства.

Своєю чергою Закон України «Про основи забезпечення кібербезпеки України» регулює питання кібербезпеки на державному рівні, окреслює перелік органів, що несуть відповідальність за створення умов кібербезпеки для громадян, а також основні принципи і механізми захисту інформаційних систем [1, 2]. Закон України «Про електронні довірчі послуги» регламентує правову базу використання електронних підписів та інших довірчих послуг, що є важливими для захисту інформації в електронному середовищі [3].

Варто зауважити, що наша держава є учасником кількох міжнародних угод, які регулюють питання кіберзлочинності. Так, зокрема Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція), встановлює міжнародні норми для боротьби з кіберзлочинністю та сприяє співпраці між державами. Існує також низка угод з Інтерполом, Європолом та іншими міжнародними правоохоронними організаціями, що забезпечують обмін інформацією та координацію зусиль у розслідуванні кіберзлочинів [5].

Щодо організаційної структури системи кібербезпеки нашої Вітчизни, то вагому роль тут відіграє Кіберполіція України як спеціалізований підрозділ Національної поліції, що займається розслідуванням кіберзлочинів, аналізом загроз та реалізацією заходів з протидії кіберзлочинності. Окремо також слід виокремити Державну службу спеціального зв'язку та захисту інформації України, яка відповідає за забезпечення умов кібербезпеки державних інформаційних систем та загалом захист інформації.

Національна програма кібербезпеки включає плани та заходи для зміцнення захисту інформаційних систем і підвищення обізнаності населення про кіберзагрози. Таким чином, регулювання кіберзлочинності в Україні передбачає комплексний підхід, що включає законодавчі, міжнародні та організаційні аспекти [6]. Однак, попри ці зусилля, реалізація норм у сфері кібербезпеки стикається з низкою правових проблем, які потребують термінового вирішення. Аналіз основних правових проблем у сфері кібербезпеки в Україні виявляє кілька ключових аспектів. Насамперед помітними є істотні прогалини у законодавстві: чинні норми не здатні охопити усі аспекти кіберзагроз, що, своєю чергою, ускладнює або взагалі унеможливлює діяльність державних установ. Спостерігається також певна неузгодженість нормативно-правових актів, що доволі часто призводить до плутанини у виконанні обов'язків.

Слабка координація між відомствами ускладнює реагування на кіберінциденти, підвищуючи ризики затримок у вжитті заходів. Багато установ стикаються з обмеженнями в ресурсах і фінансуванні, що заважає модернізації технологій та навчання персоналу. Крім того, наявні закони не завжди легко реалізувати через недостатню кваліфікацію правоохоронців. Усі ці чинники створюють складну ситуацію для державних установ і підкреслюють термінову необхідність вдосконалення правового поля в цій сфері.

Для покращення ситуації в Україні необхідно адаптувати європейські практики, вдосконалити законодавство, забезпечити міжвідомчу співпрацю та активно впроваджувати навчальні програми в сфері кібербезпеки. Також рекомендується розробити та впровадити стандартні процедури реагування на кіберінциденти, які були б зрозумілі та прийняті як державними, так і приватними структурами. Це дозволить зменшити час реагування на загрози та підвищити ефективність дій. Розвиток національної стратегії кібербезпеки має стати пріоритетом, що дозволить Україні зміцнити свою позицію в глобальному кіберпросторі. Лише спільними зусиллями держави, приватного сектору та суспільства можна досягти стійкості до кіберзагроз і забезпечити безпеку інформаційних систем у майбутньому.

Література:

1.Закон України «Про основні засади забезпечення кібербезпеки України». Закон України від 5 жовтня 2017 року № 2163-VIII. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19

(дата звернення: 21.08.2024).

2.Закон України «Про боротьбу з кіберзлочинністю». Закон України від 24 січня 2018 року № 2213-VIII. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2213-19 (дата звернення: 21.08.2024).

3.Закон України «Про електронні довірчі послуги». Закон України від 5 жовтня 2017 року № 2155-VIII: станом на 1 січ. 2024 р. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 21.08.2024).

4.Директива Європейського Парламенту та Ради 2013/40/ЄС Директива Європейського Парламенту та Ради від 12 серпня 2013 року про атаки на інформаційні системи. URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32013L0040 (дата звернення: 21.08.2024).

5.Кіберполіція України. (2023). Кіберполіція припинила діяльність 422 онлайн-аферистів, які фігурують у 2025 кримінальних провадженнях щодо вчинення шахрайств. URL: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-prypynyla-diyalnist--onlajn-shaxrayiv-6518/ (дата звернення: 21.08.2024).

6.Національна стратегія кібербезпеки України на 2021-2025 роки Національна стратегія кібербезпеки України на 2021-2025 роки. КМУ. URL: https://www.kmu.gov.ua/en/news/tsilova-natsionalna-strategiya-kiberbezpeky-ukrayini-na-2021-2025-roki (дата звернення: 21.08.2024).

7.Радіо Свобода. (2017). Кібератака NotPetya: як це було. URL: https://www.radiosvoboda.org/a/29336511.html# (дата звернення: 21.08.2024).

8.Укрінформ. (2020). Кібератаки в Україні: викрадення комерційних таємниць. URL: https://www.ukrinform.ua/tag-kiberataka (дата звернення: 21.08.2024).

9.ESET. (2020). Рейтинг інтернет-угроз: Україна в лідерах по кількості шкідливих програм для Android. URL: https://salo.li/11bD5ad (дата звернення: 21.08.2024).

10. The Kernel. (2015). Як захистити енергетичну інфраструктуру від кібератак. URL: https://salo.li/08F0e77 (дата звернення: 21.08.2024).

References:

1.Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine». Law of Ukraine dated October 5, 2017 No. 2163-VIII. - Official website of the Verkhovna Rada of Ukraine: https://zakon.rada.gov.ua/laws/show/2163-19 (Accessed August 21, 2024).

2.Law of Ukraine «On Combating Cybercrime». Law of Ukraine of January 24, 2018 No. 2213-VIII. Official website of the Verkhovna Rada of Ukraine: https://zakon.rada.gov.ua/laws/show/2213-19 (Accessed August 21, 2024).

3.Law of Ukraine «On Electronic Trust Services». Law of Ukraine dated October 5, 2017 No. 2155-VIII: as of January 1, 2024. 2024 Official website of the Verkhovna Rada of Ukraine - Access mode: https://zakon.rada.gov.ua/laws/show/2155-19#Text (Accessed August 21, 2024).

4.Directive 2013/40/EU of the European Parliament and of the Council Directive of the European Parliament and of the Council of August 12, 2013 on attacks on information systems: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32013L0040 (Accessed August 21, 2024).

5.Cyberpolice of Ukraine (2023). Cyberpolice stopped the activities of 422 online scammers involved in 2025 criminal proceedings for committing fraud. Access mode: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-prypynyla-diyalnist--onlajn-shaxrayiv-6518/ (Accessed August 21, 2024).

6.National Cybersecurity Strategy of Ukraine for 2021-2025. National Strategy of Cybersecurity of Ukraine for 2021-2025. CMU. Access mode: https://www.kmu.gov.ua/en/news/tsilova-natsionalna-strategiya-kiberbezpeky-ukrayini-na-2021-2025-roki (Accessed August 21, 2024).

7.Radio Liberty (2017). NotPetya cyberattack: how it happened. Access mode: https://www.radiosvoboda.org/a/29336511.html# (Accessed August 21, 2024).

8.Ukrinform (2020). Cyberattacks in Ukraine: theft of trade secrets. [Electronic resource]. Access mode: https://www.ukrinform.ua/tag-kiberataka (accessed on August 21, 2024).

9.ESET. (2020). Rating of Internet threats: Ukraine is in the lead in the number of malicious programs for Android. Access mode: https://salo.li/11bD5ad (Accessed August 21, 2024).

10. The Kernel (2015). How to protect energy infrastructure from cyberattacks. Access mode: https://salo.li/08F0e77 (Accessed August 21, 2024).

Стаття надійшла до друку 25 серпня 2024 року