УДК 343.9
DOI https://doi.org/10.51989/NUL.2022.6.2.6

ЄВРОПЕЙСЬКИЙ ДОСВІД ПОДОЛАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ В УМОВАХ СЬОГОДЕННЯ

Лугіна Наталія Анатоліївна,
кандидат юридичних наук, доцент, доцент кафедри
кримінальної юстиції
Навчального-наукового інституту права
Державного податкового університету
м. Ірпінь, Україна

Бойко Валерія Володимирівна,
здобувач першого (бакалаврського) рівня вищої освіти
Навчального-наукового інституту права
Державного податкового університету
м. Ірпінь, Україна

У статті проаналізовано таке явище, як кіберзлочинність в Україні, вплив кібератак на економічний стан держави та стан національної безпеки. Досліджено сучасний глобальний характер проблеми кіберзлочинності, оскільки сучасні кібератаки паралізують не лише приватні структури, а й органи державної влади. Виявляється, що від подібних атак не застрахована жодна країна світу, а суб'єктами, які їх здійснюють, є не лише окремі хакери чи хакерські групи, а й окремі держави, терористи та організовані злочинні угруповання, зокрема й міжнародні. Розроблено особливості правового регулювання боротьби з кіберзлочинністю з урахуванням організаційних аспектів цієї боротьби, а також визначено основні організаційно-правові засади вдосконалення боротьби з кіберзлочинністю в Україні. Розглянуто низку ймовірних способів вирішення цього питання шляхом євроінтеграційних процесів.

Проаналізовано міжнародні ініціативи, реалізовані для посилення захисту кіберпростору. Досліджено міжнародно-правову систему норм, спрямованих на створення правової основи співпраці держав у боротьбі з кіберзлочинністю. У цьому розділі розглянуто основні нормативно-правові практики та міжнародні документи, а також визначено способи вдосконалення правового регулювання на майбутнє. Доведено, що національна безпека дуже залежить від інформаційної безпеки і ця залежність лише посилюється з технологічним розвитком. Об'єктом пильної уваги та впливу держави є інформація, яка є економічною та соціальною гарантією існування та розвитку суспільства і держави. Глобальність кіберзлочинності очевидна в усьому світі, особливо в Україні. Деталізовано керівні принципи модернізації політики захисту даних на рівні ООН.

Визначено пріоритети міжнародного співробітництва у забезпеченні кібербезпеки між Україною та НАТО. Тож у сьогоднішньому контексті ситуація навколо майбутнього глобального кіберпростору перебуває на перетині двох паралельних тенденцій: з одного боку, офіційні зусилля міжнародної спільноти роззброїти кіберпростір і запобігти його перетворенню на нову арену збройного конфлікту, а з іншого – основний процес полярного конфлікту триває.

Ключові слова: *кіберзлочинність, кібератака, кібервійна РФ проти України, протидія кіберзлочинам, міжнародна співпраця протидії кіберзлочинам, НАТО як основний регулятор вирішення кіберзлочинності у співпраці з Україною.*

Nataliia Luhina, Boyko Valeria. European experience of overcoming cybercrime in Ukraine in today's conditions

The article analyzes such a phenomenon as cybercrime in Ukraine, the impact of cyberattacks on the economic state of the state and the state of national security. The modern global nature of the problem of cybercrime is studied, since modern cyberattacks paralyze not only private

structures, but also state authorities. It turns out that no country in the world is immune from such attacks, and the subjects that carry them out are not only individual hackers or hacker groups, but also individual states, terrorists and organized criminal groups, including international ones. The peculiarities of the legal regulation of the fight against cybercrime have been developed, taking into account the organizational aspects of this fight, and the main organizational and legal principles of improving the fight against cybercrime in Ukraine have also been defined. A number of possible ways of solving this issue through European integration processes were considered.

International initiatives implemented to strengthen cyberspace protection are analyzed. The international legal system of norms aimed at creating a legal basis for the cooperation of states in the fight against cybercrime has been studied. In this section, the main regulatory and legal practices and international documents are considered, as well as the ways of improving legal regulation for the future are determined. It has been proven that national security is highly dependent on information security, and this dependence only increases with technological development. The object of close attention and influence of the state is information, which acts as an economic and social guarantee for the existence and development of society and the state. The global nature of cybercrime is evident all over the world and especially in Ukraine. The guiding principles of the modernization of data protection policy at the UN level are detailed.

The key priorities of international cooperation in ensuring cyber security between Ukraine and NATO have been determined. So in today's context, the situation surrounding the future of global cyberspace is at the intersection of two parallel trends. On the one hand, the official efforts of the international community to disarm cyberspace and prevent it from turning into a new arena of armed conflict, while the main process of polar conflict continues.

Key words: *cybercrime, cyberattack, cyberwar of the Russian Federation against Ukraine, combating cybercrime, international cooperation in combating cybercrime, NATO as the main regulator of solving cybercrime in cooperation with Ukraine.*

Виникнення криз унаслідок загострення політичних конфліктів, що призводить до воєнних реалій, є негативним явищем у будь-якій економіці, незалежно від її розвитку чи регіональної актуальності. Тим паче, коли основним завданням є підрив державної безпеки України та деморалізації нації будь-яким способом, тому злочинці провадять свою діяльність через кібервтручання. Крім того, причини криз, а також масштаби і глибина поширення безпосередньо пов’язані з політикою, яку провадить конкретна держава. Саме цей політичний аспект призводить до найнебезпечніших наслідків у всіх сферах функціонування держави, пов’язаних із ліквідацією або розв’язанням різних військових конфліктів.

Кризи, які є результатом переходу від нормального стану до військового, є глибокими і тривалими та впливають на економічну, фінансову, соціальну та навіть демографічну сфери.

В епоху інформаційних технологій безпеці у віртуальному просторі слід приділяти велику увагу. Однак зі швидкими темпами науково-технічного розвитку людське суспільство переміщує багато сфер суспільного життя у кіберпростір, що надає широкі можливості злочинцям здійснювати свою протиправну діяльність. Ураховуючи курс України на входження у світовий інформаційний простір, ми переконані у необхідності створення національної моделі забезпечення кібербезпеки держави, громадян, а також підприємств, установ та організацій. Він потребує координації зусиль правоохоронних органів, судової системи, спеціальних служб, а також їх відповідного кадрового та матеріально-технічного забезпечення [1, с. 595].

У сучасному контексті внутрішньо- та зовнішньополітичні успіхи країн визначаються не лише військовою та економічною могутністю, а й успішністю встановлення реального контролю над вітчизняними інформаційно-культурними процесами. Невдачі у сфері інформаційних технологій стають серйозною глобальною загрозою безпеці, оскільки створюють реальні можливості для використання інтелектуального потенціалу інших країн у власних цілях, для поширення їхніх ідеологічних цінностей, культури, мови та реалізації. Це гальмує духовний і культурний розвиток інших країн. Для досягнення своїх політичних цілей держави все більше почали використовувати методи інформаційної війни.

Висока активність росії в кіберпросторі є головним викликом і загрозою для України у сфері кібербезпеки. Російська федерація використовує кіберпростір як місце нових можливостей для ведення не лише розвідувально-підривної діяльності проти України, а й спеціальних операцій із прихованого доступу до кібермереж органів державної влади та управління, до об'єктів критичної інфраструктури та встановлення контролю над ними для отримання вигоди та захисту своїх інтересів в інформаційній, військовій, політичній, фінансово-економічній, енергетичній сферах. Загальновідомо, що росія розробила зразки кіберзброї для нейтралізації та виведення з ладу об'єктів критичної інфраструктури противника з метою підвищення ефективності майбутнього першого удару або максимального послаблення їх здатності протистояти. Однак таку кіберзброю неможливо стримати.

Після початку збройної агресії росії проти України компанії, що спеціалізуються на наданні послуг із кібербезпеки, зафіксували зростання кількості кібератак на інформаційні системи країни. Як правило, кібератаки спрямовані на таємне викрадення важливої інформації, найімовірніше, щоб дати росії стратегічну перевагу на полі бою. Жертвами російських кібератак стали державні установи України, країни ЄС, США, міністерства оборони, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, ЗМІ та дисиденти [2].

З початком російсько-української війни почали з'являтися антиукраїнські хактивістські загони, які називали себе «Кіберберкут» та проукраїнська «Майдан Кіберсотня», «Анонімі» з російською чи українською «пропискою». Незважаючи на труднощі у визначенні ступеня співпраці хакерських угруповань із державними органами, на основі зібраних доказів можна стверджувати, що на території росії діють проросійські хакерські угруповання, які ведуть свою діяльність у росії на користь Кремлівського режиму [2].

Можна стверджувати, що з початку російсько-українського конфлікту дослідники кібербезпеки покращили свою здатність виявляти, відстежувати та захищати від російських хакерських груп. Серед можливих пояснень можна виокремити той факт, що із загостренням конфлікту російські хакери не встигають своєчасно оновлювати та вдосконалювати тактику, технології та методи роботи[2].

23 лютого 2022 року, за день до масованого вторгнення росії в Україну, була зафіксована кібератака на державні ресурси та банки [3]. О 16:00 почалася нова хвиля кібератак, скомпрометовано сайти Верховної Ради, Кабінету міністрів України та МЗС. Міністерство освіти і науки заблокувало доступ до свого сайту, щоб запобігти кібератаці. За словами міністра цифрової трансформації Федорова, портал і сайт застосунку «Дія» успішно протистоять атаці [4]. Пізніше з'ясувалося, що також були зламані сайти СБУ, Міністерства стратегічних галузей промисловості, інфраструктури та агрополітики. Речниця Білого дому Джен Псакі під час брифінгу заявила, що наразі невідомо, хто стоїть за нападами, але попередні напади узгоджувалися з діями російської федерації [5]. Представники рф вважають «русофобськими» будь-які коментарі про причетність росії до кібератак [6].

Згідно з дослідженням ESET, після DDoS-атаки 23 лютого на зламаних сайтах був активований програмний інструмент Hermetica Viper, названий на честь сертифіката підпису цифрового коду від кіпрської компанії Hermetica Digital Ltd. Мета цих шкідливих програм – знищити дані із бази даних. Вірус виявили 23 лютого близько 17:00, але на хронології встановлено 28 грудня 2021 року[7].

Уночі та вранці 24 лютого 2022 року під час російської атаки на Україну сайт Київської ОДА зазнав хакерської атаки, деякі ресурси було відключено для захисту інформації [8]. На сайтах i.ua та meta.ua Держспецзв'язку виявила масові розсилки з фішинговими покликаннями на особисті адреси українських військовослужбовців та пов'язаних із ними осіб [9]. Зловмисники використовують протоколи IMAP, щоб компрометувати адреси інших електронних адрес і завантажувати електронну пошту. За даними агентства, за цим стоять білоруські хакери з групи UNC1151, яка діє в Мінську і налічує офіцерів Міноборони Республіки Білорусь [9].

Тенденція зростання кіберзлочинності та тенденція соціального та правового контролю над нею створює величезну загрозу цивілізованому світу, з якою можна боротися лише через органічне поєднання кримінально-правових та криміналістичних стратегій. Крім того, важливою частиною такої стратегії має стати більш прозора та активна міжнародна співпраця у цій сфері, оскільки вже зараз зрозуміло, що контролювати міжнародну частину кіберзлочинності та кібертероризму на рівні окремих держав неможливо. Власне, цей комплекс проблем має терміново вирішувати міжнародне співтовариство у XXI столітті.

Виходячи з теоретичних основ чинного закону, Україна, відповідно до укладених нею міжнародних договорів, співпрацює з іноземними державами у сфері кібербезпеки, їх збройними силами, правоохоронними органами та спецслужбами, здебільшого із членами НАТО та ЄС. Інформація з питань забезпечення кібербезпеки, боротьби з міжнародною кіберзлочинністю та кібертероризмом передається Україною іноземній державі на підставі міжнародних договорів. Цей формат охоплює широкий спектр нормативних, методичних, практичних, науково-освітніх питань, організацію актуальних міжнародних семінарів і конференцій, надання методичної та практичної допомоги іноземним партнерам, робочі відносини з провідними фахівцями у сфері кібербезпеки. Містить налаштування, вивчення та впровадження кращих практик кібербезпеки на батьківщині має позитивні результати.

Таким чином, міжнародне співробітництво є важливим моментом у подоланні правового розриву, який існує між динамічним розвитком інформаційних технологій і законодавчою реакцією на сучасні кіберзагрози. Міжнародне співробітництво здійснюється з метою: зміцнення взаємної довіри у сфері кібербезпеки; розробки спільних стратегій боротьби з кіберзагрозами; посилення зусиль у розслідуванні та запобіганні кіберзлочинам, запобігання використанню кіберпростору в протиправних цілях; виконання Україною зобов'язань за міжнародними договорами в частині співробітництва у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами та спеціальними службами, а також міжнародними організаціями; надання міжнародної технічної допомоги [10, с. 52].

Розвиток є одним із фундаментальних аспектів безпекової політики України. Конструктивне партнерство з НАТО на основі стандартів протидії сучасним викликам і загрозам, досягнення провідних стандартів України в обороноздатності. У межах розвитку міжнародного співробітництва у сфері кібербезпеки для України особливе значення має партнерство з НАТО, що є важливою частиною євроінтеграційного курсу, оскільки воно супроводжується необхідними реформами оборонного та безпекового секторів та внутрішніми змінами. Розроблене в такому форматі навчання є підготовкою до щорічного затвердження на державному рівні національної програми співпраці Україна-НАТО.

21–23 березня 2021 року під час офіційного візиту голови Верховної Ради України Д. Разумкова до Бельгії було оголошено, що реалізація курсу спрямована на прискорення реформ у військовій та безпековій сферах. Принципи та стандарти НАТО є пріоритетними для України. Тому визнання України стратегічним партнером НАТО з високим потенціалом є важливим кроком для реалізації євроатлантичних прагнень України. Голова Верховної Ради також наголосив, що завдання альянсу та України – відновити формат засідань комісії Україна – НАТО на найвищому рівні. За таких обставин можна сказати з упевненістю, що Євроатлантична інтеграція є пріоритетом зовнішньої та безпекової політики України.

На міжнародному рівні проблема забезпечення кібербезпеки з кожним роком зростає та постійно актуалізується перед міжнародною спільнотою та політичним керівництвом України.

Таким чином, у міжнародному кіберпросторі, незважаючи на мирне використання та повне роззброєння міжнародної спільноти, є конфлікт і протистояння між групами держав (США, російська федерація, КНР), що мають на меті довести свою домінувальну позицію та лідерство в кіберпросторі, який сьогодні є конкурентною ареною, щоб показати свою силу

та першість. Ураховуючи вищезазначене, можна сказати, що міжнародне співробітництво у сфері кібербезпеки здійснюється переважно в організаційно-правових формах та має вагоме значення для національної безпеки України.

ЛІТЕРАТУРА:

1. Дулепа В.П. Кримінологічна характеристика кіберзлочинності. *Юридичний науковий електронний журнал*. 2011. № 11. С. 592–595.

2. Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO CCD COE Publications. ISBN 978-9949-9544-5-2. URL: https://web.archive.org/web/20160816132103/https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html (дата звернення: 10.09.2022).

3. Державна служба спеціального зв'язку та захисту інформації України. «Чергова кібератака на сайти державних органів та банки» URL: https://cip.gov.ua/ua/news/chergova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki (дата звернення: 10.09.2022).

4. Укрінформ «Сайти банків та органів влади зазнали масової DDoS-атаки». URL: https://www.ukrinform.ua/rubric-technology/3410542-sajti-bankiv-ta-organiv-vladi-zaznali-masovoi-ddosataki.html (дата звернення: 10.09.2022).

5. Укрінформ «Штати пов'язують останні кібератаки в Україні з діями РФ – Білий дім». URL: https://www.ukrinform.ua/rubric-polytics/3410802-stati-povazuut-ostanni-kiberataki-v-ukraini-z-diami-rf-bilij-dim.html (дата звернення: 10.09.2022).

6. Ukraine: EU deploys cyber rapid-response team. *BBC News* (en-GB). URL: https://www.bbc.com/news/technology-60484979 (дата звернення: 10.09.2022).

7. HermeticWiper: New data-wiping malware hits Ukraine. *WeLiveSecurity.* URL: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/ (дата звернення: 10.09.2022).

8. Сайт Київської ОДА атакують хакери. *www.ukrinform.ua.* URL: https://www.ukrinform.ua/rubric-technology/3411812-sajt-kiivskoi-oda-atakuut-hakeri.html (дата звернення: 10.09.2022).

9. Email-адреси українських військових атакують хакери. *www.ukrinform.ua* (укр.). URL: https://www.ukrinform.ua/rubric-technology/3412829-emailadresi-ukrainskih-vijskovih-atakuut-hakeri.html (дата звернення: 10.09.2022).

10. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України*. *Серія: «Державне управління».* URL: http://nbuv.gov.ua/UJRN/Vnadu_2015_4_10 (дата звернення: 10.09.2022).