УДК 342.951

ЖЕРЕБЕЦЬ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-2059-2045.

РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ЗАКОНОДАВЧИЙ АСПЕКТ

Анотація. *У статті розглядаються актуальні питання реалізації державної політики у сфері протидії кіберзлочинності. Розкриваються сутність, ознаки та види кіберзлочинів. Виокремлюються напрями протидії кіберзлочинності на концептуальному, законодавчому та інституціональному рівнях. Виявляються недоліки імплементації положень Конвенції про кіберзлочинність у чинне законодавство України. Пропонуються шляхи підвищення ефективності протидії кіберзлочинності.*

Ключові слова: *кіберзагроза, кіберзлочинність, кіберзлочин, протидія, законодавство.*

Summary. *The article considers topical issues of state policy implementation in the field of combating cybercrime. The essence, signs and types of cybercrimes are revealed. Areas of combating cybercrime at the conceptual, legislative and institutional levels are identified. The shortcomings of the implementation of the provisions of the Convention on Cybercrime in the current legislation of Ukraine are revealed. Ways to increase the effectiveness of combating cybercrime are proposed.*

Keywords*: cyberthreat, cybercrime, counteraction, legislation.*

Аннотация. *В статье рассматриваются актуальные вопросы реализации государственной политики в сфере противодействия киберпреступности. Раскрываются сущность, признаки и виды киберпреступлений. Выделяются направления противодействия киберпреступности на концептуальном, законодательном и институциональном уровнях. Выявляются недостатки имплементации норм Конвенции о киберпреступности в действующее законодательство Украины. Предлагаются пути повышения эффективности противодействия киберпреступности.*

Ключевые слова: *киберугроза, киберпреступность, киберпреступление, противодействие, законодательство.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій створює умови для появи нових ризиків та кіберзагроз. Незважаючи на позитивний вплив на всі сфери людського життя, цей розвиток зумовив зростання й поширення кіберзлочинів. З упевненістю можна сказати, що кіберзлочини – це одна з основних проблем XXI ст., вирішення якої потребує сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування [1].

Як на міжнародному, так і національному рівні кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами. До цього часу не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці [2].

Оцінки загроз кіберзлочинності національній безпеці окремих держав та міжнародному порядку визначають, що: 1) це небезпечна тенденція, пов'язана зі збільшенням технико-технологічної залежності держави від транскордонних проявів кібертерористів;

2) комп'ютерні атаки практично неможливо прогнозувати або прослідкувати в реальному часі [3, с. 10].

Отже, протидія кіберзлочинності на сьогодні є одним з пріоритетних напрямків забезпечення національної безпеки держави.

Результати аналізу наукових публікацій. У вітчизняній юридичній літературі науковим розвідкам окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як В. Брижко [4], В. Бутузов [5], С. Лівчук, О. Петровський [6], В. Пилипчук, В. Сірко [7], А. Тарасюк [8], А. Марущак [9], М. Швець [4], О. Юрченко та інші. Водночас ефективність протидії кіберзлочинності зумовлює необхідність вжиття додаткових заходів на законодавчому та організаційному рівнях.

Метою статті є аналіз реалізації державної політики у сфері протидії кіберзлочинності та вироблення шляхів її удосконалення.

Виклад основного матеріалу. У Законі України "Про основні засади забезпечення кібербезпеки України" кіберзлочинність розуміється як сукупність кіберзлочинів, а кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [10].

Сутність кіберзлочинів або ІТ-злочинів полягає в тому, що це протиправні суспільно небезпечні діяння, тобто злочини, під час яких використовується інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача [3, с. 11].

Центральне місце на національному рівні в механізмі правового регулювання боротьби з такими злочинами займають норми: Європейської Конвенції про взаємну правову допомогу у кримінальних справах 1959 р. (ратифікована із застереженнями і заявами Законом України від 16.01.98 р. № 4498-ВР), Конвенції Ради Європи про кіберзлочинність від 23 листопаду 2001 року (ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV), Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 року (ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV), загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору [3, с. 17].

Відповідно до Конвенції про кіберзлочинність кіберзлочини поділяються на наступні категорії:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (так звані "CIA-злочини"), зокрема:

незаконний доступ, наприклад, шляхом злому, обману і іншими засобами;

нелегальне перехоплення комп'ютерних даних;

втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

втручання у систему, включаючи навмисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на критичну інформаційну інфраструктуру;

зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою здійснення "CIA-злочинів";

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія;

4) правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад, незаконне відтворення і використання комп'ютерних програм, аудіо/відео і інших видів цифрової продукції, а також баз даних і літератури

5) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем[11].

Згадана Конвенція (ратифікована 58 державами, серед яких усі держави-члени Ради Європи (за винятком Російської Федерації) й такі, що не входять до Європейської спільноти, зокрема Канада, Ізраїль, США, Японія та країни Південної Америки) – це договір, згідно з яким держави, що до неї приєдналися, узяли на себе зобов'язання відносно зближення між собою внутрішньодержавних положень кримінального права щодо кіберзлочинів та створення можливостей для застосування ефективних засобів розслідування таких правопорушень [3, с. 17]. Тому Конвенцією прямо передбачено заходи, що мають здійснюватися на національному рівні в матеріальному кримінальному праві (ч. 1 розділ 2) й кримінально-процесуальному (так званому "процедурному") праві (ч. 2 розділ 18), а також систему міжнародного співробітництва (розділ 3) та питання юрисдикційного характеру (ч. 3 розділ 2) [3, с. 17-18]. Зазначене зумовлює потребу завершення процесу імплементації положень цієї Конвенції в чинне законодавство України, що є одним із напрямів реалізації державної політики у сфері протидії кіберзлочинності.

Виокремити інші напрями протидії кіберзлочинності дуже складно через багатогранність цього соціального явища [12, с. 34-35]. В юридичній літературі виділяють два основних напрямки [7, с. 104]. До першого напряму відносять: попередження кіберзлочинності, що передбачає створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного і програмного захисту інформації; створення спеціалізованих організаційних структур організацій і служб кібербезпеки, спрямованих на забезпечення надійного функціонування засобів захисту, генерація ключів і паролів, контроль щодо їх використання, зміні й знищенню. Другий напрямок протидії кіберзлочинності містить виявлення і попередження кіберзлочинів. Нині проблема кінцевого вирішення організації ефективної взаємодії та координації суб'єктів протидії кіберзлочинності знаходиться на стадії завершення. Саме багатогранність суб'єктів протидії кіберзлочинності передбачає багаторівневу координацію їх діяльності [7, с. 104]. Питанням кібербезпеки сьогодні опікуються різноманітні суб'єкти забезпечення кібербезпеки: Державна служба спеціального зв'язку і захисту інформації, Служба безпеки України, Міністерство внутрішніх справ, Національний банк. Водночас, цілісна політика у цій сфері поки що відсутня, як і універсальні індикатори кібербезпеки, що могли б охарактеризувати її рівень [13].

Для ефективної боротьби з кіберзлочинністю в Україні, за прикладом зарубіжних країн, варто було б: створити політичне підґрунтя (концептуальний рівень), удосконалити систему законодавства (законодавчий рівень), визначити систему органів, основними функціями яких було б забезпечення кіберзахисту України (інституціональний рівень) [6, с. 54]. Перші кроки у напрямку формування політичного підґрунтя (концептуальний рівень) та системи суб'єктів забезпечення кібербезпеки (інституціональний рівень) відбулися ще у 2016 році. Зокрема на концептуальному та інституціональному рівні:

- у березні 2016 року Урядом України схвалено Стратегію кібербезпеки України, яка мала на меті створення національної системи кібербезпеки;
- у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки. Першим етапом його роботи стало здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки;
- у вересні 2016 року Верховна Рада України у першому читанні прийняла Закон "Про основні засади забезпечення кібербезпеки України" [13].

Розпорядженням Кабінету Міністрів України від 10.03.17 р. № 155-р "Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України" було затверджено заходи, спрямовані на: удосконалення нормативно-правового регулювання кібербезпеки; створення технологічної складової національної системи кібербезпеки; налагодження більш тісного співробітництва з міжнародними партнерами України; налагодження процесу підготовки кадрів у сфері кібербезпеки [14].

Із введенням 14 вересня 2020 року в дію нової Стратегії національної безпеки України було дано старт і підготовці проектів низки стратегічних документів, одним з яких є Стратегія кібербезпеки України, яку було затверджено Указом Президента України від 26.08.21 р. № 447 [15]. У цій Стратегії зазначається, що подолання негативної ситуації, що склалася у світі й в Україні з кіберзлочинністю, потребує спільних скоординованих дій світового співтовариства, усунення суперечностей між законодавством різних країн.

Важливим є і врахування у новій Стратегії базових стратегічних засад, визначених (ст. 4) у Стратегії національної безпеки України 2020 року – стримування, стійкості та взаємодії [16].

Відповідно до Стратегії для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є: посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування) [15].

Кіберстійкість, у свою чергу, передбачає спроможність всіх суб'єктів кібербезпеки своєчасно ідентифікувати загрози кібербезпеці, розбудовувати захист, впроваджувати інструменти виявлення кібератак, забезпечувати належну реакцію на них та швидко відновлювати стабільну роботу під час та після кібератак [16].

Для формування потенціалу стримування необхідним є досягнення стратегічних цілей Стратегії, серед яких заслуговує на увагу ціль С.3, яка сформульована так: "Ефективна протидія кіберзлочинності – Україна має забезпечити набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів" [15].

Проголошується, що для досягнення цієї цілі Україна посилить спроможності у протидії кіберзлочинності шляхом:

завершення імплементації в законодавство України положень Конвенції про кіберзлочинність;

врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав-членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки;

розроблення концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей);

запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних веб-сайтах;

проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати та реагувати на кіберзагрози;

забезпечення підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів;

забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів;

залучення приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів [15].

Підвищить ефективність розслідування кіберзлочинів імплементація у вітчизняне законодавство статей 16 – 18 Конвенції про кіберзлочинність, а саме невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сайту, веб-сторінки, тощо) із забезпеченням їх цілісності [9, с. 130]. Потребують впровадження у вітчизняне законодавство норми статті 19 (Обшук і арешт комп'ютерних даних, які зберігаються) Конвенції про кіберзлочинність шляхом закріплення можливості копіювати електронні дані, здійснювати їх пошук, а також їх блокувати/арештовувати.

Відповідні процесуальні дії доцільно здійснювати на підставі ухвали слідчого судді, суду, а фактичні дані, отримані подібними способами вважати допустимими доказами у кримінальному провадженні [9, с. 130].

Висновки.

Урахування прогресивного та ефективного міжнародно-правового досвіду у сфері протидії кіберзлочинності є вкрай необхідним для розробки національної системи заходів забезпечення кібербезпеки.

Для досягнення проголошених у Стратегії [15] цілей в контексті підвищення ефективності протидії кіберзлочинності доцільно:

завершити імплементацію в чинне законодавство України положень Конвенції про кіберзлочинність, зокрема, шляхом встановлення відповідальності за: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних;

провести чітке розмежування повноважень суб'єктів забезпечення кібербезпеки;

підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів, які використовуються для здійснення кіберзлочинів;

підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів, як це передбачено положеннями Стратегії [15].

Використана література

2. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606

3. Леонов Б.Д., Серьогін В.С. Поняття кіберзлочинності: дискусія триває: матеріали наук.-практ. конф. *Актуальні питання кримінального права,* м. Київ, 20 жовт. 2019 р. Київ: КНУВС, 2019.

4. Самойленко О.А. Протидія кіберзлочинам: криміналістичний аспект: навчально-методичний посібник. Одеса, 2020. 133 с.

5. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, доктора економічних наук, професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

6. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ, 2010. 148 с.

7. 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.

8. Сірко В.С. Організаційно-правові питання протидії кіберзлочинності. *Право*. 2020. № 2 (68). С. 103-105.

9. Тарасюк А.В. Кібербезпека на сучасному етапі державотворення: теоретико-правові основи: монографія. Київ-Одеса: Фенікс, 2020. 404 с.

10. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право.* № 1(24)/2018. С. 127-132.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

12. Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime, concerning 455 the criminalisation of acts of a racist and xenophobic nature committed through 456 computer systems. URL:https://rm.coe.int/168008160f

13. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний університет "ІДМУ", 2003. 296 с.

14. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: https://www.gurt.org.ua/articles/34602/.

15. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 10.03.17 р. № 155-р. URL: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80#Text

16. 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. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

17. Дубов Д. Формуючи нову стратегію кібербезпеки України: чи можемо уникнути помилок першої спроби стратегування? – (Аналітична доповідь). URL: https://niss.gov.ua/doslidzhennya/informaciyna-politika/formuyuchi-novu-strategiyu-kiberbezpeki-ukraini-chi-zmozhemo

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~