УДК 343.8
DOI https://doi.org/10.24144/2788-6018.2025.03.2.60

ІМПЛЕМЕНТАЦІЯ ЗАРУБІЖНОГО ДОСВІДУ В УКРАЇНСЬКЕ ЗАКОНОДАВСТВО ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Захаревич Р.В.,
аспірант кафедри кримінального права та процесу,
Державний податковий університет
ORCID: 0009-0003-3783-9715

Захаревич Р.В. Імплементація зарубіжного досвіду в українське законодавство щодо протидії кіберзлочинам.

Стаття присвячена дослідженню можливості та шляхів імплементації зарубіжного досвіду в українське законодавство щодо протидії кіберзлочинам.

Встановлено, що проблематика протидії кіберзлочинності набуває особливої важливості в умовах запровадження воєнного стану. Сучасні інформаційні війни здатні завдати шкоди, співмірної або навіть більшої за ту, що спричиняється збройними конфліктами на полі бою. У зв'язку з цим суб'єкти, відповідальні за протидію кіберзлочинам, повинні вживати всіх можливих заходів для мінімізації кібератак, здійснюваних противником.

Зазначено, що одним із ключових напрямів удосконалення національної правової системи є запозичення та імплементація міжнародних ідей, концепцій та принципів. Розробка й уніфікація нормативно-правових актів, спрямованих на боротьбу з кіберзлочинністю, виступає одним із ефективних способів посилення протидії цим загрозам і розвитку міжнародної співпраці.

Зроблено висновок, що досвід США та Франції є надзвичайно важливим для української практики, оскільки поняття кіберзлочинності в національному праві досі не отримало чіткого теоретичного осмислення та законодавчого закріплення. Необхідним є також чітке розмежування видів кіберзлочинів залежно від їхнього впливу та негативних наслідків для соціальних процесів у державі. Якщо перший тип кіберзлочинів відповідно до французької класифікації достатньо врегульований положеннями Розділу XVI Кримінального кодексу України, то регулювання другого типу потребує ґрунтовного вивчення та впровадження ефективних підходів.

Зроблено висновок, що ефективний моніторинг негативних явищ у кіберпросторі, зокрема протиправної діяльності, вимагає значно більш активної міжнародної співпраці, ніж існуючі заходи боротьби з іншими формами міжнародної злочинності. Тому, окрім покращення та зміни кримінально-правових норм, постає потреба у впорядкуванні процесуальних механізмів і розбудові нових форматів міжнародного партнерства.

Крім того, одним з найбільш пріоритетних напрямів удосконалення вітчизняного законодавства є імплементація міжнародного досвіду через імплементацію зарубіжних концепцій, принципів та правових моделей. Формування й гармонізація нормативно-правового забезпечення боротьби з кіберзлочинністю є важливою умовою посилення національної кібербезпеки та розвитку ефективної міжнародної співпраці в цій сфері.

Ключові слова: кіберзлочин, кіберзлочинність, протидія, міжнародний досвід, імплементація.

Zakharevych R.V. Implementation of foreign experience into Ukrainian legislation on combating cybercrime.

The article is devoted to the study of the possibility and ways of implementing foreign experience in Ukrainian legislation on combating cybercrime.

It is established that the issue of combating cybercrime acquires particular importance in the conditions of the introduction of martial law. Modern information wars are capable of causing damage comparable to or even greater than that caused by armed conflicts on the battlefield. In this regard, the subjects responsible for combating cybercrime must take all possible measures to minimize cyberattacks carried out by the enemy.

It is noted that one of the key areas of improving the national legal system is the borrowing and implementation of international ideas, concepts and principles. The development and unification of regulatory legal acts aimed at combating cybercrime is one of the effective ways to strengthen the fight against these threats and develop international cooperation.

It is concluded that the experience of the USA and France is extremely important for Ukrainian practice, since the concept of cybercrime in national law has not yet received a clear theoretical understanding and legislative consolidation. It is also necessary to clearly distinguish the types of

cybercrimes depending on their impact and negative consequences for social processes in the state. If the first type of cybercrime according to the French classification is sufficiently regulated by the provisions of Chapter XVI of the Criminal Code of Ukraine, then the regulation of the second type requires a thorough study and implementation of effective approaches.

It is concluded that effective monitoring of negative phenomena in cyberspace, in particular illegal activities, requires much more active international cooperation than existing measures to combat other forms of international crime. Therefore, in addition to improving and changing criminal law norms, there is a need to streamline procedural mechanisms and develop new formats of international partnership.

In addition, one of the most priority areas for improving domestic legislation is the implementation of international experience through the implementation of foreign concepts, principles and legal models. The formation and harmonization of regulatory and legal support for the fight against cybercrime is an important condition for strengthening national cybersecurity and developing effective international cooperation in this area.

Key words: cybercrime, cyber crime, countermeasures, international experience, implementation.

Постановка проблеми. Стрімкий розвиток цифрових технологій і глобалізація інформаційного простору призвели до різкого зростання кількості кіберзлочинів у всьому світі. Україна, як держава з високим рівнем цифровізації, не є винятком із цього процесу. Питання забезпечення ефективної протидії кіберзлочинності стало надзвичайно актуальним, особливо в умовах гібридних загроз, інформаційних атак та воєнних дій, які супроводжуються активною кіберкомпонентою.

Успішна боротьба з кіберзлочинами вимагає від українського законодавства не тільки оперативного реагування на нові виклики, але й запозичення найкращих практик міжнародного права та досвіду провідних країн у сфері кібербезпеки. Імплементація зарубіжного досвіду дозволяє не лише модернізувати національну правову систему, а й гармонізувати її з міжнародними стандартами, що є необхідною умовою для ефективної співпраці в боротьбі з транскордонною кіберзлочинністю.

Актуальність дослідження зумовлена потребою у всебічному аналізі існуючих міжнародних підходів, оцінці їх релевантності до українських реалій та розробці рекомендацій щодо адаптації і впровадження цих моделей у вітчизняну практику.

Стан опрацювання проблематики. Питання протидії кіберзлочинам у своїх працях досліджувало багато вчених, серед яких: П.Д. Біленчук, С.В. Демедюк, Б.Д. Леонов, Т.Д. Лисько, В.В. Марков, П.П. Підюков, Т.В. Рудий, В.Б. Хлевицький та інші.

Метою статті є дослідження можливості та шляхів імплементації зарубіжного досвіду в українське законодавство щодо протидії кіберзлочинам.

Виклад основного матеріалу. В 2017 році було прийнято Закон України «Про основні засади забезпечення кібербезпеки України», в якому визначаються правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [1].

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 [2, с. 21-22].

В свою чергу, О.М. Жеребець стверджує, що 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. 130].

Крім того, на нашу думку, проблематика протидії кіберзлочинності набуває особливої важливості в умовах запровадження воєнного стану. Сучасні інформаційні війни здатні завдати шкоди, співмірної або навіть більшої за ту, що спричиняється збройними конфліктами на полі бою. У зв'язку з цим, суб'єкти, відповідальні за протидію кіберзлочинам, повинні вживати всіх можливих заходів для мінімізації кібератак, здійснюваних противником.

Одним із ключових напрямів удосконалення національної правової системи є запозичення та імплементація міжнародних ідей, концепцій та принципів. Розробка й уніфікація нормативно-правових актів, спрямованих на боротьбу з кіберзлочинністю, виступає одним із ефективних способів посилення протидії цим загрозам і розвитку міжнародної співпраці.

Слід також зазначити, що серед універсальних міжнародно-правових документів, окрім згаданої Конвенції, вирізняємо Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами, 1995 рік; Конвенцію ООН проти транснаціональної організованої злочинності, 2000 рік. Одним із перших міжнародних документів у боротьбі з кіберзлочинністю є «Мінімальний список» правопорушень у цій сфері, прийнятий Європейським комітетом з проблем злочинності Ради Європи у 1990 році, який передбачав наступні злочини: комп'ютерне шахрайство, комп'ютерний підлог, пошкодження комп'ютерної інформації чи програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних систем, несанкціоноване перехоплення інформації, несанкціоноване копіювання захищених комп'ютерних програм, незаконне виготовлення топографічних копій. Згодом ця класифікація злочинних посягань була скорегована Конвенцією 2001 року. З метою протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів країн світу такі злочини класифікуються за кодифікатором міжнародної кримінальної поліції Генерального Секретаріату Інтерполу, який з 1991 року інтегровано в автоматизовану систему пошуку, і сьогодні він доступний підрозділам Національних центральних бюро Інтерполу більшості країн світу, зокрема, й НЦБ Інтерполу МВС України.

У Європейському Союзі 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 [4, с. 388].

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 [2, с. 22].

Провідну роль у забезпечення безпеки США в он-лайн просторі відіграє також 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 [5].

Слід також зазначити, що 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 [5].

Що стосується Європейського Союзу, то тут з 2013 року 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 [5].

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 [6, с. 280].

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, с. 43].

Даний досвід є надзвичайно важливим для української практики, оскільки поняття кіберзлочинності в національному праві досі не отримало чіткого теоретичного осмислення та законодавчого закріплення. Необхідним є також чітке розмежування видів кіберзлочинів залежно від їхнього впливу та негативних наслідків для соціальних процесів у державі. Якщо перший тип кіберзлочинів відповідно до французької класифікації достатньо врегульований положеннями Розділу XVI Кримінального кодексу України, то регулювання другого типу потребує ґрунтовного вивчення та впровадження ефективних підходів.

Деякі вчені стверджують, 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 [5].

Тому, з урахуванням міжнародних зобов'язань України, доцільним є доповнити Розділ XVI Кримінального кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» нормами про кримінальні правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних, в яких як обтяжуючі обставини мають визнаватися використання спеціальних програмних засобів негласного отримання інформації та інформаційних технологій [8, с. 11].

Ефективний моніторинг негативних явищ у кіберпросторі, зокрема протиправної діяльності, вимагає значно більш активної міжнародної співпраці, ніж існуючі заходи боротьби з іншими формами міжнародної злочинності. Тому, окрім покращення та зміни кримінально-правових норм, постає потреба у впорядкуванні процесуальних механізмів і розбудові нових форматів міжнародного партнерства.

Крім того, на думку деяких вчених, необхідними змінами законодавства задля протидії протиправним посяганням на електронні інформаційні ресурси має бути закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку і арешту електронних доказів, насамперед

закріплення процесуально значимої можливості копіювання інформації, а також імплементація в національне законодавство положень про невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, власниками ресурсу (веб-сайту) із забезпеченням їх цілісності. Отже, ООН та її спеціалізовані установи і організації, мета діяльності яких передбачає забезпечення мирного існування та перевагу дипломатії над воєнним характером відносин, відіграє велику роль у боротьбі із кіберзлочинністю та кібершахрайством. Прийняття низки правових актів спрямовані на підтримку інформаційної безпеки та боротьби і попередження кіберзлочинності [4, с. 391].

Висновки. Отже, на основі викладеного вище, можна зробити висновок, що актуальність проблеми протидії кіберзлочинам істотно зросла в умовах дії воєнного стану. В сучасних реаліях інформаційна війна може завдати державі та суспільству не меншої шкоди, ніж бойові дії у фізичному просторі, що обумовлює необхідність активізації заходів із протидії кіберзлочинності. Ефективне реагування на загрози в кіберсередовищі вимагає від відповідних суб'єктів вжиття комплексних і своєчасних заходів із нейтралізації діяльності противника у цифровій сфері.

Саме тому одним з найбільш пріоритетних напрямів удосконалення вітчизняного законодавства є імплементація міжнародного досвіду через імплементацію зарубіжних концепцій, принципів та правових моделей. Формування й гармонізація нормативно-правового забезпечення боротьби з кіберзлочинністю є важливою умовою посилення національної кібербезпеки та розвитку ефективної міжнародної співпраці в цій сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII / База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.04.2025).
2. Аніщук В.В., Зицик С.Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 83(3). С. 19–23.
3. Жеребець О.М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. *Інформація і право*. 2021. № 4. С. 129–134.
4. Саєнко М.І., Савела Є.А., Тополянський Ю.Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. Вип. 64. С. 386–391.
5. Мордань Є.Ю., Бардакова В.В., Сокол Л.В. Удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству на основі впровадження міжнародного досвіду. *Ефективна економіка*. 2023. № 10. URL: http://nbuv.gov.ua/UJRN/efek_2023_10_40.
6. Попко В.В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. № 66. С. 276–283.
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. Леонов Б.Д., Серьогін В.С. Проблеми правового та експертного забезпечення правоохоронної діяльності у сфері протидії кіберзлочинності. *Інформаційна безпека людини, суспільства, держави*. 2019. № 3. С. 6–15.