УДК 343.98:004.056

**ГУЦАЛЮК М.В.,** *кандидат юридичних наук, с.н.с, доцент,*
провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.

# НАПРЯМИ ПОСИЛЕННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

***Анотація.*** *В статті досліджуються сучасні проблеми міжнародного співробітництва у сфері протидії кіберзлочинності.*

*Ключові слова: кіберзлочинність, електронні докази, конвенція про кіберзлочинність, міжнародне співробітництво*

***Ключові слова:*** *міжнародне співробітництво, кіберзлочинність, правоохоронні органи, електронні докази.*

***Summary.*** *The article examines current problems of international cooperation in combating cybercrime.*

***Keywords:*** *International cooperation, cybercrime, law enforcement, electronic evidence.*

***Аннотация****. В статье исследуются современные проблемы международного сотрудничества в сфере противодействия киберпреступности.*

***Ключевые слова:*** *международное сотрудничество, киберпреступность, правоохранительные органы, электронные доказательства.*

**Постановка проблеми.** Сучасний етап економічного та соціального розвитку суспільства характеризується високими темпами цифровізації та віддаленого обміну інформацією, які значно зросли з початком пандемії CoVID-19. Водночас до нових змін швидко пристосувалась кіберзлочинність – в усьому світі зберігається тенденція збільшення кількості кібератак, їх складності та збитків від них [1]. Однією з причин недостатньої ефективності боротьби з кіберзлочинністю є неможливість протидіяти транснаціональним високотехнологічним злочинам в межах лише однієї держави та недостатнє використання механізмів міжнародної співпраці.

Як правило, кібератаки здійснюються з інших країн, аніж там, де розташовані атаковані інформаційні ресурси, а іноді одночасно з десятків країн з різних куточків світу. Це зумовлює значні труднощі щодо їх розслідування і протидії злочинній діяльності та потребує тісного міжнародного співробітництва як правоохоронних органів так і суб'єктів кібербезпеки.

**Результати аналізу наукових публікацій**. Результати аналізу наукових публікацій свідчать про те, що питання міжнародного співробітництва правоохоронних органів у боротьбі з кіберзлочинністю були предметом досліджень таких науковців, як M. Maras, A. Cerezo, J. Lopez та вітчизняних Н. Ахтирська, П. Біленчук, В. Бутузов, А. Марущак, Є. Скулиш, К. Тітуніна та інші.

Водночас сучасний розвиток технологій, зростання нових кіберзагроз, складність кібератак потребують нових підходів до підвищення ефективності протидії кіберзлочинності.

**Метою статті** є розкриття нових напрямів міжнародного співробітництва у сфері боротьби з кіберзлочинністю.

**Виклад основного матеріалу.** Комп'ютерна злочинність, яка з'явилася наприкінці минулого століття, з поширенням мережі Інтернет по всьому світу постійно змінюється та набуває нових масштабів, що безумовно турбує як окремі держави, так і в цілому світову спільноту, та вимагає тісного міжнародного співробітництва для протидії цьому явищу. З 1991 року при Генеральному секретаріаті Інтерполу діє робоча група з проблем комп'ютерної злочинності, яка вивчає цей вид злочинів у різних країнах світу, розробляє рекомендації, допомагає в стандартизації національних законодавств, напрацьовує методичний досвід запобігання й розслідування комп'ютерних злочинів [2].

В розвинутих країнах світу кримінальна відповідальність за вчинення комп'ютерних злочинів була введена у кінці 1980-х, на початку 1990-х років. В Україні стаття 198-1 "Порушення роботи автоматизованих систем" Кримінального кодексу України 1960 року була введена у 1994 році.

Вже на межі століть такі комп'ютерні віруси як Melissa, Love Letter/I LOVE YOU призвели до значних збитків по всьому світу, а злочинці свою увагу звернули на віддалений несанкціонований доступ до банківської інфраструктури, що було менш небезпечним та більш прибутковим аніж традиційні напади на банківські відділення. Все це заважало нормальному функціонуванню як економіки держав, так і Інтернету. Власне через активне використання кіберпростору злочини з використанням його можливостей отримали назву кіберзлочини, а саме явище отримало назву кіберзлочинності, що пізніше було законодавчо закріплене [3].

В резолюції Генеральної Асамблеї ООН A/RES/53/70 від 4 січня 1999 року "Досягнення в сфері інформатизації і комунікації у контексті міжнародної безпеки" зазначається, що використання інформаційних технологій і засобів стосується інтересів всього міжнародного співтовариства і що міжнародна взаємодія сприяє забезпеченню максимальної ефективності. Вважаючи за необхідне запобігти неправомірному використанню або використанню інформаційних ресурсів чи технологій в злочинних чи терористичних цілях, ООН закликає держави-члени сприяти розгляду існуючих та потенційних загроз у сфері інформаційної безпеки [4].

У зв'язку з тим, що сам по собі складний характер кіберзлочинності посилюється ще й участю організованих злочинних груп у протиправній діяльності в глобальній мережі, а кіберзлочинці та їх жертви часто знаходяться в різних регіонах, ООН підкреслює необхідність відповідного міжнародного скоординованого динамічного реагування. Для цього в рамках Комісії з питань запобігання злочинності та кримінального правосуддя функціонує міжурядова група експертів для проведення всебічного дослідження проблеми кіберзлочинності. Група на своїх засіданнях надає рекомендації, щодо вдосконалення боротьби кіберзлочинності, напрацьовані в різних країнах світу.

Для налагодження тісної співпраці правоохоронних органів різних держав у 2002 році у Лондоні був проведений Перший міжнародний стратегічний конгрес "E-Crime 2002" на якому представники правоохоронних органів, приватного сектору та державних органів з усього світу обмінювалися своїм досвідом щодо протидії злочинам, які вчиняються з використанням комп'ютерів та мереж передачі даних. У роботі конгресу брали участь і українські правоохоронці [5].

Серед основних міжнародних нормативно-правових документів щодо протидії кіберзлочинності, у тому числі організованої, на сьогодні слід виокремити такі:

– Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності (United Nations Convention against Transnational Organized Crime), підписана у м. Палермо 12 грудня 2000 року та ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV(1433-15);

– Європейська Конвенція про взаємну допомогу у кримінальних справах (European Convention on Mutual Assistance in Criminal Matters), підписана у м. Страсбурзі 20 квітня 1959 року та ратифікована із заявами і застереженнями Законом України від 16.01.98 р. № 44/98-ВР;

– Конвенція про кіберзлочинність (Convention on Cybercrime), підписана 23 листопада 2001 року в м. Будапешті і ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV(2824-15).

Міжнародне співробітництво правоохоронних органів України з іноземними компетентними органами здійснюється на підставі розділу IX Кримінального процесуального кодексу України "Міжнародне співробітництво під час кримінального провадження" (ст.ст. 541-550 КПК України). Співробітництво між державами здійснюється через відповідний центральний орган. Центральними органами України є:

- під час досудового провадження – Генеральна прокуратура України;
- під час судового провадження – Міністерство юстиції України.

З метою протидії транснаціональній злочинності держави-члени Європейського Союзу об'єднали свої зусилля та створили низку спеціалізованих органів, діяльність яких спрямована на підтримання правопорядку і сприяння роботі національних правоохоронних органів. До таких органів належать, зокрема: Європейське поліцейське відомство (Європол), Європейська організація з питань юстиції (Євроюст), Європейська агенція управління оперативним співробітництвом на зовнішніх кордонах ЄС (FRONTEX). Поряд із ними існує низка спеціалізованих допоміжних органів, серед яких Європейський моніторинговий центр з наркотиків та наркотичної залежності, Постійний комітет із питань оперативного співробітництва у сфері внутрішньої безпеки, Група експертів із питань торгівлі людьми, Європейська мережа попередження злочинності, Європейський офіс боротьби з шахрайством тощо. Усі ці органи створювалися в різний час, виходячи з рівня інтеграційних процесів та досягнень у рамках ЄС, а також нагальних потреб його держав-учасниць.

У 2013 році для посилення реагування правоохоронних органів на кіберзлочинність у ЄС Європол створив Європейський центр кіберзлочинності (European Cybercrime Centre – EC3) для захисту європейських громадян, бізнесу та уряду від злочинності в Інтернеті. З моменту свого створення EC3 вніс значний внесок у боротьбу з кіберзлочинністю: Центр брав участь у десятках гучних операцій та сотнях операцій щодо оперативної підтримки на місцях, що призвело до сотень арештів, і проаналізував сотні тисяч файлів, переважна більшість з яких виявилися шкідливими. EC3 продовжує проводити науково-дослідні роботи у сфері цифрової криміналістики, здійснює стратегічний аналіз організованої кіберзлочинності та забезпечує розвиток навчання правоохоронців щодо протидії кіберзлочинності [6].

Створення міжнародної нормативної бази та функціонування міжнародних та європейських інституцій по боротьбі з кіберзлочинністю надало змогу підняти на новий рівень протидію кіберзлочинності, що жодна з країн не здатна зробити самотужки.

Водночас і кіберзлочинці не зупиняються на відточенні своїх навичок, розширенні методів, створенні сервісів на кшталт "кіберзлочини як послуга" та посиленні організованості кіберзлочинності, у тому числі угруповань, які підтримуються урядами певних країн.

Сьогодні, коли кількість активних користувачів Інтернет перевищила 5 млрд. [7], питання кібербезпеки постають як ніколи гостро. Зокрема за даними компанії з кібербезпеки CrowdStrike кожен день створюється понад 360000 нових шкідливих програм (ШП), а атаки програм-вимагачів досягли "стратосферного рівня" і складають на

сьогодні 69 % всіх атак [8], пов'язаних з ШП. Середня вартість викупу програм-вимагачів у 2021 році оцінюється експертами у $6,3 млн. США. Прогноз глобальних витрат від пошкодження програм-вимагачів становитиме $20 млрд. до кінця 2021 року, що набагато більше, ніж це було у минулі роки. Особливо небезпечними є напади на об'єкти критичної інфраструктури.

Так уряд США оголосив надзвичайний стан після кібератаки хакерського угруповання DarkSide на один з найбільших трубопроводів країни Colonial Pipeline, що сталася 7 травня 2021 року. Для кібератаки хакерське угруповання DarkSide використало шкідливу програму-вимагач та погрожувало оприлюднити близько 100 ГБ даних.

Через кібератаку Colonial Pipeline перекрила частину трубопроводу довжиною майже 9 тисяч кілометрів. Компанія транспортує близько 2,5 мільйони барелів палива на схід та південь Сполучених Штатів, зокрема забезпечує паливом штат Нью-Йорк і його найбільші аеропорти [9].

Також 2 липня 2021 року було здійснено хакерську атаку на американську компанію Kaseya, що спеціалізується на розробці програмного забезпечення для мережевої інфраструктури. Як наслідок, робота принаймні 200 компаній у США була паралізована. У ЗМІ повідомляли, що кібератака вивела з ладу обчислювальні системи у 800 шведських супермаркетах, 11 школах Нової Зеландії і двох ІТ-компаніях Данії. Ймовірно, за атакою стояло хакерське угруповання з РФ REvil, кіберзлочинці якого вимагали $70 млн. викупу в криптовалюті для повернення вкраденої ним інформації [10].

А у німецькому регіоні Ангальт-Біттерфельд, що у федеральній землі Саксонія-Ангальт, 10 липня 2021 року оголосили перший в історії країни режим надзвичайного стану через кібератаку. Унаслідок дій зловмисників майже повністю заблокувалася робота місцевої влади, внаслідок чого населення регіону (157 тисяч) не могло отримати соціальні виплати й не мало доступу до інших послуг місцевої влади [10].

Таке збільшення у геометричній прогресії кіберзагроз потребує розробки нових стратегій кібербезпеки та посилення міжнародної співпраці щодо протидії кіберзлочинності.

Слід зазначити, що одночасне та скоординоване проведення розслідувань та арештів кіберзлочинців в різних країнах призводить до відчутного результату. Наприклад, під час масштабної операції за участі правоохоронців 30 країн з ліквідації кібермережі "Avalanche" у 2016 році, яка проходила за підтримки Центру боротьби з кіберзлочинністю Європолу (EC3) та Об'єднаної групи боротьби з кіберзлочинністю (J-CAT), а також Євроюсту та Європейської банківської федерації (EBF) було заарештовано 178 осіб-співучасників, у тому числі і її організатори в Україні.

Останніми роками участь українських правоохоронців у таких операціях значно поширилась. Зокрема у 2020 році кіберполіція провела 10 міжнародних поліцейських операцій із викриття "хакерських" угруповань, учасники яких завдали збитків країнам ЄС, Великої Британії та США на суму понад $300 млн. [11].

Разом з тим, під час під час досудового розслідування кіберзлочинів, особливо тих, докази про вчинення яких знаходяться в юрисдикції іншої країни, виникають певні труднощі у їх отриманні, зберіганні та оперативному аналізі. Крім того, Україною ще не імплементовані такі статті Конвенції про кіберзлочинність, як: ст. 16 – "Термінове збереження комп'ютерних даних, які зберігаються" та ст. 17 – "Термінове збереження і часткове розкриття даних про рух інформації". Відповідний законопроект за № 4004 вже більше року як зареєстрований Верховною Радою України та потребує розгляду.

Комітет Ради Європи 12 квітня 2021 року опублікував проект *"Другий додатковий протокол до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття*

*електронних доказів",* яким, зокрема, передбачається: пряма співпраця з постачальниками послуг (стаття 6) та суб'єктами, що надають доменне ім'я реєстраційні послуги (стаття 7) для розкриття інформації для ідентифікації підозрюваних; прискорення форм співпраці між Сторонами для розкриття інформації про абонентів та даних про рух (стаття 8); пришвидшення співпраці з розкриття інформації у надзвичайних ситуаціях (статті 9 та 10); додаткові інструменти взаємодопомоги (статті 11 та 12); захист даних та інші гарантії верховенства права (статті 13 та 14). Обговорення вказаних новацій та пропозиції своїх варіантів цього міжнародного акту повинні стати важливим етапом усіх зацікавлених суб'єктів протидії кіберзлочинності [12].

У грудні 2019 року в своїй резолюції 74/247 Генеральна Асамблея ООН вирішила створити Спеціальний міжурядовий Комітет експертів відкритого типу, представників усіх регіонів, для розробки всеосяжної міжнародної *Конвенції про протидію використанню інформаційно-комунікаційних технологій у кримінальних цілях* з урахуванням існуючих міжнародних документів та зусиль на національному, регіональному та міжнародному рівнях щодо протидії використанню інформаційно-комунікаційних технологій у кримінальних цілях та результатів роботи міжурядової групи експертів відкритого типу для проведення комплексного дослідження з питань кіберзлочинності.

26 травня 2021 р. Генеральна Асамблея ООН прийняла Резолюцію "Протидія використанню інформаційно-комунікаційних технологій у кримінальних цілях" № 75/282. Серед іншого у Резолюції визначено, що Спеціальний комітет скликає щонайменше шість сесій по 10 днів кожна, щоб розпочати у січні 2022 року заключну сесію в Нью-Йорку та подати проєкт Конвенції Генеральній Асамблеї на її сімдесят восьмій сесії.

Указом Президента України від 26.08.21 р. № 447/2021 затверджена нова Стратегія кібербезпеки України. У документі визначені основні виклики та загрози для України у сфері кібербезпеки на сучасному етапі, серед яких:

- активне використання кіберзасобів у міжнародній конкуренції;
- мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;
- нарощення арсеналу кіберзброї державою-агресором, використання кібератак проти об'єктів критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсії) та здійснення розвідувальної та розвідувально-підривної діяльності.
- кіберзлочинність, яка призводить до значних матеріальних втрат та використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів тощо.
- використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності тощо.

Для ефективної протидії кіберзлочинності у Стратегії передбачена важлива ціль *"Прагматичне міжнародне співробітництво"* – Україна спрямує відносини з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками.

Україна забезпечить активну участь у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази.

Для налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед США, державами-членами ЄС та НАТО, створення платформи такого обміну.

В Стратегії також чітко зазначено необхідність забезпечення участі України у доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах, розширення шляхом діалогу з міжнародними партнерами доступу правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу I-24/7.

Тобто у Стратегії чітко визначені напрями посилення міжнародного співробітництва у сфері протидії кіберзлочинності. В той же час виконання зазначеної роботи залежить від якісного планування конкретних заходів та їх своєчасного виконання, що не завжди відбувалося при виконанні Стратегії кібербезпеки України 2016 – 2020 років.

Одночасно, визнаючи необхідність посилення та ефективнішої співпраці між державами та приватним сектором щодо розкриття електронних даних, інших форм збору електронних доказів кримінального правопорушення необхідно дотримуватися верховенства права та європейських приписів щодо демократії. Тобто повинні бути створені умови для вільного, відкритого та безпечного кіберпростору, без тоталітарного ведення стеження та безпідставного блокування користувачів у кіберпросторі. На практиці знайти оптимальний баланс у вказаних напрямах діяльності є досить складним завданням.

Також запровадження нових норм та правил міжнародного співробітництва повинно спростити, а не ускладнити існуючі процедури взаємодії, що є вкрай важливим під час розслідування кіберзлочинів.

**Висновки.**

Постійно зростаюче використання інформаційних технологій, збільшення кількості користувачів Інтернет з різних регіонів світу продовжують загострювати проблему їх безпечного використання.

Разом з тим, ефективна боротьба з кіберзлочинністю вимагає тісного міжнародного співробітництва на основі міжнародних конвенцій, договорів, завдяки обміну передовим досвідом та внаслідок проведення спільних.

Прийняття нової Стратегії кібербезпеки України та її реалізація повинні стати ефективним механізмом у боротьбі з кіберзлочинністю, у тому числі і з її організованими транснаціональними формами.

## Використана література

1. Клименко О.А., Гуцалюк М.В. Кримінальний опортунізм кіберзлочинності як загроза національній безпеці України. *Юридичний вісник "Повітряне і космічне право"*. Т. 1. № 58 (2021). С. 177-184.

2. Комп'ютерна злочинність: навч. посібник / Біленчук П.Д., Бут В.В., Гавловський В.Д., Гуцалюк М.В., Романюк Б.В. Київ: Атіка, 2002. С. 150.

3. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України". Станом на 1 січня 2019 року / Гуцалюк М.В. та ін. ; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

4. Developments in the field of information and telecommunications in the context of international security / Resolution adopted by the general assembly UN A/RES/53/70 4 January 1999. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english

5. Гуцалюк М. Перший міжнародний стратегічний конгрес "E-CRIME 2002". *Крок.* 2002. № 24. С. 7.

6. European Cybercrime Centre – EC3. URL: www.europol.europa.eu/about-europol/europ ean-cybercrime-centre-ec3

7. Internet live stats. URL: https://www.internetlivestats.com

8. Отчёт: программы-вымогатели составляют 69 % всех атак, связанных с вредоносным ПО. URL: https://internetua.com/otcset-programmy-vymogateli-sostavlyauat-69-vseh-atak-svya zannyh-s-vredonosnym-po

9. US fuel pipeline hackers 'didn't mean to create problems'. URL: https://www.bbc.com/news/ business-57050690

10. Хакери, причетні до масштабної кібератаки, вимагають 70 мільйонів доларів у Bitcoin за доступ до вкрадених даних. URL: https://hromadske.ua/posts/hakeri-prichetni-do-masshtabnoyi-kiberataki-vimagayut-70-miljoniv-dolariv-u-bitcoin-za-dostup-do-vkradenih-danih

11. У 2020 році кіберполіція провела 10 міжнародних поліцейських операцій із викриття "хакерських" угруповань – Олександр Гринчак. URL: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-provela--mizhnarodnyx-policzejskyx-operaczij-iz-vykryttya-xakerskyx-ugrupovan--olek sandr-grynchak-5855

12. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. URL: https://rm.coe.int/0900001680a2aa1c

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