УДК 341.456
DOI https://doi.org/10.32782/ln.2024.23.43

Стріяшко Г.М.
к.ю.н., доцент,
методист вищої категорії відділу програм підвищення кваліфікації,
Інститут післядипломної освіти та підвищення кваліфікації
Державного податкового університету
ORCID ID: 0009-0002-1768-5889

Замрига А. В.
к.е.н., д.ю.н., доцент,
професор кафедри
публічного та міжнародного права,
Київський національний економічний університет імені Вадима Гетьмана»
ORCID ID: 0000-0001-8919-6633

ІНТЕРПОЛ ЯК СУБ'ЄКТ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ: НОВІ ЗАГРОЗИ В ЦИФРОВУ ЕПОХУ

Постановка проблеми. У цифрову епоху кіберзлочинність стрімко зростає, стаючи серйозним викликом для сучасного суспільства. З розвитком інформаційних технологій злочинці використовують все більш складні методи, такі як хакерські атаки, крадіжка персональних даних та фінансові шахрайства, що завдають значної шкоди економіці та безпеці окремих осіб і держав. Транснаціональний характер цих злочинів ускладнює їхню протидію на національному рівні, оскільки злочинці часто діють з-за кордону, використовуючи глобальну мережу Інтернет для приховування своєї діяльності. Війна в Україні додатково ускладнила ситуацію, оскільки кібератаки стали інструментом гібридної війни, спрямованих на дестабілізацію критичної інфраструктури та інформаційних систем країни. Це підкреслює необхідність посилення міжнародної співпраці у боротьбі з кіберзлочинністю та розробки ефективних стратегій захисту. Крім того, впровадження нових цифрових технологій, таких як штучний інтелект та блокчейн, створює додаткові виклики для правоохоронних органів, які повинні постійно оновлювати свої методи та інструменти для ефективної протидії сучасним кіберзагрозам. Запровадження цифрових технологій також викликає питання щодо безпеки даних та захисту приватності, що стає особливо актуальним у контексті зростання кількості кібератак. Законодавчі ініціативи на національному рівні часто не встигають за швидким розвитком технологій, що створює прогалини у правовому регулюванні та ускладнює міжнародну координацію зусиль. Відсутність уніфікованого підходу до боротьби з кіберзлочинністю призводить до розривів у співпраці між державами та знижує ефективність заходів безпеки.

Таким чином, ефективна боротьба з кіберзлочинністю вимагає глибокого дослідження ролі міжнародних організацій, таких як Інтерпол, у створенні та впровадженні стратегій протидії новим загрозам у цифровому просторі, враховуючи сучасні геополітичні виклики та швидкий розвиток технологій.

Аналіз останніх досліджень та публікацій. Діяльність Інтерполу (НЦБ Інтерпол) завжди викликала значний інтерес серед науковців-правників різних галузей права, включаючи міжнародне, адміністративне та

кримінально-процесуальне право, а також дослідників у сферах криміналістики та оперативно-розшукової діяльності. Серед провідних дослідників, які активно вивчають цю тематику, виділяються такі вчені, як В. А. Бабич, О. М. Бандурка, Я. М. Бельсон, П. Д. Біленчук, І. П. Блищенко та інші. Їхні роботи охоплюють різні аспекти правового статусу та функціонування НЦБ Інтерполу в Україні, аналізуючи його роль у боротьбі з транснаціональною злочинністю та кіберзлочинністю.

Метою цієї статті є аналіз ролі Інтерполу у боротьбі з кіберзлочинністю, а також виявлення нових загроз, що виникають у цифрову епоху. Дослідження спрямоване на оцінку ефективності міжнародної співпраці та впровадження інноваційних стратегій захисту, що використовуються Інтерполом для протидії сучасним кіберзагрозам.

Виклад основного матеріалу дослідження.

Військові дії, що розгорнулися в Україні з початку конфлікту, суттєво вплинули на рівень та характер злочинності в країні. Збільшення напруженості та нестабільності створює сприятливі умови для різних форм кримінальної діяльності, зокрема кіберзлочинності. Атакуючі сторони використовують цифрові засоби для дестабілізації критичної інфраструктури, розповсюдження пропаганди та здійснення економічних атак, що ускладнює завдання правоохоронних органів у забезпеченні безпеки громадян та держави.

Зростання злочинності, зокрема кіберзлочинності, вимагає активізації роботи різних служб та організацій, що займаються боротьбою зі злочинністю. На національному рівні це включає діяльність Національної поліції, Служби безпеки України та інших правоохоронних органів, які посилюють свої зусилля щодо моніторингу, розслідування та запобігання кіберзлочинам. Водночас важливою є координація між цими органами для ефективного реагування на нові виклики, пов'язані з цифровими загрозами.

У цьому контексті діяльність Інтерполу стає надзвичайно важливою для міжнародної співпраці у боротьбі з кіберзлочинністю. Інтерпол забезпечує оперативний обмін інформацією між країнами-членами, що дозволяє оперативно реагувати на загрози та координувати спільні дії проти кіберзлочинців. Спеціалізовані підрозділи Інтерполу, такі як Global Cybercrime Programme, займаються розробкою та впровадженням стратегій боротьби з кіберзлочинністю, а також підтримкою національних органів у розслідуванні складних випадків.

Діяльність Інтерполу регулюється низкою міжнародних та національних документів, які визначають правові основи його функціонування та співпраці з національними органами влади. Основним документом є Статут Міжнародної організації кримінальної поліції – Інтерпол, прийнятий 13 червня 1956 року в Ліоні. Цей Статут визначає мету організації, її структуру, повноваження членів та механізми співпраці між країнами-членами. Статут встановлює принципи нейтралітету, незалежності та невтручання у внутрішні справи держав, що є фундаментальними для функціонування Інтерполу на міжнародній арені [1].

До ключових нормативних актів України щодо регулювання діяльності Інтерполу в Україні належать рішення Кабінету Міністрів України про вступ країни до Інтерполу, прийняті 30 вересня 1992 року (Постанова No 555), що офіційно підтвердило членство України в організації та визначило рамки співпраці з міжнародними партнерами. Крім того, Закон України «Про Національну поліцію» від 2 липня 2015 року [2] та внесені до нього зміни від 15 березня 2022 року створюють правову базу для ефективної взаємодії Національного центрального бюро Інтерполу (НЦБ Інтерполу) з міжнародними структурами. Ці законодавчі акти регулюють організаційну структуру Національної поліції, визначають повноваження та обов'язки її підрозділів, зокрема Департаменту міжнародного співробітництва, який наразі відповідає

за координацію діяльності НЦБ Інтерполу та забезпечення дотримання міжнародних стандартів у сфері кримінальної поліції.

Зокрема, Закон України «Про Національну поліцію» встановлює механізми обміну інформацією між НЦБ Інтерполу та іншими правоохоронними органами країни, а також визначає процедури запиту та надання міжнародної допомоги у розслідуванні кримінальних справ. Додаткові нормативні акти, такі як Закон України від 15 березня 2022 року про внесення змін до законів України «Про Національну поліцію» та «Про Дисциплінарний статус Національної поліції України», спрямований на оптимізацію діяльності поліції під час воєнного стану, також впливає на функціонування НЦБ Інтерполу, забезпечуючи більшу гнучкість та оперативність у реагуванні на кіберзагрози та інші форми злочинності [3].

Крім того, діяльність Інтерполу регулюється міжнародними угодами та протоколами, такими як Протокол про оперативну співпрацю у боротьбі з кіберзлочинністю, який був прийнятий у 2010 році, він є частиною Будапештської конвенції (Конвенції про кіберзлочинність). Це перший багатосторонній договір, спрямований на боротьбу з кіберзлочинністю на міжнародному рівні. Основна мета Протоколу – підвищити співпрацю між країнами та спростити доступ до електронних доказів для правоохоронних органів. Протокол включає механізми, що дозволяють державам обмінюватися інформацією та співпрацювати у розслідуваннях кіберзлочинів країнам-членам Інтерполу. Відповідно до цих норм, НЦБ Інтерполу в Україні активно співпрацює з міжнародними партнерами, використовуючи інструменти, такі як червоні сповіщення, які допомагають виявляти та затримувати міжнародних кіберзлочинців. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, також регулюється цими угодами [4].

На сьогоднішній день діяльність НЦБ Інтерполу в Україні координується через Департамент міжнародного співробітництва Національної поліції, який забезпечує дотримання міжнародних стандартів, взаємодію з іншими національними та міжнародними організаціями, а також реалізацію стратегій боротьби з кіберзлочинністю. Цей департамент відповідає за впровадження новітніх технологій та методик, що дозволяють ефективніше протидіяти сучасним кіберзагрозам, а також за навчання та підвищення кваліфікації співробітників НЦБ Інтерполу.

Департамент міжнародного співробітництва Національної поліції України відіграє ключову роль у боротьбі зі злочинністю на міжнародному рівні, зокрема з кіберзлочинністю. Однією з основних функцій цього департаменту є координація міжнародних розслідувань. Департамент відповідає за організацію та управління спільними розслідуваннями з іншими країнами та міжнародними організаціями. Це включає обмін інформацією, проведення спільних операцій та використання міжнародних юридичних інструментів для затримання та притягнення до відповідальності кіберзлочинців. Такий підхід дозволяє ефективно реагувати на транснаціональні загрози та забезпечувати належний рівень безпеки на глобальному рівні.

Крім того, департамент забезпечує ефективний обмін інформацією та аналітику між Національною поліцією України та її міжнародними партнерами. Використовуючи інструменти, такі як червоні сповіщення Інтерполу, департамент може швидко реагувати на загрози та координувати дії з метою запобігання та розслідування кіберзлочинів. Це дозволяє оперативно виявляти та нейтралізувати кіберзагрози, а також забезпечувати своєчасний обмін критично важливою інформацією між різними правоохоронними органами.

Розробка та впровадження стратегій боротьби з кіберзлочинністю є ще однією важливою функцією Департаменту міжна-

родного співробітництва. Департамент бере активну участь у створенні національних та міжнародних стратегій, спрямованих на протидію кіберзлочинності. Це включає впровадження новітніх технологій, розробку сучасних методик розслідування та організацію навчання співробітників для ефективної боротьби з цифровими загрозами. Завдяки цьому департамент здатен адаптуватися до швидкоплинних змін у сфері кібербезпеки та забезпечувати високий рівень готовності до протидії новим викликам.

Департамент міжнародного співробітництва Національної поліції України використовує різноманітні бази даних та інформаційні системи для ефективної боротьби з кіберзлочинністю та іншими формами міжнародної злочинності. Ці бази даних забезпечують доступ до критично важливої інформації, сприяють оперативному обміну даними з міжнародними партнерами та підвищують ефективність розслідувань. Так, в роботі використовується інтерполівська база даних I-24/7, яка є глобальною мережею обміну інформацією між країнами-членами Інтерполу. Ця база даних дозволяє оперативно отримувати та обмінюватися інформацією про розшукуваних осіб, кримінальні справи, червоні сповіщення та іншу важливу інформацію. Завдяки I-24/7, Департамент міжнародного співробітництва може швидко реагувати на загрози, координувати спільні операції та забезпечувати своєчасне затримання кіберзлочинців, які діють на міжнародному рівні. Європоловська інформаційна система (Europol's Information System – EIS) є ключовим ресурсом для обміну даними між правоохоронними органами Європи. Ця система містить інформацію про транскордонну злочинність, кіберзагрози, терористичні мережі та інші види серйозної злочинної діяльності. Департамент міжнародного співробітництва використовує EIS для отримання актуальної інформації про загрози, що походять з Європи, а також для координації розслідувань з європейськими партнерами. Для боротьби з фінансовими аспектами кіберзлочинності, такими як відмивання грошей та фінансові шахрайства, Департамент використовує доступ до баз даних Фінансової групи дій (Financial Action Task Force). Ці бази даних включають інформацію про фінансові транзакції, підозрілі операції та осіб, пов'язаних з фінансовими злочинами. Використання цих даних дозволяє відстежувати фінансові потоки, пов'язані з кіберзлочинцями, та співпрацювати з міжнародними фінансовими установами для запобігання відмиванню грошей. Національна кримінальна база даних України містить інформацію про зареєстровані кримінальні справи, судові рішення, особисті дані громадян, а також інформацію про судимих осіб. Департамент міжнародного співробітництва має доступ до цієї бази даних для використання національної інформації у міжнародних розслідуваннях, забезпечуючи ефективне поєднання національних та міжнародних ресурсів у боротьбі з кіберзлочинністю. Система обміну кримінальною інформацією (Criminal Information Exchange System) є спеціалізованою системою для обміну кримінальною інформацією між різними правоохоронними органами. Ця система дозволяє Департаменту міжнародного співробітництва обмінюватися даними про розслідування, кримінальні справи та особисті дані осіб, залучених у злочинну діяльність. Використання CIES сприяє оперативному обміну інформацією та координації дій між Україною та її міжнародними партнерами. База даних CERT-UA (Computer Emergency Response Team of Ukraine) є національною кібербезпековою базою, яка відповідає за моніторинг, виявлення та реагування на кіберінциденти. Ця база даних містить інформацію про кіберзагрози, спроби злому, поширення шкідливого програмного забезпечення та інші кіберзлочини. Департамент міжнародного співробітництва використовує дані CERT-UA для аналізу кіберзагроз, обміну інформацією з міжнародними партнерами та

координації заходів з протидії кіберзлочинності. Для забезпечення ефективного обміну інформацією з міжнародними партнерами, Департамент використовує спеціалізовані платформи та бази даних, які дозволяють швидко передавати та отримувати інформацію про злочинців, їх діяльність та методи. Це включає інтеграцію з системами інших країн, що забезпечує оперативний доступ до актуальної інформації та сприяє швидкому реагуванню на кіберзагрози. Такі системи дозволяють оперативно обмінюватися даними про нові загрози, методи їх здійснення та успішні стратегії протидії.

Правове забезпечення міжнародної співпраці є критично важливим аспектом діяльності департаменту. Він забезпечує дотримання міжнародних та національних законодавчих норм у процесі співпраці з іншими країнами. Це включає роботу з нормативними актами, такими як Статут Інтерполу, Протокол про оперативну співпрацю у боротьбі з кіберзлочинністю та інші міжнародні угоди. Завдяки цьому департамент гарантує, що всі дії здійснюються в рамках правового поля, що підвищує ефективність та законність міжнародних розслідувань.

Навчання та підвищення кваліфікації співробітників Національної поліції є ще одним важливим напрямком діяльності департаменту. Він організовує навчальні програми та тренінги для співробітників з метою підвищення їхніх навичок у сфері міжнародної співпраці та боротьби з кіберзлочинністю. Співробітники проходять навчання з використання інструментів кібербезпеки, аналізу цифрових доказів, а також методів протидії різноманітним формам кіберзлочинності, включаючи фішинг, шахрайство з криптовалютами, кібератаки на критичну інфраструктуру та інші сучасні загрози. Крім технічних навичок, велика увага приділяється розвитку аналітичного мислення, здатності працювати з великими обсягами інформації та приймати швидкі та обґрунтовані рішення у стресових ситуаціях. Це забезпечує підвищення рівня професіоналізму та готовності до вирішення складних міжнародних випадків, що є необхідним для ефективної протидії сучасним загрозам. Завдяки цим заходам, співробітники Національної поліції України стають більш підготовленими до викликів глобальної кібербезпеки, що сприяє зміцненню національної безпеки та захисту громадян від цифрових загроз. Це сприяє підвищенню рівня професіоналізму та готовності до вирішення складних міжнародних випадків, що є необхідним для ефективної протидії сучасним загрозам.

Взаємодія з міжнародними організаціями, такими як Європол, НАТО та інші, є ще одним важливим аспектом роботи департаменту. Департамент активно співпрацює з цими організаціями для обміну досвідом, інформацією та кращими практиками у сфері боротьби з кіберзлочинністю. Така взаємодія сприяє зміцненню міжнародної безпеки та ефективній протидії глобальним загрозам, забезпечуючи більш скоординовані та результативні заходи проти кіберзлочинності.

Висновок. У сучасну цифрову епоху боротьба з кіберзлочинністю набуває все більшої важливості через стрімкий розвиток інформаційних технологій та глобалізацію суспільства. Зростаюча кількість кіберінцидентів, що впливають на безпеку окремих осіб та держав, вимагає комплексного підходу та ефективної координації міжнародних зусиль. Важливою складовою цього процесу є співпраця між національними правоохоронними органами та міжнародними організаціями, такими як Інтерпол, яка забезпечує обмін інформацією та координацію дій на глобальному рівні.

Інтерпол, як міжнародна організація кримінальної поліції, відіграє ключову роль у створенні та підтримці механізмів протидії кіберзлочинності. Завдяки своїй глобальній мережі та доступу до сучасних інформаційних систем, організація здатна оперативно реагувати на нові загрози та забезпечувати ефективну співпрацю між країнами-членами.

Це дозволяє не лише розслідувати та затримувати кіберзлочинців, але й запобігати потенційним атакам через обмін аналітичними даними та найкращими практиками у сфері кібербезпеки.

Таким чином, лише через тісну міжнародну співпрацю, обмін інформацією та постійне вдосконалення методів боротьби можна досягти значущих результатів у захисті цифрового простору від кіберзлочинності.

Анотація

У сучасному світі цифрові технології проникають у всі сфери життя, сприяючи розвитку економіки, науки та суспільства. Проте разом з перевагами вони створюють нові загрози, особливо в сфері безпеки. Кіберзлочинність стає однією з найсерйозніших проблем глобального масштабу, оскільки злочинці використовують інтернет для здійснення атак на критичну інфраструктуру, фінансові системи та приватних осіб. Різноманіття форм кіберзлочинності та постійне вдосконалення технічних засобів злочинців ставить перед правоохоронними органами нові виклики, що вимагають відповідної координації зусиль на міжнародному рівні.

Інтерпол, як міжнародна організація, відіграє важливу роль у боротьбі з транснаціональною злочинністю, зокрема у сфері кіберзлочинності. Завдяки своїй глобальній мережі, Інтерпол може забезпечувати оперативний обмін інформацією між країнами, що є важливим для запобігання і розслідування злочинів, здійснених через інтернет. Одним із ключових інструментів Інтерполу в цьому контексті є спеціалізовані підрозділи, що займаються виключно питаннями кіберзлочинності, серед яких особливої уваги заслуговує Global Cybercrime Programme.

Сучасна кіберзлочинність охоплює такі явища, як хакерські атаки, крадіжка персональних даних, шкідливе програмне забезпечення, а також більш складні форми шахрайства з криптовалютою та фінансовими ресурсами. Інтерпол співпрацює з провідними компаніями у сфері інформаційних технологій для розробки інноваційних рішень, що дозволяють не лише розслідувати злочини, але й попереджувати їх. Проте швидкий розвиток технологій вимагає постійного оновлення методів боротьби, щоб випереджати злочинців на крок вперед.

Ключовим аспектом успішної боротьби з кіберзлочинністю є співпраця між державами, оскільки цифрові злочини часто перетинають національні кордони. Інтерпол надає платформу для такого співробітництва, дозволяючи країнам обмінюватися досвідом і ресурсами. Незважаючи на це, ефективність боротьби залежить не лише від міжнародної співпраці, але й від законодавчих ініціатив на національному рівні, спрямованих на посилення відповідальності за кіберзлочини та запровадження інноваційних заходів безпеки.

Таким чином, нові загрози в кіберпросторі потребують глибокого дослідження, а роль Інтерполу у їхній нейтралізації має стати предметом широкого аналізу.

Ключові слова: Інтерпол, кіберзлочинність, кібербезпека, хакерські атаки, цифрові загрози, шахрайство, криптовалюта, персональні дані, шкідливе програмне забезпечення, кіберпростір, міжнародна співпраця, транснаціональна злочинність, інноваційні рішення, законодавчі ініціативи, кіберзахист.

Striiashko H.M., Zamryha A. V. Interpol as an entity in the fight against cybercrime: new threats in the digital age

Summary

In the modern world, digital technologies permeate all aspects of life, driving the development of the economy, science, and society. However, alongside the benefits, they also create new threats, particularly in the realm of security. Cybercrime has become one of the most serious global issues, as criminals use the internet to launch attacks on critical infrastructure, financial systems, and individuals.

The variety of cybercrime forms and the constant advancement of criminal technologies present new challenges for law enforcement agencies, requiring coordinated international efforts.

Interpol, as an international organization, plays a crucial role in combating transnational crime, including cybercrime. Through its global network, Interpol can facilitate the exchange of information between countries, which is essential for preventing and investigating crimes committed via the internet. One of Interpol's key tools in this context is its specialized units focusing exclusively on cybercrime, among which the Global Cybercrime Programme deserves particular attention.

Modern cybercrime encompasses phenomena such as hacking attacks, theft of personal data, malicious software, and more complex forms of fraud involving cryptocurrency and financial resources. Interpol collaborates with leading technology companies to develop innovative solutions that not only investigate crimes but also prevent them. However, the rapid technological development requires continuous updates to combat methods to stay ahead of criminals.

A critical aspect of effective cybercrime combat is cooperation between states, as digital crimes often cross national borders. Interpol provides a platform for such cooperation, allowing countries to exchange experiences and resources. Despite this, the effectiveness of the fight depends not only on international collaboration but also on national legislative initiatives aimed at enhancing accountability for cybercrimes and implementing innovative security measures.

Thus, the new threats in cyberspace require in-depth research, and Interpol's role in their neutralization should be the subject of extensive analysis.

Key words: Interpol, cybercrime, cybersecurity, hacking attacks, digital threats, fraud, cryptocurrency, personal data, malicious software, cyberspace, international cooperation, transnational crime, innovative solutions, legislative initiatives, cyber defense.

Список використаних джерел:

1. Міжнародна організація кримінальної поліції – Інтерпол. Статут Міжнародної організації кримінальної поліції – Інтерполу. Прийнятий 13 червня 1956 року. URL: https://www.interpol.int/en/How-we-work/Legal-tools/INTERPOL-Statut
2. Про Національну поліцію: Закон України від 2 липня 2015 року, №580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text
3. Про внесення змін до законів України «Про Національну поліцію» та «Про Дисциплінарний статут Національної поліції України» з метою оптимізації діяльності поліції, у тому числі під час дії воєнного стану: Закон України від березня 2022 року, №2123-IX. URL: https://zakon.rada.gov.ua/laws/show/2123-20#n610
4. Протокол ратифіковано із застереженням Законом N 23-V (23-16) від 21 липня 2006. Відомості Верховної Ради, 2006. N 39. Ст. 328.