ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ В УМОВАХ ВОЄННОГО СТАНУ

КОГУТ Іван Анатолійович - асистент кафедри кримінального права та процесу, аспірант кафедри кримінального права та процесу, Хмельницький університет управління та права імені Леоніда Юзькова
https://orcid.org/0000-0001-9900-2273
УДК 343.9
DOI: https://doi.org/10.71404/LAW.UA.2025.1.15

Дослідження присвячене комплексному аналізу особливостей розслідування кіберзлочинів в умовах воєнного стану в Україні. Розглянуто питання правового регулювання кіберзлочинності, зокрема зміни до Кримінального кодексу України та Кримінального процесуального кодексу України, спрямовані на підвищення ефективності боротьби з кіберзлочинністю в умовах воєнного стану.

На основі актуальних статистичних даних і чинного нормативно-правового регулювання досліджено специфіку виявлення та розслідування кіберзлочинів у контексті російської агресії. У роботі проаналізовано законодавче визначення поняття «кіберзлочин» відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», а також досліджено ключові характеристики кіберзлочинності як явища, зокрема її глобальний характер, стрімкий технологічний розвиток, високий рівень анонімності та різноманітність мотивацій правопорушників.

Проаналізовано випадки масштабних кібератак на українські державні установи та об'єкти критичної інфраструктури з початку повномасштабного вторгнення. Наведено статистичні дані Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, які свідчать про значне зростання кіберінцидентів у 2023 році порівняно з попередніми роками.

Висвітлено специфічні проблеми розслідування кіберзлочинів в умовах воєнного стану, зокрема підвищену складність виявлення зловмисників через використання анонімайзерів, ризики для життя слідчих під час проведення розслідувань у зонах активних бойових дій, труднощі з фіксацією слідів та доказів у цифровій мережі, а також отримання даних з тимчасово окупованих територій.

Розглянуто особливості кіберзлочинів у військовому середовищі, зокрема специфіку доступу до конфіденційної інформації та державної таємниці, вплив стресових умов на особовий склад, використання спеціального програмного забезпечення та систем оперативного управління. Окрему увагу приділено проблемі спеціального суб'єкта кіберзлочину у військовому середовищі – посадової військової особи.

Ключові слова: кіберзлочин, кіберзлочинність, воєнний стан, розслідування, кіберполіція, військове середовище, кібератака, кіберінцидент, кібербезпека, цифрові докази, кримінальне провадження,

Постановка проблеми

Світова тенденція до цифровізації багатьох процесів, які стосуються публічного управління, зумовила виникнення абсолютно нової категорії порушень, для яких характерною рисою є їх вчинення в комп'ютерному просторі. Мова йде про виникнення явища кіберзлочинності, яку можна описати як сукупність кіберзлочинів. Кіберзлочинність створює серйозну загрозу національній безпеці України, оскільки українська інформаційна сфера страждає не лише від кіберзлочинів побутового масштабу, а й від масових кібератак з боку росій-

ської федерації. У результаті на небезпеку наражаються не лише електронно-обчислювальні машини та комп'ютерні мережі в межах військової інфраструктури, а й цивільної.

На поширення кіберзлочинів вплинуло багато факторів, що виникли після початку повномасштабного вторгнення, зокрема втрата людьми домівок, близьких, введення режиму воєнного стану, втрата постійної роботи тощо. Інтернет-шахраї отримали простір, на якому можуть більш активно здійснювати свою діяльність, а також велику кількість потенційних жертв, які сьогодні є надзвичайно вразливими через різні обставини. Водночас населення відчуває вплив масових кібератак, що завдаються українським об'єктам критичної інфраструктури, оскільки через них робота державних органів та органів місцевого самоврядування може призупинятися на певний час. Кіберзлочини незалежно від їх масштабу мають певні особливості розслідування, а воєнний стан лише додає окремі проблемні аспекти, з якими стикаються суб'єкти розслідування кіберзлочинів. Відтак виникає низка питань щодо того, якою є специфіка здійснення розслідування кіберзлочинів у зв'язку із запровадженням на території України воєнного стану.

Мета дослідження

Метою дослідження є проведення комплексного аналізу особливостей розслідування кіберзлочинів в умовах воєнного стану в Україні.

Стан опрацювання проблематики

Станом на сьогодні проблематика розслідування кіберзлочинів, зокрема тих, що вчиняються в умовах воєнного стану, є надзвичайно актуальною. Тому її дослідженню присвячені праці таких науковців, як А. М. Вейц, І. О. Воронов, О. А.Самойленко, Б. М. Головкін, О. І. Денькович, А. С. Колодіна, В. В. Луцик, О. А. Матвієнко, І. М. Осика, Д. М. Цехан, В. М. Шевчук та інших. Попри значну увагу з боку науковців, проблематика розслідування кіберзлочинів залишається актуальною та потребує подальших наукових розвідок.

Виклад основного матеріалу

Відповідно до законодавчого визначення кіберзлочину, наведеного в Законі України «Про основні засади забезпечення кібербезпеки України», кіберзлочином (комп'ютерним злочином) є суспільно небезпечне винне діяння, вчинене у кіберпросторі та/або з його використанням, за яке передбачена відповідальність законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Погоджуємося з думкою, що найбільш істотною ознакою кіберзлочину є використання інформаційних (комп'ютерних) систем під час його вчинення. Злочинець застосовує специфічні можливості та властивості таких систем для реалізації свого кримінально протиправного умислу [2, с. 235].

Серед ознак кіберзлочинності доцільно виділити характеристики, на які звернув увагу Коцман І. І., а саме:

1) транснаціональність та глобальність кіберзлочинів – вони не мають кордонів і можуть вчинятися в будь-якій точці світу або з будь-якої точки світу, що ускладнює регулювання кіберзлочинності на національному рівні;

2) швидка еволюція технологій – кіберзлочинці постійно вдосконалюють свої знання, навички маскування в Інтернеті та використовують у своїй діяльності бекдори, експлойти, TOR- і VPN-мережі, інструменти для фішингу, анонімайзери тощо;

3) високий рівень анонімності – кіберпростір дає змогу злочинцям залишатися анонімними та швидко приховувати свої сліди, що ускладнює роботу правоохоронних органів;

4) різноманітні мотивації правопорушень – кіберзлочини можуть вчинятися з різних причин: фінансова вигода, ідеологічні, соціальні чи політичні мотиви, особиста помста, шпигунство тощо;

5) залежність від технологічних вразливостей – кіберзлочинці використовують слабкі місця в системах захисту та програмному забезпеченні для їх ураження. Тому кібербезпека стає ключовою складовою корпоративної політики та державного регулювання [3, с. 248].

З огляду на останню зазначену ознаку кіберзлочинності, варто вказати, що це явище присутнє не лише на побутовому рівні, оскільки воно також може яскраво проявлятися і в міждержавному полі. Особливо «болючим» питання кіберзлочинності постало для України після початку повномасштабного вторгнення, під час якого українські сервери зазнали численних кібератак з боку російської федерації.

Серед прикладів масових кібератак можна навести такі випадки:

- атака хакерського угруповання Strontium 08.04.2022 року, коли було зроблено спробу отримати доступ до комп'ютерних мереж ЄС, США та України для забезпечення тактичної підтримки фізичного вторгнення рф та викрадення конфіденційної інформації;

- кібератака на українські державні установи від 23.03.2022 року з використанням програми Cobalt Strike Beacon, яка уражає комп'ютер у разі відкриття програми;

- кібератака на українського провайдера Укртелеком від 28.03.2022 року, під час якої ворог намагався проаналізувати налаштування української ІТ-інфраструктури, вивести з ладу сервіси та обладнання, а також отримати контроль над мережею компанії [4].

Наведені випадки є лише прикладами масових кібератак. Щодо атак менших масштабів можна лише здогадуватися, оскільки про випадки персональних зламів та ураження конкретизованих інтернет-користувачів повідомляється рідко.

Крім того, випадки кібератак на українські об'єкти критичної інфраструктури були зафіксовані ще в 2014 році. Ці атаки здійснювались різними кібергрупами за підтримки урядових структур рф на такі об'єкти, як Закарпаттяобленерго, Центральна виборча комісія, Укрзалізниця, банківські установи, Бориспільський аеропорт тощо [5, с. 113].

Одні з останніх статистичних даних щодо кіберзлочинів в Україні демонструють результати, які свідчать про ретельний розгляд повідомлень про вчинення кіберзлочинів. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України повідомляє, що за 2023 рік за допомогою Системи виявлення вразливості і реагування на кіберінциденти та кібератаки було опрацьовано 18 млрд подій. При первинному аналізі було детектовано 133 млн подій, під час фільтрації підозрілих подій та вторинного аналізу опрацьовано 148 тис. критичних подій, а аналітики безпеки зареєстрували 1105 кіберінцидентів. У порівнянні з 2022 роком кількість зареєстрованих кіберінцидентів у 2023 році зросла на 62,5%, що є дуже високим показником. Більшість з кіберінцидентів пов'язана з впливом шкідливого програмного коду. Серед інших — збір зловмисником інформації, спроби втручання, порушення доступності, порушення властивостей інформації, шахрайство тощо [6]. Попри це українська інформаційна структура продовжує функціонувати. Значною мірою такий результат можливий завдяки своєчасним заходам з посилення кібербезпеки, які надавалися такими міжнародними партнерами, як Великобританія, ЄС, США та інші країни [5, с. 113].

Початок повномасштабного вторгнення зумовив мобілізацію всіх сил забезпечення безпеки країни, зокрема й відділів кібербезпеки, для забезпечення оборони. Це створило умови, за яких злочинна діяльність, зокрема для кібершахраїв, стала легшою для здійснення. Бідність населення, завантаженість правоохоронних органів, втрата місця проживання, страждання через втрату близьких, психічне перенавантаження – усе це сприяє активізації кібершахрайства. У 2021 році кіберполіція скерувала до суду близько 2200 кримінальних проваджень щодо інтернет-шахрайств. У 2022 році кількість проваджень зросла до понад 6600 одиниць. Інтернет-шахрайства є надзвичайно поширеними, і 70% звернень до кіберполіції становлять саме такі звернення [7, с. 547].

Відтак постає питання не лише про забезпечення фізичної оборони держави в гібридній війні, а й про кібероборону України. Для реалізації кібероборони необхідно визначити нові стратегії та методи її здійснення, а також оновлювати відповідне правове регулювання в цій галузі. Усе це потрібно для налаштування діяльності правоохоронних органів у сфері розслідування

кіберзлочинів та протидії кіберзлочинам держави-агресора. Правоохоронним органом, який має безпосередній зв'язок із розслідуванням кіберзлочинів, є Департамент кіберполіції Національної поліції України, що функціонує з жовтня 2015 року [8].

Станом на сьогодні у сфері правового регулювання здійснено оптимізацію кримінального процесуального та кримінального законодавства: прийнято закони, що визначають підстави та процесуальні механізми притягнення кіберзлочинців до кримінальної відповідальності. Мова йде про Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24.03.2022 та Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15.03.2022. У зв'язку з цим кримінальна відповідальність за кіберзлочини передбачається за вчинення кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України (кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, ст.ст. 361-3631), а також за кримінальне правопорушення, передбачене ч. 4 ст. 190 Кримінального кодексу України (шахрайство, вчинене у великих розмірах або шляхом незаконних операцій з використанням електронно-обчислювальної техніки) [9].

Вказані кримінальні правопорушення, які загалом можна описати як кіберзлочини, мають свою специфіку, оскільки вони вчиняються в мережі Інтернет. Через це регламентовані в КПК України заходи здійснення розслідування можуть бути неефективними. Крім того, окрему категорію кіберзлочинів складають ті, що вчиняються у військовому середовищі. Як наголошує А.М. Вейц, специфіка цих злочинів полягає в конфіденційності інформації, яка доступна для військовослужбовців, доступі до державної таємниці, впливі стресових умов на особовий склад, використанні спеціального програмного забезпечення та вимогах щодо наявності певних технічних знань тощо. У зв'язку з цим, а також враховуючи постійний вплив агресії рф, військове середовище стає особливо вразливим і, відтак, ідеальною мішенню для кіберзлочинців [2, с. 236].

З огляду на вказане, можна виділити наступні аспекти, які існують у розслідуванні кіберзлочинів і які варто розглянути для розуміння специфіки правопорушень цієї категорії – підвищена складність виявлення зловмисників. Як зазначалося раніше, сьогодні широко доступні такі інструменти, як анонімайзери. Це сукупність інструментів, які дозволяють користувачу мережі залишатися анонімним. З одного боку, ці інструменти служать для захисту приватності особи, якщо користувач бажає залишитися анонімним у мережі. З іншого боку, вони допомагають кіберзлочинцям залишатися непоміченими, через що суб'єкти, які розслідують кіберзлочини, мають мінімальні інформаційні сліди, за які вони можуть зачепитися при здійсненні розслідування.

Серед різноманіття анонімайзерів можна виділити такі:

1) сайти-анонімайзери («Хамелеон», «FilterBypass», «HideMe», «ProxySite» тощо). Ці сайти дозволяють користувачу анонімно відкривати інші інтернет-ресурси, змінюючи IP-адресу особи;

2) VPN-плагіни («Touch VPN», «ZenMate», «Browsec», «Betternet», «Hotspot Shield», «Free VPN», «TurboVPN», «VPN Master» тощо). Ці плагіни шифрують дані, що проходять через мережу, приховують IP-адресу користувача та роблять невидимою історію трафіку. Плагіни можуть бути платними та безкоштовними. Серед останніх найпоширенішими є ті, що функціонують у вигляді розширень для браузерів, таких як «Chrome», «Firefox» тощо;

3) анонімні браузери («Tor Browser», «Epic Browser», «DuckDuckGo» та інші). Ці браузери не фіксують запити користувача, тому історія пошуку не зберігається, так само як і кеш та файли cookies [10].

Погоджуємося з позицією А.М. Вейца, що фактично весь кіберпростір є середовищем для вчинення кіберзлочину, а сліди

цього злочину – це будь-які інформаційні зміни, що відбуваються в кіберпросторі. Сліди кіберзлочину можуть бути зафіксовані лише на пристрої, з якого вчинено злочин, або на іншій мережі чи комп'ютерній системі, де вони залишилися. Це створює суттєві труднощі, оскільки доступ до машин або мереж може бути обмежений, зокрема в умовах воєнного стану, що ускладнює процес збору доказів. Крім того, самі сліди можуть бути змінені, знищені або безповоротно зникнути ще до виявлення злочину, під час його вчинення, або навіть у процесі досудового розслідування. Ще однією проблемою є те, що кіберпростір не має фізичних меж, і, як зазначає науковець, він є надзвичайно важким для повного контролю. Це означає, що на відміну від традиційних злочинів, де сліди можуть бути зафіксовані в конкретних місцях, кіберзлочини можуть залишати значно менше видимих або конкретних доказів, а зловмисники мають доступ до інструментів, що дозволяють їм залишатися невидимими або маскувати свої дії. Враховуючи швидкість змін і еволюцію технологій, злочинці мають можливість оперативно стирати або модифікувати сліди, що додатково ускладнює роботу правоохоронних органів [2, с. 236]. Усі ці фактори зумовлюють потребу в удосконаленні методів збору, фіксації та збереження цифрових доказів, що є критичними для розслідування кіберзлочинів».

Висновки

З викладеного матеріалу можна сформулювати висновки щодо наступного. Розслідування кіберзлочинів в умовах воєнного стану характеризується низкою специфічних особливостей та викликів. Основними проблемами в цій сфері є складність виявлення зловмисників через використання засобів забезпечення анонімності, ризики для життя слідчих у зонах активних бойових дій, труднощі з отриманням цифрових доказів, зокрема з окупованих територій, тощо. Особливу категорію становлять кіберзлочини, що вчиняються у військовому середовищі. Вони мають підвищений рівень складності через специфіку суб'єкта вчинення та наявність доступу до конфіденційної інформації. Ефективне розслідування таких злочинів ускладнюється також відсутністю спеціалізованих органів військової юстиції.

Кіберінциденти та кібератаки є поширеним явищем серед українців. Статистичні дані свідчать про значне зростання кількості кіберінцидентів за останні роки, що вимагає вдосконалення правового регулювання та посилення міжнародної співпраці у сфері кіберзлочинності. Важливим аспектом залишається також потреба в постійному підвищенні кваліфікації слідчих, а також забезпеченні правоохоронних органів належним технічним обладнанням та оснащенням.

Література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.01.2025).

2. Вейц А.М. Особливості розслідування кіберзлочинів, вчинених у військовому середовищі. *Інформація і право*. 2024. Вип. 4. С. 233-242.

3. Коцман І. І. Державне регулювання протидії кіберзлочинності в Україні: поняття та основні напрямки. *Публічне управління та адміністрування в Україні*. 2024. Вип. 40. С. 245-252.

4. Єрема М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *Liga:Zakon*. 2022. URL: https://shorturl.at/7gEsn (дата звернення: 27.01.2025).

5. Мазанка Е. В., Гасімов Ш. Ю., Копилов Е. В. Щодо окремих питань протидії кіберзлочинності в умовах воєнного стану. *Colloqium journal*. 2023. Вип. 31. С. 112-115.

6. Звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. *Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України*. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (дата звернення: 29.01.2025).

7. Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний*

науковий електронний журнал. 2022. Вип. 11. С. 546-549.

8. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13.10.2015 №831. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text (дата звернення: 29.01.2025).

9. Кримінальний кодекс України: Закон України від 05.04.2001 №2341-III. *Верховна Рада України. Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 31.01.2025).

10. Нагорна А. Кращі безкоштовні анонімайзери: VPN, онлайн, браузери. Для тих, кому важлива приватність. *Dev.ua*. 2022. URL: https://dev.ua/news/best-free-anonymizers-vpn (дата звернення: 31.01.2025).

Kohut I. A.
kohut.ivan99@gmail.com

PECULIARITIES OF CYBERCRIME INVESTIGATION UNDER MARTIAL LAW

The study is dedicated to a comprehensive analysis of the peculiarities of cybercrime investigations under martial law in Ukraine. It examines the legal regulation of cybercrime, including amendments to the Criminal Code of Ukraine and the Criminal Procedure Code of Ukraine, aimed at improving the effectiveness of the fight against cybercrime under martial law.

Based on current statistical data and existing legal regulation, the study investigates the specifics of detecting and investigating cybercrimes in the context of Russian aggression. The work analyzes the legislative definition of the concept of "cybercrime" according to the Law of Ukraine "On the Fundamentals of Cybersecurity of Ukraine" and explores the key characteristics of cybercrime as a phenomenon, including its global nature, rapid technological development, high level of anonymity, and the diversity of motivations of offenders.

The study analyzes cases of large-scale cyberattacks on Ukrainian government institutions and critical infrastructure since the beginning of the full-scale invasion. Statistical data from the State Cyber Protection Center of the State Special Communications and Information Protection Service of Ukraine are provided, showing a significant increase in cyber incidents in 2023 compared to previous years.

The study highlights specific problems of investigating cybercrimes under martial law, such as the increased difficulty in identifying perpetrators due to the use of anonymizers, risks to the lives of investigators during investigations in active combat zones, challenges in securing traces and evidence in digital networks, and the acquisition of data from temporarily occupied territories.

The study also examines the peculiarities of cybercrimes in the military environment, including access to classified information and state secrets, the impact of stress conditions on personnel, the use of special software, and operational management systems. Special attention is given to the issue of the special subject of cybercrime in the military environment – military officials.

Key words: cybercrime, cybercrime, martial law, investigation, cyberpolice, military environment, cyberattack, cyberincident, cybersecurity, digital evidence, criminal proceedings.