DOI https://doi.org/10.36059/978-966-397-501-6-104

КІБЕРРОЗВІДКА І КОНТРРОЗВІДКА В УКРАЇНІ: ПРАВОВІ МЕЖІ ПІД ЧАС ВОЄННОГО СТАНУ

Ларченко Марина Олександрівна
кандидат юридичних наук, доцент,
доцент кафедри кібербезпеки та математичного моделювання,
Національний університет «Чернігівська політехніка»
м. Чернігів, Україна;
доцент кафедри політології, права та філософії,
Ніжинський державний університет імені Миколи Гоголя
м. Ніжин, Україна

У сучасних умовах широкомасштабної збройної агресії проти України особливого значення набуває проблема функціонування системи національної безпеки в кіберпросторі. Воєнний стан, запроваджений на всій території України з 24 лютого 2022 року, не лише змінив безпековий ландшафт держави, але й трансформував правові механізми реагування на загрози у цифровому середовищі. Особливої актуальності набули питання кіберрозвідки та контррозвідки як інструментів стратегічного забезпечення обороноздатності країни. Утім, стрімкий розвиток цифрових технологій, відсутність усталених міжнародних стандартів у сфері кібердіяльності та наявність прогалин у національному законодавстві створюють низку нормативно-правових колізій, які ускладнюють розмежування між легітимною діяльністю спецслужб та потенційно кримінально караною поведінкою.

Метою даного дослідження є системний аналіз правових меж здійснення кіберрозвідки та контррозвідки в Україні в умовах дії правового режиму воєнного стану, визначення кримінально-правових орієнтирів такої діяльності, а також ідентифікація існуючих проблем у законодавстві, яке потребує вдосконалення.

У національному правовому полі відсутнє чітке нормативне визначення понять «кіберрозвідка» та «кіберконтррозвідка». Водночас, на доктринальному рівні під кіберрозвідкою розуміється комплекс дій, спрямованих на здобуття інформації з кіберпростору про потенційні або наявні загрози національній безпеці, а також на виявлення діяльності іноземних розвідок, кіберугруповань чи інших ворожих суб'єктів. Кіберконтррозвідка, своєю чергою, охоплює заходи з попередження, виявлення і нейтралізації кібершпигунства, деструктивного впливу, проникнення у державні системи та критичну інформаційну інфраструктуру.

Ключовим суб'єктом у сфері контррозвідувальної діяльності відповідно до Закону України «Про Службу безпеки України» є СБУ. Окремі функції також покладаються на Головне управління розвідки Міністерства оборони України (ГУР МО) та Службу зовнішньої розвідки України (СЗРУ). Збройні сили України (зокрема їх кіберпідрозділи) залучаються до виконання окремих завдань з оборони у кіберпросторі, однак не мають автономного мандата на проведення розвідувальної діяльності.

Законодавство України не містить окремого нормативного акта, що врегульовував би правовий режим здійснення кібероперацій у період воєнного стану. Водночас, деякі положення можна інтерпретувати як такі, що створюють правову основу для відповідної діяльності. Серед них: Закони України «Про розвідку» (2020), «Про контррозвідувальну діяльність» (2002), «Про національну безпеку України» (2018), Укази Президента України про введення в дію рішень РНБО з питань кібербезпеки.

Важливою є також Стратегія кібербезпеки України (затверджена у 2021 році), яка передбачає розвиток спроможностей у сфері кіберрозвідки та кіберзахисту, а також створення системи кібероборони, інтегрованої в загальну архітектуру національної безпеки.

Разом із тим, законодавство не встановлює чітких процедур, меж та умов здійснення кібероперацій, зокрема пов'язаних із втручанням у цифрові системи, отриманням даних без згоди суб'єкта, або проведенням наступальних дій проти об'єктів критичної інфраструктури противника.

Ключовою проблемою є відсутність чіткого розмежування між легітимними діями державних суб'єктів у кіберпросторі та діяннями, які можуть кваліфікуватися як злочини, передбачені Кримінальним кодексом України. Серед таких – втручання в роботу електронно-обчислювальних систем (ст. 361 КК України), несанкціоноване збирання інформації (ст. 362), незаконне використання інформації з обмеженим доступом (ст. 328, 330, 361-2).

Проблематика посилюється в умовах воєнного стану, коли виникає потреба у проведенні гнучких, швидких і часто несанкціонованих дій у кіберпросторі. Наприклад, здійснення атаки на ворожі сервери або перехоплення комунікацій може одночасно вважатися актом кібероборони і порушенням норм національного чи міжнародного права, якщо такі дії не були належним чином санкціоновані або перевищують межі необхідного.

Додаткову складність становлять дії цивільних осіб, зокрема учасників неформального об'єднання «ІТ-армія України», які можуть

брати участь у кібератаках проти інфраструктури ворога [1]. Відсутність правового статусу таких суб'єктів створює ризики кваліфікації їх дій як самоуправства або навіть диверсії, з точки зору формальної логіки КК України.

Закон України «Про розвідку» передбачає, що оперативно-розшукова та розвідувальна діяльність повинна здійснюватися в межах повноважень, визначених законом, з дотриманням принципів законності, професійності, пропорційності та необхідності. Відхилення від цих принципів може призвести до перевищення влади або службових повноважень (ст. 365 КК), зловживання владою (ст. 364), порушення недоторканності приватного життя (ст. 182), або розголошення державної таємниці (ст. 328).

У зв'язку з цим особливої ваги набуває обґрунтування правомірності кібероперацій, що здійснюються державними органами. Ключовим елементом має бути наявність чітко визначеного правового мандата, належного процесуального оформлення (наказ, дозвіл, протокол взаємодії) та фіксації результатів діяльності. В іншому випадку виникає юридична невизначеність, що підриває правові гарантії контролю за діяльністю спецслужб та створює потенціал для зловживань.

У міжнародному праві досі не сформовано уніфікованих правил щодо здійснення кіберрозвідки, однак ряд документів, зокрема Талліннський мануал з міжнародного права, що застосовується до кібероперацій, пропонують підхід, який базується на принципах суверенітету, ненападу, невтручання, пропорційності і необхідності. Водночас, ці документи не є обов'язковими до виконання, що створює простір для юридичної маневреності [2].

Україна у своїй практиці послуговується принципом самооборони в умовах збройної агресії (ст. 51 Статуту ООН), що дає легітимну підставу для здійснення як оборонних, так і проактивних дій у кіберпросторі. Проте правова доктрина досі не містить остаточного визначення правових меж таких дій.

Таким чином, діяльність у сфері кіберрозвідки та контррозвідки в Україні в умовах воєнного стану є необхідною та виправданою з точки зору національної безпеки. Водночас, нормативно-правове поле цієї діяльності залишається фрагментарним, що створює ризики для порушення законності з боку державних органів та залучених суб'єктів. Необхідним є: 1) визначення на законодавчому рівні термінів «кіберрозвідка», «кіберконтррозвідка», «наступальна кібероперація»; 2) встановлення чітких процедур санкціонування, документування і контролю кібероперацій; 3) розробка правового статусу цивільних учасників кібероборони (зокрема «ІТ-армії»); 4) гармонізація національного законодавства з міжнародними стандартами та

рекомендаціями у сфері кібербезпеки; 5) посилення парламентського і громадського контролю за діяльністю спецслужб у цифровому просторі.

Успішне вирішення зазначених проблем сприятиме посиленню спроможності України захищатися в умовах гібридної війни, збереженню принципів правової держави та захисту прав людини навіть в екстремальних умовах.

Література:

1. Ivan Savych. Понад 400 російських компаній зазнали збитків від наших дій лише протягом останнього року». Речник IT Армії України – про боротьбу в кіберпросторі. DOU. 8 грудня 2023. URL: https://dou.ua/lenta/interviews/it-army-operations/

2. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Gen. ed. Michael N. Schmitt. – Cambridge University Press, 2017. URL: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

DOI https://doi.org/10.36059/978-966-397-501-6-105

РИМСЬКИЙ СТАТУТ У ПРАКТИЦІ КАСАЦІЙНОГО КРИМІНАЛЬНОГО СУДУ У СКЛАДІ ВЕРХОВНОГО СУДУ

Марченко Андрій Романович
асистент кафедри процесуального права,
Чернівецький національний університет імені Юрія Федьковича
м. Чернівці, Україна

20 травня 2021 року Верховна Рада (Парламент України) ухвалила законопроєкт № 2689 «Про внесення змін до деяких законодавчих актів щодо імплементації норм міжнародного кримінального та гуманітарного права» 248 голосами «за» з 363 присутніх народних депутатів. Ухвалення законопроєкту є історичною подією, яка дозволить Україні притягнути до відповідальності за міжнародні злочини, скоєні на сході України та окупованій території Криму в контексті збройного конфлікту, а також забезпечить ефективний внутрішньодержавний доступ до правосуддя для жертв.

01 січня 2025 року Статут набрав чинність для України та став частиною національного законодавства. Цьому передувало прийняття Закону України від 21 серпня 2024 року № 3909-IX «Про ратифікацію