Пономаренко Віктор Володимирович, *викладач кафедри адміністративного права та процесу навчально-наукового інституту права та соціального менеджменту ДонДУВС*

ПРАВОВІ ЗАСАДИ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ В УМОВАХ СУЧАСНИХ БЕЗПЕКОВИХ ВИКЛИКІВ

Сучасний етап розвитку української державності характеризується наявністю значної кількості внутрішніх та зовнішніх загроз, які безпосередньо впливають на стан національної безпеки. Повномасштабна збройна агресія проти України, активізація диверсійної діяльності, кібератак, інформаційно-психологічних операцій, а також зростання терористичних ризиків актуалізували питання ефективного функціонування органів сектору безпеки і оборони. У цих умовах особливе місце належить Службі безпеки України як державному органу спеціального призначення з правоохоронними функціями, на який покладається забезпечення державної безпеки, захист суверенітету, конституційного ладу та територіальної цілісності держави [1].

Правові засади діяльності Служби безпеки України визначаються насамперед Конституцією України [2], Законом України «Про Службу безпеки України» [1], Законом України «Про національну безпеку України» [3], а також іншими нормативно-правовими актами, що регулюють сферу державної безпеки. Конституція України закріплює положення про те, що забезпечення державної безпеки та захист державного кордону покладаються на відповідні військові формування та правоохоронні органи держави [2]. Водночас саме СБУ наділена широким колом повноважень щодо виявлення, попередження та припинення злочинів проти основ національної безпеки України.

В умовах сучасних безпекових викликів діяльність СБУ зазнала суттєвих трансформацій. Якщо раніше основна увага зосереджувалася переважно на контррозвідувальній діяльності та боротьбі з тероризмом, то сьогодні перед Службою постали нові завдання, пов’язані із протидією гібридним загрозам, кіберзлочинності, інформаційним диверсіям та агентурному проникненню. Значного поширення набули злочини колабораційного характеру, державна зрада, пособництво державі-агресору, що потребує оперативного реагування та удосконалення правових механізмів діяльності СБУ.

Одним із ключових напрямів роботи Служби безпеки України є контррозвідувальна діяльність. В умовах воєнного стану вона набуває особливого значення, оскільки спрямована на недопущення підривної діяльності іноземних спецслужб та захист стратегічно важливих об’єктів держави. Практика останніх років свідчить про зростання кількості виявлених агентурних мереж, осіб, причетних до коригування ворожого вогню, передачі інформації про переміщення військових підрозділів та об’єкти критичної інфраструктури. У зв’язку з цим виникає необхідність постійного вдосконалення законодавства у сфері оперативно-розшукової діяльності та забезпечення ефективної взаємодії між суб’єктами сектору безпеки і оборони.

Не менш важливим напрямом діяльності СБУ є боротьба з тероризмом. В умовах збройного конфлікту терористичні загрози можуть проявлятися у формі диверсій, підривів об’єктів інфраструктури, організації масових заворушень та інформаційної дестабілізації суспільства. Саме тому антитерористична функція Служби безпеки України має комплексний характер та включає не лише безпосереднє припинення терористичної діяльності, а й превентивні заходи, спрямовані на усунення причин та умов її виникнення.

Окремої уваги заслуговує питання забезпечення кібербезпеки держави. У сучасних умовах кіберпростір став одним із основних напрямів ведення гібридної війни. Кібератаки на державні інформаційні ресурси, банківську систему, об’єкти енергетики та зв’язку можуть спричинити серйозні наслідки для функціонування держави. У зв’язку з цим СБУ бере активну участь у забезпеченні кіберзахисту критичної інфраструктури, виявленні кібершпигунства та протидії незаконному втручанню в інформаційні системи органів державної влади.

Разом із тим діяльність Служби безпеки України в умовах сучасних викликів супроводжується рядом проблем. Насамперед це стосується необхідності реформування СБУ відповідно до європейських стандартів. Протягом останніх років в Україні активно обговорюється питання демілітаризації окремих функцій Служби, звуження її невластивих повноважень у сфері економічних злочинів та посилення контррозвідувального напряму діяльності. Важливим аспектом також є забезпечення належного парламентського та громадського контролю за діяльністю СБУ, що сприятиме підвищенню рівня довіри суспільства до цього органу.

Особливого значення набуває проблема дотримання прав і свобод людини під час здійснення заходів у сфері державної безпеки. В умовах воєнного стану держава змушена застосовувати додаткові обмеження, пов’язані із забезпеченням безпеки населення та оборони країни. Проте навіть за таких умов діяльність правоохоронних органів повинна здійснюватися виключно на підставі закону, із дотриманням принципів верховенства права, законності та пропорційності. Саме тому важливим завданням залишається забезпечення балансу між інтересами національної безпеки та гарантіями прав людини.

Отже, у сучасних умовах Служба безпеки України відіграє ключову роль у системі забезпечення національної безпеки держави. Сучасні безпекові виклики потребують від цього органу високого рівня оперативності, ефективності та адаптивності до нових форм загроз. Водночас подальший розвиток правових засад діяльності СБУ має бути спрямований на вдосконалення законодавства, посилення демократичного контролю, впровадження сучасних механізмів протидії гібридним загрозам та забезпечення належного балансу між інтересами державної безпеки і правами людини. Лише за таких умов можливо забезпечити ефективне функціонування Служби безпеки України як одного з основних елементів системи захисту держави в умовах сучасних кризових процесів.

Список використаних джерел

1. Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229-XII. *Відомості Верховної Ради України.* 1992. № 27. Ст. 382.

2. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

3. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. *Відомості Верховної Ради України.* 2018. № 31. Ст. 241.

Приходько Юрій Павлович, *професор кафедри криміналістичного забезпечення та судових експертиз навчально-наукового експертно-криміналістичного інституту НАВС, кандидат юридичних наук, доцент;*

Поліщук Віталій Вячеславович, *старший викладач кафедри криміналістичного забезпечення та судових експертиз навчально-наукового експертно-криміналістичного інституту НАВС*

ВИКОРИСТАННЯ OSINT-ДАНИХ ЯК НАЛЕЖНИХ І ДОПУСТИМИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ ПРО ВОЄННІ ЗЛОЧИНИ

Сучасний збройний конфлікт, спричинений повномасштабною воєнною агресією російської федерації проти народу України, сильно змінив парадигму криміналістичної науки та практики застосування сучасних технологій. Теперішній стан поточних подій полягає у безпрецедентній «цифровій прозорості» театру воєнних дій, оскільки впровадження нових сучасних методів розвивається швидко.

Розслідування злочинів, передбачених ст. 438 КК України (порушення законів та звичаїв війни), відбувається в умовах, коли традиційні методи збору доказів – огляд місця події, вилучення речових доказів, допити свідків – часто є фізично неможливими через тривалу окупацію територій, щільне за мінування або постійні активні бойові дії.

У таких реаліях розвідка на основі відкритих джерел (Open Source Intelligence, надалі – OSINT) набула статусу критично важливого інструменту формування доказової бази. Величезні обсяги візуального контенту (відео з камер спостереження, контент із соціальних мереж, стрими), супутникові знімки високої роздільної здатності, дані про переміщення техніки та геолокаційні позначки стали тими «цифровими слідами», які дозволяють реконструювати події злочину з високою точністю. Проте, незважаючи на беззаперечну ефективність OSINT для оперативного виявлення злочинців, доктринальна та законодавча база України потребує суттєвої адаптації для належної імплементації цих даних у кримінальний процес.

Основна проблема полягає у відсутності в КПК України чітких процедурних механізмів, які б забезпечували «легалізацію» даних, отриманих із глобальної мережі, гарантуючи їх автентичність, цілісність та процесуальну допустимість для національних та міжнародних судових інстанцій.

Основним викликом для органів досудового розслідування є процес перетворення отриманої «інформації» на «доказ». Відповідно до вимог ст. 86 КПК України, доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим Кодексом [1]. Натомість, більшість OSINT-інструментів діють у межах «вільного пошуку», який не завжди співпадає з класичними слідчими діями, передбаченими главами 20–23 КПК України.

По-перше, критичним є питання ідентифікації та автентифікації джерела. В умовах кібервійни та активного використання ворогом методів дезінформації, будь-який візуальний контент, що вилучається з інтернету, стає об’єктом потенційних маніпуляцій, включаючи використання технологій Deepfake. Доведення «ланцюга зберігання» (chain of custody) стає практично неможливим без застосування спеціальних технічних засобів хешування цифрових даних у момент їх отримання.

Як зазначають вітчизняні науковці, сучасна криміналістика вимагає від слідчого правоохоронного органу навичок не лише збору, а й верифікації цифрових доказів шляхом аналізу технічних метаданих, вивчення цифрового «відбитка» пристрою та контекстуальної перевірки обставин публікації [2].

По-друге, існує проблема процесуальної кваліфікації результатів OSINT. На сьогодні у вітчизняній слідчій практиці, результати OSINT найчастіше долучаються до матеріалів провадження як «інші документи» (ст. 99 КПК). Така практика створює серйозні ризики для сторони обвинувачення, оскільки сторона захисту має право ставити під сумнів походження та цілісність таких документів, а суд може