УДК 342.9:004.056
DOI https://doi.org/10.32782/2307-1745.2025.76.4

Мазепа С. О.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права та процесу
Західноукраїнського національного університету,
міжнародний дослідник
Оснабрюцького університету

РОЛЬ СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРАВООХОРОННІЙ СФЕРІ: ПРАВОВИЙ СТАТУС ТА ФУНКЦІОНАЛЬНІ ПОВНОВАЖЕННЯ

Анотація. У статті здійснено комплексний аналіз правового статусу та функціональних повноважень суб'єктів інформаційної безпеки у правоохоронній системі України. Досліджено сучасні тенденції нормативно-правового регулювання діяльності компетентних органів у сфері забезпечення інформаційної безпеки у контексті правоохоронної функції держави.

Окреслено систему суб'єктів інформаційної безпеки правоохоронної сфери, що включає Службу безпеки України, Національну поліцію, органи прокуратури, спеціалізовані підрозділи кіберполіції та інші уповноважені органи. Визначено їх основні компетенції, механізми міжвідомчої взаємодії та координації у сфері протидії кіберзагрозам та захисту критичної інформаційної інфраструктури.

Проаналізовано правові засади функціонування зазначених суб'єктів на базі чинного законодавства України, зокрема законів «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України» та відповідних підзаконних нормативних актів. Проведено порівняльний аналіз повноважень різних органів з виявленням випадків дублювання функцій та прогалин у правовому регулюванні.

Розглянуто практичні аспекти реалізації повноважень суб'єктів інформаційної безпеки, що охоплюють механізми виявлення, попередження та розслідування кіберзлочинів, захисту персональних даних, протидії інформаційним операціям та забезпечення безпеки державних інформаційних ресурсів.

Виявлено ключові проблеми правового регулювання діяльності суб'єктів інформаційної безпеки, серед яких недостатня міжвідомча координація, прогалини у законодавчому забезпеченні, дефіцит кваліфікованих кадрів та технічних ресурсів. Вказано на особливості функціонування системи інформаційної безпеки в умовах воєнного стану та необхідність адаптації правоохоронних органів до нових викликів.

Резюмовано, що підвищення ефективності діяльності суб'єктів інформаційної безпеки потребує вдосконалення їх правового статусу та функціональних можливостей. Запропоновано практичні рекомендації щодо покращення законодавчого регулювання, оптимізації міжвідомчої взаємодії та зміцнення потенціалу протидії сучасним кіберзагрозам у контексті європейської інтеграції та цифрової трансформації державного управління.

Ключові слова: інформаційна безпека, правоохоронна сфера, кібербезпека, правове забезпечення, адміністративно-правовий аспект, кримінальна відповідальність, адміністративна відповідальність, євроінтеграція, гармонізація законодавства, міжнародні стандарти, НАТО, Європейський Союз (ЄС), державна інформаційна політика, загрози інформаційній безпеці, імплементація права, суб'єкти інформаційної безпеки, юридична відповідальність, інформаційні правопорушення, пропаганда, штучний інтелект.

Постановка проблеми. Стрімкий розвиток інформаційних технологій та глобальна цифровізація громадських процесів кардинально трансформували характер сучасних загроз національній безпеці України. В умовах триваючої російської агресії особливе значення набуває ефективного функціонування системи інформаційної безпеки держави, що зумовлює необхідність чіткого правового визначення статусу та повноважень суб'єктів, відповідальних за захист інформаційного простору. Правоохоронні органи як ключові елементи системи забезпечення національної безпеки потребують удосконалення нормативно-правових засад своєї діяльності у сфері протидії кіберзагрозам, інформаційним атакам та іншим проявам деструктивного впливу на інформаційну інфраструктуру країни.

Сучасні виклики інформаційної безпеки України характеризуються високим рівнем технологічної складності та транскордонним характером, що потребує координованої діяльності різних правоохоронних структур. Водночас існуюча система розподілу повноважень між суб'єктами інформаційної безпеки містить ряд прогалин та суперечностей, які негативно впливають на ефективність протидії інформаційним загрозам. Відсутність чітко визначених між компетенцією окремих відомств, дублювання функцій та недостатня регламентація механізмів міжвідомчої взаємодії створюють передумови для зниження результативності правоохоронної діяльності в цій критично важливій сфері.

Європейський вектор розвитку України та процеси адаптації національного законодавства до стандартів Європейського Союзу актуалізують питання приведення системи забезпечення інформаційної безпеки у відповідність до міжнародних норм та найкращих практик. Імплементація директив ЄС щодо мережевої та інформаційної безпеки потребує суттєвого перегляду існуючих підходів до організації діяльності правоохоронних органів у цій сфері, що зумовлює необхідність ґрунтовного наукового аналізу чинної нормативно-правової бази та розробки пропозицій щодо її удосконалення.

Практична потреба у підвищенні ефективності протидії кіберзлочинності, захисту критичної інформаційної інфраструк-

тури та забезпечення інформаційного суверенітету держави вимагає формування науково обґрунтованих рекомендацій щодо оптимізації правового статусу та функціональних повноважень суб'єктів інформаційної безпеки у правоохоронній сфері. Відсутність комплексних досліджень, присвячених цій проблематиці, та нагальна потреба практикуючих юристів у теоретичному осмисленні сучасних тенденцій розвитку законодавства у сфері інформаційної безпеки обумовлюють високу актуальність обраної теми дослідження.

Аналіз останніх досліджень і публікацій. Проблематика правового статусу та функціональних повноважень суб'єктів інформаційної безпеки у правоохоронній сфері привертає значну увагу вітчизняних та зарубіжних дослідників. Фундаментальні засади теорії інформаційної безпеки було закладено у роботах В.А. Ліпкана, О.А. Баранова, В.М. Фурашева, які досліджували концептуальні засади формування системи забезпечення інформаційної безпеки держави [1; 2]. Зарубіжні вчені, такі як М. Данн Кавелті (M. Dunn Cavelty), А. Клімбург (A. Klimburg), Дж. Най (J. Nye), зробили суттєвий внесок у розвиток теоретичних підходів до розуміння кіберзагроз та механізмів протидії їм у контексті національної безпеки [3; 4].

Актуальні питання правового регулювання діяльності правоохоронних органів у сфері інформаційної безпеки розглядалися у працях С.С. Єсімова, М.В. Гуцалюка, А.О. Селіванова, які проаналізували особливості функціонування кіберполіції та спеціалізованих підрозділів [5; 6]. Особлива увага у науковій літературі приділяється дослідженню компетенцій Служби безпеки України в інформаційній сфері, що знайшло відображення у роботах В.П. Горбуліна, О.С. Власюка [8]. Дані дослідження формують теоретичну основу розуміння ролі різних суб'єктів у забезпеченні інформаційної безпеки держави.

Проблеми координації діяльності суб'єктів інформаційної безпеки та вдосконалення їхньої взаємодії досліджувалися І.В. Діордіцею, С.О. Гбур, Р.А. Калюжним [9; 10]. Автори акцентують увагу на необхідності створення ефективної системи міжвідомчої взаємодії та усунення дублювання функцій між різними органами. Міжнародний досвід організації системи кібербезпеки та роль правоохоронних органів у цій сфері аналізувався у контексті адаптації української моделі до європейських стандартів [11].

Сучасні виклики цифрової трансформації та їх впливом геть діяльність правоохоронних органів розглядаються у роботах молодих дослідників, як-от К.С. Муравйов, Д.В. Калаянов, О.М. Юрченка [12; 13]. Особлива увага приділяється аналізу нових видів кіберзагроз, методів їх виявлення та протидії, а також необхідності модернізації правової бази відповідно до технологічних змін. Вплив воєнного стану на функціонування системи інформаційної безпеки та адаптація правоохоронних органів до нових умов стає предметом окремих досліджень [14].

Незважаючи на значну кількість публікацій, у науковій літературі недостатньо комплексних досліджень, які системно аналізували б правовий статус усіх суб'єктів інформаційної безпеки у правоохоронній сфері з урахуванням сучасних викликів та загроз. Відсутні роботи, які б пропонували конкретні механізми вдосконалення координації між різними органами та оптимізації їх функціональних повноважень в умовах європейської інтеграції України.

Формулювання цілей статті. Мета даного дослідження полягає у комплексному аналізі правового статусу та функціональних повноважень суб'єктів інформаційної безпеки у системі правоохоронних органів України, визначенні їхньої ролі у забезпеченні захисту інформаційного простору держави та виявленні проблемних аспектів нормативно-правового регулювання їх діяльності.

Виклад основного матеріалу. Правові основи діяльності суб'єктів інформаційної безпеки у правоохоронній сфері України базуються на конституційних засадах та спеціальному законодавстві. Відповідно до статті 17 Конституції України, забезпечення інформаційної безпеки є однією з найважливіших функцій держави та справою всього українського народу [15]. Базовим нормативним актом виступає Закон України «Про національну безпеку України» від 21 червня 2018 року, який визначає основи та принципи національної безпеки, цілі та основні напрямки державної політики, яка гарантує суспільству та кожному громадянину захист від загроз [16]. Цей закон встановлює систему суб'єктів забезпечення національної безпеки та їх повноваження в інформаційній сфері.

Ключове значення для правового регулювання має Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, який визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України у кіберпросторі [17]. Закон встановлює повноваження суб'єктів забезпечення кібербезпеки, визначає їх права та обов'язки, механізми координації та взаємодії. У контексті міжнародно-правового регулювання важливе значення має Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), ратифікована Україною у 2005 році [18].

Система суб'єктів інформаційної безпеки у правоохоронній сфері України включає кілька ключових органів із різними повноваженнями та сферами відповідальності. Служба безпеки України згідно із Законом України «Про Службу безпеки України» виступає основним суб'єктом забезпечення державної безпеки, включаючи інформаційну безпеку [19]. СБУ здійснює контррозвідувальну діяльність, бореться з тероризмом та захищає державну таємницю в інформаційній сфері. Повноваження СБУ у кібербезпеці включають виявлення, попередження та припинення злочинів проти основ національної безпеки в інформаційній сфері, захист державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Національна поліція України відіграє важливу роль у забезпеченні інформаційної безпеки через діяльність спеціалізованого підрозділу – Департаменту кіберполіції. Відповідно до Закону України «Про Національну поліцію» та відповідних підзаконних актів, кіберполіція здійснює протидію кіберзлочинності, захист громадян та організацій від злочинних посягань у кіберпросторі. Функції кіберполіції включають розслідування кіберзлочинів, профілактичну роботу, міжнародне співробітництво у боротьбі з транскордонною кіберзлочинністю, а також забезпечення кібербезпеки критичної інфраструктури приватного сектору.

Прокуратура України виконує наглядові функції у сфері інформаційної безпеки та здійснює кримінальне переслідування за злочини у кіберпросторі. Відповідно до Закону України «Про прокуратуру» та Кримінального процесуального кодексу України, прокурори здійснюють процесуальне керівництво досудовим розслідуванням кіберзлочинів, підтримують державне звинувачення в суді. Спеціалізовані прокурори з кіберзлочинів мають особливі знання та навички для ефективного виконання

своїх функцій у цифровій сфері. Координаційна роль прокуратури проявляється у організації взаємодії різних правоохоронних органів під час розслідування складних кіберзлочинів.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) виступає центральним органом виконавчої влади, відповідальним за реалізацію державної політики у сферах криптографічного та технічного захисту інформації. Відповідно до Положення про Державну службу спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України, Держспецзв'язок здійснює державне регулювання у сфері захисту інформації. Служба контролює дотримання вимог законодавства щодо захисту інформації в державних органах, ліцензує діяльність із захисту інформації, проводить атестацію засобів захисту інформації.

Національний банк України має спеціальні повноваження у сфері інформаційної безпеки фінансового сектора. Відповідно до Закону України «Про Національний банк України» та відповідних нормативних актів НБУ, центральний банк встановлює вимоги до кібербезпеки банків та інших фінансових установ. НБУ здійснює нагляд за дотриманням вимог кібербезпеки, проводить стрес-тестування систем, координує реагування на кіберінциденти у фінансовому секторі. Особливе значення має створення Центру кібербезпеки НБУ, який забезпечує моніторинг загроз та координацію протидії їм.

Координація діяльності суб'єктів інформаційної безпеки здійснюється через Національний координаційний центр кібербезпеки, створений при Раді національної безпеки та оборони України. Відповідно до Указу Президента України «Питання Національного координаційного центру кібербезпеки», цей орган забезпечує координацію діяльності органів сектору безпеки та оборони з питань кібербезпеки. Центр розробляє пропозиції щодо формування та реалізації державної політики кібербезпеки, координує реагування на кіберінциденти національного рівня, забезпечує інформаційний обмін між суб'єктами кібербезпеки.

Функціональні повноваження суб'єктів інформаційної безпеки у правоохоронній сфері розрізняються за обсягом та змістом. Превентивні функції включають моніторинг загроз, аналіз уразливостей, розробку заходів захисту та профілактичну роботу. Реактивні функції охоплюють реагування на інциденти, розслідування кіберзлочинів, відновлення порушених систем та притягнення до відповідальності правопорушників. Аналітичні функції передбачають дослідження трендів кіберзагроз, прогнозування розвитку ситуації, підготовку аналітичних матеріалів для ухвалення управлінських рішень.

Міжнародне співробітництво є важливим компонентом діяльності суб'єктів інформаційної безпеки. Україна є учасником різних міжнародних організацій та ініціатив у галузі кібербезпеки. Співпраця з Європолом, Інтерполом, НАТО, Європейським Союзом здійснюється на основі відповідних угод та меморандумів про взаєморозуміння. Особливе значення має участь у Глобальному альянсі проти дитячої порнографії в Інтернеті, ініціативах боротьби з кібертероризмом, програмах технічної допомоги щодо зміцнення потенціалу кібербезпеки.

Сучасні виклики для суб'єктів інформаційної безпеки включають зростання складності та масштабів кіберзагроз, появу нових видів злочинів у цифровій сфері, необхідність захисту критичної інфраструктури від кібератак. Військова агресія російської федерації проти України значно ускладнила завдання забезпечення інформаційної безпеки, створивши потребу у нових підходах та методах роботи. Гібридні загрози, що включають кібератаки у поєднанні з інформаційними операціями, потребують комплексної протидії з боку різних суб'єктів безпеки.

Аналіз ефективності діяльності суб'єктів інформаційної безпеки виявляє низку проблем, які потребують вирішення. Недостатня координація між різними органами призводить до дублювання функцій та неефективного використання ресурсів. Прогалини у законодавстві створюють правову невизначеність та ускладнюють практичну діяльність. Нестача кваліфікованих кадрів та сучасного технічного оснащення знижує потенціал протидії кіберзагрозам. Необхідність удосконалення міжнародного співробітництва та адаптації до європейських стандартів кібербезпеки потребує системних змін в організації роботи суб'єктів інформаційної безпеки.

Висновки. Проведене дослідження дозволило встановити, що сучасна система суб'єктів інформаційної безпеки в правоохоронній сфері України характеризується складною багаторівневою структурою, яка включає спеціалізовані підрозділи Національної поліції, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, а також інші правоохоронні органи. Аналіз нормативно-правової бази засвідчив наявність розгалуженої системи законодавчих та підзаконних актів, що регламентують діяльність зазначених суб'єктів, проте виявив значні прогалини у визначенні чітких меж їхньої компетенції. Встановлено, що правовий статус окремих суб'єктів інформаційної безпеки потребує уточнення з огляду на динамічний розвиток інформаційних технологій та появу нових видів кіберзагроз.

Дослідження функціональних повноважень суб'єктів інформаційної безпеки у правоохоронній сфері виявило проблему дублювання компетенцій та недостатньої координації діяльності між різними відомствами. Встановлено, що відсутність єдиної методології розподілу повноважень призводить до неефективного використання ресурсів та зниження результативності протидії інформаційним загрозам. Особливо гострою є проблема розмежування повноважень у сфері розслідування кіберзлочинів, захисту критичної інформаційної інфраструктури та забезпечення кібербезпеки державних інформаційних систем. Аналіз практики застосування чинного законодавства засвідчив необхідність створення більш чіткої системи правового регулювання взаємодії між різними суб'єктами інформаційної безпеки.

Компаративний аналіз вітчизняного та зарубіжного досвіду організації діяльності суб'єктів інформаційної безпеки в правоохоронній сфері показав, що європейські країни демонструють більш високий рівень інституційної спроможності та координації у цій сфері. Встановлено, що адаптація українського законодавства до стандартів Європейського Союзу вимагає суттєвого перегляду існуючих підходів до розподілу повноважень та створення ефективних механізмів міжвідомчої взаємодії. Особливу увагу слід приділити імплементації принципів пропорційності, субсидіарності та взаємного визнання у сфері забезпечення інформаційної безпеки, що сприятиме підвищенню ефективності правоохоронної діяльності та зміцненню довіри громадян до державних інституцій.

На основі проведеного аналізу сформульовано комплекс рекомендацій щодо вдосконалення правового регулювання ді-

яльності суб'єктів інформаційної безпеки у правоохоронній сфері України. Запропоновано прийняття уніфікованого нормативно-правового акта, який би чітко визначив компетенцію кожного суб'єкта інформаційної безпеки та встановив ефективні механізми координації їхньої діяльності. Обґрунтовано необхідність створення спеціалізованого міжвідомчого органу координації у сфері інформаційної безпеки, який би забезпечував стратегічне планування, моніторинг загроз та координацію оперативного реагування. Практична реалізація запропонованих рекомендацій сприятиме підвищенню ефективності системи забезпечення інформаційної безпеки України та зміцненню її національної безпеки в цілому.

Література:

1. Ліпкан В.А. Теорія національної безпеки: підручник. Київ: КНТ, 2009. 631 с.
2. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. № 2(42). С. 54–62.
3. Dunn Cavelty M. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London: Routledge, 2008. 224 p.
4. Klimburg A. The Darkening Web: The War for Cyberspace. New York: Penguin Press, 2017. 352 p.
5. Єсімов С.С. Кіберполіція в Україні: організаційно-правові засади діяльності. *Науковий* вісник Національної академії внутрішніх справ. 2017. № 1(102). С. 206–218.
6. Гуцалюк М.В. Правові основи діяльності підрозділів кіберполіції Національної поліції України. *Підприємництво, господарство і право*. 2018. № 5. С. 150–155.
7. Мазепа С. Класифікація загроз інформаційній безпеці в правоохоронній діяльності. *Держава та регіони*. 2024. С. 290–295.
8. Горбулін В.П., Власюк О.С., Лібанова Е.М. Україна і світ: гуманітарні виклики. Київ: НІСД, 2020. 284 с.
9. Діордіца І.В. Кібербезпека: сутність поняття та проблеми правового регулювання. *Юридичний науковий електронний журнал*. 2018. № 6. С. 88–91.
10. Калюжний Р.А., Коропатник І.М., Курило В.І. Правові основи кібербезпеки України: монографія. Київ: «МП Леся», 2017. 236 с.
11. Шевчук О., Ментух Н.Ф. Реалізація політики державної інформаційної безпеки України в контексті запобігання корупції: адміністративно-правовий аспект. *Науковий* вісник Ужгородського національного університету. Серія: Право. 2021. Випуск 64. С. 282–287. URL: http://visnyk-juris-uzhnu-uz.com/wp-content/ uploads/2021/06/ NVUzhNU_64.pdf
12. Муравйов К.С. Кібербезпека як складова національної безпеки України. Актуальні проблеми міжнародних відносин. 2019. Вип. 139. С. 77–89.
13. Калаянов Д.В. Правове регулювання кібербезпеки в Україні: сучасний стан та перспективи розвитку. Право і безпека. 2020. № 2(77). С. 36–42.
14. Юрченко О.М. Особливості забезпечення кібербезпеки в умовах воєнного стану. *Право і суспільство*. 2022. № 3. С. 15–21.
15. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. База даних «*Законодавство України*». ВР України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр
16. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. База даних «*Законодавство України*». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2469-19
17. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. База даних «*Законодавство України*». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19
18. Convention on Cybercrime (Budapest Convention). Council of Europe Treaty Series No. 185. Budapest, 23.XI.2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Mazepa S. The role of information security subjects in law enforcement: legal status and functional powers

Summary. The article provides a comprehensive analysis of the legal status and functional powers of information security subjects in the law enforcement system of Ukraine. The author examines current trends in the legal regulation of the activities of competent authorities in the field of information security in the context of the law enforcement function of the State.

The author outlines the system of information security subjects in the law enforcement sphere, which includes the Security Service of Ukraine, the National Police, prosecutors, specialised cyber police units and other authorized bodies. Their main competences, mechanisms of interagency cooperation and coordination in the field of countering cyber threats and protecting critical information infrastructure are defined.

The author analyses the legal framework for the functioning of these entities on the basis of the current legislation of Ukraine, in particular, the Laws of Ukraine 'On National Security of Ukraine', 'On the Basic Principles of Ensuring Cybersecurity of Ukraine' and relevant by-laws. A comparative analysis of the powers of various bodies is carried out to identify cases of duplication of functions and gaps in legal regulation.

The article examines the practical aspects of exercising the powers of information security entities, including the mechanisms for detecting, preventing and investigating cybercrime, protecting personal data, countering information operations and ensuring the security of state information resources.

The author identifies the key problems of legal regulation of the activities of information security entities, including insufficient interagency coordination, gaps in legislative support, and a shortage of qualified personnel and technical resources. The author points out the peculiarities of functioning of the information security system under martial law and the need to adapt law enforcement agencies to new challenges.

It is concluded that improving the efficiency of information security entities requires improvement of their legal status and functional capabilities. The author offers practical recommendations for improving legislative regulation, optimising interagency cooperation and strengthening the capacity to counter modern cyber threats in the context of European integration and digital transformation of public administration.

Key words: information security, law enforcement, cybersecurity, legal support, administrative-legal aspect, criminal liability, administrative liability, European integration, harmonization of legislation, international standards, NATO, European Union (EU), state information policy, information security threats, implementation of law, subjects of information security, legal liability, information offenses, propaganda, artificial intelligence.

Дата надходження статті: 30.07.2025
Дата прийняття статті: 08.09.2025
Опубліковано: 30.09.2025