АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 351.74:004.056
DOI 10.36919/3041-1149(Print).9.2025.43-49

А. М. Новицький,
доктор юридичних наук, професор,
професор кафедри цивільно-правових дисциплін,
Національна академія СБУ
email: izipg@ukr.net
ORCID 0000-0001-6860-9654;
В. О. Підгородецький,
здобувач вищої освіти,
Державний податковий університет
email: valintin2002mu@gmail.com
ORCID 0000-0001-7812-7384

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Дослідження присвячене аналізу правового забезпечення інформаційної безпеки в діяльності правоохоронних органів України в умовах збройного конфлікту. Актуальність теми обумовлена інтенсифікацією кіберзагроз, які супроводжують сучасні збройні конфлікти, та потребою в адаптації правоохоронної системи до нових викликів інформаційної війни.

У роботі проаналізовано нормативно-правову базу, що регулює питання інформаційної безпеки правоохоронних органів, досліджено особливості функціонування цієї системи в умовах воєнного стану, виявлено основні загрози й уразливості інформаційних систем органів правопорядку. Особлива увага приділяється аналізу міжнародного досвіду правового регулювання кібербезпеки в правоохоронній сфері під час збройних конфліктів. Методологія дослідження базується на комплексному підході, що охоплює порівняльно-правовий аналіз, системний підхід, формально-логічний метод. Використано аналіз національного законодавства, міжнародних правових актів і наукових джерел.

Результати дослідження свідчать про наявність суттєвих прогалин у правовому регулюванні інформаційної безпеки правоохоронних органів в умовах збройного конфлікту. Виявлено недостатність координації між різними відомствами, обмеженість ресурсів для забезпечення належного рівня кібербезпеки, неузгодженість окремих нормативних актів. Обґрунтовано потребу в удосконаленні законодавчої бази через прийняття спеціального закону про кібербезпеку правоохоронних органів, створення єдиної системи моніторингу кіберзагроз, підвищення кваліфікації персоналу у сфері інформаційної безпеки. Запропоновано механізми міжвідомчої взаємодії та міжнародного співробітництва у сфері протидії кіберзлочинності. Практичне значення роботи полягає в розробці конкретних рекомендацій щодо вдосконалення правового забезпечення інформаційної безпеки правоохоронних органів, які можуть бути використані під час реформування відповідних структур і вдосконалення законодавства. Результати дослідження мають важливе значення для забезпечення ефективності правоохоронної діяльності в умовах гібридних загроз сучасності.

Ключові слова: *інформаційна безпека, правоохоронні органи, збройний конфлікт, кібербезпека, правове регулювання, воєнний стан, кіберзагрози.*

© Новицький А. М., Підгородецький В. О., 2025

Постановка проблеми та її актуальність. Сучасні збройні конфлікти характеризуються кардинальною трансформацією парадигми ведення військових дій, що проявляється не лише в традиційних формах бойового протиборства, але й в активному використанні інформаційно-комунікаційних технологій як стратегічного інструменту досягнення геополітичних цілей. Інформаційна складова набула статусу невід'ємного компонента гібридної війни, що детермінує потребу в кардинальному переосмисленні концептуальних підходів до забезпечення безпеки держави загалом та правоохоронних органів як критично важливої складової системи національної безпеки зокрема.

Погоджуємось із думкою О. Буряченко, яка в своєму дослідженні зазначає, що сучасні конфлікти виходять за межі традиційних військових дій, породжуючи нову форму протистояння – гібридну війну. Це багатовимірне явище поєднує конвенційні військові операції з асиметричними методами: інформаційними атаками, економічним тиском, кібервійною та використанням нерегулярних збройних формувань. Гібридна війна стала ефективним інструментом сучасної геополітики, що дає змогу державам досягати стратегічних цілей без прямого військового втручання, ускладнюючи ідентифікацію агресора й формування міжнародної відповіді [1, с. 25].

Україна, опинившись у стані безпрецедентного збройного протистояння з російською федерацією, зіткнулася із масштабними проявами кіберагресії та систематичними інформаційними атаками, що за своєю інтенсивністю й деструктивним потенціалом не мають аналогів у сучасній історії міжнародних конфліктів. Правоохоронні органи України, виконуючи функції ключового елемента архітектури національної безпеки, стали одними із пріоритетних об'єктів ворожих кібернападів та інформаційно-психологічних операцій. Зазначені обставини обумовлюють критичну важливість забезпечення адекватного сучасним викликам рівня інформаційної безпеки в діяльності правоохоронних структур.

Аналіз останніх досліджень і публікацій. Незважаючи на значну кількість наукових праць, присвячених правовому забезпеченню інформаційної безпеки правоохоронних органів, реалії воєнного стану актуалізують потребу в постійному оновленні теоретичних підходів і практичних механізмів розв'язання цих проблем.

Досліджуючи актуальні питання інформаційної безпеки в діяльності Національної поліції України, І. Іванов наголосив на проблемі глобального протиріччя між можливостями інформаційних технологій і загрозами їхнього використання [2, с. 183].

Зі свого боку Н. Моргун, О. Шевчук та С. Марчевський у науковій статті проаналізували поняття інформаційної безпеки в діяльності Національної поліції України, виділивши ключові ознаки та правову базу її забезпечення. Автори дослідили повноваження поліції у сфері інформаційної безпеки й діяльність спеціалізованих підрозділів – Департаменту режиму та технічного захисту інформації і Департаменту кіберполіції. Науковці дійшли висновку, що інформаційна безпека в діяльності Національної поліції є складовою національної безпеки України та здійснюється на чотирьох рівнях: відомчому, державному, міждержавному та міжнародному [4].

Науковиця Я. Свічкарьова в своєму дослідженні розглядає сутність інформаційної безпеки в діяльності правоохоронних органів України. Дослідниця зазначає, що процес інформатизації надає широкі можливості доступу до інформаційних ресурсів, які використовуються для забезпечення охорони прав і свобод людини, протидії злочинності та підтримання публічної безпеки. Авторка підтримує думку науковців про те, що підвищення ефективності роботи правоохоронних органів може бути досягнуто через впровадження надійної системи інформаційної безпеки, яка убезпечить інформаційні ресурси від несанкціонованого доступу [10].

Основні аспекти інформаційної культури правоохоронців в Україні дослідили М. Повалена та І. Здреник, аналізуючи проблеми недосконалої законодавчої бази, відсутності єдиних етичних стандартів і неефективної внутрішньої комунікації. Автори порівнюють українську практику з міжнародними стандартами ЄС та США, пропонуючи способи вдосконалення через впровадження нових технологій і рекомендації щодо безпечного використання пристроїв. Дослідники підкреслюють потребу в реалізації запропонованих заходів для підвищення ефективності правоохоронних органів і зміцнення суспільної довіри в умовах цифрової трансформації [5].

Науково-теоретична та практична актуальність дослідження посилюється тим фактом, що існуюча нормативно-правова база України у сфері інформаційної безпеки формувалася переважно в мирний період державного розвитку і, відповідно, не повною мірою враховує специфічні особливості функціонування правоохоронних органів в екстремальних умовах збройного конфлікту й воєнного стану. Відсутність комплексного та системного правового регулювання цієї сфери суспільних відносин створює серйозні ризики для забезпечення національної безпеки й ефективності правоохоронної діяльності, що може мати далекосяжні негативні наслідки для державної безпеки загалом.

Водночас накопичений досвід провідних країн світу, зокрема держав-членів НАТО та Європейського Союзу, переконливо демонструє можливість та ефективність комплексного правового забезпечення інформаційної безпеки навіть в екстремальних умовах ведення військових дій і протистояння гібридним загрозам. Це робить особливо актуальним поглиблене вивчення, критичний аналіз та адаптацію кращих міжнародних практик до специфічних українських реалій з урахуванням національних особливостей правової системи й геополітичного контексту.

Метою дослідження є здійснення комплексного та всебічного аналізу сучасного стану правового забезпечення інформаційної безпеки в діяльності правоохоронних органів України в умовах збройного конфлікту, виявлення системних недоліків і прогалин існуючого нормативно-правового регулювання, а також розробка науково обґрунтованих рекомендацій щодо його вдосконалення відповідно до сучасних викликів національній безпеці.

Виклад основного матеріалу дослідження. Правове забезпечення інформаційної безпеки правоохоронних органів України ґрунтується на фундаментальних конституційних засадах і розгалуженій системі спеціального законодавства, що формує багаторівневу архітектуру нормативного регулювання. Стаття 17 Конституції України закріплює принципово важливий обов'язок держави забезпечувати інформаційну безпеку як невід'ємний елемент національної безпеки, що створює непорушну конституційну основу для відповідного правового регулювання та визначає інформаційну безпеку справою всього Українського народу, підкреслюючи її загальнонаціональний характер і стратегічне значення [3].

Конституційні положення отримують конкретизацію в статті 3 Основного Закону, яка проголошує людину, її життя та здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю, що безпосередньо стосується захисту персональних даних громадян, які обробляються правоохоронними органами [3]. Зі свого боку стаття 32 Конституції України гарантує недоторканність приватного життя, що потребує особливого врахування під час розробки засобів інформаційної безпеки правоохоронних структур [3].

Варто вважати, що базовим нормативно-правовим актом у сфері інформаційної безпеки є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини й громадянина, суспільства та держави від багатоманітних загроз у кіберпросторі [9]. Проте детальний аналіз положень цього Закону свідчить про його переважно загальний характер і недостатнє врахування специфічних особливостей діяльності правоохоронних органів в умовах збройного конфлікту та воєнного стану.

На нашу думку, суттєве значення для правового регулювання досліджуваної сфери має Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який встановлює правові засади організації захисту інформації в інформаційних системах різного призначення [7]. Однак норми цього Закону потребують значної конкретизації стосовно специфіки діяльності правоохоронних органів, особливо в частині забезпечення безпеки критично важливої інформації під час ведення активних військових дій і протистояння гібридним загрозам.

Варто також зазначити, що важливу роль у правовому регулюванні відіграє Закон України «Про Національну поліцію», який містить окремі положення щодо забезпечення інформаційної безпеки в діяльності поліцейських підрозділів [8]. Проте ці норми мають фрагментарний характер і не формують цілісної системи правового захисту інформаційних ресурсів правоохоронних органів.

Не менш важливу роль у правовому забезпеченні інформаційної безпеки відіграють відомчі нормативні акти, зокрема накази Міністерства внутрішніх справ України, Служби безпеки України, Генеральної прокуратури України та інших правоохоронних відомств, які деталізують порядок забезпечення інформаційної безпеки в межах відповідних відомств і конкретизують загальні законодавчі положення.

Реальний досвід демонструє брак уніфікованих підходів та недостатню взаємодію між правоохоронними органами, що породжує слабкі місця в системі й перешкоджає результативній боротьбі із кіберзлочинністю. Розрізненість методів забезпечення кібербезпеки в різних відомствах призводить до розпорошення зусиль і нераціонального витрачання доступних ресурсів.

Погоджуємось із думкою Д. Смотрича та Л. Браілко, які зазначають, що багато процесів у сфері інформаційних технологій залишаються неврегульованими на законодавчому рівні, що створює труднощі в притягненні до відповідальності за дії, які можуть нашкодити інформаційній безпеці. Водночас відбувається поступовий розвиток цих напрямів через прийняття нормативних актів, які встановлюють правила використання іноземних технологій у військовому обладнанні, що постачається до підрозділів [11].

Введення воєнного стану в Україні внесло кардинальні корективи в правове регулювання інформаційної безпеки та створило нову парадигму функціонування інформаційних систем. Указ Президента України про введення воєнного стану встановив особливий порядок функціонування інформаційних систем і значно посилив вимоги до їхнього захисту від зовнішніх загроз [6]. Воєнний стан передбачає можливість застосування особливих заходів забезпечення національної безпеки, включно із тимчасовими обмеженнями окремих конституційних прав і свобод громадян у сфері інформаційних відносин. Проте ці обмеження повинні бути чітко пропорційними існуючим загрозам, тимчасовими за характером і не порушувати основоположні принципи правової держави й демократії.

Правоохоронні органи України в умовах збройного конфлікту стикаються з надзвичайно широким і постійно еволюціонуючим спектром кіберзагроз, що вимагає комплексного підходу до їхньої класифікації та аналізу. До основних категорій таких загроз належать: цілеспрямовані атаки на інформаційні системи з метою викрадення критично важливої інформації, охоплюючи персональні дані громадян та оперативну інформацію; масштабні DDoS-атаки на вебресурси та електронні сервіси правоохоронних органів з метою порушення їхнього нормального функціонування; впровадження складних форм шкідливого програмного забезпечення в корпоративні мережі й інформаційні системи; застосування методів соціальної інженерії та фішингових атак для компрометації облікових записів співробітників; атаки на системи відеоспостереження й електронного контролю доступу до об’єктів правоохоронних органів.

Особливо небезпечними та деструктивними є спеціалізовані атаки, спрямовані на компрометацію баз даних правоохоронних органів, що містять конфіденційні персональні дані громадян, інформацію про кримінальні справи та розслідування, оперативні дані й відомості про співробітників правоохоронних структур. Втрата контролю над такою інформацією або несанкціонований доступ до неї може мати катастрофічні наслідки не лише для національної безпеки, але й для особистої безпеки громадян і співробітників правоохоронних органів.

Досвід провідних європейських країн і Сполучених Штатів Америки переконливо демонструє критичну важливість комплексного та системного підходу до правового забезпечення кібербезпеки правоохоронних органів. Зокрема, у Сполучених Штатах діє розгалужена система федеральних законів, включно із Cybersecurity Enhancement Act та Federal Information Security Management Act, які встановлюють деталізовані й обов’язкові стандарти кібербезпеки для всіх федеральних агентств, охоплюючи правоохоронні структури [12].

Європейський Союз розробив та успішно імплементував Директиву NIS (Network and Information Systems), яка встановлює загальні й обов’язкові вимоги до кібербезпеки критично важливих секторів економіки та державного управління, включно із правоохоронними органами. Ця директива передбачає створення національних стратегій кібербезпеки, призначення компетентних національних органів і встановлення чітких вимог до звітності про кіберінциденти [13].

На сьогодні в Україні функціонує розгалужена та багаторівнева система державних органів, відповідальних за забезпечення різних аспектів кібербезпеки. До цієї системи входять Служба безпеки України як головний орган у сфері забезпечення державної безпеки в кіберпросторі, Національна поліція України з її спеціалізованими підрозділами, Департамент кіберполіції Національної поліції, Державна служба спеціального зв'язку та захисту інформації України, а також інші спеціалізовані структури.

Проте детальний аналіз функціонування цієї системи свідчить про потребу в суттєвому вдосконаленні координації між різними структурами та подоланні дублювання функцій. Ключовою системною проблемою є відсутність єдиного координаційного центру, який би забезпечував оперативний і ефективний обмін інформацією про кіберзагрози та координував заходи швидкого реагування на інциденти.

Аналіз технічного стану інформаційних систем правоохоронних органів України свідчить про наявність серйозних системних проблем, що створюють критичні вразливості для кіберагресії. Найбільш проблематичними є застарілі інформаційні системи, які не отримують регулярних оновлень безпеки через брак фінансування або технічних можливостей, а також системи з принципово недостатнім рівнем захисту від зовнішніх атак сучасного рівня складності.

Також, на нашу думку, особливої уваги потребує питання створення єдиної системи моніторингу кіберзагроз для всіх правоохоронних органів. Така система повинна забезпечувати цілодобове автоматизоване спостереження за станом інформаційних систем, автоматичне виявлення аномалій і підозрілої активності, а також забезпечення швидкого та координованого реагування на виявлені інциденти.

Висновки. Отже, правове забезпечення інформаційної безпеки правоохоронних органів України в умовах збройного конфлікту є однією з ключових передумов ефективного функціонування системи національної безпеки. У процесі дослідження встановлено, що існуюча нормативно-правова база лише частково відповідає сучасним викликам, зокрема в умовах гібридної війни та кіберзагроз. Потреба в оперативному реагуванні на нові загрози вимагає гармонізації національного законодавства із міжнародними стандартами, зокрема у сфері кібербезпеки. Законодавчі акти України часто не містять чітких механізмів реалізації положень про захист інформації в діяльності правоохоронних органів. Водночас позитивним є наявність тенденції до оновлення підходів до інформаційної безпеки, що простежується в стратегічних документах державної політики. Важливим чинником підвищення рівня інформаційної захищеності є міжвідомча взаємодія та створення єдиного координаційного центру. Також актуальним залишається питання забезпечення належного технічного й кадрового ресурсу в сфері інформаційної безпеки. Наукове осмислення проблематики дає підстави для розробки комплексних рішень з урахуванням досвіду країн-членів ЄС та НАТО. Врахування зазначених аспектів сприятиме посиленню інформаційної стійкості правоохоронних органів і держави загалом. Подальші дослідження мають бути зосереджені на оцінюванні ефективності впроваджених механізмів правового регулювання та розробці нових моделей захисту інформації в умовах воєнного часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буряченко О. Гібридна війна як нова форма глобального протистояння. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2024. № 2 (74). С. 24–31. URL : https://doi.org/10.32689/2523-4625-2024-2(74)-3

2. Іванов І. Актуальні питання інформаційної безпеки у діяльності Національної поліції України. *Юридична наука*. 2020. № 3 (105). С. 183–190. URL : https://doi.org/10.32844/2222-5374-2020-105-3.23

3. Конституція України від 28.06.1996 № 254к/96-ВР. URL : https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

4. Моргун Н., Шевчук О., Марчевський С. Щодо визначення поняття інформаційної безпеки у діяльності Національній поліції України. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. № 4. С. 409–415. URL : https://doi.org/10.24144/2788-6018.2024.04.67

5. Повалена М., Здреник І. Інформаційна культура правоохоронців: проблеми та шляхи удосконалення. *Юридичний науковий електронний журнал*. 2024. № 10. С. 297–300. URL : https://doi.org/10.32782/2524-0374/2024-10/67

6. Про введення воєнного стану в Україні Указ Президента України від 24.02.2022 № 64/2022. URL : https://zakon.rada.gov.ua/laws/show/64/2022#Text

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

8. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL : https://zakon.rada.gov.ua/laws/show/580-19#Text

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

10. Свічкарьова Я. Сутність інформаційної безпеки в професійній діяльності правоохоронців. *Наукові записки. Серія: право*. 2024. Т. 1, № 15. URL : https://doi.org/10.36550/2522-9230-2023-15-64-68

11. Смотрич Д., Браїлко Л. Інформаційна безпека в умовах воєнного стану. *Вісник УжНУ. Серія: Право*. 2023. Т. 2, № 77. С. 121–127. URL : https://doi.org/10.24144/2307-3322.2023.77.2.20

12. Cybersecurity Enhancement Act of 2014 : Public Law 113–274, 18 Dec. 2014. URL : https://www.congress.gov/bill/113th-congress/senate-bill/1353

13. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

REFERENCES

1. Buryachenko, O. (2024). Hibrydna viyna yak nova forma hlobal′noho protystoyannya [Hybrid war as a new form of global confrontation]. *Naukovi pratsi Mizhrehional'noyi Akademiyi upravlinnya personalom. Politychni nauky ta publichne upravlinnya*. 2024. № 2 (74). S. 24–31. URL : https://doi.org/10.32689/2523-4625-2024-2(74)-3 [in Ukrainian].

2. Ivanov, I. (2020) Aktual′ni pytannya informatsiynoyi bezpeky u diyal′nosti Natsional′noyi politsiyi Ukrayiny [Current issues of information security in the activities of the National Police of Ukraine]. *Yurydychna nauka*. 2020. № 3 (105). S. 183–190. URL : https://doi.org/10.32844/2222-5374-2020-105-3.23 [in Ukrainian].

3. Constitution of Ukraine dated 28.06.1996 No. 254k/96-VR. URL : https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text [in Ukrainian].

4. Morhun, N. & Shevchuk, O. & Marchevs′kyy, S. (2024). Shchodo vyznachennya ponyattya informatsiynoyi bezpeky u diyal′nosti Natsional′niy politsiyi Ukrayiny [On the definition of the concept of information security in the activities of the National Police of Ukraine]. *Elektronne naukove vydannya «Analitychno-porivnyal'ne pravoznavstvo».* 2024. № 4. S. 409–415. URL : https://doi.org/10.24144/2788-6018.2024.04.67 [in Ukrainian].

5. Povalena, M. & Zdrenyk, I. (2024). Informatsiyna kul′tura pravookhorontsiv: problemy ta shlyakhy udoskonalennya [Information culture of law enforcement officers: problems and ways of improvement]. *Yurydychnyy naukovyy elektronnyy zhurnal.* 2024. № 10. S. 297–300. URL : https://doi.org/10.32782/2524-0374/2024-10/67 [in Ukrainian].

6. Decree of the President of Ukraine on the introduction of martial law in Ukraine dated February 24, 2022 No. 64/2022. URL : https://zakon.rada.gov.ua/laws/show/64/2022#Text [in Ukrainian].

7. Law of Ukraine on Information Protection in Information and Telecommunications Systems No. 80/94-VR of 05.07.1994. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр#Text [in Ukrainian].

8. Law of Ukraine on the National Police dated 02.07.2015 No. 580-VIII. URL : https://zakon.rada.gov.ua/laws/show/580-19#Text [in Ukrainian].

9. Law of Ukraine on the Basic Principles of Ensuring Cybersecurity of Ukraine dated 05.10.2017 No. 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

10. Svichkarʹova, Ya. (2024) Sutnistʹ informatsiynoyi bezpeky v profesiyniy diyalʹnosti pravookhorontsiv [The essence of information security in the professional activities of law enforcement officers]. *Naukovi zapysky. Seriya: pravo*. 2024. Т. 1, № 15. URL : https://doi.org/10.36550/2522-9230-2023-15-64-68 [in Ukrainian].

11. Smotrych, D. & Brayilko, L. (2023). Informatsiyna bezpeka v umovakh voyennoho stanu [Information security in martial law conditions]. *Visnyk UzhNU. Seriya: Pravo.* 2023. Т. 2, № 77. S. 121–127. URL : https://doi.org/10.24144/2307-3322.2023.77.2.20 [in Ukrainian].

12. Cybersecurity Enhancement Act of 2014 : Public Law 113–274, 18 Dec. 2014. URL : https://www.congress.gov/bill/113th-congress/senate-bill/1353 [in Ukrainian].

13. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148 [in English].

A. M. Novytskii, V. O. Pidhorodetskyi. LEGAL SUPPORT FOR INFORMATION SECURITY IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES UNDER CONDITIONS OF ARMED CONFLICT

The study is devoted to the analysis of legal support for information security in the activities of law enforcement agencies of Ukraine under conditions of armed conflict. The relevance of the topic is driven by the intensification of cyber threats accompanying modern armed conflicts and the need to adapt the law enforcement system to new challenges of information warfare.

The paper analyzes the legal framework regulating information security issues in law enforcement, explores the specific functioning of this system under martial law, and identifies the main threats and vulnerabilities of law enforcement information systems. Special attention is paid to the analysis of international experience in the legal regulation of cybersecurity in the law enforcement sphere during armed conflicts. The research methodology is based on a comprehensive approach that includes comparative legal analysis, a systems approach, and the formal-logical method. The study uses the analysis of national legislation, international legal acts, and scientific sources.

The results of the study indicate the existence of significant gaps in the legal regulation of information security for law enforcement under armed conflict. A lack of interagency coordination, limited resources to ensure an adequate level of cybersecurity, and inconsistencies in certain regulations have been identified. The study substantiates the need to improve the legislative framework through the adoption of a special law on cybersecurity for law enforcement, the creation of a unified system for cyber threat monitoring, and the improvement of staff qualifications in the field of information security. Mechanisms of interagency cooperation and international collaboration in combating cybercrime are proposed.

The practical significance of the study lies in the development of specific recommendations to improve the legal framework for information security in law enforcement, which may be used in the reform of relevant structures and legislation. The results are of great importance for ensuring the effectiveness of law enforcement activities in the context of modern hybrid threats.

Keywords: *information security, law enforcement agencies, armed conflict, cybersecurity, legal regulation, martial law, cyber threats.*