ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ

УДК 351.746.1:004.056 (477)
DOI https://doi.org/10.32782/2709-9261-2025-2-14-17

Волобоєв Артур Олегович,
доктор філософії в галузі права,
завідувач кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-7138-5847

Зеленський Сергій Миколайович,
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-0945-4485

ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Статтю присвячено комплексному аналізу правових і організаційних засад інформаційної безпеки України, установленню основних проблем їхнього розвитку й окресленню перспективних напрямів удосконалення. Зокрема, установлено структуру організаційних засад інформаційної безпеки, до яких належать: об'єктивність, науковість, системність, комплексність, безперервність, індивідуалізація відповідальності, синергія централізованого та децентралізованого управління. Акцентовано на важливості правового регулювання суспільних відносин у сфері інформаційної безпеки.
Ключові слова: *інформаційна безпека, національна безпека, ризики, загрози, принципи.*

Постановка проблеми. Стрімкий розвиток інформаційних і комунікаційних технологій, загальна цифровізація суспільства й інтеграція із глобальним інформаційним простором створюють передумови для послаблення державного інформаційного суверенітету. Глобалізаційні процеси в інформаційному середовищі чинять істотний вплив на параметри інформаційної безпеки та функціонування інформаційного суспільства загалом, породжують безпрецедентні загрози у ключових сферах суспільного життя. З огляду на це інформаційна безпека набуває статусу самостійного й невід'ємного елементу національної безпеки України.

Необхідність захисту національного інформаційного середовища детермінує потребу системного гарантування інформаційної безпеки, що особливо актуалізується в контексті зміцнення української державності в умовах воєнного стану. Державна інформаційна безпека України реалізується як інтегральний складник національної безпеки. У правовому вимірі вона ґрунтується на демократичних принципах правової держави та впроваджується шляхом формування і реалізації відповідних національних доктрин, стратегій, концепцій і програм.

Аналіз останніх досліджень та публікацій. Категоріальний апарат, сутнісні характеристики та фундаментальні принципи інформаційної безпеки досліджено у працях вітчизняних науковців, серед яких: О. А. Габорець, О. І. Горбенко, А. М. Гребенюк, О. В. Захарова, В. А. Липкан, С. П. Морозов, І. В. Ткаченко, В. С. Цимбалюк, Г. В. Черненко й інші. Водночас, незважаючи на розгалуженість наукових напрацювань, відсутність нормативного закріплення поняття інформаційної безпеки на законодавчому рівні, визначаємо доцільність подальших досліджень і визначення правових і організаційних засад цього феномену.

Метою статті є проведення комплексного аналізу правових і організаційних засад інформаційної безпеки

України, установлення основних проблем її розвитку, окреслення перспективних напрямів удосконалення.

Виклад основного матеріалу. Організаційні засади інформаційної безпеки України доцільно визначати як комплекс організаційних і організаційно-технічних заходів, що створюють сприятливе середовище для функціонування і прогресивного розвитку інформаційного простору [1].

До фундаментальних організаційних засад інформаційної безпеки належать: об'єктивність, науковість, системність, комплексність, безперервність, індивідуалізація відповідальності, синергія централізованого та децентралізованого управління.

Практичне застосування організаційних засад формує основу, що об'єднує всі елементи інформаційної безпеки в єдину функціональну систему. Варто зазначити, що організаційні засади характеризуються значно вищою стабільністю порівняно із правовими. Вони відображають універсальні правила й методологічні підходи до гарантування інформаційної безпеки, що можуть бути адаптовані будь-якою соціально-політичною та економічною системою. Організаційні засади функціонування державного апарату слугують детермінантами змісту діяльності окремих управлінських структур. Структурні принципи, закріплені у відповідних нормативно-правових актах, забезпечують ухвалення обґрунтованих управлінських рішень, упровадження раціональних адміністративних процедур і ефективний контроль у сфері виконавчої влади [2, с. 46].

Так, принцип об'єктивності посідає центральне місце в системі організаційних засад захисту інформації. Лише на основі неупередженої оцінки реальних і потенційних загроз інформаційній безпеці, а також стану правового й організаційного регулювання можна забезпечити надійний захист інформаційних ресурсів або мінімізувати вплив деструктивних чинників [3]. Об'єктивному оцінюванню підлягають реальні можливості використання матеріально-технічних, людських і фінансових ресурсів, принаймні в мінімально необхідному обсязі. Принцип об'єктивності передбачає дотримання вимог законів у всіх управлінських процесах, урахування їхніх закономірностей, ретельний аналіз наявного потенціалу держави та постійний моніторинг ризиків і загроз [4, с. 11].

Система інформаційної безпеки та механізми управління нею потребують проактивності, безперервності та превентивних заходів з боку держави й інших суб'єктів інформаційної діяльності. Тільки за таких умов можна очікувати на позитивну динаміку в цій сфері. Інакше кажучи, лише на підґрунті об'єктивної оцінки реального стану інформаційної безпеки та врахування закономірностей еволюції інформаційного середовища можна розробити й імплементувати ефективні заходи щодо захисту інформації та сфери її поширення. Особливо якщо враховувати сучасний стан, коли зростає значення штучного інтелекту та його соціальної інтеграції, а юридичний складник індустрії штучного інтелекту набуває не номінального, а вже реального характеру [5, с. 177].

Отже, принцип об'єктивності забезпечується врахуванням альтернативних думок, стратегічним плануванням і дослідженням закономірностей розвитку інформаційної сфери. Лише на основі комплексного врахування всіх аспектів принципу об'єктивності можливі розбудова та вдосконалення ефективної системи захисту й управління інформаційними ресурсами [6, с. 54].

Науковий підхід до організації інформаційної безпеки передбачає всебічне дослідження законів і закономірностей функціонування та розвитку інформаційної сфери. Наукове осмислення правового механізму захисту інформаційного простору передбачає ідентифікацію всього комплексу проблем, пов'язаних із формуванням і вдосконаленням системи захисту інформації та управління цією системою на рівні законодавчих і нормативно-правових актів.

В Україні сформовано специфічну систему гарантування інформаційної безпеки та реалізуються заходи щодо її вдосконалення. Водночас результати проведеного аналізу наукового дискурсу та законотворчих процесів засвідчують, що ця діяльність характеризується деякою інертністю. Попри розгалуженість наукових пошуків у сфері інформаційної безпеки, на нормативному рівні залишається нерозв'язаною проблема визначення понятійно-категоріального апарату. Тому дослідження у вирішенні цієї актуальної проблеми й інших є основою для розроблення та впровадження відповідних ефективних механізмів регулювання суспільних відносин у контексті гарантування інформаційної безпеки та прав суб'єктів у сфері інформаційної діяльності як на національному, так і на міжнародному рівнях. Саме тут принцип комплексного підходу до організації інформаційної безпеки передбачає створення інтегрованої системи сил, засобів і спеціальних методів, спрямованих на гарантування безпеки інформаційних ресурсів [7, с. 805].

Для практичної реалізації цього принципу необхідне всебічне розуміння всіх компонентів об'єкта захисту, зокрема джерел інформації, які потребують захисту, серед яких і відомості, що становлять державну таємницю, інші види інформації з обмеженим доступом, відкриті дані, що мають значення для особи, суспільства й держави. До сфери розповсюдження інформаційних ресурсів, що потребують захисту, належать державні органи та підприємства, установи й організації незалежно від форм власності; інформаційні комунікаційні системи різного класу та призначення, зокрема й системи збору, обробки, зберігання та поширення інформації, засоби її захисту. Громадяни, зокрема й коло посадових осіб і громадські організації, потребують захисту як носії інформації. Особливого значення набуває захист права на отримання, використання та поширення інформації, а також захист конфіденційних даних та інтелектуальної власності [8, с. 23].

Принцип логічного зв'язку між державними й управлінськими рішеннями в усіх сферах інформаційної діяльності можна розглядати як специфічний прояв комплексного системного підходу. Цей принцип, що має самостійне значення, передбачає узгодженість виробничих, торговельних, фінансових і режимних заходів гарантування безпеки у відповідних сферах.

Принцип безперервності інформаційної безпеки полягає в постійному застосуванні як загальних, так і спеціальних засобів і методів гарантування інформаційної безпеки на всіх етапах її реалізації.

Закон України «Про інформацію», що є фундаментальним нормативно-правовим актом в інформаційній сфері, гарантує право на інформацію і акцентує увагу на доступності отримання, збирання, зберігання, використання і поширення інформації [9]. Принцип безперервності передбачає необхідність реалізації активних, превентивних і систематичних заходів, що гарантують безпеку інформації та контролюють ступінь її поширення у просторово-часовому континуумі, ідентифікують ризики та захищають від реальних і потенційних загроз у звичайних і екстремальних умовах [10], зокрема під час дії воєнного стану.

Принцип єдиного управління передбачає обов'язковість дотримання правових норм. Відповідальність покладається на керівників органів державної влади, місцевого самоврядування, підприємств і організацій, діяльність яких пов'язана з гарантуванням інформаційної безпеки.

Шляхом визначення повноважень державних органів у сфері національної безпеки й оборони, визначення їхніх функціональних обов'язків, порядку застосування сил і розподілу ресурсів для захисту суспільних цінностей сформовано систему управління та взаємодії безпекових органів, упроваджено інтегрований підхід до аналізу, планування та контролю їхньої діяльності.

Зауважимо, що сукупність ризиків і загроз національній безпеці в умовах воєнного часу утворює багатовимірну систему індикаторів, що підлягає комплексному аналізу з метою прогнозування потенційних наслідків кожного ризику та загрози, їх оцінювання за критеріями інтенсивності, масштабу, тривалості тощо. Аналіз цих наслідків може привести до переорієнтації пріоритетних напрямів захисту від найбільш значущих ідентифікованих загроз [11, с. 43].

З урахуванням міжнародного досвіду оцінювання впливу загроз національній безпеці виокремлено такі пріоритетні об'єкти захисту: матеріальні об'єкти, зокрема й інфраструктурні елементи, житлові й адміністративні споруди, засоби комунікації; людський капітал, зокрема й життя, фізичне та психічне здоров'я і добробут населення; економічні та фінансові ресурси; екологічне середовище; соціально-політичний потенціал.

Визначення стратегічного потенціалу держави та ключових цільових груп захисту від найбільш деструктивних загроз пов'язане з оцінюванням потенціалу стійкості та здатності системи національної безпеки до захисту суспільних цінностей із допустимим рівнем втрати їхньої функціональності [12, с. 69]. Варто акцентувати увагу на параметрах допустимої шкоди, що визначаються індивідуально для кожної цільової групи з урахуванням її специфічних характеристик.

Гарантування інформаційної безпеки в Україні спрямоване на виявлення ризиків і загроз і мінімізацію потенційних негативних наслідків для електронних комунікацій, підвищення рівня безпеки процесів обробки інформації та захисту персональних даних. Досягнення оптимального рівня безпеки вимагає від держави та суспільства впровадження комплексних механізмів і заходів для належного функціонування та захисту критично важливих інформаційних ресурсів і систем.

Зростання ризиків і поширення загроз, пов'язаних із воєнною агресією Росії проти України, на всі сфери суспільного життя потребує систематичного вдосконалення методів і засобів їх виявлення та протидії. Особливо значущими є швидке виявлення вразливостей в інформаційній безпеці України, превентивний захист від кібератак і своєчасне реагування на інформацію про кіберзагрози з метою мінімізації потенційно можливих негативних наслідків цієї загрози [13].

Формування моделі ризиків і загроз інформаційній безпеці України відповідає також стратегічним інтересам держави та суспільства. Створення єдиної основи для оцінювання ризиків і загроз дозволяє своєчасно їх аналізувати та вживати відповідних заходів. Так, для досягнення цієї мети доцільно врахувати такі компоненти: гнучку загальну структуру індикаторів оцінювання ризиків і загроз; функціональну простоту основних аналітичних принципів для ефективного застосування фахівцями; включення до аналітичних звітів візуалізацій у формі діаграм і графіків; використання чіткої термінологічної бази в оцінюванні ризиків.

Залежно від характеру та походження подій, що можуть спричинити ризики та загрози інформаційній безпеці України, доцільно додатково виокремити такі категорії: штучні, природні, соціальні, воєнні.

Оцінювання ризиків створює підґрунтя для управління ними та впровадження гарантій стабільності системи інформаційної безпеки в разі виникнення реальної загрози. Аналіз і оцінювання ризиків є важливим кроком у визначенні того, які з них потребують уваги, пом'якшення та/або передачі на регіональний, національний чи наднаціональний рівень для вирішення. Такий аналіз сприяє розробленню рекомендацій з визначення пріоритетів для посилення стійкості української системи інформаційної безпеки.

Методологія аналізу ризиків призначена для структурування загроз втрати, знищення або пошкодження інформації, визначення ступеня її вразливості та потенційних наслідків реалізації загроз. Інтеграцією міжнародного досвіду й національної специфіки можна визначити головну мету оцінювання ризиків як ідентифікацію вразливостей системи інформаційної безпеки, прогнозування наслідків їх порушення та розроблення стратегії управління ризиками. У цьому контексті оцінювання має сприяти розробленню стратегій і тактик своєчасного виявлення, запобігання та боротьби з поточними загрозами, визначення вразливих місць системи інформаційної безпеки.

Оцінювання ризиків реалізується на системній основі з використанням комплексного підходу. Водночас не лише аналізуються загрози, але й досліджуються їхні сутнісні характеристики й інтенсивність проявів.

Загрозу інформаційній безпеці визначаємо як джерело потенційної небезпеки, що впливає на систему захисту інформації і характеризується визначеною величиною та можливістю реалізації. Аналіз загроз є процесом систематичного дослідження та оцінювання інформації про реальні чи потенційні небезпеки з метою виявлення ключових факторів ризику та формулювання обґрунтованих висновків [14, с. 9]. Метою оцінювання загрози є її виявлення, опис і вимірювання з погляду величини та ймовірності настання.

Загрози необхідно вимірювати для можливості їх порівняння та визначення пріоритетів. Щоб виміряти величину загрози, спочатку необхідно визначити одиницю її вимірювання. Наприклад, у разі кіберзагроз одиницею вимірювання може бути кількість суб'єктів, підозрюваних у здійсненні кібератак. Усі вимірювання мають стосуватися визначеного місця та періоду часу (наприклад, місяця, кварталу чи року).

Оцінювання загрози передбачає вивчення її природи (характеру) і ступеню. Окрім того, важливо встановити шанс виникнення загрози та потенціал шкоди, яку вона може спричинити. Визначення характеру та розміру можливих збитків відносимо до основної компоненти оцінювання ризику.

Як і будь-який аналітичний процес, оцінювання загрози починається із чіткого формулювання дослідницького питання і окреслення необхідного масштабу аналізу. Оцінки можуть варіюватися від макрорівня (наприклад, загальнонаціональні кібератаки) до локальних проявів (наприклад, кібератаки в межах окремого міста). Спрямованість і масштаб аналізу залежать від завдань компетентного державного органу. Наприклад, аналітик може оцінювати специфічні методи, частоту інцидентів, потенційно небезпечних суб'єктів або злочинні угруповання в конкретному регіоні.

Аналіз загрози передбачає визначення чинників, що зумовили її виникнення, наявного потенціалу для її нейтралізації, формування профілю об'єкта загрози, а також прогнозування тенденцій її розвитку. Інтенсивність загрози оцінюється за допомогою відповідних індикаторів, зокрема через встановлення кількості негативних інцидентів і прогнозування ймовірності їх повторення в певному просторово-часовому континуумі.

Вразливість системи інформаційної безпеки можна визначити як її нездатність ефективно протидіяти загрозам. У спрощеному розумінні вразливість є функцією ймовірності реалізації загрози та неспроможності системи запобігти її деструктивному впливу. Аналіз вразливості спрямований на визначення характеру й інтенсивності потенційних загроз, а також ефективності наявних механізмів захисту. Метою оцінювання вразливості є комплексний аналіз здатності інформаційної системи протистояти ідентифікованим загрозам. Оцінювання негативних чинників передбачає виявлення тих, які можуть посилити інтенсивність або ймовірність реалізації загрози.

Висновки. У підсумку варто підкреслити важливість правового регулювання інформаційної безпеки, що зумовлено зростанням ролі інформації в усіх сферах життєдіяльності особи та держави, а також впливом багатовимірних загроз інформаційному середовищу. Розвиток інформаційних відносин потребує запровадження гарантій дотримання та захисту конституційних прав і законних інтересів суб'єктів інформаційної та комунікаційної сфери. Адже національні інтереси України нерозривно пов'язані з дотриманням фундаментальних прав людини щодо створення, зберігання, отримання та використання інформації, формуванням сприятливих умов для розвитку сучасних інформаційних і комунікаційних технологій, захистом державних і приватних інформаційних інтересів від потенційних загроз [15].

У контексті зростання цінності інформації як стратегічного ресурсу значення інформаційної безпеки та захисту даних в інформаційних і комунікаційних системах постійно зростає. У зв'язку із цим до ключових правових засад гарантування інформаційної безпеки в Україні варто відносити: верховенство права; пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері; своєчасність і адекватність заходів щодо захисту національної безпеки від актуальних і потенційних інформаційних загроз; свободу створення, збирання, зберігання, використання та поширення інформації; забезпечення достовірності, повноти й об'єктивності інформаційних ресурсів; захист приватності особи; законність обмеження доступу до інформації; гармонізацію особистих, суспільних і державних інтересів; чіткий розподіл повноважень і відповідальності суб'єктів гарантування інформаційної безпеки; пріоритетний розвиток національних інформаційних технологій, ресурсів і послуг; інтеграцію до міжнародних систем інформаційної безпеки; гармонізацію національного інформаційного законодавства з міжнародними нормами та стандартами Європейського Союзу.

Уважаємо, що окреслені нами засади є основним орієнтиром для подальших досліджень з розкриттям їхнього змісту, а також визначенням окремих елементів єдиної системи правового й організаційного гарантування інформаційної безпеки України.

Список використаних джерел

1. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469–VIII. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

2. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навчальний посібник. Дніпро : ДДУВС, 2020. 144 с.

3. Про Стратегію інформаційної безпеки : Указ Президента України від 28.12.2021 р. № 685/2021. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

4. Інформаційна безпека : підручник / В. В. Остроухов та ін. ; за заг. ред. В. В. Остроухова. Київ : Ліра-К, 2021. 412 с.

5. Тихомиров О. О. Права людини: інформаційний вимір : монографія. Одеса : Юридика, 2023. 304 с.

6. Дзьобань О. П. Філософія інформаційного права: світоглядні й загальнотеоретичні засади : монографія. Харків : Майдан, 2013. 360 с.

7. Габорець О. А. Значення біометричної автентифікації в сучасних системах безпеки. *Наука і техніка сьогодні :* електронний журнал. Серія «Техніка». Київ : Наукові перспективи, 2024. № 6 (34). С. 799–806.

8. Правове регулювання національної безпеки : навчальний посібник / О. Г. Боднарчук та ін. Ірпінь : Державний податковий університет, 2024. 202 с.

9. Про інформацію : Закон України від 02.10.1992 р. № 2657–XII. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

10. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

11. Бочарніков В. П., Свєшніков С. В. Безпекове середовище 2030 : монографія. Київ : Майстер книг, 2019. 76 с.

12. Франчук В. І. Теоретико-методологічні та управлінські засади розвитку безпекового середовища. *Науковий вісник Львівського державного університету внутрішніх справ.* Серія «Економічна». 2023. № 2. С. 63–73.

13. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 р. № 447/2021. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

14. Strategic communications in the formation of the Ukrainian national security system : monograph / under general editorship of L. S. Khorishko. Riga, Latvia : Baltija Publishing, 2023. 188 p.

15. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

References

1. Pro natsionalnu bezpeku Ukrainy. Zakon Ukrainy 21.06.2018 № 2469–VIII [On National Security of Ukraine. Law of Ukraine of June 21, 2018, № 2469–VIII]. *Vebportal Verkhovnoi Rady Ukrainy – Web portal of the Verkhovna Rada of Ukraine.* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].

2. Hrebeniuk, A. M., & Rybalchenko, L. V. (2020). *Osnovy upravlinnia informatsiinoiu [Fundamentals of information security management].* Dnipro: DDUVS [in Ukrainian].

3. Pro Stratehiiu informatsiinoi bezpeky. Ukaz Prezydenta Ukrainy vid 28.12.2021 № 685/2021 [On the Information Security Strategy. Decree of the President of Ukraine dated December 28, 2021, № 685/2021]. *Vebportal Verkhovnoi Rady Ukrainy – Web portal of the Verkhovna Rada of Ukraine.* Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].

4. Ostroukhov, V. V. (Ed.) (2021). *Informatsiina bezpeka [Information security].* Kyiv: Lira-K [in Ukrainian].

5. Tykhomyrov, O. O. (2023). *Prava liudyny: informatsiinyi vymir [Human Rights: Information Dimension].* Odesa: Yurydyka [in Ukrainian].
6. Dzoban, O. P. (2013). *Filosofiia informatsiinoho prava: svitohliadni y zahalnoteoretychni zasady [Philosophy of information law: worldview and general theoretical foundations].* Kharkiv: Maidan [in Ukrainian].
7. Haborets, O. A. (2024). Znachennia biometrychnoi avtentyfikatsii v suchasnykh systemakh bezpeky [The significance of biometric authentication in modern security systems]. *Elektronnyi zhurnal "Nauka i tekhnika sohodni" – Electronic journal "Science and Technology Today",* 6, 799–806 [in Ukrainian].
8. Bodnarchuk, O. H., Bodnarchuk, O. I., Hlukh, M. V., & Harbinska-Rudenko, A. V. (2024). *Pravove rehuliuvannia natsionalnoi bezpeky [Legal regulation of national security].* Irpin: Derzhavnyi podatkovyi universytet [inUkrainian].
9. Pro informatsiiu. Zakon Ukrainy vid 02.10.1992 № 2657–XII [About information. Law of Ukraine dated October 2, 1992, № 2657–XII]. *Vebportal Verkhovnoi Rady Ukrainy – Web portal of the Verkhovna Rada of Ukraine.* Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].
10. Pro Stratehiiu natsionalnoi bezpeky Ukrainy. Ukaz Prezydenta Ukrainy vid 14.09.2020 № 392/2020 [On the National Security Strategy of Ukraine. Decree of the President of Ukraine dated September 14, 2020, № 392/2020]. *Vebportal Verkhovnoi Rady Ukrainy – Web portal of the Verkhovna Rada of Ukraine.* Retrieved from: https://zakon.rada.gov.ua/laws/show/392/2020#Text [in Ukrainian].
11. Bocharnikov, V. P., & Svieshnikov, S. V. (2019). *Bezpekove seredovyshche 2030 [Safe Environment 2030].* Kyiv: Maister knyh [in Ukrainian].
12. Franchuk, V. I. (2023). Teoretyko-metodolohichni ta upravlinski zasady rozvytku bezpekovoho seredovyshcha [Theoretical, methodological and managerial principles of developing a security environment]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav – Scientific Bulletin of the Lviv State University of Internal Affairs, 2,* 63–73 [in Ukrainian].
13. Pro Stratehiiu kiberbezpeky Ukrainy. Ukaz Prezydenta Ukrainy vid 26.08.2021 № 447/2021 [On the Cybersecurity Strategy of Ukraine. Decree of the President of Ukraine dated August 26, 2021, № 447/2021]. *Vebportal Verkhovnoi Rady Ukrainy – Web portal of the Verkhovna Rada of Ukraine.* Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].
14. Khorishko, L. S. (Ed.). (2023). *Strategic communications in the formation of the Ukrainian national security system.* Riga, Latvia: Baltija Publishing [in English].
15. Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh. Zakon Ukrainy vid 05.07.1994 № 80/94-VR [On the Protection of Information in Information and Communication Systems. Law of Ukraine dated July 5, 1994, № 80/94-VR]. *Vebportal Verkhovnoi Rady Ukrainy – Web portal of the Verkhovna Rada of Ukraine.* Retrieved from: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [in Ukrainian].

Voloboiev Arthur,
PhD in Law,
Head of the Department of Operational and Investigative Activities and Information Security
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-7138-5847

Zelenskyi Serhii,
Candidate of Law Sciences, Associate Professor,
Associate Professor at the Department of Operational and Investigative Activities and Information Security
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-0945-4485

LEGAL AND ORGANIZATIONAL PRINCIPLES FOR ENSURING INFORMATION SECURITY IN UKRAINE

The rapid development of information and communication technologies, the comprehensive digitalization of society, and integration into the global information space create preconditions for the weakening of state information sovereignty. Globalization processes in the information environment significantly affect the parameters of information security and the functioning of the information society as a whole, generating unprecedented threats in key areas of public life. In view of this, information security acquires the status of an independent and integral element of Ukraine's national security.

The need to protect the national information environment determines the necessity of a systematic approach to information security, which is especially relevant in the context of strengthening Ukrainian statehood under martial law. Ukraine's state information security is implemented as an integral component of national security. In the legal dimension, it is based on democratic principles and the rule of law and is carried out through the development and implementation of relevant national doctrines, strategies, concepts, and information security programs.

Accordingly, this article provides a comprehensive analysis of the legal and organizational principles of Ukraine's national information security system, identifies the main challenges to its development, and outlines promising directions for its improvement. In particular, the structure of these organizational principles is defined as including: objectivity, scientific approach, systematicity, comprehensiveness, continuity, individualization of responsibility, and the synergy between centralized and decentralized management. Emphasis is placed on the importance of legal regulation of social relations in the field of information security.

Key words: *information security, national security, risks, threats, principles.*