# АДМІНІСТРАТИВНЕ, ІНФОРМАЦІЙНЕ, ФІНАНСОВЕ ТА ПОДАТКОВЕ ПРАВО

**УДК 342.951:351.74:355.4:004.9**
**DOI: 10.36550/2522-9230-2025-19-66-70**

**Кондратенко Віталій Миколайович,**
доктор юридичних наук, професор,
професор кафедри загальноправових дисциплін та державного управління
Центральноукраїнського державного університету
імені Володимира Винниченка
kondratenkovitals@gmail.com
ORCID ID: 0000-0001-6015-8326

**Чинченко Світлана Миколаївна,**
аспірантка кафедри галузевого права та правоохоронної діяльності
Центральноукраїнського державного університету
імені Володимира Винниченка
schynchenko@gmail.com
ORCID ID: 0009-0007-0605-1983

## АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗДІЙСНЕННЯ КОНТРОЛЮ ЗА БЕЗПЕЧНИМ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ОБОРОННІЙ ТА ПРАВООХОРОННІЙ СФЕРІ УКРАЇНИ

Стаття присвячена дослідженню адміністративно-правових механізмів контролю за безпечним використанням інформаційних ресурсів у діяльності поліції, інших правоохоронних органів та Збройних Сил України (ЗСУ). У центрі аналізу – поєднання вимог відкритості публічної влади та права громадян на доступ до інформації з обов'язком держави забезпечувати захист даних в умовах цифровізації та гібридної агресії. Показано, що ускладнення інформаційних потоків, зростання кількості кіберінцидентів і спроб несанкціонованого втручання в роботу публічних систем задають підвищену потребу у чітких, зрозумілих процедурах доступу, нагляду та юридичної відповідальності. Схарактеризовано специфіку контрольних функцій правоохоронних органів і структур оборонного сектору, які мають документувати порушення та реагувати на загрози, здійснювати превентивний моніторинг, аудит інформаційних систем і забезпечувати узгодженість міжвідомчих дій. Розкрито проблеми практичного застосування законодавства: формалізм під час розгляду інформаційних запитів, нечіткість критеріїв обмеження доступу, однорідність підходів у різних органах, недостатність незалежного контролю та різний рівень цифрової грамотності.

Особливу увагу приділено впливу цифрових сервісів і державних платформ на режим доступності інформації, а також необхідності формування внутрішньої культури відкритості як умови реальної підзвітності влади. Підкреслено, що ефективність інформаційної політики у сфері національної безпеки залежить від здатності держави забезпечити баланс між прозорістю та захистом критичних даних. Обґрунтовано напрями вдосконалення адміністративно-правового регулювання контролю за використанням інформаційних ресурсів у правоохоронній та оборонній сферах.

Наголошено, що результативність контрольних процедур визначається чітким розмежуванням повноважень між суб'єктами нагляду, прозорістю рішень щодо обмеження доступу та наявністю дієвих механізмів зовнішнього контролю. Здатність правоохоронних органів і ЗСУ гарантувати безпечний обіг даних, дотриматися вимог законності та мінімізувати ризики для обороноздатності держави розглядається як ключова умова стабільного функціонування публічної влади в умовах зростання цифрових загроз.

**Ключові слова:** адміністративно-правовий механізм, верховенство права, законність, Збройні Сили України (ЗСУ), інформаційні ресурси, інформаційна безпека, контроль, контрольні функції, національна безпека, Національна поліція України, правопорушення, правоохоронні органи, публічна влада, публічна інформація, сектор безпеки та оборони.

**Kondratenko V., Chynchenko S. ADMINISTRATIVE AND LEGAL MECHANISMS FOR CONTROLLING THE SAFE USE OF INFORMATION RESOURCES IN THE DEFENSE AND LAW-ENFORCEMENT SECTORS OF UKRAINE**

The article examines the administrative and legal mechanisms for controlling the safe use of information resources in the activities of the police, other law-enforcement bodies, and the Armed Forces of Ukraine (AFU). The analysis focuses on the interplay between the requirements of openness of public authorities and the citizens' right of access to information, on the one hand, and the state's obligation to ensure data protection under conditions of digitalisation and ongoing hybrid aggression, on the other.

The study demonstrates that the increasing complexity of information flows, the growing number of cyber incidents,

and attempts at unauthorised interference in the operation of public systems create an intensified need for clear and predictable procedures of access, oversight, and legal accountability. The specific features of the control functions of law-enforcement agencies and defense-sector structures are outlined, including the duty to document violations, respond to threats, conduct preventive monitoring, audit information systems, and coordinate actions.

Special attention is given to the impact of digital services and state platforms on the regime of information accessibility, as well as to the need to cultivate an internal culture of openness as a prerequisite for genuine governmental accountability. The article emphasizes that the effectiveness of information policy in the national-security sphere depends on the state's ability to maintain a balance between transparency and the protection of critical data. Directions for improving administrative and legal regulation of control over the use of information resources in law-enforcement and defense institutions are substantiated.

It is stressed that the effectiveness of control procedures is determined by a clear delineation of supervisory powers, transparency of decisions regarding access restrictions, and the availability of effective mechanisms of external oversight. The capacity of law-enforcement bodies and the AFU to ensure the secure circulation of data, comply with legal requirements, and minimize risks to the state's defense capability is presented.

**Keywords:** Administrative-legal mechanism, control, control functions, defense and security sector, information resources, information security, lawfulness, law-enforcement agencies, national security, public authorities, public information, rule of law, the Armed Forces of Ukraine (AFU), the National Police of Ukraine, violations.

**Постановка проблеми.** Динаміка розвитку інформаційного суспільства висуває до держави та її органів підвищені вимоги щодо захисту інформації, належного використання електронних ресурсів і забезпечення відкритості публічної влади. Швидкість обміну даними та масштаб комунікацій створили умови для активної участі громадян у контролі за діяльністю публічних інституцій, підвищили рівень прозорості та сприяли зміцненню довіри до суб'єктів влади. Право на доступ до публічної інформації стало складовою демократичного устрою та важливим елементом цивільного контролю.

Поряд із новими перевагами цифрового середовища посилюються ризики небезпечного використання інформаційних ресурсів. Дані, що переходять у відкритий доступ, нерідко стають підставою для завдання шкоди державним інтересам, приватним особам, організаціям. Загрозливими є спроби втручання у роботу державних інформаційних систем, несанкціонований доступ до реєстрів, поширення дезінформації та інші дії, що здатні підірвати стабільність безпекового середовища. Для оборонної сфери, зокрема для ЗСУ, такі ризики набувають критичного значення, оскільки навіть незначний витік даних може вплинути на раціональність виконання бойових завдань і загальний рівень обороноздатності.

Національна поліція України та інші суб'єкти сектору національної безпеки опинилися в ситуації, коли необхідно поєднувати вимоги відкритості й підзвітності з обов'язком гарантувати контроль за безпечним використанням інформаційних ресурсів. Це потребує чітких адміністративно-правових процедур, які визначають порядок доступу до відомостей, встановлюють критерії їх захисту та передбачають відповідальність за порушення установлених правил.

**Аналіз останніх досліджень та публікацій.** Проблематика контролю за використанням інформаційних ресурсів в оборонній та правоохоронній сферах сформувалася як окремий науковий напрям.

Значний внесок у дослідження цих питань зробили О.П. Плужник, Л.В. Кириченко, В.П. Діхтієвський, О.Ф. Андрійко, та інші дослідники, які звертали увагу на природу державних інформаційних систем, вимоги до їх захисту та особливості адміністративно-правового впливу. До кола авторів, що вивчають специфіку інформаційної безпеки у діяльності силових структур, належать О.М. Бандурка, А.П. Гетьман, В.М. Шаповал.

У сфері оборони окремого значення набули праці О.Ю. Наливайка, О.В. Дзюби, О.М. Стародубцевої, які вивчали специфіку безпеки військових інформаційних систем, ризики витоку даних, механізми внутрішнього та зовнішнього контролю в ЗСУ. У цих дослідженнях простежується тенденція до розширення спектра інструментів адміністративного контролю над інформаційними ресурсами – від процедур доступу до комплексних моделей аудиту та реагування на кіберінциденти. Незважаючи на наявність вагомих напрацювань, низка питань залишається недостатньо систематизованою.

**Мета статті** полягає у з'ясуванні змісту та особливостей адміністративно-правових механізмів контролю за безпечним використанням інформаційних ресурсів у діяльності правоохоронних органів і ЗСУ. Дослідження спрямоване на виявлення ключових проблем у функціонуванні систем контролю, аналіз нормативних вимог і практичних процедур, а також формулювання пропозицій щодо вдосконалення правового регулювання з урахуванням безпекових викликів і розвитку європейської інтеграції України.

**Виклад основного матеріалу дослідження.** У демократичних правопорядках інформація становить основу підзвітності публічної влади та є дієвим інструментом контролю за її діяльністю. Реалізація права на доступ до публічної інформації забезпечує громадянам можливість отримувати достовірні відомості про управлінські процеси, оцінювати їх відповідність принципу верховенства права та вимогам законності, а також впливати на формування державної політики. Відкритість інформаційних потоків сприяє зміцненню інституційної відповідальності та попередженню зловживань у сфері публічного управління [1, с. 33-35; 2, с. 55-56].

За умов розвитку цифрових технологій роль громадянина у системі публічної влади істотно змінюється. Доступ до інформації трансформує його з пасивного спостерігача на свідомого учасника, спроможного оцінювати якість публічних послуг і впливати на легітимність рішень державних органів. Саме через інформованість забезпечується реальна участь суспільства у механізмах контролю за діями

посадових осіб та органів влади.

В умовах гібридної агресії та посилення зовнішніх загроз інформація набуває значення елементу національної безпеки. Для України це питання виходить за межі індивідуального права і стосується стійкості державного управління, довіри до інституцій і здатності держави ефективно та вчасно виконувати свої функції [3, с. 80]. Прозорість бюджетних рішень, відкритість процедур, поширення достовірних даних. Окреслене надає дієві запобіжники для зовнішнього впливу та укріплює легітимність публічної влади.

У таких умовах особливого значення набуває адміністративно-правовий механізм, який забезпечує належний порядок використання інформаційних ресурсів. Його зміст складають чітко визначені процедури доступу, контроль за дотриманням установлених правил, відповідальність за порушення режимів інформаційної безпеки, а також інституційні гарантії усталення законності. Цифровізація документообігу, впровадження електронних сервісів, розвиток державних реєстрів потребують нормативних рішень, що гарантують безпечне функціонування інформаційних систем у всіх секторах, включаючи оборонний та правоохоронний.

Загалом розширення і вдосконалення правових, організаційних та технічних інструментів реалізації права на доступ до публічної інформації повинно розглядатися як стратегічний пріоритет державної політики. Забезпечення формальної відповідності європейським стандартам та створення внутрішньої культури відкритості – середовища, в якому прозорість, підзвітність і діалог із суспільством є нормою функціонування кожної владної інституції. Такий підхід зміцнює державність, підвищує ефективність публічного адміністрування й формує передумови для побудови якісно нової моделі взаємодії влади й громадян.

Практична реалізація принципів відкритості та підзвітності стикається з низкою системних обмежень. Наявність умовних процедур доступу до інформації сама по собі не гарантує прозорості діяльності органів публічної влади. У багатьох випадках механізми громадського контролю залишаються недостатньо розвиненими, а інструменти внутрішнього й зовнішнього аудиту рішень не забезпечують належного рівня законності та ефективності. За таких умов особливо важливою стає роль правоохоронних органів і структур сектору національної безпеки, які зобов’язані захищати державні інтереси, здійснювати контроль за використанням інформаційних ресурсів, реагувати на порушення режимів доступу та запобігати неправомірному втручанню в роботу інформаційних систем [4, с. 217; 5].

Попит суспільства на відкритість діяльності органів влади, включно з силовими структурами, посилюється у періоди криз, воєнного стану та масштабних соціальних трансформацій [6]. Громадяни очікують своєчасного й достовірного інформування про роботу оборонних і правоохоронних відомств, реалізацію реформ, використання бюджетних коштів та інші питання, що впливають на публічну безпеку. Довіра до держави значною мірою залежить від того, наскільки оперативно і в повному обсязі надається важлива інформація. Водночас надмірна відкритість або поширення даних без належного контролю створюють додаткові ризики: полегшують дії зовнішніх загроз, сприяють дезінформаційним кампаніям, розширюють можливості для маніпуляцій і кіберзловживань. Саме тому питання розробки балансу між прозорістю і безпечним використанням інформаційних ресурсів набуває першорядного значення для всієї системи публічного управління.

Активна цифровізація публічного управління та поширення електронних сервісів істотно змінили характер обігу інформації в публічній сфері. Дані пересуваються між інформаційними системами з високою швидкістю, а глобальна мережа робить можливим їх миттєве поширення за межі національного юрисдикційного простору. За таких умов контроль за безпечним використанням інформаційних ресурсів ускладнюється, а ймовірність витоку конфіденційних відомостей зростає. Кіберінциденти, спроби несанкціонованого доступу до державних реєстрів, втручання у роботу електронних систем і маніпуляції у цифровому середовищі стали невід’ємною частиною сучасного безпекового контексту [7].

Наведені обставини висувають підвищені вимоги до Національної поліції, інших правоохоронних органів та структур сектору національної безпеки. Їхня діяльність повинна охоплювати реагування на порушення та превентивний контроль за станом інформаційної безпеки, виявлення джерел кібератак, документування неправомірного використання інформаційних ресурсів і законності в роботі з даними. Водночас належить гарантувати дотримання конституційних прав громадян на доступ до публічної інформації та запобігати зловживанням, які можуть порушити баланс між прозорістю та безпекою. Комплексність контрольних функцій зумовлює потребу в чітких правових механізмах нагляду у правоохоронній та оборонній сферах.

Підходи до регулювання доступу до інформації формуються під впливом міжнародних стандартів, зокрема рекомендацій Ради Європи та практики Європейського суду з прав людини, де наголошується на необхідності поєднання прозорості з гарантіями захисту чутливих даних. Досвід держав із розвиненими цифровими інфраструктурами демонструє, що ефективність системи доступу значною мірою залежить від наявності дієвих інструментів контролю за використанням інформаційних ресурсів та дотриманням вимог законності.

В умовах гібридної війни та активних інформаційних впливів питання балансу між відкритістю і безпекою набуває особливої ваги. Законодавство України, зокрема «Про доступ до публічної інформації», «Про Національну поліцію України», «Про Збройні Сили України», поєднує загальні засади прозорості з

конкретними підставами для обмеження доступу до даних, якщо їх розкриття може завдати шкоди обороноздатності, міжнародним відносинам, національній безпеці чи правам інших осіб [8–10]. Такі норми укорінюють правову визначеність і підтримують принцип верховенства права у площині інформаційних відносин.

Практичне виконання цих вимог покладається на правоохоронні органи та відповідні структури оборонного сектору. Їм належить здійснювати контроль за дотриманням установлених процедур, реагувати на порушення режимів доступу, документувати випадки неправомірного розкриття інформації та координувати взаємодію між відомствами для забезпечення належного рівня інформаційної безпеки. Виконання окреслених функцій сприяє підтриманню законності та захисту інтересів держави в умовах зростання цифрових загроз.

Останні роки засвідчили суттєве зростання випадків складних кіберінцидентів та спроб несанкціонованого доступу до захищених державних даних. Масштаб атак спрямовується передусім на інформаційні системи органів публічної влади, оборонного сектору та силових структур, де обробляються відомості про критичну інфраструктуру, військову логістику, персонал, службові реєстри. У публічних звітах фіксується тенденція до збільшення кількості спроб втручання, а наслідки виходять за межі суто технічних порушень. Окремі інциденти впливали на функціонування місцевих органів влади, доступність соціальних послуг і реалізацію оборонних заходів.

У протидію державні органи, відповідальні за забезпечення інформаційної безпеки в правоохоронній та оборонній сферах, удосконалюють протоколи реагування, тимчасово обмежують доступ до окремих категорій даних (зокрема інформації про переміщення військових підрозділів або об’єкти критичної інфраструктури), здійснюють аудит інформаційних систем та підвищують вимоги до кібергігієни персоналу [11]. У ЗСУ посилюється контроль за дотриманням режимів інформаційної безпеки, включно з впровадженням внутрішніх процедур перевірки, моніторингу цифрових каналів і відповідальності за неналежне поводження з інформаційними ресурсами. Вказані заходи спрямовані на забезпечення законності у сфері використання даних та мінімізацію ризиків для обороноздатності держави.

Розвиток цифрових платформ, державних сервісів і порталів відкритих даних суттєво змінив порядок взаємодії громадян з органами публічної влади. Автоматизація розгляду інформаційних запитів спрощує доступ до необхідних відомостей, однак водночас ускладнює завдання із захисту інформаційних ресурсів від несанкціонованого втручання. Зростає потреба у належних гарантіях безпечного використання даних, чітких правилах їх обробки та потрібному контролі за дотриманням режимів інформаційної безпеки. У цій системі правоохоронні органи виконують важливу роль: вони реагують на інциденти, документують правопорушення, здійснюють моніторинг кіберзагроз і беруть участь у підвищенні цифрової грамотності державних службовців, формуючи практичні інструкції щодо роботи з інформацією.

Попри прогрес відповідних технологій, низка проблем залишається невирішеною. У практиці трапляються випадки бюрократичного підходу до розгляду інформаційних запитів, необґрунтованих відмов у наданні даних або, навпаки, розкриття відомостей, які підлягають захисту. Нечіткість критеріїв обмеження доступу, недостатня координація між органами влади й правоохоронними структурами, обмеженість незалежного зовнішнього контролю та нерівномірний рівень підготовки персоналу створюють умови для порушення принципу законності. Наслідки таких ситуацій можуть зачіпати як інтереси держави, так і права приватних осіб.

За вказаних обставин актуальною є потреба у вдосконаленні адміністративно-правових механізмів контролю: оновленні процедур, чіткішому визначенні підстав для обмеження доступу, розширенні можливостей аудиту та моніторингу, системному підвищенні кваліфікації працівників. Саме попереджувальні заходи здатні гарантувати належний рівень законності та безпеки з питань використання інформаційних ресурсів.

**Висновки.** Проведений аналіз свідчить, що у цифровому середовищі головним викликом стає створення контрольованого і безпечного використання інформаційних ресурсів при одночасному збереженні відкритості публічної влади. Право громадян на доступ до інформації залишається фундаментальною демократичною гарантією, але зростання інтенсивності кіберзагроз, поширення гібридних форм агресії та ускладнення роботи державних інформаційних систем істотно підвищують вимоги до правових механізмів їхнього захисту.

У цих умовах правоохоронні органи та структури оборонного сектору виконують складну і багатовимірну функцію: вони мають забезпечувати законність і безпеку в обігу даних, контролювати дотримання режимів захисту інформаційних ресурсів, запобігати неправомірному втручанню у роботу інформаційних систем. Потрібно гарантувати, щоб обмеження доступу застосовувалися виключно на підставах, визначених законом. Для ЗСУ питання контролю та безпечного використання інформаційних ресурсів набуває особливої ваги, оскільки навіть незначні порушення можуть вплинути на обороноздатність країни і стійкість військового управління.

Належне функціонування адміністративно-правового механізму у цій сфері залежить від чіткого розмежування повноважень між суб’єктами контролю, функціонування незалежних інституцій зовнішнього нагляду, прозорих процедур ухвалення рішень щодо обмеження доступу та можливості подальшого перегляду таких рішень. Дотримання принципів законності та верховенства права має залишатися базовою

умовою для дій, пов'язаних із захистом інформації, незалежно від рівня загроз чи воєнного стану.

**СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:**

1. Демократичний цивільний контроль над сектором безпеки і оборони: теорія і практика : навчальний посібник / за заг. ред. В. Г. Пилипчука; НДІ інформатики і права НАПрН України. Київ; Одеса : Фенікс, 2020. 224 с.

2. Сибіга О.М. Право особи на доступ до публічної інформації: адміністративно-правове забезпечення і захист : монографія. Херсон : Видавничий дім «Гельветика», 2019. 370 с.

3. Галаган В. І., Третяк Н. М., Полішко С. В. Проблемні питання під час ведення та впровадження проєктів інформатизації Збройних Сил України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2025. № 1(84). С. 79–86.

4. Бойко А. Аналіз нормативно-правової бази, що регламентує питання організації системи внутрішнього контролю у Міністерстві оборони України та підпорядкованих установах. *Social Development and Security*. 2025. Vol. 15. № 1. С. 214-226.

5. Національний координаційний центр кібербезпеки при РНБО України. URL: https://www.ncscc.gov.ua/.

6. Офіційний портал відкритих даних України. URL: https://data.gov.ua/.

7. Міністерство цифрової трансформації України. Електронні сервіси. URL: https://thedigital.gov.ua/.

8. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/law s/ show/2939-17#Text.

9. Національна поліція України : Офіційний вебпортал. URL: https://npu.gov.ua/.

10. Збройні Сили України : Офіційний вебпортал. URL: https://www.zsu.gov.ua/.

11. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: https://zakon.rada.gov. ua/laws/show/373-2006-п#Text.

**REFERENCES:**

1. Pylypchuk, V. H. (Ed.). (2020). Demokratychnyi tsyvilnyi kontrol nad sektorom bezpeky i oborony: teoriia i praktyka. Navchalnyi posibnyk. NDI informatyky i prava NAPrN Ukrainy. Kyiv; Odesa: Feniks. 224. [Democratic civil control over the security and defense sector: theory and practice. Textbook]. [in Ukrainian].

2. Sybiha, O. M. (2019). Pravo osoby na dostup do publichnoi informatsii: administratyvno-pravove zabezpechennia i zakhyst. Monohrafiia. Kherson: Vydavnychyi dim "Helvetyka". 370. [The individual's right of access to public information: administrative-legal support and protection]. [in Ukrainian].

3. Halahan, V. I., Tretiak, N. M., Polishko, S. V. (2025). Problemni pytannia pid chas vedennia ta vprovadzhennia proiektiv informatyzatsii Zbroinykh Syl Ukrainy. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy. No 1(84). 79–86. [Problematic issues in conducting and implementing informatization projects of the Armed Forces of Ukraine]. [in Ukrainian].

4. Boiko, A. (2025). Analiz normatyvno-pravovoi bazy, shcho rehlamentuie pytannia orhanizatsii systemy vnutrishnoho kontroliu u Ministerstvi oborony Ukrainy ta pidporiadkovanykh ustanovakh. Social Development and Security. Vol. 15, No 1. 214–226. [Analysis of the legal framework regulating the organisation of the internal control system in the Ministry of Defense of Ukraine and subordinated institutions]. [in Ukrainian].

5. Natsionalnyi koordynatsiinyi tsentr kiberbezpeky pry RNBO Ukrainy. URL: https://www.ncscc.gov.ua/. [National Cybersecurity Coordination Center under the NSDC of Ukraine]. [in Ukrainian].

6. Ofitsiinyi portal vidkrytykh danykh Ukrainy. URL: https://data.gov.ua/. [Official open data portal of Ukraine]. [in Ukrainian].

7. Ministerstvo tsyfrovoi transformatsii Ukrainy. Elektronni servisy. URL: https://thedigital.gov.ua/. [Ministry of Digital Transformation of Ukraine. Electronic services]. [in Ukrainian].

8. Pro dostup do publichnoi informatsii: Zakon Ukrainy vid 13.01.2011 No 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text. [On Access to Public Information: Law of Ukraine]. [in Ukrainian].

9. Natsionalna politsiia Ukrainy: Ofitsiinyi vebportal. URL: https://npu.gov.ua/. [National Police of Ukraine: Official web portal]. [in Ukrainian].

10. Zbroini Syly Ukrainy: Ofitsiinyi vebportal. URL: https://www.zsu.gov.ua/. [Armed Forces of Ukraine: Official web portal]. [in Ukrainian].

11. Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh systemakh: Postanova Kabinetu Ministriv Ukrainy vid 29.03.2006 No 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-p#. [On approval of the Rules for ensuring information protection in information, electronic communication and information-communication systems: Resolution of the Cabinet of Ministers of Ukraine]. [in Ukrainian].

Стаття надійшла до редакції: 10.11.2025