| | |
|---|---|
| **Секція Право** | |
| **УДК 342.9:351.86:004.056(477)** | |
| **Дата першого надходження статті до видання** | 2026-03-15 |
| **Дата прийняття статті до друку після рецензування** | 2026-04-25 |
| **Дата публікації/оприлюднення** | 2026-04-25 |

# Адміністративно-правове регулювання органів публічного управління в механізмі забезпечення інформаційної безпеки України

**Чистоклетов Леонтій Григорович**
доктор юридичних наук, професор,
професор кафедри адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»,
ORCID iD: 0000-0002-3306-1593

**Струтинська Вікторія Миронівна**
здобувачка другого магістерського рівня
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»,
ORCID iD: 0009-0004-9653-3799

**Анотація.** В статті розглянуто основні аспекти адміністративно-правового регулювання органів публічного управління в механізмі забезпечення інформаційної безпеки України. Також проведено комплексний аналіз адміністративно-правового регулювання діяльності органів державного управління в системі інформаційної безпеки України. Досліджено еволюцію поняття «інформаційна безпека» від філософських концепцій епохи Відродження до сучасних стандартів цифрової стійкості. Особлива увага приділяється Стратегії інформаційної безпеки 2021 року як базовому нормативному документу, що визначає стан захисту суверенітету та прав громадян у цифровому просторі.

У роботі детально описано систему суб'єктів інформаційної безпеки, класифікуючи їх за компетенцією та рівнями управління. Визначено специфіку функцій та повноважень ключових органів: Служби безпеки України (контррозвідувальний захист), Державної служби спеціального зв'язку та захисту інформації (технологічне ядро та кіберзахист), а також Ради національної безпеки і оборони України (стратегічна координація).

Також була приділена увага методам адміністративно-правового регулювання, серед яких виділяються імперативний, диспозитивний, методи сертифікації, реєстрації та колегіального контролю. У контексті європейської інтеграції аналізується зарубіжний досвід Німеччини, Франції та США, зокрема щодо впровадження стандартизованих планів реагування («Playbooks») та нагляду за критичною інфраструктурою. На основі проведеного дослідження сформульовано висновки щодо необхідності подальшої гармонізації законодавства України з європейськими стандартами (GDPR, NIS) та вдосконалення міжвідомчої співпраці для посилення національної стійкості в умовах гібридної агресії.

**Ключові слова**: безпека, інформаційна безпека, національна безпека, органи публічного управління, адміністративно-правове регулювання, система органів публічного управління, зарубіжний досвід.

# Administrative and legal regulation of public administration bodies in the mechanism of ensuring information security in Ukraine

**Chystokletov Leontii**
Professor of the Department of
Administrative and Information Law
of the Educational and Scientific Institute of Law,
Psychology and Innovative Education
Lviv Polytechnic National University,
Doctor of Law, Professor
ORCID iD: 0000-0002-3306-1593

**Strutynska Viktoriia**
second (master's) level higher education student
of the Educational and Scientific Institute of Law,
Psychology and Innovative Education
Lviv Polytechnic National University
ORCID iD: 0009-0004-9653-3799

**Abstract.** The article examines the fundamental aspects of the administrative and legal regulation of public administration bodies within the mechanism of ensuring Ukraine's information security. A comprehensive analysis of the administrative and legal regulation of state management activities within the information security system of Ukraine is conducted. The study explores the evolution of the concept of "information security," spanning from Renaissance philosophical concepts to modern digital resilience standards. Particular attention is paid to the 2021 Information Security Strategy as the foundational regulatory document defining the protection of sovereignty and citizens' rights in the digital space.

The work provides a detailed description of the system of information security actors, classifying them by competence and levels of management. It identifies the specific functions and powers of key authorities: the Security Service of Ukraine (counterintelligence protection), the State Service of Special Communications and Information Protection of Ukraine (the technological core and cyber defense), and the National Security and Defense Council of Ukraine (strategic coordination).

Attention is also given to methods of administrative and legal regulation, highlighting imperative and dispositive methods, as well as methods of certification, registration, and collegial control. In the context of European integration, the study analyzes foreign experiences from Germany, France, and the USA, particularly regarding the implementation of standardized response plans ("Playbooks") and the oversight of critical infrastructure. Based on the conducted research, conclusions are formulated regarding the necessity for further harmonization of Ukrainian legislation with European standards (GDPR, NIS) and the improvement of interagency cooperation to strengthen national resilience in the face of hybrid aggression.

**Keywords:** security, information security, national security, public administration bodies, administrative and legal regulation, system of public administration bodies, foreign experience.

## Вступ

У сучасному світі, що проходить крізь процеси цифрової трансформації інформація як така перетворилася на стратегічний ресурс, що за своїм значенням не поступається природним багатствам чи фінансовим ресурсам. Стрімкий розвиток

інформаційно-комунікаційних технологій, невпинна цифровізація у сферах державного управління та суспільного життя однозначно вплинули на глобальну світобудову, зробивши держави більш ефективними, але водночас більш вразливими до нових видів загроз. У таких умовах інформаційна безпека перестає бути вузькотехнічним питанням і трансформується у фундаментальну частину національної стійкості та безпеки. Сучасні виклики та загрози з якими стикаються у багатьох державах (кібератаки, агресивна пропаганда, поширення неправдивої інформації тощо) вказують на однозначну важливість та пріоритетність вивчення питання інформаційної безпеки як складової національної безпеки. Безпека, в тому числі інформаційна – це в першу чергу стабільний стан відсутності об'єктивних загроз та протиправних зазіхань. Для того, щоб зберігати стабільність цього стану з боку держави повинні діяти ефективні механізми забезпечення інформаційної безпеки. Складовою такого механізму є адміністративно-правова діяльність органів публічного управління. Через наділення органів публічного управління відповідними повноваженнями для забезпечення інформаційної безпеки держава створює систему реагування на інформаційні загрози.

Дослідженням виникнення та еволюції поняття інформаційної безпеки займалися такі науковці: М. Шевчук, В. Новицький, С. Лисенко, Д. Казмірук, С. Суслін, А. Крупнова. Детальніше про методи адміністративно-правового регулювання діяльності органів публічного управління у механізмі забезпечення інформаційної безпеки досліджували: П. Яковлєв, В. Котляров, О. Малашко.

Іноземний досвід правового забезпечення інформаційної та кібербезпеки досліджували: С. Кавун, І. Брацюк, А. Литвиненко, Т. Ребом, К. Сандкул, Т. Кемеріч, М. Керолл.

Метою статті є ґрунтовний аналіз та характеристика адміністративно-правових засад діяльності органів публічного управління для забезпечення інформаційної безпеки України. Додатково, метаю також є розробка пропозицій для вдосконалення законодавства України у цій сфері.

**Результати дослідження**

Абсолютно логічним видається те, що дослідження адміністративно-правового регулювання органів публічного управління в механізмі забезпечення інформаційної безпеки України слід розпочати із з'ясування сутності поняття інформаційної безпеки та її значення як складової національної безпеки України. Якщо зробити невеликий екскурс в історію виникнення та розвитку поняття інформаційної безпеки, то ми побачимо, що інформаційна безпека як така виникла на основі першочергового поняття безпеки. В свою чергу питання безпеки стало актуальним та обговорюваним у періоди воєн. До прикладу, формування елементів науково-філософського розуміння безпеки розпочалось ще в епоху Відродження. В цей період центральною цінністю стала людина та її інтелектуальна (інформаційна) незалежність. Ідея антивоєнного розвитку суспільства виникла з прагнення гуманістів ліквідувати соціальну несправедливість та релігійний гноблення. Водночас XVI століття дало поштовх розвитку технологій політичної маніпуляції: Нікколо Макіавеллі першим описав техніки інформаційно-психологічного контролю. Історія показує, що з того часу потужна пропаганда та дезінформація неодноразово ставали вирішальними силами у світовій політиці [1, с. 135]. Основи сучасних наукових уявлень про національну безпеку та її інформаційний аспект були закладені Томасом Гоббсом та Іммануїлом Кантом. Їхньою спільною точкою зору був природний стан «війни всіх проти всіх» та відсутність правових норм, що вимагали б створення цивілізованої державної системи для гарантування індивідуальної безпеки. Пізніше, в епоху Просвітництва, Джон Локк, Вольтер та Дені Дідро доповнили цю концепцію розумінням миру, заснованим на релігії та етиці. Класична німецька філософія, представлена Й. Фіхте та Й. Гердером, переосмислила

безпеку крізь призму національного суверенітету. Особливе місце займала теорія Анрі Бергсона, який пов'язував інформаційну безпеку з концепцією «відкритого» та «закритого» суспільств. Він стверджував, що ізоляція неминуче призводить до конфлікту, а стан справжньої безпеки може бути досягнутий лише шляхом духовного оновлення людства та пріоритету «духовності» над «матеріалізмом» [2, с. 39]. Однозначний прорив у розумінні інформаційної безпеки настав з появою та активним використанням комп'ютерних систем, що породило нові переваги та проблеми щодо забезпечення інформаційної безпеки комп'ютерних систем.

Динаміка розвитку інформаційної безпеки першочергово знайшла свої відображення у правовій науці, адже саме наука здатна швидше реагувати на сучасні виклики порівняно з офіційним законодавством. Саме тому нам потрібно звернути увагу на доктринальний аспект та як науковці підходили до визначення поняття інформаційної безпеки. Д. М. Казмірук виконав якісне та ґрунтовне дослідження в якому констатував, що єдиного доктринального визначення поняття інформаційної безпеки немає. Натомість він наводить приклади визначень таких вчених: В. Гурковського, О. Данильяна, О. Дзьобан, М. Панова, В. Ліпкана та І. Бондар. Найбільш широкими та всеохоплюючими є пропозиції В. Гурковського та І. Бондар. Згідно із позицією цих дослідників інформаційна політика – це:

1) сукупність суспільних взаємодій, що гарантують захист фундаментальних інтересів особистості, суспільства та власне держави від зовнішніх і внутрішніх загроз в інформаційному середовищі. Вона виступає базисом для збереження національної ідентичності, духовних і матеріальних надбань, а також є ключовим фактором стійкого розвитку та зміцнення суверенітету України;

2) злагоджена діяльність системи засобів, спрямованих на захист інформаційних систем державного, корпоративного та приватного рівнів, що охоплює як програмно-технічне забезпечення автоматизованих процесів, так і правові механізми,, що гарантують дотримання прав людини та захист інтересів суспільства й держави в інформаційному просторі [3, с. 23].

Як бачимо науковий підхід до визначення поняття інформаційної безпеки є більш ширшим та варіативним, бо якщо ми поглянемо на нормативно-правовий аспект, то зможемо виявити, що в українському законодавстві міститься одне чітке та повне визначення у Стратегії інформаційної безпеки, яка була затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. Згідно з положенням цього документу інформаційна безпека України розглядається як складова частина національної безпеки України, що передбачає перебування держави у стані захищеності свого суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих інтересів людини, суспільства і держави, при цьому належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, а також існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом тощо [4]. Ця Стратегія була прийнята з метою посилення спроможностей задля забезпечення інформаційної безпеки в державі, в її інформаційному просторі, за допомогою інформаційних засобів та заходів підтримки стабільності в державі, в системі її оборони. Для досягнення цієї мети та інших стратегічних цілей держава має мати систему органів публічного управління, що наділені відповідними повноваженнями в цій сфері та повинні виконувати покладені на них функції.

Перш ніж перейти до детальної характеристики органів публічного управління, що здійснюють адміністративно-правове регулювання у механізмі забезпечення інформаційної безпеки слід зробити важливу ремарку: власне система органів публічного управління передбачає, що кожен із далі зазначених органів не існує відірвано від інших, усі вони якраз таки створюють цілісну взаємопов'язану систему адміністративно-правового забезпечення інформаційної безпеки. Тепер можемо перейти до класифікації та характеристики цих органів публічного управління.

Система суб'єктів інформаційної безпеки в Україні характеризується складною багаторівневою ієрархією. Ключовим елементом тут є адміністративно-правова держава, яка через норми публічного права визначає межі повноважень, обов'язків та відповідальності кожного учасника. Для державних інституцій ця держава має характер публічної влади, що надає їм право здійснювати контроль, координацію та застосовувати примусові заходи. Структура цієї системи включає такі органи публічного управління: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; Міністерство цифрової трансформації; Міністерство з питань реінтеграції тимчасово окупованих територій України; Міністерство внутрішніх справ; Міністерство оборони України; Національна поліція України; Служба безпеки України; Служба зовнішньої розвідки України; Державна служба спеціального зв'язку та захисту інформації України; Збройні Сили України та інші органи виконавчої влади та військові формування, які входять до сектору інформаційної безпеки; органи місцевого самоврядування; судові органи [5, с. 319]. Органи публічного управління із зазначеного переліку можна класифікувати за такими критеріями:

1. Органи стратегічного управління та загальної компетенції:
   - Президент України:
   - Верховна Рада України;
   - Кабінет міністрів України;
2. Координаційні та дорадчі органи:
   - Рада національної безпеки і оборони України;
3. Органи виконавчої влади галузевої та міжгалузевої компетенції:
   - Міністерство цифрової трансформації;
   - Міністерство внутрішніх справ;
   - Міністерство оборони України;
   - Міністерство з питань реінтеграції тимчасово окупованих територій України;
   - та інші органи виконавчої влади;
4. Спеціальні органи та військові формування:
   - Служба безпеки України;
   - Державна служба спеціального зв'язку та захисту інформації;
   - Служба зовнішньої розвідки України;
   - Збройні сили України;
   - Національна поліція України;
5. Органи правосуддя (суди);
6. Органи місцевого самоврядування.

Кожен із цих органів на своєму рівні має повноваження приймати правові акти для забезпечення інформаційної безпеки. Звичайно Президент України, Верховна рада України, Кабінет міністрів України уповноважені приймати нормативно-правові акти (закони та підзаконні нормативно-правові акти), що поширюють свою дію та є обов'язковими до виконання на всій території України. Натомість інші органи публічної влади свої правові акти на виконання вже прийнятих попередніми суб'єктами.

Як вдало підкреслює А. О. Крупнова, Верховна Рада України та Кабінет Міністрів України є ключовими суб'єктами, що визначають пріоритетні напрямки захисту

життєво важливих інтересів у сфері інформаційної безпеки, формують правову основу регулювання інформаційних відносин та регулюють порядок функціонування відповідних державних органів. Зокрема, Верховна Рада України, у межах своїх конституційних повноважень, розробляє державну політику та законодавчу базу в інформаційній сфері, одночасно здійснюючи контроль за дотриманням нормативних актів суб'єктами безпеки та їх посадовими особами. Верховна Рада здійснює парламентський контроль, приймає закони, що визначають компетенцію органів інформаційного сектору, затверджує бюджетні асигнування на їхні потреби та розглядає звіти про використання цих коштів. Для виконання контрольних функцій Верховна Рада створює спеціалізовані комітети, а для детального вивчення конкретних питань або розслідування суспільно значущих інцидентів у сфері інформаційної безпеки – тимчасові спеціальні та слідчі комісії, а також ініціює тематичні парламентські слухання. Паралельно, Кабінет Міністрів України відповідає за безпосереднє формування та практичну реалізацію державної інформаційної політики, гарантуючи інформаційний суверенітет та фінансову підтримку програм безпеки. Уряд розробляє та затверджує детальний план заходів щодо реалізації Стратегії інформаційної безпеки, яка стає основою для роботи органів виконавчої влади, та звітує про результати цієї діяльності перед Президентом та Верховною Радою. Кабінет Міністрів також безпосередньо керує підпорядкованими йому структурами виконавчої влади, що входять до системи захисту інформаційного простору, координуючи розробку та впровадження ними конкретних заходів безпеки. Спільна діяльність Верховної Ради та Уряду забезпечує найважливіші управлінські, регуляторні та контрольні функції, що дозволяє будувати адаптивну та ефективну політику в секторі інформаційної безпеки, що є критично важливим для національної стабільності. Завдяки комплексному правовому регулюванню та системному контролю за діяльністю відповідальних суб'єктів зміцнюється суспільна довіра та підвищується рівень безпеки національного інформаційного простору, що створює надійну основу для виживання держави в умовах сучасних геополітичних викликів [6, с. 280-281].

Серед спеціальних органів особливе значення та місце займають Служба безпеки України (СБУ), Державна служба спеціального зв’язку та захисту інформації (Держспецзв’язку) та РНБО як координаційний та дорадчий орган. СБУ функціонує як спеціалізований орган, на який покладено пріоритетне завдання із забезпечення державної безпеки, зокрема в контексті адміністративно-правового захисту інформаційного простору. У межах своєї компетенції СБУ здійснює державне управління у сфері безпеки, здійснюючи системний моніторинг вітчизняних та іноземних засобів масової інформації, а також мережі Інтернет. Використовуючи специфічні методи та інструменти, Служба виявляє актуальні загрози національним інтересам в інформаційній сфері та ефективно протидіє ворожим спецопераціям, спрямованим на підрив конституційного ладу, порушення територіальної цілісності держави або дестабілізацію соціально-політичної та економічної ситуації [7]. Служба безпеки України у своїй діяльності окремим напрямком виділяє захист інформаційного та кіберпростору. Так, СБУ здійснює комплексний контррозвідувальний захист кібер- та інформаційного простору держави. Діяльність спецслужби у цій сфері зосереджена на запобіганні, виявленні та нейтралізації злочинів проти миру та безпеки людства, скоєних у цифровому середовищі. Ключовими завданнями СБУ є проведення контррозвідувальних операцій з метою боротьби з кібершпигунством та кібертероризмом, а також протидія кіберзлочинності, яка може зашкодити стратегічним інтересам України. Фахівці служби розслідують атаки на об'єкти критичної інфраструктури та державні інформаційні ресурси, одночасно відбиваючи

спеціальні інформаційні операції противника, спрямовані на дестабілізацію соціально-політичної ситуації та підрив конституційного ладу.

В умовах повномасштабної російської агресії значення кібербезпеки критично зросло, оскільки військові дії рф супроводжуються постійним цифровим тиском. Статистика свідчить про стрімку ескалацію: якщо у 2020 році було зафіксовано близько 800 атак, то у 2022 році їх кількість досягла 4500. Основними цілями російських спецслужб залишаються енергетичний сектор, логістика, військові об'єкти, державні реєстри та ЗМІ. Особлива увага приділяється захисту сфери цифрової трансформації та ІТ-індустрії. Для ефективної відсічі СБУ поглиблює координацію з міжнародними партнерами з НАТО та ЄС, а також залучає світову ІТ-спільноту. Окремим фронтом роботи є боротьба з масованими інформаційно-психологічними операціями (ІІПСО), які спрямовані на розкол українського суспільства та дискредитацію держави на міжнародній арені. У рамках захисту інформаційного простору кіберпідрозділи СБУ успішно ліквідували десятки бот-ферм, заблокували численні антиукраїнські канали та притягнули до відповідальності сотні пропагандистів. Потужний ресурсний потенціал дозволяє Україні не лише підтримувати оборону, а й проводити наступальні операції в кіберсфері [8].

Згідно з ст. 2 ЗУ «Про Державну службу спеціального зв'язку та захисту інформації України» Державна служба спеціального зв’язку та захисту інформації України – це державний орган, основне призначення якого забезпечення функціонування і розвиток державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону. Також згідно з положенням цього ж Закону Державна служба спеціального зв’язку та захисту інформації України виконує комплекс стратегічних завдань, спрямованих на формування та реалізацію державної політики у сферах кіберзахисту, криптографічного й технічного захисту даних, а також забезпечення безпеки державних інформаційних ресурсів в інформаційно-комунікаційних системах. Служба відповідає за стабільне функціонування та розвиток державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, поштового зв’язку спеціального призначення та фельд’єгерської служби, одночасно здійснюючи активну протидію агресії в кіберпросторі. До компетенції відомства належить захист об’єктів критичної інформаційної інфраструктури та технологічної інформації, визначення вимог до їхньої безпеки, ведення відповідних реєстрів, а також впровадження заходів із протидії технічним розвідкам. Державна служба спеціального зв’язку та захисту інформації України бере безпосередню участь у регулюванні електронного документообігу, що містить державну таємницю або службову інформацію, здійснює нагляд за дотриманням законодавства у сфері електронних довірчих послуг та ідентифікації. Важливим аспектом діяльності Служби є створення та забезпечення роботи спеціалізованого Центру активної протидії агресії у кіберпросторі, здійснення галузевої стандартизації, підтримка суб’єктів боротьби з тероризмом та виконання інших функцій, визначених оновленим законодавством у сфері кібербезпеки [9].

Відповідно до положень Конституції, Рада національної безпеки і оборони України функціонує як координаційна структура з питань оборони та безпеки при главі держави. Відповідно до ст. 3 відповідного Закону України «Про Раду національної безпеки і оборони України» її ключові функції в контексті адміністративно-правового захисту інформаційного простору включають: розробку та подання Президенту пропозицій щодо реалізації внутрішньої та зовнішньої політики у сфері інформаційної

безпеки, а також координацію та контроль діяльності органів виконавчої влади у цій сфері як у мирний час, так і в умовах воєнного чи надзвичайного стану чи під час виникнення гострих кризових ситуацій, що загрожують державі [10]. Важливою складовою структури РНБО є Центр протидії дезінформації, створений Рішенням від 11 березня 2021 року № 106. Цей підрозділ спрямовує зусилля на нейтралізацію поточних та потенційних загроз національним інтересам, виявлення дезінформаційних кампаній, боротьбу з пропагандою та деструктивними впливами, запобігання маніпуляціям масовою свідомістю. У межах своєї компетенції Центр аналізує та висвітлює тенденції, пов’язані з оборонним сектором, оборонною промисловістю, правопорядком, боротьбою з корупцією, зовнішньою політикою, економікою, захистом критичної інфраструктури, медициною, екологією та соціальними процесами. Працюючи в рамках апарату РНБО, Центр ефективно протидіє інформаційному тероризму та поширенню фейків, тим самим підтримуючи стабільність країни. Пріоритетним напрямком є протидія іноземним інформаційним операціям, що особливо важливо в умовах збройного конфлікту, оскільки це дозволяє Україні захистити свій суверенітет та зберегти суспільну довіру [11]. Таким чином, РНБО забезпечує належні умови для виконання Президентом своїх конституційних обов'язків у сфері інформаційної безпеки, виявляє загрози та формує стратегічні програми контрзаходів.

Таким чином, на підставі вище зазначеного – Служба безпеки України є основним суб'єктом контррозвідувального захисту та боротьби з кібертероризмом. Її діяльність спрямована на нейтралізацію прямих загроз конституційному ладу, викриття ворожих ОСЗ та притягнення до відповідальності тих, хто здійснює деструктивний інформаційний вплив. Державна служба спеціального зв'язку виконує роль технологічного та регуляторного хабу, забезпечуючи стабільність критичної інформаційної інфраструктури, надійність урядового зв'язку та впровадження єдиних стандартів кіберзахисту. Велика увага приділяється активній протидії агресії в цифровій сфері та захисту державних інформаційних ресурсів. Рада національної безпеки і оборони України виконує стратегічну координаційну функцію, об'єднуючи зусилля всіх відомств для розробки єдиної державної політики. Діяльність Центру протидії дезінформації при РНБО дозволяє вести системну боротьбу з маніпуляціями суспільною свідомістю та інформаційним тероризмом.

Додатково вважаємо за потрібне звернути увагу на питання того, які методи органи публічного управління використовують у процесі здійснення повноважень у механізмі забезпечення інформаційної безпеки. З огляду на складність забезпечення інформаційної безпеки як напрямку державного управління, що вимагає не лише розгалуженої системи організаційно-правових заходів, а й постійної адаптації до стрімкого розвитку ІТ-індустрії, методи адміністративно-правового регулювання у цій сфері мають низку специфічних особливостей. По-перше, вони базуються на чіткій спеціалізації державних органів, кожен з яких наділений конкретними повноваженнями щодо захисту інформаційного простору. По-друге, ці методи синхронізовані з процесами глобальної соціально-технічної модернізації та активно інтегрують новітні досягнення науково-технічного прогресу в управлінську практику. Ефективне впровадження таких методів можливе лише за умови суворого дотримання посадовими особами законодавства та виконання розпоряджень вищих органів влади в порядку підпорядкування. Крім того, адміністративне регулювання у цій сфері характеризується яскраво вираженим організаційно-розпорядчим характером, що дозволяє структурувати державну інформаційну політику шляхом встановлення обов'язкових правил поведінки, визначення юридичних зобов'язань та здійснення системного контролю. Нарешті, застосування цих методів забезпечує практичну реалізацію норм

урядових та відомчих актів, а також реалізацію конкретних окремих нормативних вимог, спрямованих на гарантування кіберстійкості держави [12, с. 67-68].

Сама система забезпечення інформаційної безпеки має свої функції, що спрямовані на виконання своїх обов'язків. повинна виконувати. В. Котляров у своїй науковій статті наголошує на таких важливих функціях цієї системи:

1. Першочерговою функцією є формування основи для системи, що передбачає не лише створення відповідних державних органів, а й забезпечення їхньої життєдіяльності через розробку якісної законодавчої бази, чіткий розподіл повноважень та профільну підготовку спеціалістів;
2. Функція стратегічного управління та координації, що передбачає визначення довгострокових стратегій та алгоритмів, безпосереднє керівництво процесами та контроль за їх виконанням та кінцеву оцінку співвідношення витрачених ресурсів із отриманими результатами;
3. Функція оперативної діяльності та протидії загрозам означає проведення моніторингу та прогнозування можливих інформаційних загроз, нейтралізацію джерел небезпеки та локалізацію інформаційних конфліктів;
4. Функція глобальної інтеграції та міжнародної взаємодії передбачає участь у створенні міжнародних стандартів та угод у сфері інформаційної безпеки, участь у спільних навчаннях, тренінгах та симуляціях [13, с. 48].

На нашу думку, важливість виконання вище зазначених функції дає можливість оптимально використовувати методи публічного управління, застосування яких спрямовано на урегулювання інформаційно-правових відносин у системі забезпечення інформаційної безпеки органами публічного управління.

Так, П. О. Яковлєв наголошує на важливості та першочерговості застосування таких методів адміністративно-правового регулювання забезпечення інформаційної безпеки України: імперативного, диспозитивного, субординаційного, координаційного, стимулюючого та контролю.

Так, імперативний метод адміністративно-правового регулювання у сфері інформаційної безпеки базується на суворій централізації та системі обов'язкових до виконання владних приписів. Сутність цього методу полягає у встановленні та дотриманні чіткої вертикалі підпорядкування, де суб'єкт сектору безпеки, а також вищі органи державної влади діють виключно в межах жорстко визначених законом алгоритмів. Також характерною особливістю цього методу є відсутність дискреції, тобто можливості суб'єкта владних повноважень обирати серед варіантів поведінки на власний розсуд. Що ж стосується диспозитивного методу – він є практичною протилежністю імперативному через те, що передбачає юридичну рівність учасників правовідносин на противагу ієрархічному підпорядкуванню. Звичайно на відміну від безальтернативного державного регулювання, такий підхід надає суб'єктам певну свободу вибору та можливість діяти на власний розсуд у межах, встановлених законом. Яскравим проявом такої автономії є процедура акредитації представників медіа. Закон не зобов'язує державний орган застосовувати автоматичні санкції, а навпаки, надає йому право самостійно оцінювати дії журналіста. Таким чином, посадова особа уповноважена приймати рішення про припинення співпраці лише тоді, коли бачить порушення професійних обов'язків у діях медіаособи, що демонструє перехід від жорсткої вертикалі до регулювання, заснованого на ситуаційній оцінці та праві вибору.

Ефективність функціонування системи інформаційної безпеки України забезпечується поєднанням методів субординаційної координації, стимулювання та контролю, що є спеціальними методами. Субординаційна координація є ключовим інструментом для подолання міжвідомчих бар'єрів, де, наприклад, Рада національної безпеки і оборони України разом з Кабінетом Міністрів відіграють роль стратегічних

центрів, що спрямовують діяльність різних міністерств і служб в єдиний напрямок державної політики. Паралельно метод стимулювання створює необхідну мотиваційну базу для персоналу, використовуючи систему моральних та матеріальних стимулів для досягнення найвищих показників професійної діяльності. Важливим є також метод контролю, який у складних та мінливих умовах оперативної обстановки дозволяє оперативно виявляти відхилення від стратегічних цілей та коригувати управлінські рішення. Такий нагляд, що реалізується через відомчі, державні та громадські механізми, є гарантією дотримання законності та гнучкості державної системи захисту інформації в умовах надзвичайних викликів [12, с. 68-69].

Серед інших О. Є. Малашко виділяє так методи адміністративно-правового регулювання забезпечення інформаційної безпеки України: колегіального контролю за додержанням режиму секретності, сертифікації засобів захисту інформації, реєстраційний, адміністративного примусу. Окремо характеризуючи ці методи, слід вказати, що метод колегіального контролю за додержанням режиму секретності серед перелічених автор вважає найактуальнішим і ми з цим погоджуємся. Специфіка цього методу полягає у проведенні систематичних комісійних перевірок, що дозволяє забезпечити об'єктивність та всебічність оцінки стану захисту державної таємниці. Цей механізм реалізується на різних рівнях управлінської ієрархії: від місцевого внутрішнього аудиту безпосередньо в апаратах державних органів та на підприємствах до масштабних галузевих та відомчих перевірок. Водночас загальнонаціональний нагляд здійснюється спеціально уповноваженими установами у чітко визначені терміни, що гарантує безперервність моніторингу та своєчасне виявлення вразливостей у системі захисту інформації з обмеженим доступом [14, с. 147].

Наступним є метод сертифікації засобів захисту інформації, що також включає ліцензування діяльності у сфері захисту відомостей, що становлять державну таємницю, сертифікацію системи телекомунікаційного обладнання й програмного забезпечення автоматизованих систем обробки інформації [14, с. 147].З цього приводу слід зазначити, що цей метод спрямований на забезпечення верифікації засобів захисту, телекомунікаційного обладнання та програмного забезпечення та має на меті забезпечення інформаційної безпеки на стійкості до можливих загроз. Особливо в умовах гібридної війни та постійних кіберзагроз, такий суворий державний контроль у цих сферах виконує важливу стратегічну роль.

Ще одним є реєстраційний метод, який посідає вагоме місце в ієрархії адміністративно-правових інструментів, виступаючи однією з ключових контрольно-наглядових функцій органів виконавчої влади. У контексті медіапростору цей механізм перетворюється на обов'язкову правову передумову. Так, без офіційної реєстрації засобів медіа процес їх створення, відтворення та розповсюдження не вважається легітимним. Таким чином, реєстрація виступає не просто формальністю, а державним фільтром, що регулює діяльність суб'єктів інформаційного сектору та забезпечує прозорість функціонування медіаринку.

Заключним із перелічених метод виступає адміністративний примус. Як специфічний метод державного управління, він є формою правового впливу на фізичних та юридичних осіб, дії чи бездіяльність яких створюють реальні або потенційні загрози державним інтересам. Ключовим фактором, що визначає вибір конкретних примусових заходів, є безпосередня мета їх застосування – чи то запобігання правопорушенню, чи то припинення протиправних дій, чи то притягнення до відповідальності за порушення інформаційного законодавства [14, с. 147].

Для повного розкриття теми нашого дослідження доцільно також звернути увагу на зарубіжний досвід адміністративно-правового регулювання органів публічного

управління в механізмі забезпечення інформаційної безпеки. Основними напрямками європейської політики забезпечення інформаційної політики є:

1. Розробка європейської системи попередження та інформування про нові загрози;
2. Надання технологічної підтримки. Пріоритет надається розвитку досліджень у сфері мережевої та інформаційної безпеки;
3. Підтримка ринково-орієнтованої стандартизації та сертифікації;
4. Правове забезпечення;
5. Посилення безпеки на державному рівні;
6. Розвиток міжнародного співробітництва з питань інформаційної безпеки [15, с. 138].

Головним завданням ЄС є посилення діалогу Європейської Комісії з міжнародними організаціями та партнерами з питань мережевої безпеки та, зокрема, щодо зростаючої залежності від електронних мереж.

Сьогодні в більшості країн, включаючи країни Європейського Союзу, законодавство у сфері кібербезпеки (інформаційної безпеки) перебуває на стадії активного розвитку. Формування правового забезпечення кіберзахисту базується, з одного боку, на національних принципах, а з іншого – на основі єдиної міжнародної платформи.

Як приклад наведемо Німеччину. Німецька правова база, що застосовується до кібербезпеки, включає закони про моніторинг, виявлення, запобігання, пом'якшення наслідків та управління інцидентами. Вона включає, наприклад, закони про захист даних та електронну конфіденційність, закони про інтелектуальну власність, закони про конфіденційність, закони про інформаційну безпеку, контроль імпорту/експорту тощо. Основним актом є Закон Німеччини про безпеку (IT-Sicherheitsgesetz) від 25 липня 2015 року, який вніс зміни до низки законів, зокрема: Закону про телемедіа (Telemediengesetz), Закону про телекомунікації (Telekommunikationsgesetz), Загального регламенту ЄС про захист даних (GDPR), Федерального закону про захист даних (Bundesdatenschutzgesetz) та Закону про Федеральне відомство з безпеки інформаційних технологій. Окрім офіційного законодавства, у Німеччині існують важливі неофіційні положення щодо безпеки IT: Базовий стандарт BSI, Загальні критерії оцінки безпеки інформаційних технологій (ISO/IEC 15408) та методологія COBIT. Дотримання законних вимог забезпечується Федеральним відомством з безпеки інформації (BSI), компетентними органами захисту даних та Федеральним мережевим агентством. BSI є головним органом з кібербезпеки в Німеччині, відповідальним за превентивні заходи та отримання повідомлень про порушення безпеки критичної інфраструктури [15, с. 139]. При цьому у багатьох федеральних землях, окрім захисту даних, існують юридично обов'язкові правила щодо інформаційної безпеки. Аспекти кібербезпеки ще не були належним чином враховані, як і муніципальні аспекти. У всіх федеральних землях існує потреба усунути розрив – від критичної інфраструктури громад (держави та економіки) до муніципальних постачальників та самих муніципалітетів. У федеральних землях існує мало правових підстав для втручання в конфіденційність телекомунікацій, яка необхідна для стійкості до кібератак, зокрема для розкриття зашифрованих з'єднань. На жаль, немає правової основи для використання хмарних сервісів; натомість федеральні землі покладаються на традиційні механізми аудиту відповідно до рамкових норм або федеральних рекомендацій, таких як каталог вимог BSI [16, с. 12].

У Франції також сформувалася досить оптимальна правова база для забезпечення інформаційної безпеки. Найважливіші закони у сфері кібербезпеки у Франції, які сформували її регуляторну платформу: Закон Годфрі № 88-19 від 15 січня 1988 року; Закон про захист даних № 78-17 від 6 січня 1978 року (Loi Informatique et Libertés); Закон

про цифрову республіку № 2016-1321 від 7 жовтня 2016 року. У 2018 році до нього було внесено змін Законом № 2018-493 від 20 червня 2018 року для узгодження його з GDPR; Закон про безпеку мереж та інформаційних систем (the «NIS Law»); Указ від 14 вересня 2018 року, що визначає правила безпеки (the «NIS Rules»). CNIL (Національна комісія з інформаційних технологій та свобод) контролює належне застосування законодавства про захист даних. Комісія має значні повноваження щодо моніторингу, розслідування інцидентів та накладення адміністративних та фінансових санкцій, включаючи призупинення обробки даних. Щодо застосування Регламенту NIS, ANSSI (Національне агентство з безпеки інформаційних систем) є національним органом, відповідальним за реагування на інциденти кібербезпеки, спрямовані проти стратегічно важливих установ. Міністерство оборони та Міністерство внутрішніх справ також відіграють певну роль у запобіганні всім формам кіберзлочинності [15, с. 141].

Ще проаналізуємо практики, що використовують у США. Можемо відмітити, що у США Міністерство внутрішньої безпеки США (DHS) створило Раду з розгляду кібербезпеки (CSRB) відповідно до Указу президента Байдена № 14028. CSRB розслідує інциденти, що стосуються найнебезпечніших суб'єктів загроз, які вплинули на критично важливі об'єкти інфраструктури. CSRB є незалежним органом, що складається з висококваліфікованих представників федерального та приватного секторів. Вивчаючи минулі інциденти, CSRB надає рекомендації щодо запобігання майбутнім інцидентам з метою підвищення кіберстійкості. Також в рамках підтримки інформаційної безпеки у США передбачається розробка та використання планів реагування на кіберінциденти та вразливості – так звані Playbooks, що слугують вичерпним посібником, який дозволяє організаціям ефективно керувати кіберінцидентами та реагувати на них. У випадку федерального уряду США ролі та обов'язки визначаються на національному рівні з посиланням на низку урядових документів високого рівня, таких як виконавчі укази, закони та інші обов'язкові вимоги. Однією з найбільших переваг такого плану є стандартизований підхід, який він забезпечує для виявлення, розслідування та пом'якшення наслідків кіберінцидентів покроково. Він скеровує організацію через «дорожню карту» дій, які необхідно вжити під час кризи. Структура плану охоплює найкращі практики, рекомендації та процедури, яких організація повинна дотримуватися в чіткій послідовності. Акцент на ранньому виявленні кіберінцидентів є однією з ключових переваг [17, с. 112-113].

Таким чином, аналіз зарубіжного досвіду адміністративно-правового регулювання у сфері інформаційної безпеки свідчить про формування багаторівневих та високотехнологічних систем управління, що поєднують жорстку законодавчу базу з гнучкими інструментами реагування. Європейська модель, яскраво представлена досвідом Німеччини та Франції, базується на принципах запобігання та суворого державного нагляду за об'єктами критичної інфраструктури. Німецький підхід характеризується централізацією функцій у Федеральному відомстві з інформаційної безпеки (BSI) та інтеграцією стандартів безпеки в усі сфери державного управління, хоча й стикається з труднощами у залученні муніципального рівня та регулюванні хмарних сервісів. Французька система демонструє ефективний розподіл ролей між спеціалізованими агентствами, такими як ANSSI та CNIL, що дозволяє гармонійно поєднувати захист національних інформаційних систем із забезпеченням прав громадян на конфіденційність у рамках регламентів GDPR та NIS. Водночас досвід США пропонує унікальні механізми стратегічного рівня, включаючи незалежну Раду з огляду кібербезпеки (CSRB) та впровадження стандартизованих планів реагування (Playbooks).

**Висновок**

Підсумовуючи дослідження, варто зазначити, що сучасне адміністративно-правове регулювання інформаційної безпеки в Україні – це не просто набір норм, а

живий механізм, який пройшов довгий шлях еволюції. Ми бачили, як суто філософське розуміння свободи думки та перші спроби маніпуляцій часів епохи Відродження трансформувалися у складну цифрову архітектуру, яка сьогодні є основою нашого суверенітету. Наразі основою цієї системи в Україні є Стратегія інформаційної безпеки 2021 року, яка нарешті змістила акцент на реальний захист інтересів людини та держави в цифровому просторі. Практична стабільність цього механізму спирається на скоординовану роботу ключових суб'єктів: Служби безпеки України, яка зосереджена на контррозвідці, Державної служби спеціального зв'язку як технологічного ядра та Ради національної безпеки і оборони, яка координує стратегічні рішення. Аналіз показав, що змінюються і методи управління: держава переходить від жорстких наказів до більш гнучких інструментів, таких як сертифікація та постійний моніторинг, що надзвичайно важливо в умовах гібридної війни.

Погляд на досвід Німеччини, Франції та США підтверджує, що світовим трендом сьогодні є чіткі алгоритми дій (на кшталт американських «Playbooks») та суворий нагляд за критичною інфраструктурою. Для України головним викликом залишається не лише гармонізація нашого законодавства з європейськими стандартами GDPR та NIS, а й побудова такої взаємодії між державними органами, яка б дозволила нам миттєво реагувати на загрози. Тільки завдяки поєднанню технологічної експертизи та гнучкого правового регулювання ми зможемо побудувати надійний щит для національного інформаційного простору в ці непрості часи.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шевчук М.О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія Право.* 2023. Вип. 73 ч. 2. С. 134-139. URL: https://doi.org/10.24144/2307-3322.2023.78.2.21

2. Новицький В.А. Генеза поняття «інформаційна безпека»: походження та становлення. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування.* 2024. №4. С. 38-44. URL: https://doi.org/10.32782/TNU-2663-6468/2024.4/06

3. Казмірук Д.М. Інформаційна безпека як складова національної безпеки в умовах повномасштабної війни. *Науковий журнал «Політикус».* 2025. №1. С. 21-26. URL: https://doi.org/10.24195/2414-9616.2025-1.3

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

5. Суслін С.В. Система суб'єктів забезпечення інформаційної безпеки: адміністративно-правовий статус та повноваження. *Успіхи і досягнення у науці*. 2025. №11(21). 315-325. URL: https://doi.org/10.52058/3041-1254-2025-11(21)

6. Крупнова А. О. Система суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні. *Науковий вісник Ужгородського Національного Університету. Серія Право.* 2024. №83 (2). С. 277-287. URL: https://doi.org/10.24144/2307-3322.2024.83.2.40

7. Про службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#n145

8. Захист інформаційного та кіберпростору: офіційний веб-сайт СБУ. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky

9. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

10. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. №183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

11. Положення про Центр протидії дезінформації: Указ Президента України від 07.05.2021 р. №187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text

12. Яковлєв П.О. Методи адміністративно-правового регулювання забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського національного університету. Серія Право.* 2020. №61. С. 66-69. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/02/17-1.pdf

13. Котляров В. Система забезпечення інформаційної безпеки України. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління.* 2024. №2(74). С. 45-49. URL: https://doi.org/10.32689/2523-4625-2024-2(74)-6

14. Малашко О.Є. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні. *Scientific Notes of Lviv University of Business and Law.* 2020. №24. С. 145-149. URL: https://nzlubp.org.ua/index.php/journal/article/view/251

15. Kavyn S., Bratsuk I., Lytvynenko A. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. *Teisė.* 2021. №121. P. 135-147. URL: https://www.zurnalai.vu.lt/teise/en/article/view/25171/24464

16. Rehbohm T., Sandkuhl K., Kemmerich T. On Challenges of Cyber and Information Security Management in Federal Structures – The Example of German Public Administration. *BIR Workshops.* 2019. P. 1-13. URL: https://ceur-ws.org/Vol-2443/paper01.pdf

17. Carroll J. M. The U.S. National Cybersecurity Strategy: A Vehicle with an International Journey: *Proceedings of the 23rd European Conference on Cyber Warfare and Security*. 2024. P. 107-115. URL: https://www.researchgate.net/publication/381651738_The_US_National_Cybersecurity_Strategy_A_Vehicle_with_an_International_Journey.

**REFERENCES**

1. Shevchuk M.O. Do pytannya henezy ponyattya informatsiynoyi bezpeky yak skladovoyi natsional'noyi bezpeky. Naukovyy visnyk Uzhhorods'koho Natsional'noho Universytetu. Seriya Pravo. 2023. Vyp. 73 ch. 2. S. 134-139. URL: https://doi.org/10.24144/2307-3322.2023.78.2.21

2. Novyts'kyy V.A. Heneza ponyattya «informatsiyna bezpeka»: pokhodzhennya ta stanovlennya. Vcheni zapysky TNU imeni V.I. Vernads'koho. Seriya: Publichne upravlinnya ta administruvannya. 2024. №4. S. 38-44. URL: https://doi.org/10.32782/TNU-2663-6468/2024.4/06

3. Kazmiruk D.M. Informatsiyna bezpeka yak skladova natsional'noyi bezpeky v umovakh povnomasshtabnoyi viyny. Naukovyy zhurnal «Politykus». 2025. №1. S. 21-26. URL: https://doi.org/10.24195/2414-9616.2025-1.3

4. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 15 zhovtnya 2021 roku "Pro Stratehiyu informatsiynoyi bezpeky": Ukaz Prezydenta Ukrayiny vid 28.12.2021 r. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

5. Suslin S.V. Systema sub"yektiv zabezpechennya informatsiynoyi bezpeky: administratyvno-pravovyy status ta povnovazhennya. Uspikhy i dosyahnennya u nautsi. 2025. №11(21). 315-325. URL: https://doi.org/10.52058/3041-1254-2025-11(21)

6. Krupnova A. O. Systema sub"yektiv administratyvno-pravovoho zabezpechennya informatsiynoyi bezpeky v Ukrayini. Naukovyy visnyk Uzhhorods'koho Natsional'noho Universytetu. Seriya Pravo. 2024. №83 (2). S. 277-287. URL: https://doi.org/10.24144/2307-3322.2024.83.2.4.

7. Pro sluzhbu bezpeky Ukrayiny: Zakon Ukrayiny vid 25.03.1992 r. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#n145

8. Zakhyst informatsiynoho ta kiberprostoru: ofitsiynyy veb-sayt SBU. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky

9. Pro Derzhavnu sluzhbu spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrayiny: Zakon Ukrayiny vid 23.02.2006 r. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

10. Pro Radu natsional'noyi bezpeky i oborony Ukrayiny: Zakon Ukrayiny vid 05.03.1998 r. №183/98-VR. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

11. Polozhennya pro Tsentr protydiyi dezinformatsiyi: Ukaz Prezydenta Ukrayiny vid 07.05.2021 r. №187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text

12. Yakovlyev P.O. Metody administratyvno-pravovoho rehulyuvannya zabezpechennya informatsiynoyi bezpeky Ukrayiny. Naukovyy visnyk Uzhhorods'koho natsional'noho universytetu. Seriya Pravo. 2020. №61. S. 66-69. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/02/17-1.pdf

13. Kotlyarov V. Systema zabezpechennya informatsiynoyi bezpeky Ukrayiny. Naukovi pratsi Mizhrehional'noyi akademiyi upravlinnya personalom. Politychni nauky ta publichne upravlinnya. 2024. №2(74). S. 45-49. URL: https://doi.org/10.32689/2523-4625-2024-2(74)-6

14. Malashko O.YE. Administratyvno-pravovi zasoby zabezpechennya informatsiynoyi bezpeky v Ukrayini. Scientific Notes of Lviv University of Business and Law. 2020. №24. S. 145-149. URL: https://nzlubp.org.ua/index.php/journal/article/view/251.

15. Kavyn S., Bratsuk I., Lytvynenko A. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. Teisė. 2021. №121. R. 135-147. URL: https://www.zurnalai.vu.lt/teise/en/article/view/25171/24464

16. Rehbohm T., Sandkuhl K., Kemmerich T. On Challenges of Cyber and Information Security Management in Federal Structures – The Example of German Public Administration. BIR Workshops. 2019. P. 1-13. URL: https://ceur-ws.org/Vol-2443/paper01.pd

17. Carroll J. M. The U.S. National Cybersecurity Strategy: A Vehicle with an International Journey: *Proceedings of the 23rd European Conference on Cyber Warfare and Security*. 2024. P. 107-115. URL: https://www.researchgate.net/publication/381651738_The_US_National_Cybersecurity _Strategy_A_Vehicle_with_an_International_Journey