УДК 342.9
DOI https://doi.org/10.32844/2618-1258.2025.6.83

ДРОЗД О.Ю., КАПЕЛЮХА А.В.

ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В США

FEATURES OF THE ADMINISTRATIVE-LEGAL REGULATION OF CYBERSECURITY IN THE USA

Здійснено комплексний адміністративно-правовий аналіз особливостей регулювання кібербезпеки в Сполучених Штатах Америки. Актуальність обраної проблематики обумовлена тим, що за умов стрімкого розвитку цифрових технологій, ускладнення характеру кіберзагроз і зростання залежності держави, суспільства та приватного сектору від належного функціонування інформаційних систем забезпечення кібербезпеки набуває значення одного з пріоритетних напрямів сучасного публічного адміністрування. Обґрунтовано, що адміністративно-правове регулювання кібербезпеки в США доцільно розглядати як комплексну систему правових, організаційних, координаційних, контрольних, стандартизаційних, інформаційно-аналітичних, закупівельних і стимулюючих засобів публічного адміністрування, застосування яких спрямоване на управління кіберризиками, захист федеральних інформаційних систем, забезпечення стійкості критичної інфраструктури, своєчасне реагування на кіберінциденти й узгодження діяльності державних і недержавних суб'єктів.

Розкрито багаторівневу побудову адміністративно-правового регулювання кібербезпеки в США. Проаналізовано значення федеральних законів, якими визначаються компетенція органів публічної адміністрації, обов'язки федеральних агентств, правові засади діяльності Агентства з кібербезпеки та безпеки інфраструктури США (CISA), механізми інформаційного обміну, засоби захисту ланцюгів постачання, правила використання хмарних сервісів і процедури повідомлення про кіберінциденти. Схарактеризовано роль підзаконних нормативних актів органів виконавчої влади та секторальних регуляторів, зокрема правил, що застосовуються у фінансовій сфері, системі охорони здоров'я, діяльності публічних компаній, енергетиці, телекомунікаціях, транспорті та інших галузях. Окрему увагу приділено значенню президентських виконавчих наказів та управлінських документів федеральної адміністрації, які конкретизують завдання органів виконавчої влади, сприяють модернізації федеральних інформаційних систем, посиленню захищеності програмного забезпечення, вдосконаленню процедур реагування на кіберінциденти та впровадженню перспективних технологічних рішень.

Систематизовано основні особливості адміністративно-правового регулювання кібербезпеки в США та почергово схарактеризовано сутність кожної з них. Доведено, що адміністративно-правове регулювання кібербезпеки в США спрямоване на забезпечення балансу між правовою визначеністю, інституційною координацією, федеративним розподілом повноважень, технологічною адаптивністю, секторальною спеціалізацією, захистом прав людини та необхідністю гарантування стійкості державних і суспільно значущих цифрових систем.

Ключові слова: *кібербезпека, адміністративно-правове регулювання, публічне адміністрування, кіберризики, кіберінциденти, CISA, NIST, державно-приватна взаємодія, федеральні інформаційні системи, адміністративне законодавство, інформаційна безпека, досвід США.*

© ДРОЗД О.Ю. – доктор юридичних наук, професор, професор кафедри поліцейської діяльності (Національна академія внутрішніх справ) https://orcid.org/0000-0002-4514-6594

© КАПЕЛЮХА А.В. – доктор філософії в галузі права, https://orcid.org/0009-0007-9867-5311
Стаття поширюється на умовах ліцензії CC BY 4.0

In the article comprehensive administrative and legal analysis of the features of cybersecurity regulation in the United States of America is provided. The relevance of the selected issues is due to the fact that in the conditions of the rapid development of digital technologies, the complexity of the nature of cyber threats and the growing dependence of the state, society and the private sector on the proper functioning of information systems, cybersecurity is becoming one of the priority areas of modern public administration.

It is substantiated that the administrative and legal regulation of cybersecurity in the United States should be considered as a comprehensive system of legal, organizational, coordination, control, standardization, information and analytical, procurement and incentive tools of public administration, the application of which is aimed at managing cyber risks, protecting federal information systems, ensuring the stability of critical infrastructure, timely response to cyber incidents and coordinating the activities of state and non-state actors.

The multi-level structure of administrative and legal regulation of cybersecurity in the United States is revealed. The significance of federal laws that determine the competence of public administration bodies, the responsibilities of federal agencies, the legal framework for the activities of the US Cybersecurity and Infrastructure Security Agency (CISA), information exchange mechanisms, means of protecting supply chains, rules for using cloud services, and procedures for reporting cyber incidents is analyzed. The role of subordinate regulatory acts of executive authorities and sectoral regulators is characterized, in particular, rules applied in the financial sector, the healthcare system, the activities of public companies, energy, telecommunications, transport, and other industries.

Special attention is paid to the importance of presidential executive orders and administrative documents of the federal administration, which specify the tasks of executive bodies, contribute to the modernization of federal information systems, strengthen software security, improve cyber incident response procedures, and implement promising technological solutions.

The article systematizes the main features of the administrative and legal regulation of cybersecurity in the United States and characterizes the essence of each of them in turn. It is concluded that the administrative and legal regulation of cybersecurity in the United States is aimed at ensuring a balance between legal certainty, institutional coordination, federal division of powers, technological adaptability, sectoral specialization, protection of human rights, and the need to guarantee the stability of state and socially significant digital systems.

Key words: *cybersecurity, administrative and legal regulation, public administration, cyber risks, cyber incidents, CISA, NIST, public-private interaction, federal information systems, administrative legislation, information security, US experience.*

Вступ. Дослідження особливостей адміністративно-правового регулювання кібербезпеки в Сполучених Штатах Америки має важливе значення, оскільки американська модель не зводиться до дії одного кодифікованого нормативно-правового акта або функціонування єдиного органу публічної адміністрації, наділеного виключною компетенцією у відповідній сфері. Її зміст формується внаслідок взаємодії федерального законодавства, президентських актів, управлінських документів органів виконавчої влади, стандартів технічного характеру, механізмів федеральних закупівель, процедур обміну інформацією, програм фінансової підтримки штатів і територіальних громад, а також інструментів державно-приватної співпраці. У межах адміністративно-правового аналізу предметом дослідження має бути також організаційна побудова публічного адміністрування, розподіл компетенції між федеральними органами, правові засоби координації, стандартизації та контролю, особливості взаємодії держави з приватними власниками критичної інфраструктури, порядок повідомлення про кіберінциденти, засоби стимулювання належного рівня кіберстійкості, а також механізми забезпечення відповідності регуляторних вимог реальним ризикам.

У науковій літературі слушно зауважено, що адміністративно-правове регулювання кібербезпеки в США тривалий час розвивалося фрагментарно [1, с. 985–1002], що дозволяє відмежувати адміністративно-правове регулювання кібербезпеки від суто кримінально-правової протидії несанкціонованому втручанню в комп'ютерні системи. Криміналізація окремих діянь

є необхідною складовою правового реагування, однак не замінює системи превентивного управління ризиками, державного контролю, інституційної координації та забезпечення стійкості інформаційної інфраструктури.

Федеральне законодавство США формує розгалужену систему адміністративних обов'язків, процедур звітування, контрольних повноважень, координаційних механізмів і стандартів. В окремих секторах діють спеціальні вимоги щодо програм інформаційної безпеки, технічних та організаційних заходів, управлінської відповідальності, документування, розкриття інформації та повідомлення про інциденти. У сфері федерального управління додатково застосовуються засоби бюджетного, закупівельного та організаційного впливу.

Постановка завдання. Метою статті є аналіз особливостей адміністративно-правового регулювання кібербезпеки в США. Реалізація окресленої мети передбачає врахування наявних напрацювань у цій сфері. Так, певною мірою проблематика особливостей адміністративно-правового регулювання кібербезпеки в зарубіжних країнах, зокрема в США, слугувала предметом дослідження низки вчених, серед яких: С. П. Арпентій, Ю. В. Геращенко, О. Ю. Дрозд, І. М. Коропатнік, К. П. Кочман, Н. П. Литвиненко, Н. О. Погоріла, М. М. Сливка, Г. В. Форос, Д. О. Хом'яков, В. В. Шемчук та інші. Водночас належним чином комплексного дослідження особливостей адміністративно-правового регулювання кібербезпеки в США, а також аналізу їх сутності донині не було представлено в доктрині адміністративного права, що й обумовлює актуальність тематики.

Результати дослідження. У науковій літературі США традиційно розглядають як одну з провідних держав світу за рівнем розвитку механізмів забезпечення інформаційної безпеки та формування державної політики в інформаційній сфері. Показово, що навіть Японія, яка посідає вагоме місце у виробництві цифрового обладнання та впровадженні новітніх інформаційних технологій, за окремими показниками інформаційного розвитку поступалася США більш ніж на п'ять років. Ідеться, зокрема, про масштаби поширення персональних комп'ютерів, кабельного телебачення, цифрового телефонного зв'язку, а також про інші напрями реалізації інформаційної політики держави [2, с. 34]. Напрацьовані в США підходи до стратегічного планування у сфері кібербезпеки становлять значний практичний інтерес для України, зокрема в частині вдосконалення адміністративно-правових засад формування та реалізації державної політики у відповідній сфері. Американський досвід засвідчує, що за сучасних умов кіберпростір перетворився на самостійне середовище виникнення загроз і здійснення як захисних, так і наступальних заходів. Це обумовлює необхідність узгодженої взаємодії органів публічної влади, військових формувань, спеціально уповноважених суб'єктів сектору безпеки і оборони, а також представників цивільного сектору. Важливого значення набувають належна ідентифікація джерел кіберзагроз, визначення кола стратегічних партнерів держави та чіткий розподіл компетенції між суб'єктами, залученими до забезпечення кібербезпеки [3, с. 144]. У США одним з ключових напрямів державної політики у сфері кібербезпеки є забезпечення системної протидії кіберзлочинності на загальнонаціональному рівні, а також створення належних організаційно-правових механізмів для залучення представників приватного сектору до реалізації заходів із захисту кіберпростору [4, с. 120]. З огляду на зазначене, варто зауважити, що адміністративно-правове регулювання кібербезпеки в США є комплексною системою правових, організаційних, координаційних, контрольних, стандартизаційних, інформаційно-аналітичних, закупівельних і стимулюючих засобів публічного адміністрування, спрямованих на управління кіберризиками, захист федеральних інформаційних систем, забезпечення стійкості критичної інфраструктури, своєчасне реагування на кіберінциденти та узгодження діяльності державних і недержавних суб'єктів.

Система адміністративно-правового регулювання кібербезпеки в США має багаторівневу структуру. На першому рівні знаходяться федеральні закони, які встановлюють компетенцію органів публічної адміністрації, визначають обов'язки федеральних агентств, закріплюють правові засади функціонування Агентства з кібербезпеки та безпеки інфраструктури США (CISA), регламентують обмін інформацією, захист мережі постачання, використання хмарних сервісів і майбутню систему обов'язкового звітування про визначені кіберінциденти.

Другий рівень утворюють нормативні акти органів виконавчої влади та регуляторів. До них належать, зокрема, правила Федеральної торгової комісії США (FTC), вимоги щодо захисту електронної медичної інформації, затверджені в межах законодавства HIPAA, правила Комісії з цінних паперів і бірж США (SEC), а також секторальні акти, які застосовуються до окремих видів критичної інфраструктури. Їхня особливість полягає в тому, що адміністративні вимоги адаптуються до специфіки відповідного сектору, характеру оброблюваних даних, рівня суспільного ризику та компетенції конкретного регулятора.

Третій рівень становлять президентські виконавчі накази й управлінські документи федеральної адміністрації. Вони відіграють значну роль у визначенні завдань органів виконавчої влади, координації їхньої діяльності та конкретизації напрямів модернізації федеральних інформаційних систем. Суттєвий вплив на розвиток відповідної системи справило розпорядження від

12 травня 2021 року № 14028 «Підвищення кібербезпеки нації», яким було визначено напрями посилення безпеки федеральних мереж, розвитку архітектури нульової довіри, вдосконалення реагування на інциденти та підвищення безпеки програмного забезпечення [5]. Подальший розвиток окремих положень відбувся з урахуванням розпорядження від 6 червня 2025 року № 14306, яким були переглянуті та збережені окремі пріоритетні заходи, зокрема щодо безпечного розроблення програмного забезпечення, постквантової криптографії та використання сучасних технологій у федеральному управлінні [6].

Четвертий рівень формують стандарти, рекомендації та рамкові документи Національного інституту стандартів і технологій США (NIST). У приватному секторі вони переважно не мають універсально обов'язкового характеру. Водночас їхнє значення не можна зводити до факультативних технічних рекомендацій. Вони здатні набувати юридично значущого характеру через пряме включення до нормативних актів, федеральних контрактів, закупівельних процедур, умов авторизації, відомчих політик або критеріїв оцінювання належної поведінки суб'єктів.

П'ятий рівень представлений стратегічними документами. Наприклад, Стратегії мають політико-управлінський характер і не створюють самостійно нових адміністративних обов'язків для приватних осіб. Проте їх положення є важливими для прогнозування подальшої нормотворчості та визначення змісту регуляторної політики.

Шостий рівень охоплює регулювання штатів. У межах цього дослідження основна увага приділяється федеральному рівню, однак ігнорування законодавства штатів призвело б до неповної характеристики системи. Штати ухвалюють власні акти щодо повідомлення про витоки даних, захисту персональної інформації, організації діяльності органів влади та встановлення додаткових вимог до окремих суб'єктів. Унаслідок цього американська модель поєднує федеральне регулювання з елементами правового плюралізму.

На підставі аналізу законодавства, підзаконних актів, стратегічних документів і наукових джерел вважаємо за доцільне виокремити такі основні особливості адміністративно-правового регулювання кібербезпеки в США:

1) поліцентричність, багаторівневість і відсутність єдиного кодифікованого режиму [7] – адміністративно-правове регулювання кібербезпеки в США формується сукупністю взаємопов'язаних федеральних законів, підзаконних актів, секторальних правил, президентських документів, технічних стандартів і нормативних актів штатів, а не одним комплексним кодифікованим актом універсальної дії;

2) функціональна централізація координації за збереження розподіленої компетенції [8] – CISA виконує роль основного координаційного центру у сфері цивільної кібербезпеки, однак нормотворчі, контрольні, організаційні та правозастосовні повноваження залишаються розподіленими між численними федеральними органами й секторальними регуляторами відповідно до предмета їх відання;

3) ризик-орієнтований, результативно спрямований і технологічно нейтральний характер регулювання [9] – полягає у встановленні обов'язку суб'єктів обирати пропорційні засоби кіберзахисту з урахуванням ідентифікованих загроз, уразливостей, потенційних наслідків і специфіки відповідних інформаційних систем;

4) диференціація правових режимів захисту федеральних систем, критичної інфраструктури та інших приватних інформаційних систем – застосування відмінних за змістом адміністративно-правових інструментів залежно від форми власності, функціонального призначення цифрових активів, рівня суспільної значущості відповідних систем і масштабу потенційної шкоди в разі кіберінциденту;

5) секторальна спеціалізація адміністративних вимог – установлення окремих правових режимів для фінансової сфери, охорони здоров'я, діяльності публічних компаній, енергетики, телекомунікацій, транспорту та інших галузей, у межах яких зміст обов'язків суб'єктів конкретизується відповідно до характеру оброблюваної інформації та притаманних відповідному сектору кіберризиків;

6) пріоритет захисту критичної інфраструктури на основі державно-приватної взаємодії – поєднання владно-регуляторних засобів із партнерськими механізмами координації, інформаційного обміну, технічної підтримки та спільного управління ризиками, що зумовлено переважно недержавним характером власності на значну частину суспільно важливих об'єктів;

7) поєднання добровільного обміну інформацією з поступовим розширенням обов'язкового звітування про кіберінциденти – перехід від переважно партнерської моделі передання індикаторів кіберзагроз до формування юридично визначених процедур обов'язкового повідомлення компетентних органів про найбільш значущі інциденти та пов'язані з ними платежі у зв'язку з вимогами викупу;

8) використання федеральних закупівель, системи контролю постачання та авторизації хмарних сервісів як інструментів непрямого адміністративного впливу [10] – поширення вимог кібербезпеки на приватних постачальників через умови участі у федеральних контрактах, оцінювання ризиків цифрових продуктів, контроль походження програмного забезпечення

й обладнання та стандартизовані процедури допуску хмарних сервісів до використання органами влади;

9) особлива роль NIST і технічної стандартизації в системі публічного адміністрування – розроблені NIST стандарти, рамкові документи та рекомендації забезпечують науково-технічну конкретизацію правових вимог і можуть набувати юридично значущого характеру внаслідок їх включення до нормативних актів, адміністративних процедур, контрактів і відомчих політик;

10) федералізм, програмно-цільове фінансування та стимулювання кіберстійкості штатів і територіальних громад – федеральний уряд не підміняє компетенцію органів штатів і місцевого рівня, а сприяє розвитку їхньої спроможності шляхом надання грантів, координаційної підтримки, технічної допомоги та встановлення організаційних умов для належного планування заходів кібербезпеки.

Висновки. Отже, проведений аналіз дозволяє резюмувати, що адміністративно-правове регулювання кібербезпеки в США розкривається через поєднання кількох взаємопов'язаних компонентів. У сфері федеральних інформаційних систем діє структурований режим управлінської відповідальності, програмування, оцінювання ризиків, контролю й аудиту. У сфері критичної інфраструктури застосовується партнерська модель, що поєднує координацію, технічну допомогу, секторальне регулювання, інформаційний обмін та поступове розширення обов'язкового звітування. NIST забезпечує експертно-стандартизаційну основу, яка дозволяє інтегрувати технічні знання в систему правового регулювання без надмірної технологічної деталізації законів. Федеральні закупівлі, авторизація хмарних сервісів і система контролю постачання перетворюються на дієві засоби непрямого адміністративного впливу. Грантові програми та діяльність координаторів CISA у штатах забезпечують вертикальну взаємодію без скасування федеративного розподілу повноважень. Особливості адміністративно-правового регулювання кібербезпеки у США виявляються в тому, що є прагнення досягти балансу між правовою визначеністю, інституційною координацією, технологічною адаптивністю, секторальною спеціалізацією, захистом прав людини та необхідністю забезпечення стійкості державних і суспільно значущих цифрових систем.

Список використаних джерел:

1. Kosseff J. Defining Cybersecurity Law. Iowa Law Review. 2018. Vol. 103. Issue 3. P. 985–1031. URL: https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law

2. Брижко В. До питання сучасної інформаційної політики. *Вісник Академії управління Міністерства внутрішніх справ.* 2009. № 2. С. 32–36.

3. The White House, The National Strategy to Secure Cyberspace, February 2003. Unclassified. URL: https://nsarchive.gwu.edu/document/21412-document-16.

4. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник Національної академії внутрішніх справ.* 2020. № 4. С. 119–124.

5. Executive Order No. 14028. Improving the Nation's Cybersecurity. 86 Fed. Reg. 26633 (May, 2021). URL: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

6. Executive Order No. 14306. Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144. 90 Fed. Reg. 24723 (June, 2025). URL: https://www.federalregister.gov/documents/2025/06/11/2025-10859/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694

7. Federal Information Security Modernization Act of 2014. Pub. L. No. 113–283, 128 Stat. 3073 (Dec. 18, 2014); codified at 44 U.S.C. §§ 3551–3559. URL: https://www.congress.gov/bill/113th-congress/senate-bill/2521

8. Cyber Incident Reporting for Critical Infrastructure Act of 2021. URL: https://www.congress.gov/bill/117th-congress/house-bill/5440

9. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: NIST, Feb. 26, 2024. DOI: 10.6028/NIST.CSWP.29. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

10. Federal Acquisition Supply Chain Security Act of 2018, title II of the SECURE Technology Act: Pub. L. No. 115–390, 132 Stat. 5173 (Dec. 21, 2018); codified at 41 U.S.C. §§ 1321–1328. URL: https://www.govinfo.gov/content/pkg/PLAW-115publ390/html/PLAW-115publ390.htm

Дата першого надходження статті до видання: 09.10.2025
Дата прийняття статті до друку після рецензування: 10.11.2025
Дата публікації (оприлюднення) статті: 24.11.2025