# ШЛЯХИ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНОГО ЗАКОНОДАВСТВА У СФЕРІ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ

# IMPROVING ADMINISTRATIVE LEGISLATION FOR CYBER THREAT COUNTERMEASURES: ADMINISTRATIVE AND LEGAL REGULATION

**Кочман Костянтин Павлович**
orcid.org/0009-0001-3194-1220
аспірант ІІ курсу денної форми навчання
кафедри кримінального аналізу та інформаційних технологій
(Одеський державний університет внутрішніх справ, м. Одеса, Україна)
**Форос Ганна Володимирівна**
https://orcid.org/0000-0002-9504-3681
завідувачка кафедри кримінального аналізу
та інформаційних технологій, к.ю.н., доцент
(Одеський державний університет внутрішніх справ, м. Одеса, Україна

***Анотація:*** *Стаття є дослідженням сучасного стану адміністративно-правового регулювання кібербезпеки в Україні в умовах зростаючих кіберзагроз, спричинених воєнною агресією російської федерації проти нашої держави та активізацією технологічно складних атак, зокрема із застосуванням штучного інтелекту. Проаналізовано ключові нормативно-правові акти, зокрема базові закони, нові постанови Кабінету Міністрів, положення Стратегії кібербезпеки 2021 року, а також суттєві законодавчі зміни, які були прийняті у 2025 році. Виокремлено роль спеціалізованих державних органів, зокрема CERT-UA та Держспецзв'язку, у функціонуванні національної системи кіберзахисту, а також у координації заходів реагування на інциденти та моніторингу критичної інформаційної інфраструктури. Досліджено процес адаптації національного правового поля до європейських вимог у сфері кібербезпеки, зокрема імплементацію положень Директиви NIS2, а також трансформацію концептуальних засад – від жорстких процедурно-орієнтованих комплексної системи захисту інформації до гнучких, динамічних та ризикоорієнтованих моделей управління інформаційною безпекою. Наголошено на важливості міжвідомчої взаємодії, залучення приватного сектору, а також підвищення ролі користувачів через запровадження систематичної кібергігієнічної освіти. Окрема увага приділена питанням адміністративної відповідальності. Актуалізовано необхідність проактивного регулювання з урахуванням викликів, пов'язаних із безпекою IoT-пристроїв, зловживанням штучним інтелектом та зростанням складності атак. У результаті сформульовано напрями вдосконалення адміністративного законодавства у сфері кібербезпеки, які мають забезпечити системність, адаптивність та відповідність сучасним загрозам у цифровому середовищі.*

***Ключові слова:*** *кіберзагрози, адміністративне законодавство, кіберзахист, штучний інтелект.*

*Abstract: This article examines the current state of administrative and legal regulation of cybersecurity in Ukraine amid growing cyber threats caused by the russian federation's military aggression against our state and the intensification of technologically sophisticated attacks, particularly those employing artificial intelligence. Key regulatory legal acts are analyzed, including fundamental laws, new Cabinet of Ministers resolutions, provisions of the 2021 Cybersecurity*

*Strategy, as well as significant legislative amendments adopted in 2025. The role of specialized state bodies, particularly CERT-UA and the State Service of Special Communications, in the functioning of the national cyber defense system, as well as in coordinating incident response measures and monitoring critical information infrastructure, is highlighted. The process of adapting the national legal framework to European cybersecurity requirements is examined, including the implementation of NIS2 Directive provisions, as well as the transformation of conceptual foundations – from rigid procedurally-oriented comprehensive information protection systems to flexible, dynamic, and risk-oriented information security management models. The importance of inter-agency cooperation, private sector involvement, and enhancing users' role through the introduction of systematic cyber hygiene education is emphasized. Special attention is given to issues of administrative liability. The necessity of proactive regulation is actualized, taking into account challenges related to IoT device security, artificial intelligence abuse, and the growing complexity of attacks. As a result, directions for improving administrative legislation in the field of cybersecurity are formulated, which should ensure systematicity, adaptability, and compliance with contemporary threats in the digital environment.*

*Keywords: cyber threats, administrative legislation, cyber defense, artificial intelligence.*

**Постановка проблеми.** В умовах широкомасштабної агресії російської федерації проти України, що супроводжується масштабними кібератаками, Україна стикається з необхідністю швидкої адаптації свого адміністративного законодавства до реалій сучасного кіберпростору. Зростаюча кількість кіберінцидентів, збільшення складності атак, а також використання штучного інтелекту – вимагають переорієнтації державної політики від формального нормативного контролю до ризикоорієнтованої, результативної моделі управління. Актуальність дослідження зумовлена як внутрішніми викликами, пов’язаними з безпекою критичної інфраструктури та персональних даних, так і зовнішнім фактором – потребою гармонізації з вимогами Директиви NIS2 ЄС у межах інтеграції до європейського кіберпростору. Це зумовлює необхідність комплексного наукового аналізу адміністративно-правових засад кібербезпеки України, їхньої ефективності, гнучкості та здатності до активної протидії загрозам.

**Аналіз останніх досліджень і публікацій.** Питанню протидії кіберзагрозам і забезпечення кіберзахисту держави присвячена низка праць вчених і дослідників. Так, окреслене питання висвітлювали: Бухарєв В., Горулько В., Дутчак С., Крамар Р., Кульчицький Т., Микола Б., Пахненко О., Повалена М., Резворович К. та інші. Втім, в умовах триваючої агресії російської федерації проти України окреслена тема потребує подальших ґрунтовних досліджень.

**Мета статті полягає** у розгляді шляхів щодо удосконалення адміністративного законодавства у сфері адміністративно-правового регулювання забезпечення протидії кіберзагрозам.

**Виклад основного матеріалу.** Україна послідовно розвиває своє адміністративне законодавство у сфері кібербезпеки, ефективно реагуючи на зростаючі загрози, внаслідок агресії російської федерації та прагнучи до інтеграції з міжнародними стандартами. Правова база країни охоплює комплекс ключових нормативних актів, що забезпечують захист інформації та протидію кіберзлочинності.

Основоположним нормативно-правим актом у сфері кібербезпеки України є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [9]. Цей Закон визначає правові та організаційні основи захисту національних інтересів у кіберпросторі, встановлює стратегічні цілі, принципи та напрями державної політики в цій сфері, а також регламентує повноваження та обов’язки державних інституцій.

У межах цього Закону створено Національну систему кібербезпеки, до складу якої входять Рада національної безпеки і оборони України, Національний координаційний центр кібербезпеки, як її робочий орган та ін.

Вищевказаний Закон України має динамічний характер і неодноразово зазнавав змін. Останні суттєві поправки були внесені Законом України № 4336-IX від 27 березня 2025 року [6]. Ці зміни запроваджують національну систему реагування на кіберінциденти, кібератаки та кіберзагрози, а також механізми обміну інформацією між суб’єктами кібербезпеки.

Серед ключових новацій – розвиток команд реагування на комп’ютерні інциденти (CSIRT / CERT-UA) на національному, галузевому та регіональному рівнях, із можливістю залучення до цього процесу приватного сектору. Цей підхід побудовано з урахуванням положень Директиви NIS2 Європейського Союзу.

Особливої уваги заслуговує закладення нормативної основи для впровадження системи оцінки стану кіберзахисту та авторизації систем безпеки,

яка має поступово замінити традиційний підхід, орієнтований на побудову комплексних систем захисту інформації (КСЗІ). Така трансформація сигналізує перехід від формального, процедурного контролю до гнучкої, результатоорієнтованої моделі управління безпекою, що базується на ризикоорієнтованому підході.

Закон також чітко визначає необхідність залучення приватного сектору до процесів кіберзахисту, а також гармонізації з європейськими стандартами, що підкреслює важливість міжсекторальної взаємодії та міжнародної інтеграції в цій сфері. Такий підхід відображає сучасне розуміння кібербезпеки як колективної відповідальності, яка потребує адаптивного управління, а не лише нормативного регулювання.

Крім того, передбачено створення спеціалізованих структур з кіберзахисту в державних органах та на об’єктах критичної інфраструктури з уніфікованими вимогами до їх організації, кадрового складу та компетенцій. Також встановлено обов’язковість регулярних тренінгів і навчань із питань кібергігієни.

Прийняття відповідних змін стало однією з умов фінансової допомоги Україні в межах Плану підтримки Ukraine Facility від Європейського Союзу й спрямоване на наближення українського законодавства до вимог Директиви NIS2 [1].

Указ Президента України від 26 серпня 2021 року № 447 / 2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»» став важливим етапом у формуванні державної політики у сфері кібербезпеки. Цей документ не лише затвердив нову редакцію стратегії, замінивши попередню від 2016 року, але й визначив основні напрями та механізми її реалізації, що стало важливим кроком у контексті удосконалення законодавства щодо протидії кіберзагрозам.

З точки зору удосконалення адміністративного законодавства України з протидії кіберзагрозам, окреслена Стратегія кібербезпеки України має низку ключових значень.

По-перше, вона закріпила нову правову основу: скасовує частини попередньої Стратегії 2016 року, виправляючи її недоліки – відсутність індикаторів виконання, обмежене залучення суб'єктів (громадськість, наука) та слабку координацію.

По-друге, Указ покладає контроль на Секретаря РНБО, що теоретично забезпечує централізацію відповідальності та моніторинг виконання заходів Стратегії.

По-третє, Стратегія інтегрована в систему національних безпекових документів (конституція, Стратегія нацбезпеки 2020, міжнародні договори), підвищуючи її легітимність та відповідність міжнародним стандартам.

Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI – має фундаментальне значення поряд із спеціальним законодавством у сфері кібербезпеки. Його положення визначають правові засади обробки та захисту персональних даних, закріплюють права суб'єктів персональних даних, обов'язки розпорядників та володільців даних, а також передбачають відповідальність за порушення встановлених вимог. Актуальність цього закону зумовлена тим, що витоки персональної інформації часто є наслідком кібератак, що свідчить про тісний взаємозв'язок між правовим регулюванням у сфері захисту даних та кібербезпеки. Кібератаки, як правило, мають на меті або спричиняють порушення конфіденційності персональної інформації, тому правове забезпечення кібербезпеки має бути органічно узгоджене із законодавством про захист персональних даних. Відтак, удосконалення адміністративно-правового регулювання у сфері кібербезпеки повинно здійснюватися з урахуванням положень законодавства про захист персональних даних, аби забезпечити системний, комплексний та скоординований підхід до запобігання, виявлення та реагування на загрози, пов'язані з обробкою персональної інформації [8].

Кабінетом Міністрів України було прийнято низку постанов, які закріплюють адміністративно-правові основи у сфері кібербезпеки, встановлюють процедури реагування на інциденти, визначають правила захисту

критичної інфраструктури та уточнюють розподіл повноважень між державними органами. Серед ключових документів:

1. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» від 19 червня 2019 року № 518;
2. Постанова Кабінету Міністрів України «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» від 11 листопада 2020 року № 1176;
3. Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» від 23 грудня 2020 року № 1295;
4. Постанова Кабінету Міністрів України «Про затвердження Положення про організаційно-технічну модель кіберзахисту» від 29 грудня 2021 року № 1426;
5. Постанова Кабінету Міністрів України «Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 4 квітня 2023 року № 299 та ін.

Варто зазначити, що Кабінетом Міністрів України було прийнято Постанову №447 від 28 березня 2025 року, яка істотно посилює вимоги до кіберзахисту державних інформаційних ресурсів і об’єктів критичної інформаційної інфраструктури. Документ передбачає обов’язкове щорічне проведення оцінки стану кібербезпеки, включаючи залучення незалежних аудиторів, а також впровадження систем виявлення, запобігання та нейтралізації кіберзагроз. Зокрема, акцент зроблено на аналізі мережевої телеметрії, реагуванні на інциденти та кібератаки, що демонструє перехід від реактивного до проактивного підходу в управлінні інформаційною безпекою. Такий підхід

відповідає сучасним світовим практикам, орієнтованим на дані та безперервне вдосконалення.

Варто окремо підкреслити, що особливе значення надано обов'язковому аудиту інформаційної безпеки на об'єктах критичної інфраструктури. Відповідний Порядок визначає чіткі вимоги до проведення незалежних аудитів, а також встановлює виключення для банків, об'єктів, що працюють із державною таємницею, та непублічних мереж, які підлягають окремим регуляторним режимам. Це свідчить про прагнення уряду створити сфокусований і ефективний механізм контролю саме в тих сферах, які найбільш вразливі до кіберзагроз.

Адміністрація Держспецзв'язку виконує ключову роль у реалізації цих вимог – вона формує та веде перелік атестованих аудиторів інформаційної безпеки, а також здійснює узагальнений аналіз результатів проведених аудитів. Централізація цієї функції забезпечує послідовність, якість та прозорість процесів, а також дає змогу державі отримувати цілісну картину рівня кіберзахищеності критичної інфраструктури, що, у свою чергу, сприяє формуванню ефективної політики у сфері національної кібербезпеки [7].

Також, варто зазначити, що 19 липня 2025 року Кабінет Міністрів України ухвалив постанову №893, яка змінює підходи до створення та розвитку державних інформаційних систем. Документ спрощує процедури, оновлює стандарти та відкриває ринок для ширшого кола IT-компаній.

Нові правила передбачають:

1. Менше паперів – для запуску системи достатньо лише технічних вимог і техзавдання, без робочої та експлуатаційної документації.
2. Міжнародні стандарти – замість застарілих радянських норм використовуються ISO та IEEE.
3. Оновлена кібербезпека – КСЗІ замінюють сучасними системами інформаційної безпеки (СІБ).
4. Електронна документація – дозволено застосовувати хмарні технології та відкритий код.

5. Без роялті за держпослуги – заборонено ліцензії з виплатою роялті, що усуває вендорлок і стимулює конкуренцію [13].

Окреслена постанова позиціонується як інструмент для зменшення бюрократії та пришвидшення цифрової трансформації. Водночас пряма згадка про «оновлену кібербезпеку» та перехід від КСЗІ до сучасних СІБ свідчить про більш глибоку мету: спрощення адміністративних процедур розглядається як механізм підвищення рівня кіберзахисту. Уряд, інтегруючи міжнародні стандарти та знімаючи регуляторні бар'єри, створює умови для впровадження новітніх і безпечних ІТ-рішень. Це підкреслює стратегічне усвідомлення того, що надмірна зарегульованість не лише стримує розвиток, а й створює потенційні вразливості в системах державного управління.

Також, варто звернути питання щодо адміністративної відповідальності. Так, в Кодексі України про адміністративні правопорушення (Стаття 212–6) за незаконний доступ до інформації в автоматизованих системах передбачено штраф у розмірі від п'яти до десяти неоподатковуваних мінімумів доходів громадян із можливістю конфіскації використаних технічних чи програмних засобів, а за повторне вчинення протягом року – від десяти до двадцяти мінімумів із конфіскацією. У разі доступу до систем із обмеженим доступом санкції зростають до тридцяти-сто мінімумів доходів із обов'язковою конфіскацією.

Незаконне копіювання або розповсюдження баз даних тягне за собою штраф від десяти до двадцяти-п'яти мінімумів із конфіскацією копій, а збут інформації – від двадцяти до ста мінімумів доходів із конфіскацією коштів або копій. Таким чином, адміністративна відповідальність слугує первинним інструментом реагування на кіберінциденти низької або середньої тяжкості, забезпечуючи оперативне реагування та запобігання масштабнішому кримінальному переслідуванню. Окрім того, чітка диференціація санкцій залежно від повторності, мети, об'єкта й майна, яке підлягало доступу або поширенню, сприяє пропорційності покарання і посиленню профілактичного ефекту [4].

Ландшафт кіберзагроз в Україні характеризується постійним зростанням кількості та складності атак, що значною мірою зумовлено геополітичною ситуацією. Аналіз статистичних даних та прикладів кіберінцидентів за останні роки дозволяє виявити ключові тенденції.

За інформацією Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, що працює при Держспецзв'язку, у 2024 році було зафіксовано та опрацьовано 4315 кіберінцидентів. Це на 69,8% більше порівняно з 2023 роком, коли в українському кіберпросторі було зафіксовано 2541 атаку. Така статистика свідчить про помітне зростання кіберзагроз [5]. У 2023–2024 роках фіксується менше критичних інцидентів (367 у 2023 році, 59 – у 2024-му), але загальна кількість кіберінцидентів зростає (4315 у 2024 році проти 2194 у 2022-му). Це свідчить про зсув акценту на шпигунські операції та розвідку [11].

У 2022 році Україна зазнала численних кібератак, зокрема на урядові вебресурси. У відповідь на ці інциденти команда CERT-UA активно впроваджувала платформу обміну інформацією про кіберзагрози MISP для оперативної передачі індикаторів компрометації (IoC), пов'язаних із шкідливими програмами, зокрема WhisperGate, міжнародним партнерам. Це сприяло своєчасному оновленню механізмів кіберзахисту.

Особливого удару зазнав фінансовий сектор: українські банки інтегрували MISP для автоматизованої ідентифікації шкідливих IP-адрес і доменів, що позитивно вплинуло на зниження ефективності фішингових атак. Починаючи з лютого 2022 року, кількість кібератак на енергетичну інфраструктуру зросла приблизно на 20–25% [14].

Фішингові кампанії продовжували залишатися одним із домінантних векторів атаки, часто експлуатуючи соціально резонансні теми – зокрема, питання військовополонених або електронні петиції. Крім того, зростає загроза з боку атак на пристрої Інтернету речей (IoT), які, за статистикою, у 98% випадків передають дані у незашифрованому вигляді, що створює серйозні ризики витоку конфіденційної інформації.

Значним інцидентом, що безпосередньо вплинув на формування законодавства, стала масштабна російська кібератака на реєстри Міністерства юстиції у грудні 2024 року [10]. Ця атака виявила критичні вразливості в державних інформаційних системах і стала безпосередньою причиною прийняття Закону України №11290 [1]. Зазначення саме цієї події, що спричинила прийняття відповідного законодавчого акта, чітко ілюструє причинно-наслідковий зв'язок між масштабними кіберінцидентами та реакцією законодавчої влади. Це свідчить, що адміністративний законодавчий процес в Україні, принаймні частково, носить реактивний характер, використовуючи значні порушення безпеки як каталізатор для проведення реформ. Така модель є поширеною у світовій практиці, однак вона підкреслює нагальність проблеми та політичну волю, що лежить в основі останніх законодавчих змін.

Прогнозовані кіберзагрози та тенденції на 2025 рік свідчать про подальшу еволюцію методів кіберзлочинності. Зокрема, очікується інтенсивне застосування технологій штучного інтелекту для автоматизованого виявлення вразливостей, що дозволяє зловмисникам ефективно обходити традиційні засоби інформаційної безпеки та динамічно адаптуватися до змін у мережевій інфраструктурі. Крім того, шифрувальні атаки, зокрема реалізовані у вигляді рансомвеєрних кампаній, прогнозуються до подальшого вдосконалення з точки зору методів проникнення, набуваючи підвищеної стелсності до моменту ініціації шифрування. Вони орієнтуватимуться не лише на великі корпорації, а й на малі та середні підприємства, що свідчить про розширення спектра цілей кіберзлочинців. В Україні та по всьому світу впроваджуються жорсткі вимоги щодо збереження конфіденційності як у контексті локального законодавства (наприклад, Закон України про основні засади забезпечення кібербезпеки України), так і міжнародних стандартів на зразок GDPR [3].

Загострення геополітичної ситуації сприятиме посиленню кіберзлочинності, зокрема з використанням легітимних інструментів, а також прогнозується збільшення випадків складних форм шантажу, таких як потрійне здирництво. Загальна кількість шкідливого програмного забезпечення зросла на

30%, тоді як загрози, спрямовані на Інтернет речей (IoT), збільшилися більш ніж удвічі – на 107% [12]. Еволюція кіберзагроз, у якій ключову роль відіграє штучний інтелект, вимагає впровадження проактивної регуляторної політики щодо новітніх технологій. Використання штучного інтелекту дозволяє здійснювати більш точні, складні й адаптивні атаки, що ставить під сумнів ефективність традиційних засобів кіберзахисту. Отже, нормативно-правова база не може обмежуватися реагуванням на вже відомі загрози, а повинна передбачати потенційні ризики, пов'язані з розвитком і застосуванням новітніх технологічних рішень. Це передбачає створення регуляторних «пісочниць», розробку етичних стандартів використання штучного інтелекту у сфері кібербезпеки, а також імплементацію вимог до захисних механізмів, що керуються штучним інтелектом. Зростання кількості шкідливих програм для IoT додатково свідчить про розширення поверхні атаки, що вимагає розширення регуляторного впливу за межі традиційних інформаційних систем.

Людський чинник стабільно залишається ключовою вразливістю в системі кібербезпеки, що обумовлює необхідність систематичного навчання персоналу базовим принципам інформаційної безпеки та дотримання норм кібергігієни. Незважаючи на те, що чинне законодавство в основному акцентує увагу на технічних та організаційних аспектах захисту, зростаюче визнання критичної ролі поведінкових чинників – зокрема, дисципліни користувачів та рівня їх обізнаності – демонструє обмеженість нормативного регулювання у вирішенні комплексних ризиків кіберпростору [2]. У цьому контексті, ефективна протидія кіберзагрозам потребує інтеграції постійних освітніх ініціатив та програм підвищення обізнаності, що, хоч і належать до сфери адміністративних заходів, не є прямими предметами законодавчого регулювання. Таким чином, кібербезпека постає як міждисциплінарна сфера, яка виходить за межі юридичної площини, охоплюючи також культурно-освітні складові, що формують основу стійкої цифрової безпеки.

**Висновки.** Отже, сучасна система адміністративно-правового регулювання кібербезпеки в Україні активно реагує на нові виклики, але залишається

недостатньо проактивною і потребує подолання фрагментарності. Впровадження ризикоорієнтованого підходу сприятиме більш гнучкому і ефективному управлінню кіберзагрозами, зменшуючи залежність від формальних процедур. Необхідне закріплення законодавчих рамок для застосування штучного інтелекту у кіберзахисті, що включатиме як етичні, так і технічні аспекти. Розширення повноважень Держспецзв'язку посилить координацію національної системи реагування на кіберінциденти. Важливим напрямом є імплементація вимог директиви NIS2, яка закріпить інтеграцію України у європейське кібербезпекове середовище. В цілому, розвиток законодавства має враховувати як національний контекст, так і міжнародні стандарти, забезпечуючи адаптивність та стійкість системи кібербезпеки.

**Список використаних джерел:**


1. Зеленський підписав закон про кібербезпеку. Що він передбачає і чому його критикують. *DOU*. URL: https: // dou. ua / lenta / news / president-signs-law-on-cybersecurity/ (дата звернення: 22.07.2025).
2. Кібербезпека в Україні 2025: виклики та перспективи. *Galera*. URL: https: // galera. news / kiberbezpeka-v-ukrayini – 2025-vyklyky-ta-perspektyvy – 7009/ (дата звернення: 22.07.2025).
3. Кіберзагрози у 2025 році: як бізнесу захиститися від атак. *Школа бізнесу*. URL: https: // online. novaposhta. education / blog / kiberzagrozi-u – 2025-roci-yak-biznesu-zahistitisya-vid-atak (дата звернення: 22.07.2025).
4. Кодекс України про адміністративні правопорушення (статті 1–212–24): Кодекс України від 07.12.1984 № 8073-X. URL: https: // zakon. rada. gov. ua / laws / show / 80731–10#Text (дата звернення: 22.07.2025
5. Прасад А. Держспецзв'язку за рік зафіксувало на 70% більше кібератак. Що найчастіше ставало ціллю хакерів. *Forbes. ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії*. URL: https: // forbes. ua / news / v-ukraini-za-rik-kilkist-kiberatak-zrosla-na – 70-nayposhirenishi-tipi-intsidentiv-i-golovni-tsili-khakeriv – 08012025–26137 (дата звернення: 22.07.2025).
6. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27.03.2025 № 4336-IX. URL: https: // zakon. rada. gov. ua / laws / show / 4336-IX#Text (дата звернення: 22.07.2025).
7. Про внесення змін щодо кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури до деяких постанов Кабінету Міністрів України : Постанова Кабінету Міністрів України від 28.03.2025 № 447. URL: https: // zakon. rada. gov. ua / laws / show / 447–2025-п#Text (дата звернення: 22.07.2025).

8. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https: // zakon. rada. gov. ua / laws / show / 2297–17#Text (дата звернення: 22.07.2025).
9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https: // zakon. rada. gov. ua / laws / show / 2163–19#Text (дата звернення: 22.07.2025).
10. Тарасовський Ю. Мін'юст повідомив про масштабний збій у роботі держреєстрів. *Forbes. ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії*. URL: https: // forbes. ua / news / derzhavni-reestri-ne-pratsyuyut-cherez-masshtabniy-zbiy-minyust – 19122024–25728 (дата звернення: 22.07.2025).
11. Татохіна О. Кібервійна Росії проти України: Держспецзв'язку презентувала звіт про три роки атак і глобальні виклики. *detector. media*. URL: https: // detector. media / infospace / article / 241232 / 2025–05–26-kiberviyna-rosii-proty-ukrainy-derzhspetszvyazku-prezentuvala-zvit-pro-try-roky-atak-i-globalni-vyklyky/ (дата звернення: 22.07.2025).
12. Тренди з кібербезпеки в благодійності у 2025 році. *Ресурсний центр ГУРТ*. URL: https: // gurt. org. ua / articles / 105442/ (дата звернення: 22.07.2025).
13. Уряд у боротьбі з бюрократією оновив правила створення держсистем. *Судово-юридична газета*. URL: https: // sud. ua / uk / news / ukraine / 336354-pravitelstvo-v-borbe-s-byurokratiey-obnovilo-pravila-sozdaniya-goscistem (дата звернення: 22.07.2025).
14. Cyber digest Огляд подій в сфері кібербезпеки, січень 2023. URL: https: // www. rnbo. gov. ua / files / 2023 / NKCK / Cyber% 20digest_january_2023_fin. pdf (дата звернення: 22.07.2025).