УДК 343.9: 004.49
DOI https://doi.org/10.24144/2307-3322.2025.89.1.21

ПРАВОВІ РАМКИ КІБЕРБЕЗПЕКИ ТА ПОЛІТИКА ЗАХИСТУ КІБЕРПРОСТОРУ РЕСПУБЛІКИ ПОЛЬЩА

Санжарова Г.Ф.,
старший викладач кафедри романської філології
Київського столичного університету імені Бориса Грінченка
ORCID: 0000-0002-0557-9192
e-mail: h.sanzharova@kubg.edu.ua

Бак В.І.,
кандидат юридичних наук, доцент,
завідувач кафедри теорії та історії держави і права ННІ права
Державного податкового університету
ORCID: 0009-0001-1269-4981
e-mail: bak.vera@gmail.com

Санжаров В.А.,
кандидат юридичних наук,
доцент кафедри теорії та історії держави і права ННІ права
Державного податкового університету
ORCID: 0000-0003-4075-8572
e-mail: v.a.sanzharov@dpu.edu.ua

Санжарова Г.Ф., Бак В.І., Санжаров В.А. Правові рамки кібербезпеки та політика захисту кіберпростору Республіки Польща.

Стаття присвячена дослідженню формування польської правової доктрини кібербезпеки та особливостям державної політики в сфері захисту кіберпростору Республіки Польща. Можна стверджувати, що Польська Республіка приділяє питанням кібербезпеки постійну увагу: відповідальність за забезпечення кібербезпеки розподілена переважно між двома міністерствами. Захист цивільного кіберпростору Польщі є одним з головних пріоритетів та прерогатив Міністерства цифрових технологій, військовий кіберпростір знаходиться в компетенції Міністерства національної оборони. Констатовано, що Польська Республіка в галузі кібербезпеки зосереджує основні зусилля на наступних основних напрямках: 1) розробка національної системи кібербезпеки; збільшення національного потенціалу для забезпечення безпеки в кіберпросторі; 2) підвищення рівня стійкості інформаційних систем державного управління та приватного сектору, а також забезпечення можливості ефективно запобігати інцидентам та реагувати на них; 3) підвищення обізнаності та компетентності громадськості в галузі кібербезпеки; 4) побудова сильної міжнародної позиції Республіки Польща в галузі кібербезпеки. Відзначено, що польські законодавці виявили певне протиріччя між забезпеченням, з одного боку, належного рівня захисту інформаційних систем, а з іншого, можливістю обмеження громадянських свобод у кіберпросторі. Позиція законодавця відносно таких обмежень: вони можуть бути запроваджені лише за умови, що кібер-захист не може бути забезпечений іншим чином. Автори вважають, що забезпечення кібербезпеки має стратегічне значення для Польщі. Зроблено висновок, що Республіка прагне будувати державну політику захисту кіберпростору шляхом підвищення рівня стійкості до кіберзагроз, посилення захисту інформації в державному, військовому та приватному секторах, а також поширення знань та передового досвіду серед підприємців та населення. «Закон про національну кібербезпеку» 2018 року започаткував процес імплементації в польське законодавство першого загальноєвропейського законодавчого акту про кібербезпеку (Директива NIS).

Ключові слова: кримінальне право, кіберпростір, кібербезпека, кіберзлочин, Національна стратегія кібербезпеки, Закон про національну кібербезпеку.

Sanzharova G.F., Bak V.I., Sanzharov V.A. Legal framework of cybersecurity and cyberspace protection policy of the Republic of Poland.

The article is devoted to the study of the formation of the Polish legal doctrine of cybersecurity and the features of state policy in the field of cyberspace protection of the Republic of Poland. It can be argued that the Republic of Poland pays constant attention to cybersecurity issues: responsibility for ensuring cybersecurity is divided mainly between two ministries. The protection of Poland's civilian cyberspace is one of the main priorities and prerogatives of the Ministry of Digital Technologies, while military cyberspace is the responsibility of the Ministry of National Defense. It was noted that the Republic of Poland focuses its main efforts in the field of cybersecurity on the following main areas: 1) development of a national cybersecurity system; increasing the national potential for ensuring security in cyberspace; 2) increasing the level of resilience of information systems of public administration and the private sector, as well as ensuring the ability to effectively prevent and respond to incidents; 3) increasing public awareness and competence in the field of cybersecurity; 4) building a strong international position of the Republic of Poland in the field of cybersecurity. It is noted that Polish legislators have identified a certain contradiction between ensuring, on the one hand, an adequate level of protection of information systems, and, on the other, the possibility of restricting civil liberties in cyberspace. The legislator's position regarding such restrictions is that they can be introduced only if cyber protection cannot be ensured in any other way. The authors believe that ensuring cybersecurity is of strategic importance for Poland. It is concluded that the Republic of Poland seeks to build a state policy for the protection of cyberspace by increasing the level of resilience to cyber threats, strengthening information protection in the public, military and private sectors, as well as disseminating knowledge and best practices among entrepreneurs and the population. The 2018 'Act on National Cybersecurity' initiated the process of implementing the first pan-European legislative act on cybersecurity (NIS Directive) into Polish law.

Key words: Criminal Law, Cyberspace, Cybersecurity, Cybercrime, National Cybersecurity Strategy, National Cybersecurity Act.

Постановка проблеми: Офіційно Польща отримала доступ до Інтернету в грудні 1991 року. Наразі відсоток польських підприємств (за виключенням великих підприємств) та домогосподарств з доступом до Інтернету все ще дещо нижчий за середній показник по ЄС, але він з року в рік зростає. Громадяни Польщі все частіше користуються послугами електронного урядування для отримання інформації з веб-сайтів державних органів, завантаження офіційних форм та подання заповнених форм. Сьогодні польська адміністрація пропонує громадянам можливість електронного користування понад 500 послугами. Портал Республіки Польща (Portal RP) стане, на думку розробників, шлюзом до всієї публічної інформації та електронних послуг. Міністерство цифрових справ Польщі (Ministerstwo Cyfryzacji) є головним урядовим відомством, відповідальним за розвиток електронного адміністрування, розвиток інфраструктури широкосмугового зв'язку, підтримку створення інтернет-контенту та електронних послуг. Польща є одним із ринків електронної комерції, що найшвидше розвиваються в Європі [1, с. 89-90]. Разом з тим, масова цифровізація сучасного суспільства створила серйозні проблеми в сфері кібербезпеки: тероризм і злочинність, дезінформацію та пропаганду, недобросовісну конкуренцію та шпигунство. У 2024 році національна «Команда реагування на інциденти комп'ютерної безпеки» (GOV CSIRT) при Агентстві внутрішньої безпеки країни зареєструвала загалом 17 439 повідомлень про потенційні IT-інциденти у сфері своєї компетенції, з них 3991 було класифіковано як фактичні інциденти IT-безпеки [2, с. 10]. Протягом 2024 року було зафіксовано 348 DDoS-атак: 1) домінували атаки з використанням методів, відомих як TCP SYN/ACK Flood та UDP Flood; 2) для перевантаження серверних ресурсів також використовувалися атаки на програми, засновані на численних HTTP GET або POST запитах. Під час аналізу джерел DDoS-атак у 2024 році слід зазначити, що геолокація найактивніших IP-адрес вказувала на США, Польщу та Фінляндію. У багатьох атаках спостерігалося використання польських IP-адрес, які були інфраструктурою VPN-сервісу. Використання описаного сервісу дозволяло зловмисникам обходити правила фільтрації мережевого трафіку на основі геолокації, що могло призвести до більшої ефективності атак. Середня тривалість зареєстрованих атак зменшилася протягом року від близько 2,5 годин до менше п'ятнадцяти

хвилин [2, с. 44–45]. DDoS-атаки не вимагають від зловмисників значних технічних навичок, а їхній ефект є переважно пропагандистським (вони зазвичай широко висвітлюються в соціальних мережах). Ці атаки спрямовані на порушення доступності інтернет-ресурсів, але зазвичай не мають довгострокових наслідків. Однак, з точки зору «хактивістів», цей тип атаки демонструє нібито слабкість ворожих країн, а також, на думку зловмисників, нібито ефективність таких дій. У випадку проросійських «хактивістів» (найвідоміші групи «Killnet», «Anonymous Sudan», «CyberArmy of Russia Reborn», «XAKNET», «Solntsepek», «UserSec», «NoName057(16)», «Zarya», «Beregini», «Z-Pentest») мотивацією, яку вони презентують у соціальних мережах, є, перш за все, підтримка дій російських військ та «покарання» країн НАТО за військову підтримку України. Постійна активність злочинних груп продовжує бути проблемою в сфері національної системи кібербезпеки.

Стан опрацювання проблематики: Кіберзлочинність завдає шкоди світовій економіці, національній безпеці і соціальній стабільності окремих країн та індивідуальним інтересам. Поточні зусилля щодо пом'якшення загроз кіберзлочинності насамперед зосереджені на технічних заходах, але цього недостатньо. Труднощі в розумінні кіберзлочинності починаються з мінливості термінології та відсутності узгодженості законодавства про кіберзлочинність у різних юрисдикціях. Кібербезпекові проблеми потребують правового визначення. Вивчення досвіду виявлення, атрибуції та протидії кіберзлочинності окремих країн, розвитку кібербезпекового законодавства та вдосконалення національних організаційних кібербезпекових структур привертають постійно зростаючу увагу дослідників (М. Карпюк, К. Качмарек, М. Мацелик, О. Павлюх, В. Пізло, В. Санжаров та інші) [3, с. 73–95; 4, с. 645–663; 5, с. 303–306; 6, с. 219–227; 7, с. 28–30]. Польський досвід створення та удосконалення кібербезпекового законанодавства, імпліментації в нього «Європейської директиви про безпеку мереж та інформаційних систем» («Network and Information System Security», NIS) від 2018 року проаналізовано в роботах Йоанни Швентковської (Świątkowska), Ізабели Альбріхт (Albrycht), Домініка Скоковського (Skokowski), Домініки Дзівіш (Dziwisz), Малгожати Чурик (Czuryk), Мирослава Карпюка (Karpiuk), Войцеха Пізло (Pizło), Кшиштофа Качмарека (Kaczmarek) та інших [8; 1, с. 89–98; 9, с. 43–52; 10, с. 31–43; 11, с. 234–245; 4, с. 645–663]. Національна стратегія та правові засади кібербезпеки Польської Республіки безумовно потребують дослідницької уваги та подальшого детального вивчення.

Метою цієї статті є дослідження формування польської правової доктрини кібербезпеки та особливостей державної політики в сфері захисту кіберпростору Республіки Польща.

Виклад основного матеріалу: Перший стратегічний документ, виключно присвячений кібербезпеці Польщі був опублікований під назвою «Політика захисту кіберпростору Республіки Польща» у червні 2013 року колишнім Міністерством адміністрації та цифровізації (Ministerstwo Cyfryzacji i Administracji, MAC) та Агентством внутрішньої безпеки (Agencja Bezpieczeństwa Wewnetrznego, ABW). У січні 2015 року Бюро національної безпеки (Biuro Bezpieczeństwa Narodowego, BBN) опублікувало другий стратегічний документ – «Доктрину кібербезпеки Республіки Польща» («Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej»). Ця доктрина є концептуальним та виконавчим документом, пов'язаним зі «Стратегією національної безпеки Республіки Польща 2014 року» («Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej»). Вона встановила пріоритети та цілі у сфері кібербезпеки, вказала на існуючі загрози, ризики та можливості, визначила найважливіші завдання в рамках побудови державної системи кібербезпеки: 1) оцінка та запобігання (протидія) кіберзагрозам, пошук можливостей зниження ризиків; 2) захист та оборону польської системи інформаційно-комунікаційних технологій; 3) відновлення ефективності та функціональності ІКТ-систем після можливої атаки. Вперше з'явилася офіційна заява про необхідність проведення не лише оборонних, а й наступальних кібер-операцій [1, с. 90–92].

Відповідальність за забезпечення кібербезпеки в Польщі розподілена переважно між двома міністерствами. Захист цивільного кіберпростору Польщі є одним з головних пріоритетів та прерогатив Міністерства цифрових технологій, створеного 7 грудня 2015 року. У складі Міністерства цифрових справ у 2015 році було створено Департамент кібербезпеки, який відповідає за координацію всіх завдань у сфері кібербезпеки. До них належать розробка, впровадження та перегляд стратегічних документів з питань кібербезпеки; ініціювання дослідницьких та розробницьких проектів та поширення знань з кібербезпеки; організація як національної, так і міжнародної співпраці у сфері кібербезпеки (особливо з Європейським Союзом); розробка навчальних планів та навчань; ведення реєстру уповноважених з кібербезпеки; забезпечення виконання завдань мі-

ністра у сфері державної оборони; вирішення питань, що стосуються кризового менеджменту; виконання функцій національного контактного пункту для збору інформації про кіберінциденти в національному масштабі; та нагляд за інформаційною та комунікаційною безпекою міністерства [1, с. 92–94].

Політика захисту кіберпростору була змінена у травні 2017 року резолюцією про Національні рамки політики кібербезпеки Республіки Польща на 2017–2022 роки. Головною метою Національної рамкової програми було заявлено забезпечення високого рівня безпеки для державного і приватного секторів економіки та громадян під час надання або використання ключових цифрових послуг. Було визначено наступні завдання майбутньої національної системи кібербезпеки: 1) досягнення здатності координувати в національному масштабі дії з запобігання, виявлення, протидії та мінімізації наслідків інцидентів, що порушують безпеку ІКТ-систем критично важливих для функціонування держави [9, с. 43–52]; 2) збільшення національного потенціалу та компетенції у сфері безпеки в кіберпросторі; 3) розбудова сильної міжнародної позиції Польщі у сфері кібербезпеки. Набрання чинності «Закону про національну кібербезпеку» від 5 липня 2018 року («Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa») [12] започаткувало процес імплементації в польське законодавство першого загальноєвропейського законодавчого акту Європейського Парламенту та Ради ЄС про кібербезпеку («Директива про безпеку мереж та інформаційних систем», Директива NIS) [13]. Польський законодавець визначив кібербезпеку як здатність інформаційних систем протистояти будь-яким діям, що ставлять під загрозу конфіденційність, цілісність, доступність та автентичність оброблюваних даних або пов'язаних з ними послуг, що надаються через системи ІКТ [12]. Було відзначено, що для забезпечення кібербезпеки необхідно забезпечити належний рівень захисту інформаційних систем. Стаття 2 (4) «Закону» навіть визнавала можливість і прийнятність в певних особливих випадках обмеження громадянських свобод у кіберпросторі заради забезпечення кібербезпеки інформаційних систем. Однак обмеження громадянських свобод можуть бути запроваджені лише за умови, що такий захист не може бути забезпечений іншим чином [12; 10, с. 31–43].

Директива NIS вимагала від усіх держав-членів ЄС гарантувати мінімальний рівень національних можливостей кібербезпеки шляхом створення компетентних органів з мережевої та інформаційної безпеки, а також команд для реагування на комп'ютерні інциденти – Європейську мережу національних CSIRT («Команд реагування на інциденти комп'ютерної безпеки») [13]. Закон від 5 липня 2018 року створив в Польщі три «команди» національного рівня. Перша при Агентстві внутрішньої безпеки (ABW) мала відповідати за виявлення, атрибуцію та реагування на інциденти пов'язані з функціонуванням державної адміністрації, Національного банку Польщі (Narodowy Bank Polski), Польського національного банку розвитку (Bank Gospodarstwa Krajowego) та операторів критичної інфраструктури. Закон про національну систему кібербезпеки виокремив кілька ключових секторів для функціонування держави: енергетику, транспорт, банківську та фінансову ринкову інфраструктуру, охорону здоров'я, постачання питної води (включаючи розподіл) та цифрову інфраструктуру [1, с. 95]. Серйозні інциденти належать до категорії інцидентів, які тягнуть за собою серйозні наслідки. Згідно зі статтею 2 (7) «Закону про національну кібербезпеку», вони визначаються як інциденти, що спричиняють або можуть спричинити серйозне погіршення якості або переривання безперервності основної послуги. Згідно зі статтею 2 (16) «Закону про національну кібербезпеку», життєво важлива послуга – це послуга, яка має вирішальне значення для підтримки критично важливої соціальної чи економічної діяльності. Таким чином, важливість цих послуг як для суспільства, так і для економіки є дуже високою. Однак серйозні інциденти не становлять значної частини всіх кібер-інцидентів за період з 2019 по 2023 роки. У 2019 році було 9 таких інцидентів, у 2020 році – 32, у 2021 році – 36, у 2022 році – 30 та у 2023 році – 40 [3, с. 84; 15]. У секторі державного управління, у 2019 році було зареєстровано 336 кібер-інцидентів, у 2020 році – 388, а у 2021 році – 429. У наступні роки тенденція до зростання продовжилася: у 2022 році було зареєстровано 757 інцидентів, а у 2023 році – 2234. Для порівняння, у сфері освіти та виховання у послідовні роки аналізованого періоду було зареєстровано відповідно 62, 71, 142, 167 та 354 кібер-інциденти [3, с. 85-86].

Друга «команда» (CSIRT MON) відповідальна за всі інциденти, пов'язані з національною обороною, була створена при Міністерстві національної оборони. Під час саміту НАТО у Варшаві у 2016 році було заявлено, що захист кіберпростору є одним з основних завдань колективної оборони НАТО. Відповідно, кіберпростір був визнаний зоною військових операцій. У 2018 році

Міністерство національної оборони запустило програму cyber.mil.pl для розвитку та зміцнення потенціалу кібербезпеки Польщі. При Міністерстві створено Національний центр кібербезпеки (Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni, NCBC) [1, с. 94-95].

Третя «команда» – «Дослідницька та академічна комп'ютерна мережа» («Naukowa Akademicka Sieć Komputerowa», NASK) відповідає за координацію інцидентів, що стосуються всіх інших суб'єктів (більшості ключових операторів і постачальників цифрових послуг та місцевих органів влади). за проведення наукової та дослідницької діяльності в галузі безпеки, організацію освітніх заходів та популяризацію ідеї інформаційного суспільства [1, с. 96].

Необхідність врахування нових викликів, пов'язаних з кібербезпекою (як от безпека хмарних обчислень та запровадження технології 5G тощо) призвели до появи оновленої «Національної стратегії кібербезпеки Польщі на 2019–2024 роки». «Стратегія» приділила більше уваги розширенню системи обміну інформацією про кіберзагрози, а також буде координації дій правоохоронних органів в боротьбі з кіберзлочинністю (включаючи кібершпигунство або гібридні інциденти) [3, с. 82–86].

У квітні 2019 року Польща приєдналася до створеної за міжнародною ініціативою в 2014 році «Спільної цільової групи з боротьби з кіберзлочинністю» («Joint Cybercrime Action Taskforce», J-CAT), яка розміщується в штаб-квартирі Європейського центру боротьби з кіберзлочинністю Європолу в Гаазі. Основні завдання J-CAT включають переслідування кіберзлочинів (таких як шкідливе програмне забезпечення, ботнети та вторгнення) або осіб, які сприяють чи посереднюють таку діяльність (непробивний хостинг, послуги боротьби з антивірусом, оренда та прокат інфраструктури, відмивання грошей, включаючи віртуальні валюти); боротьба з інтернет-шахрайством (системи онлайн-платежів, кардинг, соціальна інженерія); та сексуальна експлуатація дітей в Інтернеті (мережі peer-to-peer та анонімний доступ, як-от мережі Darknet, прямі трансляції сексуального насильства над дітьми) [14].

Висновок: Таким чином, можна стверджувати, що Польська Республіка приділяє питанням кібербезпеки постійну увагу: відповідальність за забезпечення кібербезпеки розподілена переважно між двома міністерствами. Захист цивільного кіберпростору Польщі є одним з головних пріоритетів та прерогатив Міністерства цифрових технологій, військовий кіберпростір знаходиться в компетенції Міністерства національної оборони. «Закон про національну кібербезпеку» від 5 липня 2018 року започаткував процес імплементації в польське законодавство першого загальноєвропейського законодавчого акту Європейського Парламенту та Ради ЄС про кібербезпеку («Директива про безпеку мереж та інформаційних систем», Директива NIS). Треба відзначити, що Польська Республіка в галузі кібербезпеки зосереджує основні зусилля на наступних основних напрямках: 1) розробка національної системи кібербезпеки; збільшення національного потенціалу для забезпечення безпеки в кіберпросторі; 2) підвищення рівня стійкості інформаційних систем державного управління та приватного сектору, а також забезпечення можливості ефективно запобігати інцидентам та реагувати на них; 3) підвищення обізнаності та компетентності громадськості в галузі кібербезпеки; 4) побудова сильної міжнародної позиції Республіки Польща в галузі кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Dziwisz D. Cybersecurity of Poland. Legal and organizational framework. *Routledge Companion to Global Cyber-Security Strategy* / ed. S.N. Romaniuk, M. Manjikian. London-New York: Routledge, 2021. P. 89–98.
2. Raport o Stanie Bezpieczeństwa Cyberprzestrzeni RP w 2024 roku. Warszawa, 2025. 121 p. URL: https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/983, Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2024-roku.html (дата звернення: 28.05.2025).
3. Gaie C., Karpiuk M., Spaziani A. Cybersecurity in France, Poland and Italy. *Studia Iuridica Lublinensia*. 2025. Vol. 34 (1). S. 73–95. DOI: http://dx.doi.org/ 10.17951/sil.2025.34.1.73-95.
4. Karpiuk M., Pizło W., Kaczmarek K. Cybersecurity Management – Current State and Directions of Change. *International Journal of Legal Studies*. 2023. Vol. 14 (2). P. 645–663.
5. Павлюх О.А., Санжарова Г.Ф. Атрибуція злочину як критично важлива проблема кібербезпеки. *Юридичний науковий електронний журнал*. 2024. № 9. С. 303–306. DOI: https://doi.org/10.32782/2524-0374/2024-9/72.

6. Павлюх О.А., Санжарова Г.Ф., Санжаров В.А. Виклики сучасної кібербезпеки: інституційні і правові відповіді Німеччини. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 3 (12). С. 219–227. DOI: https://doi.org/ 10.33244/2617-4154.3(12).2023.219-227.
7. Мацелик М.О., Санжарова Г.Ф., Санжаров В.А. Третя національна стратегія кібербезпеки Великої Британії: політика «на майбутнє» в динамічному технічному середовищі. *Юридичний науковий електронний журнал*. 2023. № 9. С. 28–30. DOI: https://doi.org/10.32782/2524-0374/2023-9/5.
8. Świątkowska J., Albrycht I., Skokowski D. National Cyber Security Organisation: Poland. Tallinn: NATO CCDCOE, 2017. 28 p. URL: https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf (дата звернення: 28.05.2025).
9. Czuryk M. Cybersecurity and Protection of Critical Infrastructure. *Studia Iuridica Lublinensia*. 2023. Vol. 32 (5). S. 43–52. DOI: https://doi.org/10.17951/ sil.2023.32.5.43-52.
10. Czuryk M. Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues. *Studia Iuridica Lublinensia*. 2022. Vol. 31 (3). P. 31–43. DOI: https://doi.org/10.17951/sil.2022.31.3.31-43.
11. Karpiuk M. The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law. *Cybersecurity and Law*. 2024. Vol. 12 (2). P. 234–245.
12. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. URL: https://csirt.gov.pl/cer/prawo/962,Prawo.html (дата звернення: 28.05.2025).
13. Network and Information System Security. *Nis-2-directive*: веб-сайт. URL: https://www.nis-2-directive.com (дата звернення: 28.03.2025).
14. Joint Cybercrime Action Taskforce. веб-сайт. URL: https://www. europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce (дата звернення: 28.03.2025).
15. Raport o Stanie Bezpieczeństwa Cyberprzestrzeni RP w 2023 roku. Warszawa, 2024. URL:https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980, Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html (дата звернення: 28.05.2025).