DOI https://doi.org/10.36059/978-966-397-318-0-75

Недохлєбов І.І.
здобувач кафедри конституційного та адміністративного права
Запорізького національного університету

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ США: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ

Досвід США дуже важливий для нашої держави, оскільки в умовах повномасштабного вторгнення ця країна активно допомагає Україні протидіяти інформаційному тероризму з боку держави-агресора. О. В. Соснін зазначає, що політика США у сфері інформаційної безпеки має за мету закріплення домінування держави в глобальному інформаційному просторі. Також політика США у цій сфері поєднує як ринкові інструменти лібералізації і регулювання, так і намагання встановити прямий державний контроль над інформаційними ресурсами [1, с. 158]. На нашу думку, суперечливість між цими напрямами діяльності держави може бути вирішена шляхом розподілу сфер впливу між державою та бізнесом.

Важливим суб'єктом інформаційної безпеки у США є громадянське суспільство. Зокрема, в американській державній системі забезпечення інформаційної безпеки утворилася унікальна модель державно-приватного партнерства правоохоронних, військових і розвідувальних органів, а також громадськості [2, с. 170]. Переваги цієї моделі моделі очевидні, адже за рахунок долучення суспільства, держава значно розширює власний потенціал протидії реальним і потенційним загрозам.

Американський дослідник Шон Бойн зазначає, що в рамках забезпечення інформаційної безпеки в США правоохоронним органам надані повноваження здійснювати моніторинг загроз інформаційній безпеці, зберігаючи при цьому секретність розслідувань. В свою чергу, американські суди розробили практику збалансування національних інтересів (проведення розслідувань) та конфіденційності (приватності) громадян [3, с. 329]. Цей досвід також є доволі унікальним, оскільки дозволяє розмежувати приватність особистості від національних інтересів в інформаційній сфері. До речі, це також один із засобів вирішення суперечливості між ліберальними методами та жорстким державним контролем у сфері інформаційної безпеки.

У США є декілька пріоритетних сфер діяльності, які становлять основу інформаційної безпеки. Однією з них є захист приватності. З цього приводу Міха Альтман наголошує, що на цей час у США активно працюють у напрямку захисту приватних даних, тобто персональної інформації. Зокрема, планується створення Федерального агенства із

захисту даних. В його структурі планується створення Управління громадянських прав, яке матиме право накладати штрафи за незаконні, несправедливі, оманливі, образливі дії або дискримінаційні методи обробки даних [4, с. 48]. Для нашої держави цей досвід цікавий тим, що влада надає громадськості не просто консультативно-дорадчі компетенції, а закріплює за нею реальні механізми впливу на порушників приватності, тобто суб'єктів, які забезпечують збір та обробку персональних даних.

У Національному звіті США «Захист даних у Сполучених штатах» за 2022 рік зазначаються наступні перспективні форми захисту персональних даних: 1) зобов'язання щодо захисту медичних записів, а також різноманітні вимоги відповідно до Закону про сімейні та медичні відпустки; 2) зобов'язання щодо недискримінації генетичної інформації; зобов'язання щодо захисту інформації про справедливі та точні кредитні операції. Тобто, роботодавці повинні зберігати інформацію про стан здоров'я працівника, генетику, інвалідність, розумне пристосування та позитивні результати аналізів на наркотики в окремому, конфіденційному, безпечному електронному або фізичному файлі і розкривати ці відомості виключно уповноваженим особам [5, с. 46].

Одним із визначальних напрямів забезпечення інформаційної безпеки у США є захист кіберпростору. США формують міжнародні принципи захисту кіберпростору, спираючись на власні індикатори та національні інтереси. Втім, доволі значна робота триває і на внутрішньодержавному рівні. Так, у Національній стратегії кібербезпеки США від 2023 року вказані наступні напрями політики держави: захист критичної інфраструктури; нейтралізація джерел загроз інформаційній безпеці; формування програм для підвищення безпеки та стійкості; інвестування в майбутнє; налагодження міжнародного партнерства; імплементація позитивного досвіду [6]. Слід відзначити комплексність та актуальність окреслених пріоритетних сфер діяльності, що свідчить про чітке розуміння владою США наявних і потенційних загроз.

Натомість, для досвіду США в досліджуваній сфері притаманні окремі негативні аспекти, які слід врахувати Україні. Так, особливістю політики інформаційної безпеки в США є брак наступності та послідовності. Кожна нова президентська адміністрація пропонувала і реалізовувала свої власні тактичні і стратегічні дії [7, с. 68]. На нашу думку, цей недолік свідчить про надмірну політизованість сфери інформаційної безпеки, яка грає не на користь національним інтересам та інтересам особистості. Вбачається, що наслідком цієї політизованості може бути незавершеність окремих ініціатив та нестабільність інформаційної системи держави.

Також варто зазначити, що США визнають неможливість забезпечення інформаційної безпеки в односторонньому порядку. Тому,

важливою складовою стратегії США є міжнародна співпраця з питань забезпечення інформаційної безпеки. У зв'язку з цим США прагнуть реалізувати такі можливості на міжнародному рівні: 1) заохочувати країни посилювати відповідальність за забезпечення безпеки інформаційних систем і мереж; 2) створити правовий режим, необхідний для забезпечення транскордонного доступу до інформації; 3) сформувати режим колективної безпеки в рамках НАТО та інших двосторонніх і багатосторонніх угод зі стратегічними партнерами; 4) зберегти максимально можливу свободу дій в інформаційному просторі для проведення всіх видів інформаційних операцій [8, с. 96]. Зауважимо, що розуміння неефективності одностороннього підходу лише умовно можна назвати недоліком політики США.

Таким чином досвід США у сфері забезпечення інформаційної безпеки є позитивним, і може бути імплементований Україною в частині формування національного інформаційного простору, розбудови механізмів попередження та наукового обгрунтування загроз, створення системи громадського інформаційного врядування, а також утвердження спеціальних владно-розпорядчих інституцій для захисту національних інтересів в інформаційній сфері.

Література

1. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України: дис. … д-ра політ. наук: 23.00.02. Одеса. 2005. 264 с.

2. Кириченко І. Стратегічні імперативи національної інформаційної безпеки адміністрації Б. Клінтона. *Актуальні проблеми міжнародних відносин.* 2011. № 103. С. 165–171.

3. Shawn Marie Boyne Data Protection in the United States. *The American journal of comparative law*. 2018. Vol. 66. P. 299–343.

4. Altman Micha Practical approaches to big data privacy over time. *International Data Privacy Law*. 2018. Vol. 8 (1). P. 29–51.

5. Data protection in the United States: U.S. national report. Robert H. McKinney School of Law. Legal Studies Research Paper. 2022. 52 p.

6. National cybersecurity strategy. March 2023. URL: https://www.whitehouse. gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (date of application: 10.01.2024).

7. Черновол І. Інформаційна безпека США в контексті актуальних загроз і викликів. «Травневі студії 2020: історія, міжнародні відносини»: Збірник матеріалів Міжнародної наукової конференції (м. Вінниця, 24 квітня 2020 р.). Вінниця: ДонНУ імені Василя Стуса. 2020. С. 67–70.

8. Саранча В. І., Шабуніна В. В., Тур О. М. Управління інформаційною безпекою: американський досвід. *Бібліотекознавство. Документознавство. Інформологія.* 2023. № 3. С. 89–98.