РОЗДІЛ VII. АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.95:004.056
DOI https://doi.org/10.24144/2788-6018.2023.06.67

МІЖНАРОДНИЙ ДОСВІД ФОРМУВАННЯ ТА СТАНОВЛЕННЯ ІНСТИТУТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК НЕВІД'ЄМНОЇ СКЛАДОВОЇ СУЧАСНОЇ ДЕРЖАВИ

Батько І.,
асистент кафедри адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»
ORCID: 0000-0002-5561-2747

Павленко Д.,
здобувач вищої освіти
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету «Львівська політехніка»

Батько І., Павленко Д. Міжнародний досвід формування та становлення інституту інформаційної безпеки як невід'ємної складової сучасної держави.

У статті проведено аналіз міжнародного досвіду формування та становлення інституту інформаційної безпеки з огляду на те, що сьогодні інформаційна безпека стала актуальною та нагальною проблемою в сучасному світі, де саме інформація є вкрай важливим ресурсом розвитку та функціонування суспільства. Швидкий технологічний прогрес, зростання кількості даних, їх обмін та зберігання на електронних пристроях викликають не лише нові можливості, але й загрози, зокрема стають небезпечними засобами впливу не тільки на окремих громадян, а й на цілі держави. Відповідно, забезпечення інформаційної безпеки – важливе завдання і для окремих осіб та компаній, і для країн усього світу. Відтак, у процесі формування і вдосконалення інформаційної безпеки вагому роль відіграє міжнародний досвід. Різні країни та організації вже розробили свої підходи до забезпечення інформаційної безпеки, впроваджуючи найкращі практики та вдосконалюючи свої стратегії відповідно до викликів сучасних реалій. Відзначено, що країни, які активно розвивають свої інформаційні технології, мають більш високий рівень захисту інформації. У багатьох країнах прийнято спеціальні закони щодо кібербезпеки, створено відповідні відомства, які відповідають за захист інформації від кібератак та інших загроз. Простежено, що у багатьох країнах ведуться дослідження та розробки нових технологій для захисту інформації від кібератак, таких як квантові комп'ютери та блокчейн-технології. Також з'ясовано, що міжнародний досвід формування та вдосконалення інформаційної безпеки показує, що для досягнення високого рівня захисту інформації потрібно мати спеціалізовані відомства та законодавство, яке регулює цю сферу. Констатовано, що міжнародний досвід формування та вдосконалення інформаційної безпеки свідчить про те, що це питання є надзвичайно важливим і потребує комплексного підходу, який охоплює моніторинг, аналіз та прогнозування ризиків, розробку стратегій та заходів щодо захисту від інформаційних загроз та постійне вдосконалення систем, які забезпечували б інформаційну конфіденційність.

Ключові слова: міжнародний досвід, інформаційна безпека, держава, правові відносини, інформаційне, право, суспільство.

Batko I., Pavlenko D. International experience in the formation and development of the information security institute as an integral component of the modern state.

The article analyzes the international experience of the formation and formation of the information security institute, given that today information security has become an urgent and urgent problem in the modern world, where information is an extremely important resource for the development and functioning of society. Rapid technological progress, the increase in the amount of data, their exchange and storage on electronic devices

cause not only new opportunities, but also threats, in particular, they become dangerous means of influencing not only individual citizens, but also the entire state. Accordingly, ensuring information security is an important task both for individuals and companies, and for countries around the world. Therefore, international experience plays an important role in the process of formation and improvement of information security. Various countries and organizations have already developed their approaches to ensuring information security, implementing best practices and improving their strategies in accordance with the challenges of modern realities. It was noted that countries that are actively developing their information technologies have a higher level of information protection. In many countries, special laws on cyber security have been adopted, and relevant departments have been created that are responsible for protecting information from cyber-attacks and other threats. It has been observed that many countries are researching and developing new technologies to protect information from cyber-attacks, such as quantum computers and blockchain technologies. It was also found that the international experience of forming and improving information security shows that in order to achieve a high level of information protection, it is necessary to have specialized agencies and legislation that regulates this area. It was established that the international experience of the formation and improvement of information security shows that this issue is extremely important and requires an integrated approach that includes monitoring, analysis and forecasting of risks, development of strategies and measures for protection against information threats, and constant improvement of systems that ensure b information confidentiality.

Key words: international experience, information security, state, legal relations, information, law, society.

Вступ. Формування та вдосконалення інформаційної безпеки є актуальною темою для багатьох країн світу, і багато з них активно розробляють та впроваджують відповідні стратегії і підходи. Як визначає Л. Д. Куренда, міжнародна інформаційна безпека є взаємодією акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз [1].

Один із прикладів – Європейський Союз (далі – ЄС), який має значні досягнення у сфері інформаційної безпеки. Початок інформаційної політики ЄС пов'язують з проголошенням 1994 року доктрини Європейського інформаційного суспільства, відомої як доповідь Мартіна Бангемана «Європа і глобальне інформаційне суспільство: рекомендації для Європейського Союзу» [2]. На сучасному етапі особливого значення для держав ЄС набувають питання мережевої та інформаційної безпеки. Європейські фахівці в галузі інформаційних систем, безпеки і стратегічного планування активно обговорюють проблеми, що виникають перед державами Європейського Союзу в умовах можливості застосування інформаційної зброї, тобто засобів спрямованого впливу на інформаційні ресурси ймовірного супротивника у воєнний і мирний час. Сьогодні на практиці реалізуються плани організаційного та технічного забезпечення національної інформаційної безпеки, створюються підрозділи, призначені для відбиття «інформаційної агресії». Уряди беруть на себе роль координаторів міжвідомчих зусиль у цій сфері [3, с. 2]. Наприклад, 2016 року було створено Європейський центр кібербезпеки, який забезпечує моніторинг та аналіз кіберзагроз, співпрацює з пов'язаними із цим сторонами та надає консультаційну допомогу державам-членам ЄС. Також створена Стратегія кібербезпеки ЄС, яка передбачає збільшення співпраці між державами-членами та розвиток інформаційних і кіберзаходів для захисту від кіберзагроз. Окрім того, у ЄС діють різноманітні центри кібербезпеки, які забезпечують координацію зусиль у цій сфері. А ще у країнах Європейського Союзу була прийнята Загальна регламентація про захист персональних даних (GDPR), яка регулює збір та обробку персональних даних у ЄС, забезпечуючи високий рівень захисту цієї інформації. У цьому контексті зауважимо, що, як наголошує О. О. Золотар, правове регулювання питань інформаційної безпеки є складовою частиною системи права окремої держави, а отже, обумовлене особливостями та специфікою такої системи і традиціями нормотворчості [4, с. 5].

Особливою значущістю та ефективністю вирізняється система інформаційної безпеки в Сполучених Штатах Америки, спираючись на достатньо деталізоване, але підпорядковане єдиній стратегії федеральне та місцеве законодавство. Загалом законодавство США у сфері забезпечення інформаційної безпеки є поєднанням федеральних законів та законів штатів, які створюють правову основу для здійснення державної політики у цій сфері.

Аналіз останніх публікацій. З огляду на актуальність задекларованої у темі статті наукової проблеми, її окремі питання досліджували такі українські та зарубіжні вчені: Брюггемен М., Замула О., Захаренко К., Золотар О., Конах В., Куренда Л., Троян С., Черниш В., Цинь Хуан та ін. З огляду на те, **мета статті** полягає у дослідженні міжнародного досвіду формування та становлення інституту інформаційної безпеки як невід'ємної складової сучасної держави.

Виклад основного матеріалу. Досить ґрунтовно в законодавстві США врегульовано питання, які безпосередньо стосуються забезпечення безпеки інформації в державних комп'ютерних системах (Закон «Про комп'ютерну безпеку», Закон «Про удосконалення інформаційної безпеки»), боротьби з комп'ютерною злочинністю (Закон «Про комп'ютерне шахрайство та зловживання», Закон «Про зловживання комп'ютерами»), регулювання співвідношення прав громадян на отримання інформації (Закон «Про свободу інформації», Закон «Про висвітлення діяльності уряду») та конфіденційність їх приватного життя (Закон «Про охорону особистих таємниць»). Адміністративно-організаційне забезпечення інформаційної безпеки в США спрямоване на координацію всіх дій із захисту інформації та проведення єдиної державної політики інформаційної безпеки. Президент США є основною відповідальною особою за забезпечення національної безпеки загалом та інформаційної безпеки зокрема [5, с. 9–10].

Цілком очевидно для багатьох, що США як наддержава можуть ставити перед собою зовсім інші цілі, ніж Україна в рамках своєї політики, що стосується забезпечення безпеки. Ми не можемо розраховувати на ті матеріальні і технологічні ресурси, які використовуються в Сполучених Штатах для забезпечення національної та громадської інформаційної безпеки. Водночас українські спеціалісти можуть перейняти технологічний досвід, а законодавці мають вивчати ті способи нормативного забезпечення інформаційної політики держави, що зарекомендували себе в США як універсальні та доволі ефективні.

Потрібно відзначити, що система інформаційної безпеки в США є надзвичайно багатомірною і складною, а 2018 року було ще створено Національний центр кібербезпеки, який координує дії для захисту від кібератак, проводить аналіз та моніторинг кіберзагроз і співпрацює з різними державними та приватними суб'єктами.

У США створена й Національна стратегія кібербезпеки, яка містить п'ять принципів: захист, виявлення, відповідь, ділення інформацією та відновлення. Для реалізації стратегії було створено Кібербезпековий центр Національного інституту стандартів і технологій США, а також інші центри кібербезпеки, що забезпечують підтримку в розробці стандартів, норм та методик безпеки. Так, наприклад, діє Федеральне агентство з кібербезпеки та інфраструктури (CISA), яке забезпечує захист інфраструктури США від кібератак, промислового шпигунства та інших загроз. Окрім того, у США є закони, що регулюють захист персональних даних громадян та компаній, забезпечуючи високий рівень захисту цієї інформації.

Менш демократично в питаннях, що стосуються інформаційної безпеки, поводиться уряд Китайської Народної Республіки (далі – КНР). В інформаційній політиці Китаю домінують принципи втілення достатньо моноцентричних оборонних і наступальних доктрин. У політичному та безпековому аспекті КНР інформація, як в її соціально-культурному, так і в технологічно-інноваційному вимірах, розглядається насамперед як збройний ресурс, як можливий та вкрай важливий засіб впливу на власних громадян та активного захисту і протидії зовнішнім інформаційним впливам. Застосування такої могутньої і широкої ресурсної бази дозволяє Китаю проводити досить ефективну інформаційну політику, навіть незважаючи на її недемократичну спрямованість. Політика інформаційної безпеки визначає пріоритетними напрямами діяльності держави розробку національних стратегій, які поєднують оборонні і наступальні доктрини для забезпечення національних інтересів і захисту внутрішнього інформаційного середовища та інформаційної інфраструктури, подолання асиметричності інформаційного розвитку щодо інформаційно розвинених країн як потенційних супротивників в інформаційному протистоянні.

Усі структурні складові державної інформаційної політики зумовлені потребою забезпечення національних інтересів шляхом реалізації китайської моделі інформаційного суспільства та специфіки інтеграції КНР у глобальне інформаційне середовище. Уведення стратегії державної інформаційної політики в урядові програми дає змогу Китаю реформувати політичну ідеологію в контексті сучасних тенденцій міжнародного розвитку.

Участь КНР у процесах міжнародної регіональної інтеграції формує стратегію інформаційної політики держави, яка полягає в одночасній інтеграції до світової системи міжнародних відносин і практичній реалізації національної моделі інформаціоналізму як чинника модернізації політичної системи КНР та її потенційного лідерства на регіональному та міжнародному рівнях [6, с. 34].

Отже, Китай реалізує власну модель інформаційної політики, яка охоплює внутрішні проблеми країни, а також регіональні та глобальні геополітичні стратегії. Завдяки цій моделі Китай поступово досягає успіху, перетворюючись на ключового гравця на глобальній геополітичній арені і створюючи значну конкуренцію не тільки Європі, але й Сполученим Штатам Америки [7, с. 84].

У Японії створено Кібербезпековий центр, який забезпечує аналіз кіберзагроз та підготовку рекомендацій для захисту від них. Також тут відбуваються регулярні тренування та навчання з питань кібербезпеки. Японія зосереджує значні зусилля на забезпеченні своєї інформаційної

безпеки. Тамтешні фахівці розробляють та впроваджують стратегії, щоб запобігти кібератакам та іншим загрозам для національної безпеки. Для цього, наприклад, створено Національну агенцію з питань кібербезпеки (NISC), яка координує заходи зі збільшення стійкості системи Японії до кіберзагроз.

Уряд Японії регулярно підписує угоди з іншими країнами, щоб обмінюватись інформацією та забезпечувати безпеку своїх інформаційних мереж. Японія активно бореться зі зростаючими загрозами кібербезпеки, такими як віруси-шифрувальники та фішингові атаки. Уряд забезпечує надійність своїх систем інформаційної безпеки, встановлюючи строгі стандарти зберігання та передачі інформації, а також регулярно тестуючи на стійкість свої системи. Крім того, вони активно працюють над забезпеченням безпеки мереж підприємств, які «тримають» економіку країни, зокрема фінансових установ, енергетичних компаній та транспортних систем [8, с. 15].

Канада створила Національний центр кібербезпеки, який координує заходи щодо кібербезпеки на рівні країни та підтримує співпрацю з іншими країнами.

Уряд Канади створив Міністерство безпеки публічної інформації та кібербезпеки, яке координує діяльність щодо захисту канадських інформаційних мереж та систем. Одним з головних завдань Міністерства є забезпечення безпеки державних інформаційних систем та мереж, що охоплює захист від кібератак та забезпечення безпеки даних. Крім того, Канада активно співпрацює з іншими країнами та міжнародними організаціями, такими як НАТО та Організація з безпеки і співробітництва в Європі (ОБСЄ), щоб зменшити загрози для кібербезпеки та обмінюватись досвідом з іншими країнами. Крім того, Канада також підтримує підприємства та громадян у питаннях кібербезпеки. Уряд Канади надає фінансову й технічну підтримку для розробки і впровадження програм безпеки та надає доступ до інформаційних ресурсів і порад з кібербезпеки.

Загалом, Канада активно діє у глобальному масштабі, щоб забезпечити свою інформаційну безпеку та боротись з кіберзагрозами, які становлять потенційну загрозу для національної безпеки та економіки країни.

Ще відзначимо, що країни, які активно розвивають свої інформаційні технології, мають більш високий рівень захисту інформації. У багатьох країнах прийнято спеціальні закони щодо кібербезпеки, створено відповідні відомства, які відповідають за захист інформації від кібератак та інших загроз.

Інформаційна безпека є однією з найважливіших складових національної безпеки країн-членів НАТО. Оскільки це об'єднання держав, то питання захисту інформації стає особливо актуальним. НАТО зосереджує свої зусилля на багатьох аспектах інформаційної безпеки, зокрема: (а) захист інформації: НАТО забезпечує захист своєї інформації від зловживання, зламу та крадіжки, використовуючи технології шифрування та інші заходи безпеки; (б) боротьба з кіберзлочинністю: НАТО веде активну боротьбу з кіберзлочинністю, яка стала серйозною загрозою для країн-членів; співпрацює зі своїми партнерами для здійснення заходів з попередження кібератак та реагування на них; (в) розвиток кіберзахисту: НАТО підтримує розвиток та збільшення потенціалу кіберзахисту країн-членів; надає фінансову і технічну підтримку для підвищення рівня кіберзахисту національних систем; (г) запобігання дезінформації: НАТО працює над запобіганням дезінформації та пропаганди, яка може викликати недовіру до організації та підривати її роботу. Для цього використовуються різні інструменти, зокрема взаємодія з медіа, соціальними мережами та іншими каналами комунікації.

Висновки. Отже, міжнародний досвід формування та вдосконалення інформаційної безпеки свідчить про те, що це питання є надзвичайно важливим і потребує комплексного підходу, який охоплює моніторинг, аналіз та прогнозування ризиків, розробку стратегій та заходів щодо захисту від інформаційних загроз та постійне вдосконалення систем, які забезпечували б інформаційну конфіденційність. Окрім того, у багатьох країнах ведуться дослідження та розробки нових технологій для захисту інформації від кібератак, таких як квантові комп'ютери та блокчейн-технології.

Загалом можна відзначити, що міжнародний досвід формування та вдосконалення інформаційної безпеки показує, що для досягнення високого рівня захисту інформації потрібно мати спеціалізовані відомства та законодавство, яке регулює цю сферу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Куренда Л.Д. Окремі аспекти забезпечення інформаційної безпеки Європейського Союзу. *Правова інформатика*. 2011. № 3-4. URL: http://ippi.org.ua/kurenda-ld-okremi-aspekti-zabezpechennya-informatsiinoi-bezpeki-%D1%94vropeiskogo-soyuzu (дата звернення: 24.10.2023).
2. Bruggemann M. Information policy and the public sphere: EU communications and the promises of dialogue and transparency. *Javnost – The Public, Journal of the European Institute for Communication and Culture*. URL: https://www.researchgate.net/publication/280810472_Information_Policy_and_the_Public_Sphere_EU_Communications_and_the_Promises_of_Dialogue_and_Transparency (дата звернення: 24.10.2023).

3. Троян С.С. Інформаційно-безпекова політика Європейського Союзу. *Зовнішні справи*. 2019. № 2-3. С. 28–32. URL: http://nbuv.gov.ua/UJRN/zovsp_2019_2-3_7 (дата звернення: 24.10.2023).
4. Золотар О. О. Досвід правового забезпечення інформаційної безпеки в країнах Східного партнерства ЄС (Молдова, Грузія). *Lex Portus.* 2017. № 3. С. 70–80.
5. Конах В.К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) : автореф. дис. … канд. політ. наук / Нац. ін-т стратег. дослідж. Київ, 2005.
6. Хуан Цинь. Інформаційна політика Китайської Народної Республіки в сучасних міжнародних відносинах: дис. … канд. політ. наук: 23.00.03 / Ін-т журналістики Київ. нац. ун-ту ім. Т. Шевченка. Київ, 2007. URL: http://www.disslib.org/informatsiyna-polityka-kytajskoyi-narodnoyi-respliky-v-suchasnykh-mizhnarodnykh.html (дата звернення: 24.10.2023).
7. Захаренко К.В. Міжнародний досвід інформаційної безпеки. *Сучасне суспільство*. 2019. Вип. 4. С. 95–109. URL: https://doi.org/10.34142/24130060.2019.17.1.09 (дата звернення: 24.10.2023).
8. Замула О.А., Черниш В.І. Аналіз міжнародних стандартів у галузі оцінювання ризиків інформаційної безпеки. *Системи обробки інформації*. 2011. Вип. 2. С. 53–56. URL: http://nbuv.gov.ua/UJRN/soi_2011_2_13 (lata звернення: 24.10.2023).