ДОСВІД НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КРАЇНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

ГОНЧАРОВ Микола Вікторович - аспірант кафедри теоретико-правових дисциплін Навчально-наукового інституту права Державного податкового університету

ORCID: https://orcid.org/0000-0003-4452-1652

УДК 340+35.078.3

DOI 10.32782/NP.2023.2.20

У статті розглянуто досвід нормативно-правового забезпечення інформаційної безпеки в країнах Європейського Союзу. Проведений аналіз дозволив виявити, що нормативно-правове забезпечення інформаційної безпеки в цілому, так і на елементному рівні характеризується науковістю, системністю та має багато аспектів.

Нормативно-правове забезпечення є науково обґрунтована, послідовна система правових і інших засобів, за допомогою яких громадянське суспільство та держава здійснює вплив на інформаційні відносини і відносини, безпосередньо пов'язані з розробкою інформаційної безпеки, виходячи з черговості завдань та поставлених цілей, що виникають перед суспільством.

Акцентовано увагу на основних завданнях державної інформаційної політики та з'ясована мета політики забезпечення інформаційної безпеки України, - це формування відкритого інформаційного суспільства, як простору цілісної держави, інтегрованого у світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

На основі досвіду ЄС та його окремих країн у сфері формування та реалізації державної політики інформаційної безпеки з'ясовано, що головними напрямами державної політики інформаційної безпеки є: забезпечення доступу до даних; створення національного інформаційного потенціалу; використання інформаційних ресурсів у національних інтересах; створення загальної системи охорони даних; сприяння міжнародній співпраці у сфері комунікації та інформації; гарантування інформаційного державного суверенітету; розвиток інформаційної інфраструктури, а також доцільність врахування цього досвіду при розробці (корегуванні) законодавства України у цій сфері.

На сьогодні одним із важливих напрямів стратегії нормативно-правового забезпечення інформаційної безпеки України є аналіз та удосконалення нормативно-правового регулювання в цій сфері. Наша держава має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері.

Ключові слова: інформаційна безпека України, забезпечення інформаційної безпеки, національна безпека, система, державна інформаційна політика.

Постановка проблеми

Проблема гарантування інформаційної безпеки держави, суспільства та особистості має комплексний характер і для її розв'язання потрібна ефективна державна політика, спрямована на системне об'єднання на державному рівні законодавчих, організаційних та програмно-технічних засобів.

Створення потужної та ефективної системи інформаційної безпеки України, а також розроблення дієвих стратегій і тактик протидії різним інформаційним загрозам

повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

Для реалізації державної політики в інформаційній сфері слід просувати міжнародні стандарти й інноваційні відкриті ринки, що означає бути готовим до підтримання вільного ринкового середовища, захисту інтелектуальної власності і комерційної таємниці від викрадення, забезпечення верховенства сумісних і безпечних стандартів.

На сьогодні, коли відбулася переоцінка соціально-економічних пріоритетів суспільного розвитку, коли на економічну ситуацію в країні впливають не тільки державні структури влади, але й суб'єктивно-об'єктивні внутрішні та зовнішні обставини, використання цього досвіду набуває пріоритетного значення.

Таким чином, забезпечення інформаційної безпеки в Україні є вирішальним фактором у забезпеченні всіх складових безпеки держави.

Вивчення практики європейських країн у побудові власних моделей правового забезпечення інформаційної безпеки, протидії кіберзагрозам, а також аналіз ряду міжнародних правових документів дає змогу нам резюмувати про відсутність єдиної моделі національної системи правового забезпечення інформаційної безпеки.

Визначившись із зовнішньополітичним курсом, Україна має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері [1, с. 18].

Стан дослідження проблеми

Вивченню цього питання приділяли увагу багато вітчизняних та зарубіжних науковців та дослідників. Зокрема, дослідження нормативно-правового забезпечення інформаційної безпеки знайшли відображення у монографіях українських вчених: О. О. Золотар «Інформаційна безпека людини: теорія і практика» (2018 р.), А. Ю. Нашинець-Наумової «Інформаційна безпека: питання правового регулювання» (2017 р.), О. А. Баранова «Правове забезпечення інформаційної сфери: теорія, методологія і практика (2014 р.), О. О. Тихомирова «Забезпечення інформаційної безпеки як функція сучасної держави», О. А. Заярний «Правове забезпечення розвитку інформаційної сфери України: адміністративно деліктний аспект» (2018 р.) і інших.

Мета дослідження – розглянути досвід нормативно-правового забезпечення інформаційної безпеки в країнах Європейського Союзу.

Виклад основного матеріалу

Наразі Європейський Союз є прикладом становлення та функціонування багаторівневої інформаційної політики та, відповідно, співпрацею вказаних рівнів між собою. Тому для України варто детально проаналізувати механізми формування та реалізації інформаційної політики розвинених країн задля переймання кращих практик та їх імплементації на українську практику.

Аналіз, оцінка та використання позитивних здобутків європейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки, як зазначають В. Шатун та- О. Гладун [2, с. 179], події останніх років у нашій державі показали неспроможність влади адекватно протистояти інформаційним війнам, позаяк проблеми інформаційної політики досі не вирішені на належному рівні.

Активну політику у сфері забезпечення інформаційної безпеки проводить Європейський Союз, який сьогодні об'єднує розвинуті країни, котрі відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах.

1991 року було розроблено «Європейські критерії безпеки інформаційних технологій», де, зокрема, визначено завдання забезпечення інформаційної безпеки, а саме: захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

У 1996 році стандарти європейської інформаційної безпеки було втілено у «Єдиних критеріях безпеки інформаційних технологій» [3], де застосовано модель тріади CIA (CIA Triad), яка передбачає такі основні характеристики інформаційної безпеки: конфіденційність; цілісність; доступність [4, с. 43].

Протягом останніх років Великобританія доклала чимало зусиль для систематизації законодавчої бази. Незабаром заплановано за допомогою консолідації нормативно-правових актів у різноманітних правових сферах проведення реформ у системі права Великобританії в напрямку його кодифікації.

Політичний курс Великобританії в галузі інформаційної політики задекларовано в національній програмі «The Government's Policy for the Information Age», якою передбачається всебічний розвиток електронної комерції для забезпечення економічного зростання, розвиток телекомунікаційного ринку країни, впровадження інформаційних та комунікаційних технологій в усі сфери життєдіяльності суспільства [5, с. 98].

У Великобританії діє Закон про захист даних, який контролює, як особисті дані людини використовуються організаціями, підприємствами або урядом. Кожна особа, відповідальна за використання персональних даних, повинна дотримуватися суворих правил, які називаються «принципами захисту даних».

Вони повинні переконатися, що інформація справедливо, законно і прозоро використовується для визначених, явних цілей; зберігається не довше, ніж це необхідно; обробляється таким чином, що забезпечує відповідну безпеку, включаючи захист від незаконної або несанкціонованої обробки, доступу, втрати, знищення або пошкодження [6].

Водночас Великобританія схвалила Стратегію кібербезпеки, яка визначає суттєвий набір цілей, дій та показників, які відображаються у трьох важливих стовпах: 1. Захист: Уряд зміцнить власні засоби захисту інформації та працюватиме з промисловістю, щоб забезпечити захист британських мереж, даних і систем від кіберзагроз. 2. Утримання: Великобританія зміцнить спроможність правоохоронних органів збільшити вартість кіберзлочинності. 3. Розвиток: Уряд допоможе розвивати критичні можливості Великобританії, включаючи кібернавички, а також зростаючу індустрію кібербезпеки країни, щоб не відставати від кіберзагроз [7].

Отже, метою державної інформаційної політики у Великобританії є покращення умов конкурентної боротьби в інформаційній сфері, посилення ефективності інформаційних послуг та запровадження інформаційних технологій у сферу державного управління.

На сьогодніі великої актуальності набуває проведення контролю над інформаційними даними зі сторони держав. На фоні цієї проблематики відбуваються інформаційні війни, у яких важливе значення відіграє сама інформація. Водночас самій Великобританії та організації інформаційної безпеки в державі властива певна консервативність.

Інформаційна політика Німеччини включає концепцію вільного транскордонного обміну інформацією, вільного вираження поглядів, розвитку комунікаційних та інформаційних мереж і систем, вільної конкуренції в інформаційній сфері, створення відповідно до нових політичних, економічних та інформаційних змін у німецькому суспільстві норм і принципів правового регулювання інформаційної діяльності.

Ще в 1996 р. було прийнято Програму федерального уряду Info-2000 (Germany's Way the Information Society) («Німецький шлях до інформаційного суспільства»). Нові політичні пріоритети, медіаконцентрація, упровадження сучасних технологій в організацію федерального й місцевого управління, розвиток інформаційного бізнесу обумовили нову стратегію національної інформаційної політики ФРН, головними напрямами якої визнано становлення інформаційного суспільства в Німеччині, створення інформаційної економіки, розвиток нових інформаційних супермагістралей, інформатизацію державного управління, лібералізацію телекомунікацій, підтримку національних виробників електронної продукції та одно-

часний розвиток державного й приватного інформаційного бізнесу [5, с. 99].

Концепція інформаційної політики Німеччини визначає безперешкодний транскордонний обмін інформацією і свободу слова та совісті; розвиток інформаційно-комп'ютерних технологій і 66 телекомунікаційних мереж; вільну конкуренцію в інформаційній сфері; створення відповідно до нових політичних та економічних умов певних норм і принципів правового регулювання інформаційної діяльності в німецькому суспільстві [8, с. 40].

У 1997 році у ФРН прийнято Закон «Про основи надання інформаційних та комунікаційних послуг», який регламентує вимоги захисту інформації лише в інформаційно-телекомунікаційних мережах загального користування [9].

Важливість захисту автоматизованих мереж технологічного управління об'єктів економіки, інших потенційно небезпечних об'єктів ФРН або так званої «критичної інфраструктури» було визначено у Німеччині на законодавчому рівні в 2009 році.

Так, Законом ФРН «Про посилення безпеки інформаційних систем» на Федеральне відомство безпеки інформаційних систем (BSI) ФРН покладено завдання попередження, реагування на інциденти, викликані кібернетичними загрозами, управління та координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема у взаємодії із приватним сектором [10].

Стратегія забезпечення кібернетичної безпеки ФРН зосереджується на десяти стратегічних напрямках: захист критично важливих інформаційних інфраструктур; захист IT-систем у Німеччині; посилення інформаційної безпеки в державному управлінні; створення національного центру кіберреакції; створення національної ради з кібербезпеки; проведення ефективного контролю за злочинністю у кіберпросторі; проведення ефективних скоординованих дій для забезпечення кібербезпеки в Європі і в усьому світі; використання надійних інформаційних технологій; розвиток персоналу у федеральних органах влади; інструменти для реагування на кібератаки [9].

Крім того, особливу увагу у напрямі забезпечення захисту інформаційних систем займає захист особистої інформації громадян під час її обміну засобами електронної пошти. Стратегією визначено впровадження цільових пільг і державної підтримки німецьким розробникам сертифікованих засобів захисту інформації, що призначені для масового використання [11, с. 28].

Інформаційна політика Франції є складовою державної стратегії розвитку країни, стратегії франкофонії та збереження національної самобутності й ідентичності, компонентом зовнішньої політики, участі Франції в інформаційних програмах і проєктах міжурядових європейських організацій, створення інформаційної економіки та поширення комп'ютерних мереж і систем, інформаційних послуг [5, с. 100].

Мета інформаційної політики Франції – розвиток інформаційних магістралей, електронного ринку і банківської сфери, лібералізація комунікацій, реформування інформаційного законодавства, стимулювання наукових досліджень у галузі, створення систем безпеки інформації і запобігання комп'ютерним злочинам.

Стратегія інформаційної політики Франції стосується також франкомовних країн Африки, Азії, Латинської Америки. У контексті глобалізації комунікацій і просування національних інтересів уряд створив Фонд допомоги і співробітництва для підтримки впровадження вітчизняних інформаційних технологій.

Французька національна стратегія кібербезпеки передбачає такі стратегічні цілі: стати кіберохороною державою у кіберзахисті; забезпечити здатність Франції ухвалювати рішення шляхом захисту інформації, пов'язаної з її суверенітетом; посилити кібербезпеку національних інфраструктур; забезпечити безпеку в кіберпросторі.

Для досягнення цих цілей було визначено сім сфер діяльності: ефективно передбачати та аналізувати навколишнє середовище, щоб прийняти відповідні рішення; виявляти та блокувати атаки, оповіщення та підтримку потенційних жертв; посилити наукові, технічні, промислові і людські можливості для підтримки незалежності країни;

захистити інформаційні системи держави та операторів для забезпечення кращої національної стійкості; адаптувати французьке законодавство до врахування технологічних розробок і нових практик; розробити ініціативи міжнародної співпраці у сфері інформаційної системи безпеки, кіберзахисту і боротьби з кіберзлочинністю з метою кращого захисту національних інформаційних систем; спілкуватися, інформувати та переконувати, щоб збільшити розуміння населення масштабів викликів, пов'язаних з інформаційними системами безпеки [12].

Проаналізувавши загальні аспекти розвитку інформаційної політики найбільш розвинених країн світу, можна констатувати, що цей вид політики направлений на формування єдиного інформаційного простору та впроваджується шляхом втілення програм та проєктів різних міжнародних організацій. Окрім того, у рамках міжнародних стратегій розглядається питання розвитку інформаційного суспільства та телекомунікаційних мереж у Європейських країнах. Важливо зауважити, що Україні доцільно запозичити найкращі світові практики та намагатися їх впровадити на українську практику.

Висновки

На основі досвіду ЄС та його окремих країн у сфері формування та реалізації державної політики інформаційної безпеки з'ясовано, що головними напрямами державної політики інформаційної безпеки є: забезпечення доступу до даних; створення національного інформаційного потенціалу; використання інформаційних ресурсів у національних інтересах; створення загальної системи охорони даних; сприяння міжнародній співпраці у сфері комунікації та інформації; гарантування інформаційного державного суверенітету; розвиток інформаційної інфраструктури, а також доцільність врахування цього досвіду при розробці (корегуванні) законодавства України у цій сфері.

Подальша розробка національної правової бази, її гармонізація з міжнародними інституціями, тобто приведення необхідних відносин у сфері інформації у відповідність до міжнародних стандартів, без сумніву, сприятиме зміцненню інформаційної безпеки України та зростанню її міжнародного авторитету як демократичної і правової держави.

Постала також необхідність розробити нові інструменти, передусім аналітично оцінного спрямування, що можуть на ранніх етапах прогнозувати та запобігати негативним наслідкам загроз інформаційній безпеці і відповідно можливим збиткам для суспільства й держави.

Україна має використовувати досвід розвинутих країн, що певною мірою мають напрацювання у сфері забезпечення інформаційної безпеки, зокрема досвід Європейського Союзу.

Література

1. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 42. 2017. С.16–22.

2. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». 2016. Т. 267. Вип. 255. С. 174–180.

3. Common Criteria for Information Technology Security Evaluation. URL:https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf

4. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45.

5. Рябоконь О. Державна інформаційна політика з формування інформаційного суспільства: зарубіжний досвід. Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2016. Вип. 43. С. 97–114.

6. The Data Protection Act [Електронний ресурс]. URL: https://www.gov.uk/data-protection (дата звернення 27.03.2023).

7. National cyber security strategy 2016-2021. URL: https://www.cipfa.org/~/media/files/services/ccfc/hm%2520government%2520national%2520cyber%2520security%2520strategy%25202016%25202021.pdf+&cd=7

&hl=ru&ct=clnk&gl=ua (дата звернення 27.03.2023).

8. Брижко В. До питання сучасної інформаційної політики. Вісник Академії управління МВС. 2009. № 2. С. 27–47.

9. Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) vom 20.12.1990. URL: http://www.gesetze-iminternet.de (дата звернення 27.03.2023).

10. Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14.08.2009. URL: https://www.bsi.bund.de (дата звернення 27.03.2023).

11. Чернухін І. О. Досвід Федеративної республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави. 2014. № 1 (14). С. 27–43.

12. Information systems defence and security. France's strategy. URL: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02- 15_Information_system_defence_and_security_-_France_s_strategy.pd (дата звернення 27.03.2023).

Honcharov M. V.

EXPERIENCE OF REGULATORY AND LEGAL PROVISION OF INFORMATION SECURITY IN THE COUNTRIES OF THE EUROPEAN UNION

The article examines the experience of regulatory and legal provision of information security in the countries of the European Union. The conducted analysis made it possible to reveal that the regulatory and legal provision of information security in general, as well as at the elemental level, is characterized by scientificity, systematicity and has many aspects.

Regulatory and legal support is a scientifically based, consistent system of legal and other means by which civil society and the state exert influence on information relations and relations directly related to the development of information security, based on the sequence of tasks and set goals that arise before society

Attention is focused on the main tasks of the state information policy and the goal of the information security policy of Ukraine is clarified, which is the formation of an open information society, as a space of an integral state, integrating into the world information space, taking into account national characteristics and interests in ensuring information security at the domestic and international level. levels

Based on the experience of the EU and its individual countries in the field of formation and implementation of the state information security policy, it was found that the main directions of the state information security policy are: ensuring access to data; creation of national information potential; use of information resources in national interests; creation of a general data protection system; promotion of international cooperation in the field of communication and information; guarantee of information state sovereignty; the development of information infrastructure, as well as the expediency of taking this experience into account when developing (adjusting) the legislation of Ukraine in this area.

Today, one of the important directions of the strategy of regulatory and legal provision of information security of Ukraine is the analysis and improvement of regulatory and legal regulation in this area. Our state should focus primarily on the **d**evelopment strategy of the European Union member states in the information field.

Keywords: information security of Ukraine, provision of information security, national security, system, state information policy.