УДК 355.451:004.7
DOI https://doi.org/10.32782/2524-0374/2021-4/56

КІБЕРБЕЗПЕКА ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

CYBERSECURITY AS AN ELEMENT OF INFORMATION STATE SECURITY

Лахтадир С.Л., старший науковий співробітник
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

Статтю присвячено дослідженню сутності та ознак кібербезпеки та з'ясуванню її ролі у сфері правового регулювання суспільних інформаційних відносин в Україні. У статті обґрунтовано, що питання забезпечення кібербезпеки в Україні є надзвичайно актуальним на тлі гібридної війни, що триває. Однак на сьогодні в нашій державі заходи з протидії викликам і загрозам у зазначеній сфері перебувають на початковому етапі та не мають комплексного характеру для подолання таких загроз. Прийняття спеціального законодавчого акта щодо кібербезпеки дозволить, окрім закріплення спеціальної термінології, визначити правові та організаційні засади державної політики в цій сфері, основні принципи та напрями забезпечення кібербезпеки. Аргументується, що державна політика у сферах національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Зроблено висновок, що правові норми, спрямовані на забезпечення національної кібербезпеки як пріоритетного напряму реалізації національної політики України, мають публічно-правову природу і становлять міжгалузевий правовий інститут у системі права України, який регулює інформаційні суспільні відносини в секторах національної інформаційної безпеки, виборчої системи, медицини, оборони, транспорту, фінансово-банківської сфери тощо та забезпечує інформаційний суверенітет держави як суб'єкта міжнародного права загалом.

У подальшому перспективними напрямами досліджень кібербезпеки як правової категорії стане розробка структури цієї категорії та її взаємозв'язок з іншими правовими категоріями в галузі інформаційного права. Особливо актуальним питанням, яке потребуватиме подальшого правового забезпечення, стане сфера та технології застосування штучного інтелекту в державному управлінні та судочинстві, що не лише допоможе здійснити квантовий стрибок у цьому напрямі, а й несе великі ризики у сфері інформаційної безпеки держави.

Ключові слова: інформація, кібербезпека, інформаційне суспільство, інформаційна безпека, гібридна війна, кіберпростір, пандемія.

The article deals with the study of the essence and features of cybersecurity and finding out its role in the field of legal regulation of social information relations in Ukraine. The article substantiates that the issue of providing cybersecurity in Ukraine is extremely relevant considering the current hybrid war. However, nowadays in our country, measures to counteract the challenges and threats in this area are at an initial stage and do not have a comprehensive nature to overcome such threats. Adoption of a special legislative act on cyber security will allow, except for the consolidation of special terminology, to determine the legal and organizational principles of state policy in this area, the basic principles and directions to provide cyber security. It is stated that state policy in the spheres of national security and defense is directed to ensure military, foreign policy, state, economic, informational, environmental safety, cybersecurity of Ukraine, etc. It is concluded that legal norms aimed at providing national cybersecurity as a priority direction of the implementation of national policy of Ukraine have public and legal nature and constitute an inter-sectoral legal institute in the system of law of Ukraine, which regulates information social relations in the sectors of national information security, electoral system, medicine, defense, transport, financial and banking sphere, etc. and provides information sovereignty of the state as a subject of international law as a whole.

In the future, prospective directions of cyber security research as a legal category will include the development of the structure of this category and its interconnection with other legal categories in the field of information law. The scope and technologies of applying artificial intelligence in public administration and legal proceedings will become a particularly relevant issue that will require further legal support, which is supposed not only to help to carry out a quantum leap in this direction, but will also bear great risks in the field of information security.

Key words: information, cybersecurity, information society, information security, hybrid war, cyberspace, the pandemic.

Актуальність дослідження. Транскордонний характер кіберпростору, його залежність від складних інформаційних технологій, активне використання електронних майданчиків і сервісів кіберпростору, які охоплюють майже всі сфери суспільного життя, визначають нові можливості, але при цьому й розвивають нові загрози правам, інтересам і життєдіяльності особистості, організації, діяльності державних органів; проведення кібератак проти інформаційних ресурсів з боку кіберзлочинців і кібертерористів; використання кіберзброї в рамках спеціальних операцій і кібервійн, зокрема тих, що супроводжують традиційні бойові дії.

Огляд останніх досліджень і публікацій. Теоретичною базою для вирішення поставленої проблеми стало компаративне дослідження національного та міжнародного законодавства щодо інформації з метою пошуку істотних ознак кібербезпеки як новітнього правового явища. Оскільки понятійно-категоріальний апарат цієї проблематики характеризується поліваріантністю тлумачення авторських дефініцій, постала необхідність також звернення до наукових напрацювань зарубіжних учених. Так, наукові теоретичні засади інформаційної безпеки держави були предметом уваги таких вітчизняних і зарубіжних дослідників, як: І.В. Арістова [1], І.Л. Бачило [2], В.В. Волинець [3], В.І. Гурковський [4], І.В. Діордіца [5], І.А. Кисарець [6], В.А. Ліпкан [7], А.І. Марущак [8], В.Я. Настюк [9], Г.П. Несвіт [10], С.В. Петров [11], Ю.В. Романчук [12], І.М. Сопілко [13], К.Г. Татарникова [14], В.С. Цимбалюк [15], О.В. Шепета [16] та ін. Разом з цим сутність кібербезпеки як елемента інформаційної безпеки до цього часу на доктринальному рівні не досліджено, що потребує детального правового аналізу.

Мета статті – з'ясування сутності та ролі кібербезпеки як елемента інформаційної безпеки держави, а також визначення місця правових норм у сфері забезпечення кібербезпеки в системі права України.

Виклад основного матеріалу. Виділяючи властивість нормативності й розглядаючи її як визначальну, найбільш загальну в складі всього комплексу властивостей права, необхідно передусім звернутися до визначення цього терміна. Нормативність – властивість права, що виявляє його зміст і призначення; у нормативності виявляється потреба затвердження в суспільних відносинах нормативних начал, пов'язаних із забезпеченням впорядкованості суспільного життя, руху суспільства до свободи, згоди й компромісу в суспільному житті, захищеного статусу автономної особистості, її прав і свободи поведінки. Право під певним кутом зору може бути схарактеризоване як «система норм», тобто загальних правил, зразків, моделей поведінки, які поширюються на всі випадки подібного роду й відповідно до яких має будуватися поведінка всіх осіб, які потрапили в нормативно регламентовану ситуацію. При цьому найістотніше полягає в тому, що праву, якщо розглядати його з глибоких інституційних позицій,

властива нормативність особливої якості. Це нормативність, що має характер загальності: якщо загальні правила є такими для всієї країни, то нормативність виступає як нормативність загальнообов'язкова.

Під нормативністю відносно права загалом слід розуміти щось більш юридично глибоке й більш соціально значуще, безпосередньо пов'язане з власною цінністю права. Нормативність у зазначеному сенсі позначає, що право за допомогою загальних правил реалізує потребу суспільства в утвердженні нормативних начал і тому охоплює всі сфери соціального життя, які потребують юридичного регулювання. Причому так, що в ньому не повинно залишатися «лакун», у яких могли б отримати притулок свавілля й беззаконня – соціальні антиподи права.

Реальні прояви кібератак мало прогнозовані, а їхнім результатом є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки й оборони. У зв'язку з цим реальні загрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. Питання забезпечення кібербезпеки є надзвичайно актуальними і для України. Однак у нашій державі заходи з протидії викликам і загрозам у зазначеній сфері перебувають на початковому етапі та не мають комплексного характеру. Прийняття законодавчого акта щодо кібербезпеки дозволить, окрім термінології, визначити правові та організаційні засади державної політики в цій сфері, основні принципи та напрями забезпечення кібербезпеки [17].

Державна політика у сферах національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо й регламентується Законом України «Про національну безпеку України» від 21 червня 2018 р. № 2468-VIII [18]. Національна інформаційна безпека є комплексним поняттям, яке по-різному розкривається в різних публічних документах, навчальних посібниках, статтях експертів. Вона не обмежується тільки інформаційною безпекою держави, її органів, сфер оборони та внутрішньої політики. Доктрина інформаційної безпеки об'єктом захисту розглядає збалансовані інтереси особистості, суспільства й держави. Без охорони інформаційних інтересів особистості і громадянина неможливо сприйняття держави як суб'єкта суспільного договору й носія суверенітету, а без цього у свою чергу неможливий захист громадян. Зміст поняття передбачає також захист інформаційної інфраструктури, який здійснюється програмними, фізичними й технічними засобами, забезпечення безпеки наукових розробок і ноу-хау. Таким чином, під національною безпекою в цифровому просторі, що включає забезпечення інформаційної безпеки особистості, суспільства, держави та інфраструктури, розуміється стан захищеності інформаційного середовища, що гарантує дотримання прав і законних інтересів особистості, суспільства й держави в інформаційній сфері, коли забезпечуються їхній захист, реалізація й можливості розвитку незалежно від кількості та якості внутрішніх і зовнішніх загроз.

Стратегія кібербезпеки України (Стратегія) – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави. Стратегія виступає документом довгострокового планування, у якому визначено пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки й оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів. Організація підготовки Стратегії кібербезпеки України здійснюється за дорученням Президента України Національним координаційним центром кібербезпеки після затвердження Стратегії національної безпеки України. Стратегія кібербезпеки України схвалюється рішенням Ради національної безпеки й оборони України та затверджується указом Президента України. Цей документ виступає основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України.

Реалізація Стратегії кібербезпеки України здійснюється на основі національного оборонного, безпекового, економічного, інтелектуального потенціалу з використанням механізмів державно-приватного партнерства, а також із залученням міжнародної консультативної, фінансової, матеріально-технічної допомоги.

У науковій доктрині запропоновано формування аргументації окремої кібернетичної функції держави для реалізації самостійного і пріоритетного напряму державної кібербезпекової політики, який здійснюється за допомогою кібернетичних засобів для досягнення кібернетичного суверенітету, вільного та безпечного розвитку кіберсуспільства в рамках національного сегменту кіберпростору конкретної держави, зокрема для захисту прав, свобод і законних інтересів людини і громадянина у сфері кібербезпеки; виступає формою досягнення інших цілей суспільства й держави в найбільш важливих сферах життєдіяльності [19, с. 36]. Під кібербезпековою політикою розуміється системна діяльність держави з протидії інформаційним загрозам, що розповсюджуються через кібернетичний простір, координація діяльності всіх державних і недержавних структур, задіяних у забезпеченні кібернетичної безпеки, убезпеченні від можливих протиправних дій у цій сфері тощо [19, с. 89]. Стрімке збільшення обороту різноманітної інформації (включаючи комерційну інформацію, інформацію про нові технології, інформацію в складі баз даних), глобалізація доступу до неї і поява нових засобів її формування, поширення й використання актуалізували питання збереження й легального використання масивів інформації.

Інформаційна безпека виходить за рамки потреб окремих власників і виступає вже одним із напрямів національних стратегій розвитку. Наприклад, Національна стратегія інтелектуальної власності, прийнята в КНР у 2013 році на п'ятирічний період, визначила кілька головних цілей: (1) заохочення створення інтелектуальної власності, тобто підвищення якості прав інтелектуальної власності та інноваційної ефективності, поліпшення оцінки патентів, товарних знаків, авторських прав, нових сортів рослин і ін., вдосконалення системи оцінки ефективності, заохочення творців ІР і перехід від кількості до якості і значення ІР для модернізації; (2) посилення впливу ІР у ключових галузях економіки через державне планування використання ІС у стратегічних нових галузях промисловості із застосуванням преференційної експертизи патентних заявок на винаходи в цих галузях і новітніх технологіях (зокрема енергозбереження та охорони навколишнього середовища, інформаційних технологій нового покоління, біології, виробництва високоякісного обладнання, нової енергії, нових матеріалів, а також технологій, що підтримують зелений розвиток, таких як низьковуглецеві та ресурсозбережувальні технології); (3) сприяння впровадженню ІР за допомогою зміцнення ключової ролі у вико-

ристанні ІР підприємствами й поліпшення комерціалізації нового покоління прав ІВ у комунікаційних технологіях, трансферу прав на технології військового та цивільного призначення, поліпшення менеджменту ІС, застосування фінансових інструментів використання ІС (заставу і кредит прав ІВ), прав на ліцензії, прав у статутних капіталах та інших активів; (4) посилення захисту ІР шляхом удосконалення законодавства й оцінки ефективності захисту ІС, підвищення ефективності судового захисту прав інтелектуальної власності та потенціалу адміністративного правозастосування, включаючи міжнародні суперечки; (5) підвищення ефективності управління ІС, включаючи інформаційні, сервісні та юридичні й патентні послуги з просування патентів, товарних знаків, авторських прав, правову оцінку ІС; (6) розвиток культури поводження ІС.

З урахуванням розробленої Національної стратегії кібербезпеки у Великобританії зараз тестується нова форма взаємодії держави і приватного бізнесу у сфері інформаційної безпеки – Партнерство з обміну інформаційної безпеки (Cybersecurity Information Sharing Partnership («CISP»)). CISP покликана встановити нове «захищене середовище» обміну й отримання інформації між державними органами і приватним бізнесом. Сучасне законодавство Великобританії вже зобов'язує всіх операторів даних застосовувати відповідні технічні та організаційні заходи проти незаконної обробки даних, а у випадках серйозного порушення інформаційної безпеки можуть накладатися грошові штрафи в розмірі до £ 500 000. Крім того, фінансові компанії зобов'язані виконувати додаткові нормативні вимоги, включаючи організацію систем і засобів контролю дотримання правил фінансових операцій [20, с. 64].

Контртерористичне управління Організації Об'єднаних Націй здійснює ряд ініціатив в галузі нових технологій. Наша Програма з кібербезпеки й нових технологій спрямована на зміцнення потенціалу держав-членів у галузі запобігання та пом'якшення наслідків неправомірного використання таких технічних досягнень. Вона передбачає протидію загрозі кібератак, що здійснюються терористичними організаціями на критично важливу інфраструктуру, а також заохочення використання соціальних мереж для збору інформації з відкритих джерел і цифрових доказів з метою протидії онлайновому тероризму й насильницькому екстремізму при дотриманні прав людини. Фахівці Програми також ділилися своїми експертними знаннями з використання безпілотних літальних апаратів на міжнародних форумах і розробляють інші проєкти в цій галузі. Цей проєкт також спрямований на пом'якшення наслідків атак на окремі системи і їх відновлення після нападу.

У ході проведення шостого огляду Глобальної контртерористичної стратегії Організації Об'єднаних Націй держави-члени висловили «стурбованість з приводу того, що в умовах глобалізованого суспільства терористи і їхні прихильники все ширше використовують інформаційно-комунікаційні технології, зокрема Інтернет та інші засоби інформації, для пропаганди терористичних актів, їх здійснення, підбурювання до їх вчинення, вербування їхніх виконавців і їх фінансування або планування». Держави-члени ООН наголосили на важливості співпраці зацікавлених сторін у здійсненні Стратегії, зокрема між державами-членами, міжнародними, регіональними та субрегіональними організаціями, приватним сектором і громадянським суспільством. У резолюції № 2341 (2017 р.). Рада Безпеки ООН закликає держави встановити або зміцнити національні, регіональні та міжнародні партнерські відносини із зацікавленими сторонами – державними і приватними – згідно з обставинами з метою обміну інформацією та досвідом і тим самим запобігання терористичних нападів на критично важливі об'єкти інфраструктури, забезпечення захисту від них, пом'якшення їхніх наслідків, їх розслідування, реагування на них і відновлення після заподіяної ними шкоди, зокрема шляхом проведення спільних навчальних заходів та застосування або створення відповідних мереж зв'язку або екстреного оповіщення [21]. Що стосується досвіду Європейського Союзу в правовому забезпеченні кіберпростору, то останнє регламентовано Директивою про кібербезпеку, на основі якої кожна держава-член Євросоюзу має прийняти власну стратегію мережевої та інформаційної безпеки («NIS»). Відповідальність за забезпечення безпеки мережевих та інформаційних систем лежить значною мірою на операторах основних послуг та надавачах цифрових послуг (Регламент Європейського Парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних)) [22]. Однак цей Регламент не застосовують до питань захисту фундаментальних прав і свобод або вільного потоку персональних даних, пов'язаних з діяльністю поза межами законодавства Союзу, наприклад, діяльністю щодо національної безпеки. Сфера застосування правових норм, спрямованих на забезпечення кібербезпеки держави, становить інститут публічного права й має публічно-правову природу.

Висновки. Державна політика у сферах національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Правові норми, орієнтовані на забезпечення національної кібербезпеки як пріоритетного напряму реалізації національної політики України, мають публічно-правову природу й становлять міжгалузевий правовий інститут у системі права України, який регулює інформаційні суспільні відносини в секторах національної інформаційної безпеки, виборчої системи, медицини, оборони, транспорту, фінансово-банківської сфери тощо та забезпечує інформаційний суверенітет держави як суб'єкта міжнародного права загалом. Прийняття спеціального законодавчого акта щодо протидії кібербезпеки дозволить, окрім закріплення спеціальної термінології, визначити правові та організаційні засади державної політики в цій сфері, основні принципи та напрями забезпечення кібербезпеки.

Подальшими перспективними напрямами досліджень кібербезпеки як правової категорії стане розробка структури цієї категорії та її взаємозв'язок з іншими правовими категоріями в галузі інформаційного права. Особливо актуальним питанням, яке потребуватиме подальшого правового забезпечення, стане сфера та технології застосування штучного інтелекту в державному управлінні та судочинстві, що не лише допоможе здійснити квантовий стрибок у цьому напрямі, а й несе собою великі ризики у сфері національної інформаційної безпеки.

ЛІТЕРАТУРА

1. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: дис. ... д-ра юрид. наук: 12.00.07. Харків, 2002. 408 с.

2. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник / под ред. Б.Н. Топорнина. Санкт-Петербург: Юридический центр Пресс, 2001. 787 с.

3. Волинець В.В. Проблеми правового забезпечення інформаційної функції держави у сучасній Україні. *Юридична Україна.* 2012. № 10. С. 4–10.

4. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис. ... канд. юрид. наук з держ. упр.: 25.00.02. Київ, 2004. 225 с.

5. Діордіца І.В. Кібербезпекова політика України: стан та пріоритетні напрями реалізації: монографія. Запоріжжя: Видавничий дім «Гельветика», 2018. 548 с.
6. Кисарець І.А. Політико-культурна парадигма державної інформаційної політики: дис. ... канд. політ. наук: 23.00.03. Київ, 2008. 195 с.
7. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення: монографія. Київ: Текст, 2003. 180 с.
8. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності: навч. посіб. Київ: Скіф; КНТ, 2008. 344 с.
9. Настюк В.Я. Адміністративно-правові режими у сфері національної безпеки та протидії тероризму: монографія. Київ, 2008. 245 с.
10. Несвіт Г.П. Інформаційна політика держави як чинник реформування суспільства: дис. ... канд. політ. наук: 23.00.02. Одеса, 2001. 193 с.
11. Петров С.В. Адміністративно-правове забезпечення реалізації права громадян на інформацію: дис. ... канд. юрид. наук: 12.00.07. Запоріжжя, 2013. 196 с.
12. Романчук Ю.В. Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти: автореф. дис. ... канд. політ. наук: 23.00.04. Київ, 2009. 20 с.
13. Сопілко І.М. Інформаційні правовідносини за участю органів державної влади України: монографія. Київ: Леся, 2013. 220 с.
14. Татарникова К.Г. Кодифікація законодавства України про інформацію: дис. ... канд. юрид. наук: 12.00.07. Київ, 2014. 212 с.
15. Цимбалюк В.С. Інформаційне право (основи теорії і практики): монографія. Київ: Освіта України, 2010. 388 с.
16. Шепета О.В. Адміністративно-правові засади технічного захисту інформації: монографія. Київ: О.С. Ліпкан, 2012. 296 с.
17. Аналітична записка щодо законопроєкту «Про основні засади забезпечення кібербезпеки України». URL: www. inau. org. ua/ download. php?bd189ae6a731113f59c7d7fcacf193f3 (дата звернення: 11.03.2021).
18. Про національну безпеку України: Закон України від 21.06.2018 р. № 2468-VIII. *Офіційний вісник України.* 2018. № 55. Ст. 1903.
19. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України: дис. на здоб. наук. ступ. докт. юрид. наук: 12.00.07. Запоріжжя, 2018. 521 с.
20. Карцхия А.М. Кибербезопасность и частная собственность. Часть 1. *Вопросы кибербезопасности.* 2014. № 1. С. 61-66.
21. Кибербезопасность. Контретеррористическое управление ООН. URL: https://www.un.org/counterterrorism/ru/cct/programme-projects/cybersecurity (дата обращения: 20.02.2021).
22. Загальний регламент про захист даних. *Офіційний вісник Європейського Союзу.* 06.05.2006. L 119/1. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 12.03.2021).