УДК 341.123 (045)
DOI https://doi.org/10.32850/sulj.2022.4.1.35

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ З УРАХУВАННЯМ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

Зуй В. В.

У даній науковій статті проаналізовано чинне законодавство щодо регулювання питання з організації кібернетичної безпеки (оборони), сформульовано та запропоновано шляхи вирішення наявних проблем. Водночас висвітлено адміністративну відповідальність у даній сфері.

Зокрема, звернено увагу на курс України до європейської інтеграції для формування належних основ правового регулювання підтримки безпеки інформаційного простору в Україні. Зазначено, що 23 червня 2022 року країни члени Європейського Союзу проголосували за надання Україні статусу країни кандидата на вступ до Європейського Союзу.

Метою дослідження є актуальні проблеми кібербезпеки (оборони), законодавче регулювання участі органів виконавчої влади у цьому, новації щодо європейської інтеграції.

Також проаналізовано правові конструкції: кібербезпека (оборона), кіберпростір, інформаційна безпека. Можемо сказати, що кібербезпека охоплює всі аспекти безпеки, що стосуються кіберпростору, а інформаційна безпека – це безпека інформації незалежно від сфери застосування. Під кіберпростором закон пропонує розглядати «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних». Перевагою даного визначення є те, що воно акцентує на «комунікативності» кібернетичного простору (тобто, зокрема, його здатності транслювати (передавати) шкідливі програмні конструкції, що виступають інструментами кібератак).

Так, кібербезпека забезпечуватиме поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів та засоби забезпечення кібербезпеки з усталеною практикою ЄС і НАТО, вжиття інших заходів, погоджених із ключовими іноземними партнерами, спрямованих на посилення кіберстійкості України.

Погодимося, що наразі існує проблема недосконалості законодавства у сфері кібербезпеки, застарілість інформаційно-правових норм, недостатній рівень стягнень за інформаційні правопорушення, повільне застосування положень європейського законодавства в даній сфері. Пропонуємо формування уніфікованого понятійно-термінологічного апарату у сфері кібербезпеки (оборони), а також погодження з термінологією чинного українського законодавства та міжнародних актів.

Ключові слова: *кібербезпека (оборона), кіберпростір, інформаційна безпека, європейська інтеграція, стратегія, інформаційні технології, адміністративна відповідальність, адміністративне правопорушення.*

Zuy V. V. Actual problems of cyber security in Ukraine, taking into account European integration

This scientific article analyzes the current legislation on the regulation of the organization of cyber security (defense), formulates and proposes ways to solve existing problems. At the same time, administrative responsibility in this area is highlighted.

In particular, attention was drawn to Ukraine's course towards European integration in order to form the proper foundations of legal regulation of support for the security of the information space in Ukraine. It is noted that on June 23, 2022, the member states of the European Union voted to grant Ukraine the status of a candidate country for joining the European Union.

The purpose of the study is the current problems of cyber security (defense), legislative regulation of the participation of executive authorities in this, innovations in European integration.

Also, legal structures were analyzed: cyber security (defense), cyber space, information security. We can say that cyber security covers all aspects of security related to cyberspace, and information security is the security of information regardless of the field of application. Under cyberspace, the law proposes to consider "the environment (virtual space) that provides opportunities for communication and/or the implementation of social relations, formed as a result of the functioning of compatible (connected) communication systems and the provision of electronic communications using the Internet and/or other global data transmission networks". The advantage of this definition is that it emphasizes the "communicability" of cyberspace (ie, in

particular, its ability to broadcast (transmit) malicious software structures that act as tools of cyberattacks).

Thus, cyber security will ensure the deepening of European integration processes by unifying approaches, methods and means of ensuring cyber security with the established practice of the EU and NATO, taking other measures, agreed with key foreign partners, aimed at strengthening Ukraine's cyber resilience.

Let's agree that there is currently a problem of imperfect legislation in the field of cyber security, outdated information and legal norms, an insufficient level of penalties for information offenses, slow application of the provisions of European legislation in this area. We propose the formation of a unified conceptual and terminological apparatus in the field of cyber security (defense), as well as agreement with the terminology of current Ukrainian legislation and international acts.

Key words: *cyber security (defense), cyber space, information security, European integration, strategy, information technologies, administrative responsibility, administrative offense.*

Постановка проблеми та її актуальність. З розвитком інформаційних технологій та становленням інформаційного суспільства виникають певні проблеми у сфері кібербезпеки, які потребують сучасних підходів та рішень. У свою чергу, розвиток інформаційного простору в умовах глобалізації та пандемія COVID-19 зумовили посилення ролі соціальних мереж у національному та світовому інформаційному просторі, їхній вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини, зокрема щодо забезпечення принципів рівності прав користувачів соціальних мереж. Відповідно до п. 5 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1]. У свою чергу, згідно з Наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» «Про прийняття національних нормативних документів гармонізованих з міжнародними нормативними документами, та скасування національних нормативних документів» від 27 грудня 2016 року № 448 кіберпростір – це складне середовище, що виникає в процесі взаємодії людей, програмного забезпечення і послуг Інтернет-послуг Інтернету, за допомогою технологічних пристроїв або об'єднаних мереж, яка не існує в будь-якій фізичній формі [2]. Варто зазначити, що інформаційна безпека – це ще один спосіб визначити безпеку даних, маючи на увазі конфіденційність, цілісність та доступність даних. Так, інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Більшість сучасних бізнес-даних зберігаються в електронному вигляді на серверах, настільних комп'ютерах, ноутбуках або в Інтернеті, але десять років тому, до того як вся конфіденційна інформація була перенесена до Інтернету, вона зберігалася в архіві та кабінеті [3, с. 162–164]. З огляду на вищезазначене потребують додаткової наукової аргументації такі правові конструкції, як кібербезпека, кіберпростір, інформаційна безпека. Зазначимо, що кібербезпека охоплює всі аспекти безпеки, що стосуються кіберпростору, а інформаційна безпека – це безпека інформації незалежно від сфери застосування. Додамо, що під кіберпростором Закон України «Про основні засади забезпечення кібербезпеки України» пропонує розглядати середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [1]. Перевагою використання правової конструкції кіберпростір є те, що воно акцентує на комунікативності кібернетичного простору (тобто, зокрема, його здатності транслювати (передавати) шкідливі програмні конструкції, що виступають інструментами кібератак).

Важливо, що 23 червня 2022 року країни члени Європейського Союзу проголосували за надання

Україні статусу країни кандидата на вступ до Європейського Союзу. Так, у Постанові Верховної Ради України «Про Звернення Верховної Ради України до держав – членів Європейського Союзу та інституцій Європейського Союзу щодо підтримки надання Україні статусу країни кандидата на вступ до ЄС» від 19 червня 2022 року, Верховна Рада України звернулася до національних парламентів, урядів держав-членів та інституцій Європейського Союзу і закликала підтримати прагнення України щодо визнання її європейської перспективи шляхом надання Україні статусу країни – кандидата на вступ до Європейського Союзу під час засідання Європейської Ради 23-24 червня 2022 року відповідно до статті 49 Договору про Європейський Союз [4]. Це великий крок під час курсу України на європейську інтеграцію та відповідно спрямування до оновлення законодавства і щодо регулювання сфери кібербезпеки в Україні і тому актуальності набирає дане питання.

Аналіз останніх досліджень і публікацій. Проблематика кібернетичної безпеки та державної політики, спрямованої на її забезпечення, виступала предметом наукових досліджень багатьох провідних учених у галузі адміністративного, конституційного та інших суміжних галузей права, як-от: В.Б. Авер'янова, І.В. Арістової, І.Л. Бачило, І.П. Голосніченка, О.Д. Довганя, Р.О. Додонова, І.М. Дороніна, Л.В. Кузенка, О.Є. Кутафіна, В.Л. Манілова, О.В. Нестеренка, Г.В. Падалка, В.П. Пєткова, С.В. Пєткова, В.Л. Сидоренко, О.Ю. Синявської, С.Г. Стеценка, В. Тертичка, М.М. Тищенка, Ю.П. Тихомірова, О.М. Шевчука, В.К. Шкарупи та інших.

Варто відмітити, що питання юридичної регламентації кібернетичної безпеки досліджували у своїх працях такі вчені, як: О.Ф. Андрійко, В.Т. Білоус, Н.П. Бортник, М.П. Вавринчук, Т.О. Гаврилюк, В.П. Горбулін, Д.В. Дубов, Д.Г. Заброда, О.М. Музичук, В.К. Колпаков, Т.О. Коломоєць, О.В. Кузьменко, Р.А. Калюжний, І.О. Корецька, Д.М. Лук'янець, Н.Р. Нижник, О.І. Остапенко, О.В. Олійник, В.М. Олуйко, І.Д. Пастух, Г.П. Ситник, І.М. Сопілко, В.О. Шамрай та інші.

Метою цієї статті є дослідження актуальних проблем кібербезпеки (оборони) в Україні з урахуванням європейської інтеграції та шляхів вирішення даних проблем під час стратегічного курсу на набуття повноправного членства України в Європейському Союзі.

Виклад основного матеріалу. Нині юридична регламентація безпеки у кіберпросторі (оборони) здійснюється на основі Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України, розпорядженнями Кабінету Міністрів України, актів міжнародного законодавства тощо. Потребують додаткового аргументування деякі з наведених вище актів. Зокрема, Постанова Кабінету Міністрів України від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», у ній закріплено: визначення загальних вимог до кіберзахисту об'єктів критичної інфраструктури; встановлення обов'язкових заходів щодо забезпечення захисту від кібератак [5]. Застосування якісно нового законодавства у сфері кібербезпеки стало можливим завдяки положенням Стратегії кібербезпеки України від 15 жовтня 2021 року [6]. Аналізуючи положення зазначеного акта, можна виділити такі її основні аспекти:

1) стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних;

2) метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина;

3) досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки;

4) в Україні триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму

координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері.

Так, кібербезпека забезпечуватиме поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів та засобів забезпечення кібербезпеки з усталеною практикою ЄС і НАТО, вжиття інших заходів, погоджених із ключовими іноземними партнерами, спрямованих на посилення кіберстійкості України.

Водночас аналіз чинного законодавства вказує на те, що існує ряд недоліків щодо регулювання питання кібербезпеки (оборони), які потребують негайного формування пропозицій щодо шляхів вирішення існуючих проблем з урахуванням європейської інтеграції. У цьому контексті слушно зазначає Г.О. Блінова про те що, держава має виступити ініціатором та гарантом ефективного розвитку і використання інформаційного простору України, особливо в оборонній сфері. Система кібербезпеки повинна бути багаторівневою і надійною, тобто такою, що унеможливить отримання несанкціонованого доступу до відомостей військового характеру, даних, що складають державну таємницю [7]. Тому деякі автори пропонують створити Інформаційний кодекс України, що містив би звід інформаційно-правових норм. Погодимося, що наразі існує проблема недосконалості законодавства у сфері кібербезпеки, застарілість інформаційно-правових норм, недостатній рівень стягнень за інформаційні правопорушення, повільне застосування положень європейського законодавства в даній сфері. Пропонуємо формування уніфікованого понятійно-термінологічного апарату у сфері кібербезпеки (оборони), а також погодження з термінологією чинного українського законодавства та міжнародних актів.

Також, доречним було б зазначити і про адміністративну відповідальність у сфері кібербезпеки. Так, у статті 12 Закону України «Про основні засади забезпечення кібербезпеки України» закріплено, що особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом [1]. В даному контексті Веселова Л.Ю. зазначає, що адміністративним проступком у сфері забезпечення кібербезпеки є протиправне, винне діяння (бездіяльність), що завдає значної шкоди відносинам у сфері кіберпростору, порушує права людини й інтереси суспільства і держави у цій сфері та встановлений правопорядок використання інформаційних й телекомунікаційних систем, а також за яке законодавством передбачено особливий вид державного примусу – адміністративну відповідальність [8, с. 15]. Прикладом санкцій за таке правопорушення є дії кібернетичних телеграм-об'єднань, спрямовані на несанкціоноване втручання у роботу телеканалів і можуть бути кваліфіковані як адміністративно-протиправне діяння, передбачене статтею 148-1 Кодексу України про адміністративні правопорушення, тобто здійснення дій, що призвели до зниження якості функціонування телекомунікаційних мереж [9].

Наголосимо, що важливого значення набувають євроінтеграційні процеси щодо кібербезпеки. В сьогоднішніх умовах євроінтеграційні прагнення України з погляду часу не є сприятливими. Реалізації намірів нашої країни заважають як зовнішні, так і внутрішні чинники. Зовнішні пов'язані з тим, що сучасний стан ЄС переживає інтенсивне кількісне і не завжди якісне поповнення завдяки постсоціалістичним країнам. Внутрішні чинники виражаються у протиставленні всередині владних структур, глибокій економічній кризі, відсутності ефективних економічних і інституційних реформ [10, с. 312]. Тому обрання нашою державою стратегічного курсу на набуття повноправного членства України в Європейському Союзі вимагає ефективної реалізації державної політики в сферах європейської інтеграції. Виконання такого завдання у своїй більшості повинно бути покладено на органи виконавчої влади, які слід розглядати як провідних суб'єктів даних суспільних відносин. Є. Ковтун у своїх наукових пошуках, присвячених проблематиці євроінтеграції України, зазначає, що Європейський Союз є унікальним явищем наддержавного демократичного утворення європейських країн. Високий рівень співпраці держав Європи в форматі ЄС приводить до того, що з кожним роком все більше і більше

країн хочуть приєднатися до цієї організації. Для України вступ до Європейського Союзу є одним з самих пріоритетних завдань у зовнішній політиці [11, с. 105].

Висновки. Узагальнено, що сьогодні стан регулювання сфери кібербезпеки (оборони) є недосконалим, особливо при курсі України до європейської інтеграції. По-перше, необхідно формування уніфікованого понятійно-термінологічного апарату у сфері кібербезпеки (оборони), по-друге, погодження з термінологією чинного українського законодавства та міжнародних актів (можливо ухвалення кодифіковано акту). По-третє, має місце недостатній рівень санкцій за інформаційні правопорушення. Тому обрання нашою державою стратегічного курсу на набуття повноправного членства України в Європейському Союзі вимагає ефективної реалізації державної політики у сферах європейської інтеграції щодо кібербезпеки (оборони) вочевидь.

Література

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Наказ Державного підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» «Про прийняття національних нормативних документів гармонізованих з міжнародними нормативними документами, та скасування національних нормативних документів» від 27 грудня 2016 року № 448. URL: https://zakononline.com.ua/documents/show/55624___55624.

3. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.

4. Постанова Верховної Ради України «Про Звернення Верховної Ради України до держав – членів Європейського Союзу та інституцій Європейського Союзу щодо підтримки надання Україні статусу країни – кандидата на вступ до ЄС» від 19 червня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/2298-20#Text.

5. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7.

6. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 року. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text.

7. Блінова Г.О., Мамедова Е.А. Інформаційне забезпечення та кібербезпека патрульної поліції: співвідношення понять. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 4.

8. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: автореф. докт. юр. наук : 12.00.07 ; Одеський державний університет внутрішніх справ, 2021. 38 с.

9. Кодексу України про адміністративні правопорушення від 7 грудня 1984 року з подальшими змінами. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text.

10. Бородій О.В. Досвід Польщі для інтеграції України в Європейський Союз. *Найковий вісник НЛТУ України*. 2010. № 20. С. 311–318.

11. Ковтун Є. Досвід інтеграції Латвії, Литви та Естонії до Європейського союзу, як приклад для України. *Емінак*. 2008. № 1-4. С. 105–109.

Зуй В. В.,
кандидат юридичних наук, доцент,
доцент кафедри адміністративного права
Національного юридичного університету
імені Ярослава Мудрого