УДК 349
DOI https://doi.org/10.24144/2788-6018.2022.01.30

ПРАВООХОРОННІ ОРГАНИ ЯК СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

Ільченко О.В.,
кандидат юридичних наук, доцент,
доцент кафедри кримінально-правових дисциплін
та судочинства Сумський державний університет
ORCID: https://orcid.org/0000-0003-4885-2205

Корощенко К.Р.,
студент Навчально-науково інституту права
Сумський державний університет
ORCID: https://orcid.org/ 0000-0002-1911-066X

Ільченко О.В., Корощенко К.Р. Правоохоронні органи як суб'єкти забезпечення кібербезпеки в інформаційному просторі України.

Інформаційна безпека в Україні є важливою галуззю з забезпечення простору від внутрішніх та зовнішніх загроз. Варто зауважити, що інформація безпека держави – широке поле для аналізу як вченими, так і для законодавчого врегулювання. Адже не припиняються намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації. Положення України в інформаційному полі є відображенням здатності держави захистити себе на всіх можливих рівнях. Дуже важливою частиною інформаційної безпеки є кібербезпека держави, ця галузь є значно вужчою для регулювання. В останні роки в Україні почали діяти реформи та модернізаційні процеси щодо цієї галузі. Неодмінно необхідно наголосити на тому, що всі процеси тісно пов'язі з євроінтеграційними заходами, це може підтвердити значна фінансова та інформаційна допомога партнерів.

Дійсно, можливі кіберзагрози спричинили справжню революцію в державній системі. Тема почала бути актуальною і для громадян, які можуть постраждати від кібератак. Тож питання кібербезпеки набувають особливого значення, стаючи невід'ємною частиною національної безпеки і як наслідок інформаційної, а заходи протидії кіберзагрозам розробляються і впроваджуються на державному рівні. У нашій країні для цих цілей був прийнятий Закон України «Про основи забезпечення кібербезпеки України», який, зокрема, регулює питання суб'єктів забезпечення кібербезпеки і виокремлює основні напрями та завдання діяльності правоохоронних органів. Державним механізмом втілення тих чи інших завдань є чітко побудована система органів, які б втілювали та виконували певні функції у правовому полі.

Правоохоронні органи мають на меті ефективне здійснення своїх повноважень, запорукою для досягнення цієї мети є системна координація одного з одним.

Важливість дослідження саме правоохоронних органів щодо функціонування кібербезпеки обумовлюється тим, що саме на ці органи покладені функції забезпечення кібербезпеки, що є питомою роллю для держави.

Ключові слова: інформаційна безпека, кібербезпека, національна безпека, інформаційний простір, правоохоронні органи, євроінтеграція.

Ilchenko O.V., Koroshchenko K.R. Law enforcement agencies as subjects of cybersecurity in the information space of Ukraine.

Information security in Ukraine is an important area for securing space from internal and external threats. It is worth noting that information and state security is a wide field for analysis by both scholars and legislation. After all, attempts to manipulate the public consciousness do not stop, in particular, by disseminating inaccurate, incomplete or biased information. Ukraine's position in the information field is a reflection of the state's ability to defend itself at all possible levels. Cybersecurity of the state is a very important part of information security. This area is much narrower for regulation. In recent years, Ukraine has launched reforms and modernization processes in this area. It is important to emphasize that all processes are closely linked to European integration measures, which can be confirmed by significant financial and information assistance from partners.

Indeed, possible cyber threats have revolutionized the state system, as well as the citizens to whom the effects of cyber attacks and cybercrime may extend. Therefore, cybersecurity issues are becoming increasingly important, becoming an

integral part of national security and as a result of information security, and measures to combat cyber threats are being developed and implemented at the state level. In our country, for these purposes, the Law of Ukraine «On the Fundamentals of Cyber Security of Ukraine» was adopted, which, in particular, regulates the issues of cyber security and identifies the main directions and objectives of law enforcement agencies. The state mechanism for the implementation of certain tasks is necessarily a well-established system of bodies that would implement and perform certain functions in the legal field.

Empowered law enforcement agencies aim to effectively exercise their powers, which did not matter, the need for coordination and cooperation with each other is becoming more and more acute.

The importance of law enforcement research on the functioning of cybersecurity is due to the effectiveness of these entities in carrying out tasks. Also, the practical definition of the activities of law enforcement agencies may reveal accompanying problems.

Key words: information security, cybersecurity, national security, information space, law enforcement agencies, European integration.

Постановка проблеми. Необхідність виокремлення кібербезпеки як складової частини інформаційної безпеки зумовив динамічний процес розвитку галузі. Забезпечення високого рівня кібербезпеки у державі неможливе без належного та ефективного функціонування правоохоронних органів як суб'єктів, які наділені повноваженнями забезпечувати кібербезпеку. На даний час існують обставини які негативно впливають на рівень кібербезпеки та потребують більш глибокого їх дослідження та напрацювання заходів щодо їх усунення.

Стан дослідження: Вивченню питань забезпечення кібербезпеки приділялася значна увага науковців-правників, зокрема, О. Панченко, І. Бінько, В. Шевчук, Б. Кормича, Ю. Уфімцев, В. Буянов, Е. Єрофеєв, проте тема не є вичерпною і дослідження функціонування правоохоронних органів у галузі забезпечення кібербезпеки залишається актуальним.

Метою статті є дослідження поняття кібербезпеки як складової національної безпеки України та актуальних питань щодо функціонування системи правоохоронних органів, як суб'єктів забезпечення кібербезпеки.

Забезпечення високого рівня кібербезпеки у державі неможливе без належного та ефективного функціонування правоохоронних органів як суб'єктів, які наділені повноваженнями забезпечувати кібербезпеку. На даний час існують обставини які негативно впливають на рівень кібербезпеки та потребують більш глибокого їх дослідження та напрацювання заходів щодо їх усунення.

Виклад основного матеріалу. Дослідження поняття «інформаційна безпека» почалось наприкінці 80-х років. Так, вчений Н.В. Сугоняко зазначав про важливий інформаційний компонент у міжнародній безпеці, а також акцентував увагу на проблемі безпеки, що пов'язується ним з інформаційними загрозами [1].

Як зазначено у Законі України «Про національну безпеку» державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Ми погоджуємося з думкою О.А. Панченко, що національний інформаційний простір України, зазнає суттєвих загроз, викликів, що становлять небезпеку функціонування держав, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури [2].

О. Л. Сорокін, вважає, що інформаційна безпека становить «стан захищеності особистості, суспільства, держави від інформації, що носить шкідливий або протиправний характер, від інформації, що надає негативний вплив на свідомість особистості, перешкоджає сталому розвитку особистості, суспільства і держави. Інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючитакож комп'ютери та інформаційно-телекомунікаційну інфраструктуру і інформацію, що в них знаходиться, який також забезпечує сталий розвиток особистості, суспільства і держави» [1].

Варто наголосити, що науковці розглядають інформаційну безпеку як один з найважливіших видів національної безпеки, також висловлюються думки, де інформаційна безпека розглядається через призму суспільних відносин.

Думку щодо співвідношення національної і інформаційної безпеки висловлює у своїй дисертації В.В. Шемчук, зокрема той факт, що у багатотомній юридичній енциклопедії інформаційна безпека України визначається як один із видів національної безпеки і важлива функція держави [3].

З іншої точки зору, крізь призму суспільних відносин В. Гуровський розглядає інформаційну як суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [4]

Ми повністю поділяємо думку Б.А. Кормича, який характеризує інформаційну безпеку як інформаційний компонент національної безпеки

по співвідношенню «частина-ціле» . Він характеризує національну безпеку як стан захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови існування людини, держави і суспільства, які гарантовані Конституцією та законами України. Тобто, будучи складовою частиною національної безпеки інформаційна безпека повинна сприйматися як стан захищеності держави від зовнішніх і внутрішніх загроз у сфері обігу інформації. Тому інформаційна безпека більшістю вчених сприймається як стан, який протистоїть загрозам ззовні та внутрішнім загрозам. Але, за умови, що всі ці загрози направлені всередину держави [5]

Кібербезпека в українській стратегії являє собою реалізацію заходів професійно підготовленими фахівцями щодо захисту та страхування дій, засобів, технологій, критично важливих об'єктів інфраструктури суспільства та держави від цифрових атак, які використовуються у кіберпросторі. Кібербезпека передбачає збереження та постійне вдосконалення властивостей безпеки, спрямованих проти відповідних кіберзагроз. Такий підхід обґрунтований і використовується в правозастосовчій сфері, в тому числі в юрисдикційної діяльності працівників правоохоронних органів. Кібербезпека забезпечується і підтримується державно-примусовими заходами. Крім того, в більшості нормативних актів правоохоронної сфери законодавець використовує досліджувану категорію саме в такому контексті [6].

Ми погоджуємось з думкою О. Баранова, який подає таке визначення: кібербезпека – це інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж. Це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [7].

На думку Б. Кормич забезпечення функціонування інформаційної безпеки у широкому сенсі, та кібербезпеки, можливе через систему правоохоронних органів, розглядає державно-правовий механізм інформаційної безпеки, систему органів державної влади загальної і спеціальної компетенції, задіяних у процесі формування та реалізації політики інформаційної безпеки, внутрішні й зовнішні ролі та відносини якої регулюються системою правових норм і принципів в [8].

Термін «система» походить з грецької мови і означає складене з частин з'єднання; у філософському сенсі розуміють ціле, утворене шляхом об'єднання закономірно пов'язаних один з одним предметів, явищ тощо. Останні є її елементами, складовими частинами [9].

В.В Шемчук, аналізуючи систему забезпечення національної безпеки пропонує розглядати систему забезпечення національної безпеки як складову системи національної безпеки, а саме – сукупність взаємопов'язаних та взаємообумовлених механізмів (інституційних, організаційних, правових та інших) та суб'єктів забезпечення національної безпеки (посадові особи держави, органи державної влади та місцевого самоврядування, державні установи та заклади, сили та засоби сектора безпеки, інститути громадянського суспільства, окремі громадяни) [3].

Відповідно до ч. 4 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [10].

О.М. Бандурка вважає, що правоохоронними органами прийнято називати ті державі установи й організації, які функціонують у суспільстві й основним завданням діяльності яких є забезпечення законності, боротьби зі злочинністю та іншими правопорушеннями [11].

Основними суб'єктами національної системи кібербезпеки є: Державна служба спеціального зв'язку та захисту інформації України; Національна поліція України; Служба безпеки України; Міністерство оборони України; Генеральний штаб Збройних Сил України; розвідувальні органи; Національний банк України.

Державна служба спеціального зв'язку та захисту інформації України (далі-ДСС). У сфері забезпечення кібербезпеки ДСС України займається формуванням і реалізацією політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність

інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення і реагування на кіберінциденти та кібератаки й усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури тощо [12].

Національна поліція України (далі- НП) забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі [10]. У своїй діяльності НП підпорядковується Кабінету Міністрів України і спрямовується та координується через Міністерство внутрішніх справ України, на яке покладається реалізація повноважень щодо: створення і забезпечення функціонування підрозділів із протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів тощо [13].

Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [10].

Якщо говорити про повноваження Міністерство оборони України (далі-МО) та Генерального штабу Збройних Сил України у сфері забезпечення кібербезпеки, то слід зазначити, що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» вони є майже ідентичними: зазначені державні органи здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану Розвідувальні органи (Служба зовнішньої розвідки України, розвідувальні органи МО, розвідувальні органи спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону здійснюють у сфері забезпечення кібербезпеки розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки [12].

Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України [10].

Як зазначає В. Бурячок, досвід іноземних країн та особливості українських реалій свідчать, що розв'язання основних завдань кібербезпеки неможливе без створення: міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки; центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення й оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад і надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін і впливу на їх інформаційно-телекомунікаційні системи; органів власної інформаційної та кібербезпеки – державних установ (відомств) і комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів [14].

Висновки. Інформаційна безпека в Україні – це важлива складова національної безпеки, яка полягає у досягненні стану захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови існування людини, держави і суспільства, які гарантовані Конституцією. Ми вважаємо, що кібербезпека є складовою інформаційної безпеки і покликана захищати життєво важливі інтереси людини і громадянина, суспільства та держави під час використання кіберпростору, своєчасне виявлення, запобігання

і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Важливим державним механізмом для забезпечення кібербезпеки в інформаційному просторі є правоохоронні органи, які у межах своїх повноважень здійснюють заходи для досягнення цілей та завдань. На сьогоднішній день кібербезпека в Україні вимагає створення міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Сугоняко Н.В. Інформаційна безпека в інформаційній діяльності суду. 2019. С. 195-201. URL: file:///C:/Users/user/Downloads/224-Article%20Text-421-1-10-20200802.pdf (дата звернення: 02.04.2022).
2. Панченко О.А. Проблеми правового забезпечення державного управління інформаційною безпекою. Державне управління: удосконалення та розвиток. 2019. № 11. URL: http://www.dy.nayka.com.ua/pdf/11_2019/5.pdf (дата звернення: 02.04.2022).
3. Шемчук В.В. Конституційно-правове забезпечення інформаційної безпеки сучасних держави: порівняльно-правовий аналіз. дис. … канд. юрид. наук: 12.00.02. Ужгород, 2020. 411 с.
4. Гурковський В.Т. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : дис. ... канд. юрид. н. за спеціальністю 25.00.02 . Київ, 2004. 225 с.
5. Рижук О.Аналіз підходів щодо визначення поняття «інформаційна безпека» в умовах глобалізації. URL: file:///C:/Users/user/Downloads/3007-11016-1-PB.pdf (дата звернення: 02.04.2022).
6. Г.В. Форос, В.С. Жогов. Особливості трактування поняття «кібербезпека» в сучасній юридичній літературі. Правова держава. 2019. № 33. С.128-133.
7. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» . Правова інформатика. 2014. № 2(42). С. 54–62.
8. Кормич Б.А. Інформаційне право : підруч. Харків : БУРУН і К., 2011. 334 с.
9. Швець С.В., Швець У.С. Основи системного аналізу : навч. посіб. Суми: Сумськ. держ. ун-т, 2017. 126 с.
10. Про основні засади забезпечення кібербезпеки України від 05.10.2017. №45/ Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.04.2022).
11. Загуменна Ю.О. Правоохоронні органи: поняття, ознаки, функції, особливості діяльності. Право і безпека. 2010.№ 3.С. 145–150.
12. Про Державну службу спеціального зв’язку та захисту інформації України від 23.02.2006. №30/ Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 02.04.2022).
13. А.В.Тарасюк.Система суб’єктів забезпечення кібербезпеки в Україні. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки.2020.№2(25). С. 119–125.
14. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. Київ : Наук.-вид. центр НА СБ України, 2013. 416 с.