УДК 338.24
DOI https://doi.org/10.32782/1813-338X-2024.3.45

С. О. Мазепа
кандидат юридичних наук, доцент
доцент кафедри кримінального права та процесу
Західноукраїнського національного університету,
міжнародний дослідник Оснабрюцького університету
ORCID ID: 0000-0003-1282-9089

КОНЦЕПТУАЛЬНЕ ОСМИСЛЕННЯ ПРАВОВИХ ОСНОВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ ГЛОБАЛЬНИХ МІЖНАРОДНИХ ТЕНДЕНЦІЙ

Актуальність проведеного дослідження викликана трансформацією права в галузі інформаційної безпеки в умовах великих викликів та загроз, а без розуміння глобальності проблематики цього явища неможливо здійснювати активну міждержавну співпрацю.

Метою дослідження стало міждержавне співробітництво щодо забезпечення інформаційної безпеки, а також розробка заходів щодо підвищення його ефективності (насамперед міжнародного законодавства, а також інших міждержавних заходів щодо попередження нових викликів та загроз).

Об'єктом дослідження стали сучасні суспільні відносини, що складаються у сфері міждержавного співробітництва щодо забезпечення інформаційної безпеки. Як предмет виступили міжнародно-правові акти, що регулюють відносини у сфері кібербезпеки, матеріали та публікації в галузі інформаційної безпеки, інтернет-ресурси з проблем цієї теми.

Автор приходить до висновку, що Як основні способи і напрямки вирішення проблем міжнародної та національної безпеки особливе місце відводиться безпеці ЄС за допомогою зосередження зусиль на обороні, боротьбі з тероризмом, кібербезпекою, гібридними загрозами.

Також країни ЄС усвідомлюють пряму залежність європейської спільноти від інформаційної сфери, тому питання забезпечення інформаційної безпеки закономірно посідає одне з провідних місць у стратегіях національної безпеки ЄС та відповідних держав. Водночас, політика забезпечення інформаційної безпеки більшості країн має проактивний характер і спирається на принципи управління ризиками інформаційної безпеки, насамперед – кібербезпеки.

Ключові слова: *інформаційна безпека, співробітництво, міжнародна безпека, міжнародне право, міжнародні організації, адміністративне право, загрози та ризики, правове регулювання, трансформація права, інформаційне суспільство.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Забезпечення національної безпеки є найголовнішою метою кожної держави. Забезпечення національної безпеки потребує постійного вдосконалення всієї системи безпеки держави для захисту таких систем як: економічна, соціально-політична, військова, конституційна та інформаційна. Протидія сучасним викликам і загрозам, що виникають внаслідок стрімкого розвитку глобального інформаційного простору останніми роками, є одним з основних завдань, що торкаються стратегічних питань забезпечення стабільності сучасного світопорядку, вирішення яких можливе лише на основі об'єднання зусиль усіх членів міжнародного співтовариства.

Складність запобігання та стримування реальних та потенційних загроз у сфері інформаційних технологій належить до найбільш значущих проблем міжнародної та національної безпеки XXI ст. Захищеність особистості, суспільства та держави від зовнішніх та внутрішніх загроз називається національною безпекою. Обов'язковим аспектом є забезпечення конституційних прав і свобод громадян, а також державний суверенітет та недоторканність від посягань інших держав за допомогою застосування військової сили або загрози застосування сили.

Національна безпека, з позиції М. Запфе *(Zapfe M. (2015))* включає оборону країни і всі

види безпеки, насамперед державну, суспільну, інформаційну, екологічну, економічну, транспортну, енергетичну безпеку, безпеку особистості [1].

Інформаційна ж безпека, як зазначає Бондар І.Р. включає безпеку інформаційних ресурсів держави, захист прав особи і суспільства від інформаційних загроз, що виходять від внутрішніх і зовнішніх джерел [2, с.70].

У сучасних умовах активізації міжнародних терористичних, екстремістських організацій і злочинних структур, що використовують інформаційні технології для реалізації своїх злочинних намірів, забезпечення інформаційної безпеки України, є однією з найважливіших складових системи забезпечення національної та міжнародної безпеки, що ще раз наголошує на актуальності обраної теми.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Загальні питання інформаційної безпеки висвітлювали у своїх працях Антипенко В. Ф., Бєглий О.В., Лукашук І.І. та ін.

Міжнародно-правові проблеми забезпечення глобальної безпеки на сучасному етапі вивчала Н.М. Ємельянова. Захисту національних інтересів України в сфері кіберпростору присвятили свої праці Д.В. Дубов та М.А. Ожеван. Питання інформаційної безпеки України у системі сучасних викликів, загроз та механізмів протидії негативним інформаційно-психологічним впливам вивчала У. Ільницька.

Правові засади інформаційної безпеки в Україні та питання її правового регулювання досліджували Біленчук П.Д. та Насинець-Наумова А.Ю. О.Д.Довгань та І.М.Доронін здійснюють моніторинг ескалації кіберзагроз національним інтересам України та досліджують правові аспекти кіберзахисту.

Ю. К. Ісмаїлов проаналізував співвідношення понять «мережева безпека» та «інформаційна безпека». О.М. Фролова розмірковує про роль ООН та НАТО у системі міжнародної інформаційної безпеки. Питання зміни політики у сфері інформаційної безпеки в міжнародних організаціях ще не досліджено цілеспрямовано, що вимагає більш обережного підходу до цієї теми.

Метою статті є дослідження особливостей забезпечення міжнародної інформаційної безпеки і, зокрема, трансформації політики міжнародних організацій у сфері інформаційної безпеки у зв'язку з новими викликами сучасності.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Проблеми правового забезпечення інформаційної безпеки є актуальними як вітчизняної правової доктрини, так і для законодавства. Кожна держава має свої національні інтереси та зацікавлена у підтримці миру та міжнародної інформаційної безпеки. У світлі тісної взаємодії різних країн, що вступають у партнерські та союзницькі відносини одна з одною, проблеми інформаційної захищеності однієї держави можуть стати тягарем і для іншої. У зв'язку з цим важливим є питання про закордонний досвід правового забезпечення інформаційної безпеки.

Досить поширеним явищем стала політика низки зарубіжних країн, спрямована на розвиток свого інформаційно-технічного потенціалу з метою негативного впливу на інформаційну інфраструктуру інших держав. У водночас, Дж. Джонсон *(Johnson, Joseph & Lincke, S.J. & Imhof, Ralf & Lim, Charles. (2014))* справедливо зазначає, що поняття «інформаційна безпека» є складним правовим явищем з погляду інформаційного права, оскільки вищезазначену дефініцію слід розглядати у праві як самостійний наднаціональний вид загальної безпеки, оскільки на сьогоднішній день інформаційне право торкається всіх сфер суспільного життя та забезпечує розвиток держави в загалом [3, с. 96].

На наш погляд, така позиція могла б мати під собою міцніше обґрунтування, якби держави прагнули забезпечити загальну міжнародну інформаційну безпеку. Проте кожна держава, враховуючи розглянуті у попередньому параграфі стратегічні документи зарубіжних країн, переважно дбає про власний інформаційний суверенітет. Інформаційна безпека інших країн найчастіше турбує інших учасників геополітичної боротьби лише тією мірою, у якій інформаційні загрози, які зачіпають інтереси однієї держави, можуть торкнутися національні інтереси іншої держави. Подібна ситуація можлива за тісної інтеграційної співпраці між країнами, яка передбачає взаємний захист секретної інформації. Вибудовування партнерських та союзницьких відносин передбачає взаємну відповідальність за інформаційну захищеність кожного з учасників інтеграційного об'єднання.

Разом з тим слід зазначити, що в Україні праві правове регулювання питань інформацій-

ної безпеки відображається в Стратегії інформаційної безпеки.[4] Зазначений нормативно-правовий акт регулює частину суспільних відносин в інформаційній сфері, завдяки яким демонструється захищеність держави в інформаційній сфері та визначається подальше вдосконалення правових інститутів з метою балансування інтересів особи, суспільства та держави в інформаційному середовищі.

Особливу увагу у науці інформаційного права віднесено питанням стану правового забезпечення досліджуваної підгалузі права, відповідно до положень Стратегії інформаційної безпеки можна назвати такі особливості національних інтересів:

1) прозорість і транспарентність діяльності держави у інформаційної сфері;

2) гарантія захисту конституційних прав і свобод громадян щодо інформаційної безпеки;

3) взаємне та узгоджене функціонування держави та громадянського суспільства, у тому числі в рамках зміцнення моральних цінностей суспільства;

4) забезпечення належного функціонування інформаційної інфраструктури як у разі безпосереднього впливу інформаційних загроз (у тому числі у воєнний час), так і в період стабільної мирної ситуації в країні;

5) стимулювання науково-технічного прогресу та розвитку економічних галузей, що сприяють забезпеченню інформаційної безпеки;

6) інтеграційна взаємодія з іншими країнами для забезпечення міжнародної інформаційної безпеки та стратегічної стабільності.

Національні інтереси у сфері інформаційної безпеки є спільними орієнтирами для органів публічної влади, на яких покладено роль нейтралізатора інформаційних загроз і конфліктів. Закріплений у документах стратегічного планування перелік національних інтересів є правовим фундаментом (поряд з цілями та завданнями), але на якому стоїть вся система національної безпеки.

Досить актуальними є підходи щодо вирішення проблем, пов'язаних із забезпеченням інформаційної безпеки міжнародно-правовими засобами. Проблема полягає в тому, що будь-які умови, що стосуються транспарентності та інформаційна прозорість, можуть сприйматися країнами як обмеження суверенітету (передусім інформаційного).

Цим, на думку Парахонського Б.О. пояснюється те, що зараз немає міжнародного договору, в якому були б закріплені базові принципи забезпечення інформаційної безпеки.[5] Єдиним способом вирішення цієї проблеми є укладення міжнародних угод у межах наднаціональних інститутів. Багато авторів присвячують свої дослідження окремим темам політико-юридичного процесу інформаційних мереж, а також розповсюдженню небажаної інформації, захисту персональних даних.

Важливо відзначити, що у 2002 р. на Загальноєвропейській конференції у Бухаресті було прийнято декларацію (), яка закріпила принцип зміцнення довіри та безпеки у процесі використання інформаційних технологій. Вона передбачає розробку «глобальної культури кібербезпеки», яка має забезпечуватись шляхом вжиття превентивних заходів та підтримуватись усім співтовариством за умови збереження свободи передачі інформації. Країни погодилися з тим, що необхідно здійснювати «запобігання використанню інформаційних технологій та ресурсів у злочинних чи терористичних цілях», а також зміцнювати міжнародну взаємодію в даній сфері [6].

Токійська декларація 2003 р. *(Tokyo declaration for the dynamic and enduring asean-japan partnership in the new millennium)* включає найбільш пріоритетні галузі дії інформаційно-комунікаційних технологій. Важливе місце посідають питання інформаційної та технологічної безпеки. Принципи справедливого, рівного та адекватного доступу до інформаційних технологій є основними, тому особлива увага сторонами приділялася загрозам потенційно військового використання інформаційних технологій.[7]

Наступним етапом стала розробка Генеральною асамблеєю ООН проекту документа «Принципи, що стосуються міжнародної інформаційної безпеки» [8].

Важливе значення даного документа, перш за все, полягала в тому, що на світовому рівні вперше було зафіксовано наявність гострих загроз інформаційній безпеці, а також визначив принципи, методи співробітництва країн у конкретній сфері. На 66-й сесії ОНН у 2011 р. країнами – учасниками було висунуто ініціативу та проект Кодексу поведінки з міжнародної інформаційної безпеки *(International Code of Conduct for Information Security (SCO))*, який був перевиданий у новій редакції у 2015 р. та внесений на новий розгляд Генеральної асамблеї ООН. [9]

Нова версія документа спирається насамперед на миротворчий характер. Документ

націлений на запобігання конфліктогенності в інформаційному просторі світу, закріплює зобов'язання держав не застосування інформаційних технологій, що ведуть до порушення міжнародного миру та балансу сил, втручання у внутрішні справи інших держав, що може призводити до підриву їх державної, політичної та економічної стабільності. Також документ передбачає зобов'язання держав до утримання від загроз та застосування сили у вирішенні міжнародних конфліктів в інформаційній сфері [9].

Безпека в глобальному кіберпросторі досягається лише за допомогою сукупності узгоджених засобів та методів на національному та міжнародному рівнях. Адже як зазначає Усман Т. *(Tariq, Usman, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat. (2023))* на рівні Європейського Союзу, беручи до уваги зміни загроз у сфері інформаційних технологій, а також об'єднання ІТ компетенцій в інститути ЄС, Європейська стратегія національної безпеки та цифровий порядок денний стануть вказівками для подальшої діяльності.[10]

Йдеться також про створення можливої кількості держав, які підпишуть кодекс державних дій у кіберпросторі, який включатиме посилення заходів безпеки. Вирішенням питання забезпечення безпеки персональних даних при їх трансатлантичній передачі, пов'язаного з розходженням законів та стандартів ЄС та США, стала угода «Safe Harbor».

Ця угода зазнала суттєвих змін у результаті рішення Європейського суду від 6 жовтня 2015 р., який ухвалив, що Safe Harbor не забезпечує належного рівня захисту персональних даних. 2 лютого 2016 р. було опубліковано нову угоду Privacy Shield (DRAFT), яка посилює вимоги щодо забезпечення безпеки даних та замінює Safe Harbor.[11]

Ця угода включає :

суворі зобов'язання для компаній, які опрацьовують персональні дані громадян ЄС, а також надійний механізм, що забезпечує їх дотримання;

заходи захисту та зобов'язання щодо забезпечення прозорості при доступі до даних з боку уряду U.S.;

захист прав громадян ЄС, що передбачає кілька варіантів відшкодування збитків. [11]

Насправді Privacy Shield поширюється не лише на взаємодію США та країн ЄС, а й на інші держави, які не входять до складу ЄС. У рамках Національної стратегії кібербезпеки 2016 р. зазначається, що «з урахуванням глобального характеру інформаційно-телекомунікаційних технологій, міжнародне співробітництво, сконцентроване на аспектах міжнародної політики та безпеки має обов'язковий характер» [12].

Таким чином, можна говорити про те, що міжнародна інформаційна безпека це комплексне явище, що впливає практично на всі аспекти міжнародної політики, які мають на меті використання економічних можливостей, що надаються інтернетом, а також забезпечення безпеки в кіберпросторі НАТО і європейського простору.

Основним принципом інформаційної безпеки НАТО є те, що інформація повинна зберігати свою ступінь захищеності на всіх етапах її передачі від джерела до одержувача, а також контроль за інформацією, що передається, а також за її поширенням і безпекою.

Також правила доступу до інформації повинні дозволяти використання інформації лише особам, яким вона потрібна для виконання службових обов'язків. Надання інформації НАТО того чи іншого грифу секретності здійснюється відповідно до правил систем безпеки країн-учасниць. Більшість країн ЄС є членами НАТО, відповідно, на них поширюються такі ключові документи Альянсу у сфері кібербезпеки, як: стандарти НАТО із захисту інформації, викладені в документі (2002) «Безпека в організації Північноатлантичного договору (НАТО)» (*Security within the North Atlantic Treaty Organization*) [13], офіційна політика НАТО у сфері кіберзахисту *(NATO Bucharest Summit Declaration)*[14], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту *(NATO Lisbon Summit Declaration)* [15] та уточнена за результатами Варшавського саміту *(Warsaw Summit Communiqué)* [16] тощо.

Як було зазначено у стратегічному дослідженні групи експертів НАТО *(на чолі з Мадлен К. Олбрайт (США))*, НАТО повинна прискорити свою діяльність з реагування на небезпеку кібератак, захищаючи власні системи зв'язку та управління, допомагаючи союзникам вдосконалити свою здатність запобігати нападам та відновлюватися після них, та розвивати сили та засоби кіберзахисту з метою ефективного виявлення та стримування кібератак. [17, с. 286].

Схожа стратегія має можливість розглядатися як допомога освіті великої кількості розрізнених інституційних формувань та організацій, що регламентують співпрацю у певних галузях

міжнародних відносин. Подібна ситуація склалася на даний момент у сфері забезпечення міжнародної інформаційної безпеки, де сформувалося багато функціональних та регіональних режимів. На даному етапі відкриваються нові можливості для формування глобального режиму міжнародної інформаційної безпеки.

Переговори на рівні різних країн щодо створення загальносвітового режиму забезпечення міжнародної інформаційної безпеки є одним із пріоритетних напрямків зовнішньої політики України, і крім того, варто зазначити, що в більшості випадків Україна виявляє ініціативу, виносячи на обговорення проблеми, пов'язані з міжнародною інформаційною безпекою, завдяки чому наша країна має значні переваги у переговорному процесі.

Висновки. Політика країн ЄС у сфері забезпечення національної безпеки будується на основних документах стратегічного планування (Стратегії, Білі Книги). Як показало проведене дослідження, на даному етапі як гострі проблеми та загрози національній безпеці та сучасній світовій спільноті відзначаються: тероризм, кіберзлочинність, міграція, гібридні загрози.

Як основні способи і напрямки вирішення проблем міжнародної та національної безпеки особливе місце відводиться безпеці ЄС за допомогою зосередження зусиль на обороні, боротьбі з тероризмом, кібербезпекою, гібридними загрозами.

Також країни ЄС усвідомлюють пряму залежність європейської спільноти від інформаційної сфери, тому питання забезпечення інформаційної безпеки закономірно посідає одне з провідних місць у стратегіях національної безпеки ЄС та відповідних держав. Водночас, політика забезпечення інформаційної безпеки більшості країн має проактивний характер і спирається на принципи управління ризиками інформаційної безпеки, насамперед – кібербезпеки.

На поточному етапі не сформувався ще єдиний міжнародний режим із забезпечення інформаційної безпеки. Згідно з проведеним дослідженням у роботі, скоріше є певна кількість регламентів, створених та спрямованих на вирішення конкретних проблем цифрової безпеки. Звичайно, у контексті досліджуваної теми, особливого значення набуває співпраця держав у міжнародних та неурядових організаціях.

Список використаної літератури:

1. Zapfe M. Nach Kabul und Krim - Deutschland in NATO und EU // Glatz R. L., Tophoven R. Am Hindukusch - und weiter? Die Bundeswehr im Auslandseinsatz. Erfahrungen, Bilanzen, Ausblicke. Bonn: Bundeszentrale für politische Bildung, 2015.
2. Бондар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014, № 1. С. 68-75.
3. Johnson, Joseph & Lincke, S.J. & Imhof, Ralf & Lim, Charles. (2014). A Comparison of International Information Security Regulations. Interdisciplinary Journal of Information Knowledge and Management. 9. 89-116. 10.28945/1963.
4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7 (Дата звернення 22.03.2024 р.)
5. Парахонський Б.О. Зовнішня політика України в умовах кризи міжнародного безпекового середовища: аналіт. доп. К.: НІСД, 2015. 100 с.
6. The Bucharest pan-european conference in preparation of the world summit on the information society: towards an information society: principles, strategy and priorities for action 9 November 2002. URL: https://data.consilium.europa.eu/doc/document/ST-12747-2002-REV-1/en/pdf (Дата звернення 22.03.2024 р.)
7. Tokyo declaration for the dynamic and enduring asean-japan partnership in the new millennium. Signed in Tokyo, Japan on 11-12 December 2003 URL: https://www.mofa.go.jp/region/asia paci/srilanka/conf0306/declaration.html (Дата звернення 22.03.2024 р.)
8. Cybersecurity in the United Nations system organizations Report of the Joint Inspection Unit. United Nations Geneva, 2021 URL: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf (Дата звернення 23.03.2024 р.)
9. International Code of Conduct for Information Security (SCO) URL: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf (Дата звернення 23.03.2024 р.)
10. Tariq, Usman, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat. 2023. "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review" *Sensors* 23, no. 8: 4117. https://doi.org/10.3390/s23084117
11. Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision - wp238/ date: 23/11/2016. URL: https://ec.europa.eu/newsroom/article29/items/640157 (Дата звернення 23.03.2024 р.)

12. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник* Харківського національного університету імені В.Н.Каразіна. Серія«ПРАВО». 2020. № 29. С. 281-288.
13. Security within the North Atlantic Treaty Organization C-M(2002)49. URL: http://www.freedominfo.org/documents/C-M(2002)49.pdf
14. NATO Bucharest Summit Declaration 3 April 2008. URL: https://www.nato.int/cps/ua/natohq/official_texts_84- 43.htm
15. NATO Lisbon Summit Declaration 20 Nowember 2010 URL: https://www.nato.int/cps/en/natohq/official_-texts_68828.htm
16. NATO Warsaw Summit Communiqué, 9 July 2016. URL: http://www.nato.int/cps/en/natohq/official_texts-_133169.htm
17. Шевчук О., Ментух Н. Ф. Реалізація політики державної інформаційної безпеки України в контексті запобігання корупції: адміністративно-правовий аспект. *Науковий* вісник Ужгородського національного університету. Серія : Право. 2021. Випуск 64. С. 282-287. URL: http://visnyk-juris-uzhnu-uz.com/wp-content/ uploads/2021/06/NVUzhNU_64.pdf

Mazepa S.O. Conceptual understanding of the legal framework of information security in the context of global international trends

The relevance of this study is caused by the transformation of law in the context of major challenges and threats, and without understanding the global nature of this phenomenon, it is impossible to carry out active interstate cooperation.

The purpose of the study is to examine interstate cooperation in ensuring information security and to develop measures to improve its effectiveness (primarily international legislation, as well as other interstate measures to prevent new challenges and threats).

The object of the study is modern social relations in the field of interstate cooperation on information security. The subject matter is international legal acts regulating relations in the field of cybersecurity, materials and publications in the field of information security, and Internet resources on the issues of this topic.

The author comes to the conclusion that as the main ways and directions of solving international and national security problems, a special place is given to EU security by focusing on defence, counter-terrorism, cybersecurity, and hybrid threats.

The EU countries are also aware of the direct dependence of the European community on the information sphere, so the issue of information security naturally occupies one of the leading places in the national security strategies of the EU and the respective states. At the same time, the information security policy of most countries is proactive and based on the principles of information security risk management, especially cybersecurity.

Key words: *information security, cooperation, international security, international law, international organisations, administrative law, threats and risks, legal regulation, transformation of law, information society.*