https://doi.org/10.31392/UDU-nc.series22.2023.33.08
УДК 32.019.5

Єгор Міненко,
аспірант навчально-наукового інституту права та політології,
Український державний університет імені Михайла Драгоманова
ORCID: 0000-0001-7169-3252 ; email: y.minenko@smdsu.org.ua

ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ФАКТОР СУСПІЛЬНО-ПОЛІТИЧНОЇ СТАБІЛЬНОСТІ

У статті проводиться аналіз організаційно-правових аспектів забезпечення інформаційної безпеки в умовах розвитку інформаційного суспільства, різних теоретичних підходів до визначення понять інформаційної та національної безпеки, їх взаємозв'язку, політико-правових механізмів їх забезпечення на шляху до розвитку суспільно-політичної стабільності. Актуальність дослідження зумовлена тим, що суперництво між державами тепер відбувається на інформаційному фронті, що стає принципово новим полем боротьби. Створення та розвиток глобального інформаційного простору призвели до зростання кіберзагроз у всіх сферах суспільного життя, зокрема політики та економіки. Осмислюється питання міжнародного співробітництва в забезпеченні інформаційної безпеки в межах Організації Об'єднаних Націй (ООН) і Європейського Союзу (ЄС), вказується на масштаби глобальних інформаційних викликів та неможливість самостійного вирішення зазначених проблем окремими державами. Проаналізовано ключові нормативно-правові акти, які були прийняті Генеральною Асамблеєю ООН та містять положення про загрози міжнародній інформаційній безпеці. Також дослідити вплив інформаційної безпеки держави на національну безпеку дозволив аналіз останніх публікацій вітчизняних і зарубіжних фахівців у сфері інформаційної політики, зокрема А. Войціховського, К. Захаренка, З. Коваля та інших.

Наукова новизна полягає у наданні практичних рекомендацій щодо вдосконалення інституційного забезпечення та політичних інститутів інформаційної безпеки та протидії загрозам кіберпростору. Акцентується на тому, що державна інформаційна політика повинна відповідати нагальним питанням, що виникли у міжнародній інформаційній сфері. Важливою задачею є розроблення та реалізація основних принципів, пріоритетів і завдань державної політики інформаційної безпеки, що потребує поліпшення інституційних, правових, організаційних механізмів управління сферою.

Ключові слова: *інформаційна безпека, кібербезпека, суспільна стабільність, інформаційна політика.*

Вступ. В сучасному світі кіберпростір є основним полем конкуренції у політичній, економічній, культурно-інформаційних сферах. Розвиток інформаційно-комунікаційних технологій дозволив створити новий віртуальний простір, в якому взаємодіють різні політичні сили та держави. У кіберпросторі відбувається багато протистоянь, зокрема між розвідувальними та військовими структурами різних країн. Ці процеси мають велике значення для сучасного політичного аналізу та політичної практики. З міркувань національної безпеки, інформаційна безпека стає невід'ємним елементом системи захисту держави. У зв'язку з цим, важливо розробляти ефективну інформаційну політику та створювати систему захисту від потенційних загроз в кіберпросторі.

В умовах повномасштабного вторгнення РФ на територію України, проблема забезпечення інформаційної безпеки стає все більш актуальною для сучасних демократій і їх стабільного розвитку. Інформаційна війна, кібератаки, шпигунство, дезінформація та інші загрози в інформаційному просторі можуть масово впливати на суспільство, викликати дестабілізацію політичної та економічної ситуації, а також негативно впливати на державну безпеку. Тому розуміння та аналіз процесів, що відбуваються в

кіберпросторі, стає надзвичайно важливим для розвитку безпекових стратегій, як для окремих держав, так і для міжнародної спільноти. Належне вивчення теми може допомогти у підвищенні рівня захисту державних та особистих інформаційних ресурсів від можливих загроз, забезпечити стійкість державної системи загалом.

Аналіз останніх досліджень і публікацій. Дослідження інституційного забезпечення інформаційної безпеки держави є важливим завданням, оскільки інформаційні загрози є динамічними та постійно змінюються в умовах розвитку інформаційного суспільства. Науковці з різних галузей знань внесли свій вклад у дослідження теоретичних питань забезпечення інформаційної безпеки, що дозволило розробити рекомендації та практичні рішення з покращення інституційного забезпечення інформаційної безпеки держави, а також у вивченні міжнародно-правових проблем цієї сфери та досвіду міжнародного співробітництва (О. Бандурка, І. Боднар, Р. Марутян, В. Горбулін, К. Захаренко, А. Войціховський, О. Запорожець, І. Івченко, Г. Ситник, Р. Калюжний, В. Ліпкан, Г. Новицький, В. Пилипчук, Є. Скулиш, А. Марущак, М. Стрельбицький, Т. Ткачук, О. Тихомиров та інші). Ці дослідження є важливим джерелом інформації для аналізу поточних загроз інформаційній безпеці держави, а також для розробки практичних рекомендацій щодо вдосконалення державної інформаційної політики.

Мета і завдання статті. Стаття присвячена аналізу сучасних загроз інформаційної безпеки, а також основним напрямкам державної інформаційної політики, необхідних для забезпечення національної безпеки та політичної стабільності. Проведений аналіз дозволить виявити потенційні загрози та визначити ефективні заходи, спрямовані на запобігання та мінімізацію негативних наслідків інформаційних атак, також розглянуті основні напрямки державної інформаційної політики, необхідні для забезпечення національної безпеки, зокрема розвиток політичних інститутів, вдосконалення правових інструментів, розвиток кібербезпеки, підвищення рівня інформаційної грамотності тощо. Для досягнення мети пропонуються такі завдання: дослідити теоретичні підходи до визначення сутності понять «інформаційна безпека» та «національна безпека»; визначити взаємозв'язок між інформаційною безпекою та національною безпекою; дати загальну характеристику політико-правової основи міжнародного співробітництва держав у забезпеченні інформаційної безпеки в межах ЄС; дослідити питання забезпечення інформаційної безпеки України, виявити реальні та потенційні інформаційні загрози для інформаційного простору країни; розробити конкретні пропозиції зі вдосконалення державної інформаційної політики. В результаті виконання цих завдань варто зробити висновки про (не)ефективність політичних інститутів інформаційної безпеки, а також розробити рекомендації для подальшого її вдосконалення на шляху розвитку суспільно-політичної стабільності.

Цілі наукової статті досягаються через залучення комплексу **методів,** серед яких центральним є проведення політико-правового аналізу сучасних загроз інформаційній безпеці та основних напрямів розвитку державних інститутів інформаційної безпеки.

Результати та дискусії. У сучасній політико-філософській думці існує два підходи до визначення поняття «національна безпека». Перший підхід, який є реалістичним, був започаткований американським фахівцем Г. Моргентау. Він визначив національну безпеку як недоторканність території та інститутів держави і наголосив на воєнній та політичній безпеці, що є традиційним розумінням. Другий підхід розвивався в межах ідеалістичної теорії міжнародних відносин, зосереджується на аналізі політико-економічних, соціальних, гуманітарних та інших проблем. Український законодавець, виходячи з другого підходу, сформував потужну правову базу політики національної

безпеки протягом років державної незалежності. Основою цієї політики є чинна Конституція України, яка встановлює засади забезпечення безпеки людини та визначає найважливіші функції держави: захист суверенітету та територіальної цілісності, забезпечення економічної та інформаційної безпеки, які є справою всього українського народу (*Конституція України, прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року*, 1996). Закон України «Про національну безпеку України», що був прийнятий 21 червня 2018 р., регулює правові засади національної безпеки України і визначає понятійний апарат у цій сфері («Про національну безпеку України», 2018).

На основі зазначених положень можна стверджувати, що до об'єктів національної безпеки України належать: права, свободи та обов'язки людини і громадянина; цінності, ресурси та навколишнє середовище суспільства; конституційний лад, територіальна цілісність, недоторканність і суверенітет держави. З огляду на складність національної безпеки, вона містить численні підсистеми, елементи та складові, серед яких можна виділити політико-економічну, соціальну, воєнну, екологічну, інноваційну, технологічну безпеку.

З урахуванням швидкого розвитку інформаційно-комунікаційних технологій і створення глобального інформаційного простору, виникли нові субстанції, такі як кіберпростір, інформаційне суспільство, які мають значний вплив на політико-економічний, соціальний і культурний розвиток держави. Інформаційне суспільство також призвело до появи багатьох кіберзагроз у важливих сферах суспільного життя, зокрема банківській, воєнній, критичної інфраструктури тощо. Тому інформаційна безпека повинна бути розглянута в якості самостійного елемента національної безпеки.

«Інформаційна безпека» є терміном, що має правове значення і означає стан захищеності національних інтересів України в інформаційній сфері. Цей стан визначається сукупністю збалансованих інтересів особистості, суспільства та держави (Войціховський, 2020).

Глобалізація сучасного інфопростору спричинює послаблення інформаційного суверенітету держави, що впливає на загальний стан державної безпеки. Це також спричинило необхідність формування та удосконалення системи заходів міжнародної інформаційної безпеки. Оскільки масштаби глобальних викликів у інформаційній сфері надзвичайно великі, і вирішення цих проблем зусиллями однієї або навіть декількох держав неможливе, необхідно розвивати міждержавне співробітництво в межах ООН.

У 1998 р. світ побачив знаковий крок у забезпеченні міжнародної інформаційної безпеки – Резолюція Генеральної Асамблеї ООН A/RES/53/70, яка засвідчила необхідність збереження інформаційної безпеки в умовах росту загроз і викликів. Цей документ став першим кроком до зміцнення міжнародної координації у питаннях інформаційної безпеки. Резолюція, прийнята в 1998 р., відкрила широку дискусію про необхідність створення міжнародного правового режиму, який визначав би статус інформації, інформаційних технологій та методів їх використання. Це стало першим кроком до створення відповідного правового інструментарію, який би регулював питання інформаційної безпеки в міжнародному співтоваристві («Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки», 1999a).

У 1999 р. була прийнята Резолюція Генеральної Асамблеї ООН A/RES/54/49, яка наголошувала на загрозах для міжнародного інформаційного простору, як для цивільної, так і військової сфери. Виконуючи цю Резолюцію, в 2000 р. були представлені принципи, що внормували б правила поведінки держав в інфопросторі та заклали основу для міжнародної співпраці з вирішення проблем інформаційної безпеки. Принципи надають визначення ключових понять системи міжнародної інформаційної безпеки, таких як

«інформаційні простори», «інформаційні війни», «інформаційні ресурси», «інформаційна зброя», «інформаційна безпека» та інші («Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки», 1999b).

Майбутні резолюції стосувались боротьби зі злочинним використанням IT-технологій, створення глобальної системи кібербезпеки та захисту інформаційної інфраструктури. Значний внесок у забезпечення міжнародної інформаційної безпеки було зроблено за допомогою Резолюції A/RES/62/17 від 5 грудня 2007 р., яка сприяла розгляду існуючих і потенційних загроз у цій сфері. Крім того, Резолюція A/RES/71/28 від 5 грудня 2016 р. відзначила досягнення в галузі інформатизації та телекомунікацій в контексті забезпечення міжнародної безпеки. Обидві резолюції зробили вагомий внесок у розвиток інтернаціонального діалогу з питань інформаційної безпеки.

ЄС є також серед ключових гравців у забезпеченні міжнародної інформаційної безпеки та кібербезпеки. Вже у 2001 р. Комісією ЄС було представлено видання «Мережева та інформаційна безпека: європейський політичний підхід», де було запропоновано концепцію розв'язання проблем інформаційної безпеки. Цей документ став важливим кроком у напрямі розробки політики, спрямованої на забезпечення безпеки інформації. Зараз ЄС продовжує вести активну політику у цій сфері та докладає зусиль для забезпечення кібербезпеки інформаційного простору. Згідно з визначенням, термін «мережева та інформаційна безпека» трактується як здатності мережі або інформаційної системи відповідати на випадкові події або зловмисні дії, які можуть становити загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, які надаються через ці мережі та системи (*Network and information security: proposal for a european policy approach, 2001*). Особливу увагу в документі приділено запобіганню зловживань у сфері інформаційної безпеки, розвитку заходів щодо протидії кіберзлочинності, створенню міжнародної співпраці в цій сфері та підтримці культури кібербезпеки.

Після прийняття документу «Мережева та інформаційна безпека: європейський політичний підхід» Комісією ЄС в 2001 р., у ЄС було прийнято значну кількість нормативно-правових актів, які містили різноманітні підходи до забезпечення інформаційної безпеки в країнах-членах.

У лютому 2013 р. Європейський Союз представив стратегію кібербезпеки «Відкритий, надійний та безпечний кіберпростір», яка закликає держави-члени розвивати міжнародне співробітництво для боротьби з кіберзагрозами. У липні 2016 р. була прийнята директива Європейського парламенту та Ради ЄС, яка зосереджується на заходах щодо забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС. Ця директива встановлює загальні правила та вимоги в галузі кібербезпеки для всіх країн-членів ЄС, що дозволяє підвищити спроможність системи кібербезпеки на всіх рівнях, а також зобов'язує операторів базових та цифрових послуг повідомляти про кіберінциденти. У вересні 2017 р. Комісія ЄС оприлюднила повідомлення про створення сильної кібербезпеки для ЄС, де наголошується на важливості кіберзахисту для безпеки держав-членів ЄС та необхідності колективного підходу у протидії кіберзагрозам.

Для поліпшення системи інформаційної безпеки в ЄС було створено спеціалізований організаційний механізм – Європейське агентство з питань мережевої та інформаційної безпеки (ENISA). Європейський агентство з мережевої та інформаційної безпеки, має на меті не тільки покращення мережево-інформаційної безпеки в ЄС, але й створення сприятливих умов для забезпечення цієї безпеки для громадян, підприємств та громадських організацій ЄС. Агентство працює над розвитком культури мережевої та інформаційної безпеки серед всіх зацікавлених сторін, зокрема веде роботу з вирішення

проблем безпеки Інтернету речей та інших технологій. Крім того, ENISA забезпечує підтримку безперебійного функціонування ринку ЄС, сприяючи розвитку стандартів та методів для забезпечення мережевої та інформаційної безпеки (*European Union Agency for Network and Information Security*). ENISA забезпечує координацію між країнами-членами ЄС у сфері кібербезпеки, сприяє обміну інформацією та надає поради щодо розробки та впровадження стратегій кібербезпеки. Крім того, ENISA допомагає забезпечити зв'язок між країнами-членами ЄС та міжнародними організаціями щодо кібербезпеки.

Беручи до уваги той факт, що ефективність інформаційного захисту в європейському кіберпросторі залежить від співпраці держав в рамках міжнародних органів, в структурі Європейського поліцейського офісу був створений Європейський центр боротьби з кіберзлочинністю у 2013 р. Цей центр покликаний розслідувати мережеві шахрайства, а також злочини, які становлять загрозу безпеці критично важливих інфраструктур та інформаційних систем ЄС. Напрямки діяльності Центру включають також співпрацю з іншими міжнародними організаціями, які займаються боротьбою з кіберзлочинністю, з метою підвищення рівня захисту інформаційної безпеки в Європі.

Слід зауважити, що ЄС нині докладає зусиль для модернізації секторів безпеки в кіберпросторі з метою відповіді на сучасні виклики. Це включає в себе оновлення нормативної бази, що забезпечує цілісність державної політики у цій сфері, розробку європейських принципів інформаційної безпеки, збільшення чисельності суб'єктів, що займаються інформаційною безпекою, посилення контролю за національним інформаційним простором, а також зміцнення захисних механізмів для критично важливої інфраструктури ЄС. Ці заходи є частиною широкої стратегії підвищення ефективності системи інформаційної безпеки в кіберпросторі ЄС і забезпечення захисту від потенційних загроз, що можуть виникнути в цьому середовищі.

Оскільки інформаційна безпека є важливим елементом національної безпеки, більшість країн по всьому світу приділяють увагу проблемі безпеки в кіберпросторі та розробляють комплексні заходи для її забезпечення. Зокрема, країни зосереджуються на створенні та вдосконаленні національного законодавства в галузі кібербезпеки, а також на створенні спеціалізованих структур, що забезпечують безпеку в кіберпросторі. Окрім того, більшість країн забезпечує посилення кваліфікації фахівців із кібербезпеки та зміцнення захисту критичної інфраструктури від кібератак. Важливим етапом вдосконалення заходів з кібербезпеки є співпраця між державами у рамках міжнародних організацій.

Сьогодні кібербезпека є однією з найважливіших проблем для держав. Розуміння необхідності її забезпечення є ключовим фактором для підвищення національної безпеки та надійності інформаційних систем держави. Велика кількість країн, зокрема США, ЄС, Японія та Індія, приділяють велику увагу розробці стратегій із кібербезпеки, що свідчить про її всесвітню актуальність. Україна також визнає проблему кібербезпеки як пріоритетну та затвердила власну Стратегію кібербезпеки, яка визначає пріоритетні напрямки та допомагає формувати політику інформаційної безпеки, що відповідає міжнародним стандартам. Вирішення цієї проблеми вимагає комплексних заходів, таких як розробка та вдосконалення законодавства в галузі кібербезпеки, а також створення спеціалізованих структур, які відповідають за її забезпечення.

Для держав надзвичайно важливою є і проблема захисту критичної інфраструктури. Під критичною інфраструктурою мають на увазі системи, мережі та активи, які є взаємозалежними та життєво необхідними для безперебійного функціонування суспільства. Така інфраструктура може бути як військовою, так і цивільною, а також мати подвійне призначення. До прикладів критичної інфраструктури можна віднести мости,

споруди зв'язку, аеропорти, енергетичну інфраструктуру, банківський сектор, виробництво та розподіл електроенергії, медичні установи, державні аварійно-рятувальні служби тощо. Забезпечення безпеки такої інфраструктури є завданням кожної країни, оскільки порушення її роботи може призвести до значних наслідків для суспільства та економіки.

Згідно з Резолюцією Ради Безпеки ООН S/RES/2341 (2017) від 13 лютого 2017 р., кожна держава самостійно визначає, які об'єкти своєї інфраструктури є критичними і як забезпечити їх ефективний захист. Однак національний перелік об'єктів критичної інфраструктури може значно відрізнятися в різних країнах. Наприклад, у США в цей перелік можуть входити не тільки об'єкти, що забезпечують життєдіяльність суспільства, а й національні пам'ятники, виборча система, дипломатичні місії та інші. Враховуючи зростаючі загрози кібербезпеці, необхідно забезпечити захист не лише традиційних об'єктів критичної інфраструктури, а й звернути увагу на нові сегменти інфраструктури, такі як мережі Інтернету речей та інші цифрові технології («Про захист критичної інфраструктури», 2017).

В сучасному світі розвитку інформаційного суспільства, критична інфраструктура безпеки не може існувати без інформаційної інфраструктури, що передбачає використання комп'ютерів та мереж, зокрема систем диспетчерського управління та збору даних. Взаємодія цих систем дозволяє обмінюватися інформацією та здійснювати аналіз, що є критично важливим для забезпечення функціонування критичної інфраструктури.

З іншого боку, доступ до управління критичною інфраструктурою за допомогою далекого доступу дозволяє підвищити ефективність та зменшити витрати, але також створює загрозу кібербезпеці. У зв'язку з цим, кібератаки на критичну інфраструктуру можуть бути використані як знаряддя військової агресії в геополітичних конфліктах. Руйнування нафтопроводів, вимкнення електростанцій, припинення постачання води та опалення комунальних підприємств може надати значну військову перевагу. Отже, забезпечення кібербезпеки критичної інфраструктури стає одним з актуальних завдань для будь-якої країни у світі. Будь-які кібератаки на критичну інфраструктуру можуть підірвати основи національної безпеки та нанести значні економічні збитки.

За останні роки кібербезпека викликає значний інтерес у світі, оскільки інформаційні технології є неодмінною складовою життя сучасного суспільства. У такому контексті, критична інфраструктура стає особливо вразливою до кібератак, що можуть мати непередбачувані наслідки для безпеки та економіки країни. Зокрема дії хакерів можуть спричинити значні збитки, знизити рівень виробництва та надійності електромереж, нафтопроводів, водопровідних систем та інших критичних інфраструктурних об'єктів, що призведе до серйозних наслідків для національної безпеки та економіки країни. У зв'язку з цим, вирішення проблеми кібербезпеки та захист критичної інфраструктури від кіберзагроз є прагненням забезпечити стабільність та безпеку держави, суспільства, економіки.

Україна не залишається осторонь проблеми інформаційної безпеки, особливо в останні роки, коли стикається з ворожим впливом, що спонукає до сепаратизму, насильства, національної ворожнечі. Це також охоплює спроби руйнування національної ідентичності, знищення міжнаціональної злагоди, порушення конституційного ладу та територіальної цілісності України. Країна стикається з інформаційною експансією, яка проводиться з боку Російської Федерації та спрямована на забезпечення домінування в українському та глобальному інформаційному просторі. Російські пропагандистські інформаційно-психологічні кампанії та медіазаходи впливають на формування не тільки громадянської ідентичності, а й міжнародного іміджу України. В умовах

повномасштабної війни забезпечення інформаційної безпеки є однією з найактуальніших проблем для України.

З метою забезпечення інформаційної безпеки України, враховуючи відповідні загрози, потрібно звернути увагу на такі заходи:

1) розвивати інформаційний суверенітет України, забезпечивши державне регулювання розвитку інформаційної сфери та національну інформаційну інфраструктуру;

2) використовувати сучасні технології, за допомогою яких надавати достовірну інформацію в українському та світовому інформаційному просторах;

3) захищати конституційне право громадян на свободу слова та доступ до інформації;

4) запобігати неправомірному втручанню державних і місцевих органів влади в діяльність медіа та переслідуванню журналістів за їх політичні погляди;

5) реалізувати комплексні заходи щодо захисту національного інформаційного простору та боротьби з монополізацією інформаційної сфери в Україні.

У законодавстві України продовжується підготовка до боротьби з загрозами критичної інфраструктури. Зокрема Закон України «Про національну безпеку України» встановлює завдання практичної реалізації нових підходів у протидії загрозам критичної інфраструктури («Про національну безпеку України», 2018). Поряд із цим прийнятий Закон «Про критичну інфраструктуру», що передбачає встановлення правових та організаційних засад забезпечення діяльності системи захисту критичної інфраструктури. Цей закон є значущим кроком у розвитку системи захисту критичної інфраструктури держави та стане невід'ємною частиною законодавства України, яке стосується національної безпеки («Про критичну інфраструктуру та її захист»). Після прийняття закону будуть визначені принципи та напрями розбудови системи захисту критичної інфраструктури, а також забезпечення необхідної законодавчої бази для її діяльності.

Висновки. Підсумовуючи наведений вище матеріал, можна зробити висновок, що в наш час захист інформаційного простору та забезпечення інформаційної безпеки стали важливими завданнями для багатьох держав світу. Загрози інформаційної безпеки мають міжнародний характер, що вимагає розробки спільної стратегії інформаційної безпеки та розвитку міжнародного співробітництва, зокрема й у рамках міжнародних організацій. Такі кроки дозволять забезпечити ефективний захист національного інформаційного простору та зменшити загрози національній безпеці. Отже, захист інформаційної безпеки – це важливе завдання, яке потребує уваги та координації зусиль на рівні країн та міжнародної спільноти.

Забезпечення інформаційної безпеки є одним із найважливіших завдань і для сучасної України. Це зумовлено необхідністю боротьби зі злочинними діями, ворожими атаками, спрямованими на посягання на інформаційний простір країни. Зважаючи на визнаний пріоритет європейської інтеграції в зовнішній політиці України, владі необхідно розвивати ефективний діалог з ЄС з питань забезпечення інформаційної безпеки.

При цьому, для досягнення максимальної ефективності у цій сфері, необхідно вивчати досвід країн, які вже мають відповідну організаційно-правову основу та успішно застосовують її. Вивчення та використання цього досвіду у національній законотворчості та реалізації заходів забезпечення інформаційної безпеки є надзвичайно важливим для України, її розвитку як суверенної та незалежної держави, а також як стабільної демократії. Перспективним вбачаємо глибший аналіз взаємозв’язку процесів подальшої демократизації та інформаційного захистку держави.

Використані джерела:

1. Конституція України, прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. (1996). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. «Про національну безпеку України», Закон України (2018). https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Войціховський, А. (2020). Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО», (29), 281–288.
4. «Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки», Резолюція A/RES/53/70 ГА ООН (1999a). https://undocs.org/en/A/RES/53/70
5. «Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки», Резолюція A/RES/54/49 ГА ООН (1999). https://undocs.org/en/A/RES/54/49
6. Network and information security: proposal for a european policy approach. (2001, 6 червня). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN
7. Council framework decision 2005/222/JHA on attacks against information systems. (2005, 24 лютого). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222
8. Towards a general policy on the fight against cyber crime. (б. д.). https://eurlex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14560
9. European Union Agency for Network and Information Security. (б. д.). https://www.enisa.europa.eu/about-enisa
10. «Про захист критичної інфраструктури», Резолюція Ради Безпеки ООН S/RES/2341 (2017). https://undocs.org/en/S/RES/2341(2017)
11. «Концепція створення державної системи захисту критичної інфраструктури», Розпорядження Кабінету Міністрів України № 1009-р (2017). https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi
12. «Про критичну інфраструктуру та її захист», Проект Закону (б. д.). https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996
13. Захаренко, К. (2021). Інституційний вимір інформаційної безпеки України [дис. д-ра політ. наук]. Національний педагогічний університет імені М. П. Драгоманова.
14. Коваль, З. (2011). Політико-правові механізми державного управління інформаційно-психологічною безпекою України [дис. канд. наук з держ. упр.].

References:

1. Konstytutsiia Ukrainy, pryiniata na piatii sesii Verkhovnoi Rady Ukrainy 28 chervnia 1996 roku. (1996). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. "Pro natsionalnu bezpeku Ukrainy", Zakon Ukrainy (2018). https://zakon.rada.gov.ua/laws/show/2469-19#Text
3. Voitsikhovskyi, A. (2020). Informatsiina bezpeka yak skladova systemy natsionalnoi bezpeky (mizhnarodnyi i zarubizhnyi dosvid). Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia «PRAVO»., (29), 281–288.
4. "Dosiahnennia u sferi informatyzatsii ta telekomunikatsii v konteksti mizhnarodnoi bezpeky", Rezoliutsiia A/RES/53/70 HA OON (1999a). https://undocs.org/en/A/RES/53/70
5. "Dosiahnennia u sferi informatyzatsii ta telekomunikatsii v konteksti mizhnarodnoi bezpeky", Rezoliutsiia A/RES/54/49 HA OON (1999). https://undocs.org/en/A/RES/54/49
6. Network and information security: proposal for a european policy approach. (2001, 6 chervnia). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN
7. Council framework decision 2005/222/JHA on attacks against information systems. (2005, 24 liutoho). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222
8. Towards a general policy on the fight against cyber crime. (b. d.). https://eurlex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14560

9. European Union Agency for Network and Information Security. (b. d.). https://www.enisa.europa.eu/about-enisa
10. "Pro zakhyst krytychnoi infrastruktury", Rezoliutsiia Rady Bezpeky OON S/RES/2341 (2017). https://undocs.org/en/S/RES/2341(2017)
11. "Kontseptsiia stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury", Rozporiadzhennia Kabinetu Ministriv Ukrainy № 1009-r (2017). https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi
12. "Pro krytychnu infrastrukturu ta yii zakhyst", Proekt Zakonu (b. d.). https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996
13. Zakharenko, K. (2021). Instytutsiinyi vymir informatsiinoi bezpeky Ukrainy [dys. d-ra polit. nauk]. Natsionalnyi Pedahohichnyi universytet imeni M. P. Drahomanova.
14. Koval, Z. (2011). Polityko-pravovi mekhanizmy derzhavnoho upravlinnia informatsiino-psykholohichnoiu bezpekoiu Ukrainy [dys. kand. nauk z derzh. upr.].

Yehor Minenko,
PhD student at the Educational and Research Institute
of Law and Political Science,
Mykhailo Drahomanov Ukrainian State University

Organizational and Legal Analysis of Information Security as a Factor of Socio-Political Stability

The article analyzes the organizational and legal aspects of ensuring information security in the context of the development of the information society, various theoretical approaches to defining the concepts of information and national security, their interconnection, and political and legal mechanisms for ensuring them on the way to the development of socio-political stability. The relevance of the study is due to the fact that the rivalry between states is now taking place on the information front, which is becoming a fundamentally new field of struggle. The creation and development of the global information space has led to an increase in cyber threats in all spheres of public life, including politics and economics.

The author discusses the issue of international cooperation in ensuring information security within the United Nations (UN) and the European Union (EU), and points out the scale of global information challenges and the impossibility of individual states to solve these problems on their own. The author analyzes the key legal acts adopted by the UN General Assembly that contain provisions on threats to international information security. The analysis of recent publications of domestic and foreign experts in the field of information policy, in particular A. Voitsikhovsky, K. Zakharenko, Z. Koval and others, allowed to study the impact of the state's information security on national security.

The scientific novelty is to provide practical recommendations for improving the institutional support and political institutions of information security and countering cyberspace threats. The author emphasizes that the state information policy should respond to the pressing issues that have arisen in the international information sphere. An important task is to develop and implement the basic principles, priorities and tasks of the State information security policy, which requires improvement of institutional, legal and organizational mechanisms for managing the sphere.

Keywords*: information security, cybersecurity, social stability, information policy.*