УДК 351.751+34.07:004.056.5(477)

Глобенко Сергій

ORCID iD 0000-0002-9751-4213
e-mail: svhlobenko@ukr.net

СТАНОВЛЕННЯ Й РОЗВИТОК ПРАВОВОГО ПОЛЯ УКРАЇНИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВИ

https://doi.org/10.33269/2618-0065-2023-2(14)-64-79

Анотація. Наведено результати дослідження чинної нормативно-правової бази України, згідно з якою унормовано питання захисту інформаційного простору держави в умовах сьогодення. З'ясовано, що захист суверенітету, територіальної цілісності та національної безпеки є ключовими завданнями для будь-якої держави, у тому числі й України. Конкретизовано виклики й загрози у сферах інформаційної та кібербезпеки, зокрема щодо відсутності цілісної державної інформаційної політики. Встановлено, що у правовому полі України інформаційна безпека передбачає захист від зовнішніх впливів і дезінформації, що потребує спільних зусиль від залучених до процесу суб'єктів управління. Глобальні виклики, які стоять перед нашою державою, та відповідні стратегічні цілі спрямовані на забезпечення захисту національних інтересів та зміцнення суспільної стабільності. Підкреслено важливість здійснення низки пріоритетних заходів щодо забезпечення захисту кіберпростору в контексті гарантування національної безпеки. Наголошено на ризиках, нормативно закріплених пріоритетах та завданнях. Розглянуто загальний контекст зазначеної проблеми й актуалізовано важливість забезпечення кібербезпеки для національної безпеки, враховуючи сучасні виклики та загрози. Охарактеризовано основні складові національної системи стійкості, поєднання яких спрямовано на забезпечення національної безпеки України в умовах сучасних загроз, зокрема гібридних. З'ясовано, що внаслідок своєї комплексності мають враховуватися різні аспекти життєдіяльності суспільства і держави, в тому числі економічні, енергетичні, інформаційні, кібернетичні, екологічні, продовольчі, охорони здоров'я, освіти та культури тощо. Зазначено про важливість дотримання моральних та етичних норм під час створення й поширення медійного контенту з урахуванням обмежень для захисту національної безпеки та інформаційної безпеки держави. Встановлено необхідність уніфікації норм чинного правового поля задля створення єдиного інформаційного простору для забезпечення безпеки інформаційної взаємодії та зміцнення національної системи стійкості.

Ключові слова: нормативно-правове регулювання, інформаційний простір держави, інформаційна безпека, захист інформаційного простору, правове поле, державна політика в інформаційній сфері, механізми державного управління.

Постановка проблеми. Проблема формування й подальшого розвитку правового поля щодо захисту інформаційного простору держави актуалізується з огляду на мінливість зовнішніх і внутрішніх факторів, що мають критичний вплив на цю сферу публічного управління. Інформаційний фронт у глобальних та національних конфліктах надзвичайно важливий. Зокрема, це контроль над засобами масової інформації, робота з дезінформацією та підтримка свободи медіа. Захист критично важливих інформаційних систем, державних електронних інформаційних ресурсів та даних є одним із ключових завдань задля забезпечення національної безпеки та суспільної стабільності, належного функціонування національної системи стійкості.

Україна постійно працює щодо удосконалення своєї правової бази у сфері захисту інформаційного простору держави, що охоплює різні напрями цієї загальної проблеми. І саме тому з урахуванням зазначених факторів становлення та розвиток правового поля України у сфері захисту інформаційного простору варто розглядати як невід'ємну складову частину забезпечення національної безпеки та збереження інформаційного суверенітету країни.

Аналіз останніх досліджень і публікацій. Проблеми, пов'язані з дослідженням правового поля України щодо захисту інформаційного простору держави (у тому числі в умовах надзвичайних ситуацій), неодноразово ставали предметом інтересу дослідників.

Так, В. Батиргареєва у своїй теоретичній розвідці розглядає питання захисту інформаційного простору України за допомогою інструментів кримінального права. Основним висновком науковиці є те, що законодавство містить різні вимоги щодо захисту інформаційних відносин, унормованих різними розділами Кримінального кодексу України. Аналіз дослідження показує, що існує дискусія щодо того, чи має виступати пріоритетом захист інформаційного простору з-поміж інших форм інформаційного комунікування. Авторка вважає, що ефективна модель захисту має містити норми, які захищають всіх суб'єктів, які можуть стати жертвами відповідних злочинів, і пропонує об'єднати їх в одному розділі

Кримінального кодексу України. Вона також наголошує на захисті інформаційного простору як унікального середовища, пов'язаного з обігом та захистом інформації в усіх її формах, а також інструментів її обміну в суспільстві. На її думку, цього можна досягти завдяки створенню єдиної платформи захисту відповідних суспільних відносин як розділу Особливої частини Кримінального кодексу України [1].

У публікації С. Усик окреслено аспекти державного регулювання в галузі забезпечення інформаційної безпеки в умовах надзвичайних ситуацій – складну проблему сьогодення. Авторка вказує, що відповідного законодавства, яке б визначало питання забезпечення безпеки інформаційної системи в умовах надзвичайних ситуацій та системи обробки й обміну інформацією у сфері захисту населення і територій від надзвичайних ситуацій та їхніх наслідків, немає. Також зазначає, що державне регулювання технічного захисту інформації та інформаційної безпеки є важливою частиною загальної системи забезпечення інформаційної безпеки, а тому має відбуватися в межах відповідної державної політики в цій галузі. Це, зокрема, передбачає розроблення комплексного законодавства, що регулюватиме ці питання та забезпечуватиме національні інтереси в інформаційній сфері в умовах надзвичайних ситуацій [2].

В. Микулець характеризує процес переходу України до інформаційного суспільства, вказуючи на те, що наша держава відстає в цьому процесі від розвинутих країн, але це дає їй змогу врахувати важливі аспекти державного регулювання в інформаційній сфері. Великої ваги набуває формування єдиного інформаційного простору для України, що має забезпечувати безпеку інформаційної взаємодії, задовольняти інформаційні потреби громадян та захищати інформаційний суверенітет держави. Такий єдиний інформаційний простір потребує дотримання загальних правил для всіх суб'єктів інформаційної взаємодії, забезпечення безпеки та рівності перед законом щодо доступу до інформаційних ресурсів, що у своїй сукупності сприяє зміцненню національного суверенітету держави [3].

Мета статті – огляд чинної нормативно-правової бази України щодо захисту інформаційного простору держави,

узагальнення підходів до нормативного закріплення відповідних стратегічних пріоритетів, цілей, завдань і заходів, виявлення недоліків зазначеної сфери та перспектив розвитку правового поля України у вказаному напрямі.

Методи дослідження. В основу дослідження покладено загальнонаукові методи: аналіз і синтез (для уявного розчленовування правового поля України в контексті захисту інформаційного простору держави на його складові частини задля виділення окремих сторін, властивостей, зв'язків із подальшим їх уявним з'єднанням, аби осягнути ціле в його єдності), індукція та дедукція (за допомогою переходу від знання окремих фактів до знання загального (аналіз фактів), переходу від знання загальних закономірностей до окремого його прояву (аналіз понять)), ідеалізації (як творення ідеалу правового поля через виокремлення та узагальнення окремих ознак інформаційного простору), логічний метод (заради пізнання і відтворення досліджуваного об'єкта) у поєднанні з контент-аналізом, описом та узагальненням.

Виклад основного матеріалу. Захист суверенітету, територіальної цілісності та забезпечення національної безпеки є найважливішими завданнями будь-якої держави, у тому числі й України, що закріплено у статті 17 Конституції України [4]. Ці аспекти є підгрунтям для гарантування всіх інших прав і свобод громадян, а також для соціального та економічного розвитку країни.

У Законі України «Про національну безпеку України» зазначається, що відповідна державна політика «…спрямовується на забезпечення… інформаційної, … кібербезпеки України та на інші її напрями» [5]. Згадані напрями конкретизовано у Стратегії національної безпеки України [6], де зазначено про критичні проблеми в інформаційній сфері, посилення інструментів національної сили (зокрема, інформаційно-психологічних та кіберзасобів), інформаційну зброю, констатовано відсутність цілісної інформаційної політики держави.

Інформаційна безпека передбачає захист інформаційного простору країни від зовнішнього впливу, дезінформації та інших загроз, що можуть шкодити суспільству та державі.

Забезпечення усіх складових національної безпеки потребує від держави і громадян спільних зусиль, а також передбачає розроблення дієвої стратегії та політики у цих сферах.

Стратегією інформаційної безпеки [7] унормовано загальні положення щодо забезпечення інформаційної безпеки України, зокрема через конкретизацію актуальних викликів та загроз у вказаній сфері. У документі визначено стратегічні цілі та завдання, спрямовані на протидію загрозам, а його мета полягає в посиленні спроможностей інформаційної безпеки держави, її інформаційного простору та на цій основі – в забезпеченні стійкості суспільства та держави. В тексті надано визначення ключових термінів, таких як «інформаційна безпека України», «інформаційна загроза», «інформаційні заходи оборони держави» тощо.

Так, інформаційною безпекою України згідно з документом є «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» [7].

Стратегія визначає основні напрями та принципи забезпечення інформаційної безпеки України, закладаючи правову, стратегічну та організаційну бази для відповідної діяльності в означеній сфері.

У ній описано різноманітні глобальні виклики та загрози, пов'язані з інформаційною безпекою. Збільшення кількості глобальних дезінформаційних кампаній, ініційованих авторитарними режимами та радикальними активістами, стало невід'ємною частиною сучасної практики, загрожуючи демократичному розвитку та міжнародній стабільності.

Особлива увага приділяється інформаційній політиці Російської Федерації, яка впливає на демократичні інституції та поглиблює протиріччя в демократичних державах через спеціальні інформаційні операції та гібридну війну.

Також виділяється роль соціальних мереж у сучасному інформаційному просторі, яка зросла під впливом глобалізації та пандемії COVID-19. Підкреслюється, що розвиток цифрових технологій може загрожувати праву на приватність та зумовити виникнення недоліків у гарантуванні безпеки персональних даних. Останній виклик, зазначений у цьому розділі, полягає в недостатньому рівні медіаграмотності, яка призводить до некритичного сприйняття інформації. Зростаюча доступність інформації разом із недостатньою медіаграмотністю сприяє поширенню дезінформації, конспірологічних теорій та маніпуляцій, що може загрожувати стабільності демократичних держав.

У розділі «Національні виклики та загрози» розглянуто інформаційні виклики та загрози, з якими стикається Україна на національному рівні. До них належить інформаційний вплив Російської Федерації як держави-агресора на населення України. РФ застосовує різні методи інформаційного впливу, спрямовані на підрив національної безпеки, ліквідацію української державності та ідентичності, спричиняючи дестабілізацію в суспільстві.

На тимчасово окупованих територіях Росія забезпечує інформаційне домінування через придушення свободи слова, контроль над засобами масової інформації, тотальне обмеження доступу до незалежних інформаційних джерел та побудову альтернативної викривленої інформаційної реальності. Україна важко реагує на ці загрози через обмежені можливості протидіяти інформаційній агресії. Відсутність ефективної системи реагування та розвиненої інформаційної інфраструктури обмежує можливість ефективно протидіяти дезінформаційним кампаніям, що загрожує національній безпеці та інтересам України.

У цьому розділі підкреслюється необхідність розвитку стратегічних підходів і національних заходів для протидії інформаційним загрозам та викликам, зокрема відповідна

підготовка та розбудова інформаційної стійкості суспільства.

Розглядаються й інші аспекти інформаційної безпеки:

– хоча в Україні й проводяться заходи щодо зміцнення інституційної спроможності у сфері стратегічних комунікацій, проте немає ефективного механізму координації та взаємодії між органами державної влади. Це унеможливлює комплексне стратегічне планування інформаційного потоку, співпрацю між ключовими суб'єктами у сфері інформаційних відносин та реалізацію політики щодо захисту національного інформаційного простору;

– наявні проблеми з регулюванням у сфері медіа та журналістики. Недостатність адаптованих до сучасних викликів нормативно-правових меж ускладнює розвиток медіаринку, зберігає залежність засобів масової інформації, інколи призводить до посягань на свободу журналістської діяльності та безпосередньо журналістів;

– намагання дестабілізувати консолідацію суспільства щодо європейської та євроатлантичної інтеграції через поширення міфів та дезінформаційних стереотипів. Це може значною мірою впливати на реформи та зовнішньополітичний курс країни;

– необхідність підвищення рівня інформаційної грамотності серед населення, щоб більш ефективно протидіяти дезінформаційним кампаніям та маніпуляціям.

Стратегічні цілі й напрями реалізації Стратегії інформаційної безпеки України [7] охоплюють різні аспекти інформаційної безпеки та націлені на захист національних інтересів, забезпечення стабільності суспільства і підвищення інформаційної культури, сприяючи його консолідації.

Очікувані результати реалізації стратегії є ключовими показниками її успішності та вказують на те, яких позитивних змін має бути досягнуто через упровадження зазначених стратегічних напрямів, а саме:

– захищений інформаційний простір України. Завдяки реалізації стратегії інформаційний простір країни буде добре захищений від негативного впливу, дезінформації та маніпуляцій, які можуть завдати шкоди національній безпеці та стабільності суспільства;

– ефективне функціонування системи стратегічних комунікацій. Органи влади та інші суб'єкти публічного управління будуть успішно співпрацювати, координувати свою інформаційну діяльність та забезпечувати взаємодію для досягнення спільних цілей;

– ефективна протидія поширенню незаконного контенту. Буде досягнута висока ефективність у протидії незаконному або шкідливому контенту в глобальній телекомунікаційній мережі;

– забезпечення інформаційної реінтеграції громадян. Громадяни, які проживають на тимчасово окупованих територіях, зможуть мати безперешкодний доступ до українського інформаційного простору та телерадіомовлення;

– підвищення рівня медіакультури та медіаграмотності. Результат полягає у досягненні високого рівня розуміння та критичного осмислення інформації серед населення, що допомагає запобігати поширенню дезінформації та маніпуляцій;

– дотримання конституційних прав. Буде забезпечено право громадян на вільне вираження своїх поглядів і переконань, а також буде гарантовано право на приватність та захист журналістів від небезпек в аспекті виконання їхньої професійної діяльності;

– формування громадянської ідентичності. Громадяни будуть мати можливість вільно формувати власну ідентичність на основі українських цінностей, традицій, культури та історії.

Вказані результати сприятимуть підвищенню інформаційної безпеки, стабільності та зміцненню суверенітету України.

Згідно зі Стратегією кібербезпеки України, затвердженою відповідним Указом Президента України [8], яка, зокрема, грунтується на положеннях Закону України «Про основні засади забезпечення кібербезпеки України» [9], розглянуто актуальність забезпечення кібербезпеки як одного із пріоритетів національної безпеки України; відзначено роль інформаційних технологій та кіберпростору в сучасному світі та наголошено на ризиках щодо їх використання; підкреслено значення захисту від новітніх кіберзагроз в аспекті активізації кібертероризму, значущість захисту об'єктів критичної інформаційної інфраструктури та інших

інфраструктурних об'єктів від кібератак.

У документі наголошено на тому, що Російська Федерація є одним з основних джерел кіберзагроз та гібридної війни проти України, що актуалізує потребу в необхідності зміни стратегії та тактики протидії кіберзагрозам та розвідувально-підривній діяльності в кіберпросторі. Наголошено на важливості співпраці всіх суб'єктів, які опікуються питаннями забезпечення кібербезпеки, задля її гарантування у цифровому світі.

Разом із тим Україна визнається як держава, яка спроможна й повинна забезпечити свій розвиток у цифровому світі та гарантувати безпеку свого кіберпростору, зокрема через визначення пріоритетів і завдань у цій сфері.

Сприятливий кібербезпековий стан важливий для національної безпеки та ефективної роботи усіх галузей, які використовують інформаційні технології, забезпечення якого неможливе без огляду сучасних викликів і загроз у сфері кібербезпеки України, що своєю чергою конкретизують та деталізують труднощі й завдання, які стоять перед країною в цій сфері.

Для розв'язання означених проблем і забезпечення кібербезпеки України потрібно здійснити низку комплексних заходів, з-поміж яких:

– розвиток та вдосконалення нормативно-правової бази у сфері кібербезпеки, зокрема законодавство, згідно з яким унормовано питання функціонування критичної інфраструктури;

– створення системи оцінювання та сертифікації безпеки інформаційних систем і продуктів;

– удосконалення підходів щодо кібергігієни та запровадження в життя заходів для підвищення цифрової грамотності серед населення;

– забезпечення відповідного фінансування та належного контролю за кіберзахистом у державних органах;

– розвиток систем інформаційно-аналітичного забезпечення сфери кібербезпеки для виявлення та реагування на кіберзагрози;

– підвищення кваліфікації фахівців у галузі кібербезпеки;

– співпраця з міжнародними партнерами для обміну

інформацією та спільного реагування на кіберзагрози.

Вказані заходи, які корелюють із пріоритетами забезпечення кібербезпеки України, стратегічними цілями у цій сфері та відповідними стратегічними завданнями, визначеними в документі, що аналізують[8], сприятимуть покращенню стану кібербезпеки України і забезпеченню стійкості в умовах зростання рівня кіберзагроз. Артикуляція Стратегії розвитку кібербезпеки України відображає серйозне ставлення до питань захисту країни в кіберпросторі та підкреслює важливість всебічної співпраці, внутрішнього координаційного механізму та відкритості для різних учасників. Орієнтація на права й свободи людини, а також на соціальний, політичний та економічний розвиток підкреслює важливість збалансованого підходу до забезпечення кібербезпеки в Україні.

Сформульовані індикатори та механізм моніторингу реалізації Стратегії кібербезпеки України відображають системний і проактивний підхід до цього питання, адже використання індикаторів стану кібербезпеки дасть змогу точно вимірювати досягнення поставлених завдань та цілей, забезпечуючи прозорість та можливість корегування стратегії в режимі реального часу.

Інформаційна безпека згідно зі Стратегією забезпечення державної безпеки – «стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдавання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі через проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України. Інформаційна безпека є складовою національної безпеки України» [10].

У документі наводиться вичерпний огляд загроз для державної безпеки України. Підкреслено, що Російська Федерація продовжує застосовувати гібридні методи впливу, зокрема кібератаки, для досягнення своїх стратегічних цілей в Україні. Окупаційна адміністрація та самопроголошені органи на окупованих територіях порушують міжнародне право та загрожують державній безпеці. Деструктивна пропаганда та відсутність цілісної інформаційної політики ускладнюють ситуацію. Важливо підтримувати та посилювати заходи з підвищення кібербезпеки, розвитку інформаційної інфраструктури, зміцнення системи стратегічних комунікацій та реформування сил безпеки для нейтралізації означених загроз і забезпечення національної безпеки загалом. Зокрема, в документі наголошено на необхідності формування й упровадження проактивного підходу на основі управління ризиками.

У контексті викладеного вище на особливу увагу заслуговує Концепція забезпечення національної системи стійкості [11], що формує розуміння і підходи держави до створення й упровадження в життя відповідної національної системи, яка охоплює найрізноманітніші аспекти управління загрозами та кризовими ситуаціями, що можуть виникати в сучасних умовах, зокрема й загрози гібридного характеру.

У документі пропонується чіткий розподіл повноважень і відповідальності між суб'єктами управління, передбачається співпраця на всіх рівнях управління, що є ключовими для реагування на різноманітні загрози та кризові ситуації. Виважений підхід до ідентифікації загроз, оцінки ризиків та розроблення планів дій, їхня систематичність є важливими елементами успішності національної системи стійкості. А для вирішення поставлених перед системою завдань необхідно враховувати всі аспекти життєдіяльності суспільства і держави, зокрема економічні, енергетичні, інформаційні, кібернетичні, екологічні, продовольчі, охорони здоров'я, освіти та культури.

Формування національної системи стійкості, що спрямована на запобігання, реагування та відновлення після надзвичайних і кризових ситуацій, є важливим кроком для гарантування національної безпеки в умовах сьогодення.

Із-поміж спроможностей з ведення протиборства в інформаційному просторі та кіберпросторі сил оборони у Стратегічному оборонному бюлетені [12] виокремлено такі, як:

– здатність до проведення інформаційних заходів оборони держави;

– створення системи кібероборони для здійснення протиборства в інформаційному просторі (у тому числі кіберпросторі);

– здатність до забезпечення ефективного кіберзахисту власної інформаційної інфраструктури (критичної інформаційної інфраструктури), проведення превентивних дій щодо виявлення, реагування на кібератаки та інциденти кібербезпеки, усунення їх наслідків в умовах здійснення противником кіберрозвідки та інтенсивного кібервпливу (кібератак);

– здатність до проведення кіберрозвідки та кібердорозвідки в інформаційно-телекомунікаційних мережах та системах державного, приватного і військового призначення (об'єктів критичної інфраструктури) противника для здобуття інформації про кіберінфраструктуру противника, її призначення, місцезнаходження, технологічні процеси, уразливість, встановлення прихованого контролю, перехоплення та дешифрування керуючих і ресурсних даних та інформації;

– здатність до підготовки та проведення скоординованих демонстраційних кібердій (кібервпливу) у кіберпросторі щодо запобігання виникненню воєнних конфліктів, стримування та відсічі воєнній агресії в кіберпросторі;

– здатність організовувати підготовку та проводити кібердії (кібервпливи, кібератаки) із застосуванням усіх видів кіберзброї або захоплення (виведення з ладу, отримання контролю), заподіяння шкоди (каскадний ефект), порушення функціонування об'єктів критичної та інформаційної інфраструктури противника з одночасним приховуванням слідів своєї діяльності в кіберпросторі;

– застосування апаратно-програмних комплексів кібербезпеки, засобів із кіберзахисту, кіберзброї для розв'язання завдань кіберборотьби.

У Законі України «Про медіа» [13] відображено важливі принципи та стандарти, яких повинні дотримуватись у сфері медіа в демократичному суспільстві. Ці принципи гарантують захист основних прав і свобод громадян, сприяють створенню вільного та відкритого інформаційного середовища.

У статті 36 згаданого нормативно-правового акта чітко визначено обмеження щодо змісту інформації, яку не можна поширювати в медіа та на платформах спільного доступу до відео на території України. Ці обмеження встановлені з метою забезпечення національної безпеки, захисту територіальної цілісності, громадського порядку та інших суспільно важливих цілей. До них, зокрема, належать:

– заклики до насильницької зміни або повалення конституційного ладу. Забороняється поширювати інформацію, що закликає до насильницької зміни конституційного ладу України;

– пропаганда тероризму. Забороняється поширювати інформацію, яка пропагує тероризм та терористичні акти;

– поширення символіки тоталітарних режимів. Забороняється інформація та символіка, що стосується комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів, яка може виправдовувати чи схвалювати їхні дії;

– дискримінація та ненависть. Забороняється інформація, яка містить висловлювання ненависті чи дискримінації на підставі різних ознак, таких як етнічне чи соціальне походження, громадянство, національність, раса, релігія та інші;

– порнографія та сексуальне насильство над дітьми. Забороняються матеріали, що містять порнографію, а також матеріали, спрямовані на сексуальну експлуатацію та насильство щодо дітей;

– пропаганда вживання наркотичних засобів. Забороняється поширювати інформацію, що пропагує вживання наркотиків;

– жорстоке поводження з тваринами. Забороняється поширювати інформацію, що пропагує жорстоке поводження з тваринами;

– заперечення злочинів тоталітарних режимів. Забороняється інформація, яка заперечує злочини комуністичного і націонал-соціалістичного (нацистського) тоталітарних режимів та інші історичні події;

– заперечення існування української держави та мови. Забороняється інформація, яка заперечує існування української держави, мови та українського народу.

Зазначені обмеження відображають загальні моральні та етичні норми й спрямовані на забезпечення інформаційної безпеки держави. Важливо неухильно їх дотримуватися під час створення та поширення медійного контенту на території України.

Висновки та напрями подальших досліджень. Стан нормативно-правового регулювання питань захисту інформаційного простору України є складним і потребує постійного оновлення та удосконалення відповідно до сучасних викликів і загроз, які з часом урізноманітнюються та ускладнюються. Україна має досить потужну законодавчу базу, яка регулює різноманітні аспекти цього явища, однак, як показує практика, є низка недоліків та розбіжностей у законодавстві, а також проблемні питання з його практичної реалізації.

Один із ключових аспектів нині – це необхідність уніфікації та узгодження норм щодо захисту інформаційного простору, створення єдиного інформаційного простору, який забезпечуватиме безпеку інформаційної взаємодії всіх суб'єктів, залучених до неї. Україна вже робить кроки у напрямі перманентного вдосконалення нормативно-правового регулювання в галузі захисту інформаційного простору, але потребує певних напрацювань задля забезпечення ефективного захисту інформації та гарантування національного інформаційного суверенітету в аспекті забезпечення національної безпеки.

Список використаних джерел

1. Батиргареєва В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право*. 2020. № 1(32). С. 110–119.
2. Усик С. Дослідження правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. *Науковий вісник : Державне управління*. 2020. № 4(6). С. 266–280.
3. Микулець В. Ю. Правові аспекти формування єдиного інформаційного простору в Україні. *Право і суспільство*. 2012. № 2. С. 173–175.
4. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. Офіційний вебпортал парламенту України. URL : https://zakon.rada.gov.ua/go/254%D0%BA/96-

%D0%B2%D1%80 (дата звернення : 03.09.2023).
5. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. Офіційний вебпортал парламенту України. URL : https://zakon.rada.gov.ua/go/2469-19 (дата звернення : 10.09.2023).
6. Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. № 392/2020. *Офіційний вісник України*. 2020. № 75. С. 127.
7. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 р. № 685/2021. *Офіційний вісник України*. 2022. № 3. С. 22.
8. Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. *Офіційний вісник України*. 2021. № 70. С. 42.
9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Офіційний вебпортал парламенту України*. URL : https://zakon.rada.gov.ua/go/2163-19 (дата звернення : 11.09.2023).
10. Про рішення Ради національної безпеки і оборони України від 30.12.2021 р. «Про Стратегію забезпечення державної безпеки» : Указ Президента України від 16.02.2022 р. № 56/2022. *Офіційний вісник України*. 2022. № 17. С. 7.
11. Про рішення Ради національної безпеки і оборони України від 20.08.2021 р. «Про запровадження національної системи стійкості» : Указ Президента України від 27.09.2021 р. № 479/2021. *Офіційний вісник України*. 2021. № 79. С. 31.
12. Про рішення Ради національної безпеки і оборони України від 20.08.2021 р. «Про Стратегічний оборонний бюлетень України» : Указ Президента України від 17.09.2021 р. № 473/2021. *Офіційний вісник України*. 2021. № 76. С. 41.
13. Про медіа : закон України від 13.12.2022 р. № 2849-IX. *Офіційний вебпортал парламенту України*. URL : https://zakon.rada.gov.ua/go/2849-20 (дата звернення : 03.09.2023).

References

1. Batyrhareieva, V. S. (2020). Kontseptualna model zakhystu informatsiinoho prostoru Ukrainy zasobamy kryminalnoho prava [Conceptual model of the Ukrainian information space's protection by means of criminal law]. *Informatsiia i parvo*, 1 (32), 110–119. [in Ukrainian].
2. Usyk, S. (2020). Doslidzhennia pravovoho mekhanizmu zabezpechennia informatsiinoi bezpeky v umovakh nadzvychainykh sytuatsii [Study of the legal mechanism for ensuring information security under emergencies]. *Naukovyi visnyk: Derzhavne upravlinnia*, 4 (6), 266–280. [in Ukrainian].
3. Mykulets V. Yu. (2012). Pravovi aspekty formuvannia yedynoho informatsiinoho prostoru v Ukraini [Legal aspects of the formation of a unified information space in Ukraine]. *Pravo i suspilstvo*, 2, 173–175. [in Ukrainian].
4. Constitution of Ukraine: Law of Ukraine from June 28 1996, № 254k/96-VR. *Ofitsiinyi veb-portal parlamentu Ukrainy*. Retrieved from https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 [in Ukrainian].
5. On the national security of Ukraine: Law of Ukraine from June 21 2018, № 2469-VIII. *Ofitsiinyi veb-portal parlamentu Ukrainy*. Retrieved from https://zakon.rada.gov.ua/go/2469-19 [in Ukrainian].
6. On the decision of the National Security and Defense Council of Ukraine from September 14, 2020 «On the National Security Strategy of Ukraine»: Decree of the President of Ukraine from September 14 2020, № 392/2020. *Ofitsiinyi visnyk Ukrainy*, 75, 127. [in Ukrainian].
7. On the decision of the National Security and Defense Council of Ukraine from October 15, 2021 «On Information Security Strategy»: Decree of the President of Ukraine from December 28 2021, № 685/2021. *Ofitsiinyi visnyk Ukrainy*, 3, 22. [in Ukrainian].
8. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 «On the Cybersecurity Strategy of Ukraine»: Decree of the President of Ukraine dated August 26 2021, № 447/2021. *Ofitsiinyi visnyk Ukrainy*, 70, 42. [in Ukrainian].
9. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine from October 05 2017, №. 2163-VIII. *Ofitsiinyi veb-portal parlamentu Ukrainy*. Retrieved from https://zakon.rada.gov.ua/go/2163-19 [in Ukrainian].

10. On the decision of the National Security and Defense Council of Ukraine from December 30 2021, «On the Strategy for Ensuring State Security»: Decree of the President of Ukraine from February 16 2022, № 56/2022. *Ofitsiinyi visnyk Ukrainy*, 17, 7. [in Ukrainian].
11. On the decision of the National Security and Defense Council of Ukraine from August 20, 2021 «On the introduction of the national stability system»: Decree of the President of Ukraine dated September 27 2021, № 479/2021. *Ofitsiinyi visnyk Ukrainy*, 79, 31. [in Ukrainian].
12. On the decision of the National Security and Defense Council of Ukraine from August 20, 2021 «On the Strategic Defense Bulletin of Ukraine»: Decree of the President of Ukraine from September 17 2021, № 473/2021. *Ofitsiinyi visnyk Ukrainy*, 76, 41. [in Ukrainian].
13. About the media: Law of Ukraine from December 13 2022, № 2849-IX. *Ofitsiinyi veb-portal parlamentu Ukrainy*. Retrieved from https://zakon.rada.gov.ua/go/2849-20 [in Ukrainian].

ESTABLISHMENT AND DEVELOPMENT OF UKRAINIAN LEGAL FIELD TOWARDS PROTECTION OF THE STATE'S INFORMATION SPACE

Hlobenko Serhii

Abstract. The results of the research on the current legal framework in Ukraine regulating issues related to the protection of the state's information space in contemporary conditions are presented. It is established that safeguarding sovereignty, territorial integrity, and national security are key tasks for any state, including Ukraine. The challenges and threats in the fields of information and cybersecurity are specified, with an emphasis on the absence of a comprehensive state information policy. In Ukraine's legal field, information security involves protection from external influences and disinformation, requiring joint efforts from all entities involved in the process. Global challenges facing our country and corresponding strategic goals in this direction are aimed at ensuring the protection of national interests and strengthening social stability. The importance of implementing a series of priority measures to ensure the protection of cyberspace within the context of guaranteeing national security is underscored. Attention is drawn to the risks, legally established priorities, and tasks. The overall context of the problem is considered, highlighting the importance of ensuring cybersecurity for national security, taking into account contemporary challenges and threats. The main components of the national resilience system are characterized, combining various aspects of society and the state, including economic, energy, informational, cyber, environmental, food, healthcare, education, culture, and more. The importance of adhering to moral and ethical norms in creating and disseminating media content, while considering limitations, is emphasized to ensure national and information security for the state. The necessity of unifying the norms of the current legal framework to create a unified information space for ensuring the security of information interaction and strengthening the national resilience system is established.

Key words: legal regulation, information space of the state, information security, protection of information space, legal field, state policy in the information sphere, mechanisms of public administration.