

УДК 327 (477)

DOI <https://doi.org/10.30970/PPS.2024.56.30>

ДО ПИТАННЯ ПРО ПОЛІТИКО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ВІД СТАНОВЛЕННЯ ДО ЗМІН ВОЄННОГО ЧАСУ

Вячеслав Пашковський

*Київський національний університет імені Тараса Шевченка,
філософський факультет,
вул. Володимирська, 60, 01033, м. Київ, Україна*

Проблеми інформаційної безпеки – серед найбільш гострих в сучасному науковому і політичному дискурсі України. Це зумовлюється вагомістю інформаційного чинника в загальній системі національної безпеки, реалізація компонентів якої, включно з військовою, політичною, економічною, іншими вимірами безпеки, неможлива без інформаційної стійкості і згуртованості суспільства на противагу відповідним викликам і загрозам. Стаття орієнтована на аналіз специфіки і об'єктивно вагомих напрямів становлення і розвитку нормативно-правових засад інформаційної безпеки з урахуванням викликів, які характеризують відповідну сферу національної безпеки України. В колі уваги -визначення тенденції підходів до формування нормативно-правових засад інформаційної безпеки України від проголошення незалежності до початку широкомасштабної агресії рф; окреслення специфіки законодавчої бази України у сфері інформаційної безпеки в умовах воєнного стану; визначення проблемних аспектів і перспектив розвитку нормативно-правових засад інформаційної безпеки України з урахуванням викликів і завдань воєнного часу.

В статті стверджується, що процес вдосконалення політико-правової бази України у сфері інформаційної безпеки має спрямовуватись на гармонізацію інтересів держави і суспільства, зокрема, з огляду на гарантування безпеки персональних даних та прав громадян; посилення відповідальності як державних, так і недержавних ЗМІ, посадових осіб не тільки за поширення несанкціонованої, а й за об'єктивність і достовірність вагомої для суспільства інформації; недопущення зловживання свободою діяльності засобів масової інформації на шкоду інтересам держави, а також правам і свободам людини. В колі проблемних аспектів, які потребують розгляду, – формування цілісної нормативно-правової бази інформаційної безпеки, яка має узагальнити відповідні правові напрацювання у сфері інформаційної безпеки періоду незалежності України, виклики та загрози інформаційній загрози в умовах воєнного стану і повоєнної відбудови країни.

Ключові слова: політико-правова база, воєнний стан, інформаційна безпека, Україна.

Проблеми інформаційної безпеки – серед найбільш гострих в сучасному науковому і політичному дискурсі України. Це зумовлюється вагомістю інформаційного чинника в загальній системі національної безпеки, реалізація компонентів якої, включно з військовою, політичною, економічною, іншими вимірами безпеки, неможлива без інформаційної стійкості і згуртованості суспільства на противагу відповідним викликам і загрозам. Так, саме неготовність України – з урахуванням як державних структур, так і суспільства – протистояти інформаційним впливам стала передумовою і однією з причин окупації Росією Криму та окремих регіонів Донецької і Луганської областей в 2014 році, сприяючи, тим самим, формуванню на цих територіях нелегітимних військових і псевдо-державницьких формувань. Стан збройного конфлікту з Росією став поштовхом водночас значних трансформаційних змін в системі політико-правового, інституційного, гуманітарного забезпечення інформаційної безпеки на державному і суспільно-політичному рівні, що визначило

готовність народу України виступити єдиним фронтом на стримування широкомасштабної агресії РФ від 24 лютого 2024 року.

Хід подій в той же час визначив не тільки досягнення, а й нові проблемні аспекти в системі інформаційної безпеки, що пов'язано із значними технічними й фінансовими можливостями агресора впливати на психологію і поведінку громадян, з одного боку, а з іншого – специфікою підтримки інформаційної безпеки України в умовах воєнного стану, що відбувається з урахуванням обмеження прав і свобод громадян, звуження відкритості інформаційного поля, доступу громадянського суспільства до управлінських механізмів у сфері безпеки і т.і. Зазначене актуалізує проблеми політико-правових засад інформаційної безпеки України з урахуванням змін і завдань, які характеризують зазначену сферу і визначають особливості її підтримки в умовах російсько-української війни.

Слід визнати, що усвідомлення вагомості інформаційного чинника в агресії Росії проти України значно посилило від 2014 року увагу вітчизняних науковців до інформаційної безпеки з урахуванням, зокрема, механізмів і шляхів реалізації політики держави і суспільства у зазначеній сфері. Відомим виданням, зокрема, є колективна монографія «Світова гібридна війна: український фронт», підготовлена співробітниками Національного інституту стратегічних досліджень під редакцією В.П. Горбуліна (2017) [1]. Особливої уваги заслуговують й індивідуальні роботи, таких авторів, як О.Д. Довгань [2], О.О. Золотар [3], Є.В. Магда [4], А.Ю. Нашинець-Наумова [5], Б.О. Парахонський, Г.М. Яворська [6], Г. Почепцов [7], інших, орієнтованих в своїх дослідженнях на проблеми сучасних інформаційних війн й інформаційної безпеки України з огляду, зокрема, на правові засади її забезпечення.

Додамо до зазначеного й напрацювання вітчизняних дослідників, зокрема, В. Алещенка [8], В. Артемова, В. Хорошка, Ю. Хохлачової, В. Погорелова [9], І. Залевської, Г. Удренас [10], О. Кантура [11], І. Котерліна [12], Н. Новицької, О. Пуди, О. Добрянської [13], С. Онопрієнка [14], І. Шинкаренка, І. Шинкаренко [14], Є. Курінного [15], Д. Смотрича, Л. Браїлка [16], А. Русакевича [17], І. Лопатченко, А. Помаза-Пономаренко, Ю. Батира [18], інших, пов'язаних з осмисленням проблем інформаційної безпеки України в умовах широкомасштабної агресії РФ.

Викладене не виключає водночас необхідність подальшого осмислення теми як з урахуванням узагальнення накопиченого матеріалу, так і поглиблення тих аспектів інформаційної безпеки України, які потребують спеціального розгляду в умовах широкомасштабної агресії РФ.

Метою статті є аналіз специфіки і об'єктивно вагомих напрямів становлення і розвитку нормативно-правових засад інформаційної безпеки з урахуванням викликів, які характеризують відповідну сферу національної безпеки України в умовах воєнного часу. З урахуванням мети передбачено реалізацію наступних завдань дослідження:

1) визначити тенденції підходів до формування нормативно-правових засад інформаційної безпеки України від проголошення незалежності до початку широкомасштабної агресії РФ;

2) окреслити специфіку законодавчої бази України у сфері інформаційної безпеки в умовах воєнного стану;

3) визначити проблемні аспекти і перспективи розвитку нормативно-правових засад інформаційної безпеки України з урахуванням викликів і завдань воєнного часу і повоєнної відбудови України.

Для реалізації поставлених завдань передбачено використання наступних методів дослідження: методу дескриптивного аналізу для описовості сформованої системи

нормативно-правових засад інформаційної безпеки України; методу історичної ретроспективи, орієнтованого на окреслення еволюції підходів до формування організаційних засад підтримки інформаційної безпеки на етапі 2014–2024 рр.; методу прогнозування, що передбачає окреслення певних перспективних підходів до вдосконалення системи інформаційної безпеки України в умовах воєнного часу і повоєнної відбудови України.

Слід визнати, окреслюючи тенденції формування політико-правових засад інформаційної безпеки України на етапі 2014–2024 рр., що від проголошення незалежності в Україні була напрацьована певна законодавча база з національної інформаційної безпеки, яка і діяла до початку збройного вторгнення Росії в країну. Основним концептуальним документом, який заклав нормативно-правову базу з інформаційної безпеки стала Конституція України, що поставила інформаційну безпеку (ст. 17) до ряду найважливіших функцій держави, таких як захист суверенітету та територіальної цілісності. Конституція України (ст. 34) [19].

Зазначені пріоритети знайшли відображення й в низці нормативно-правових актів, зокрема, Законів України, «Про інформацію» (1992), «Про друковані засоби масової інформації (пресу в Україні)» (1992), «Про телебачення і радіомовлення» (1993), «Про інформаційні агенства» (1995), «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (1997), «Про телекомунікації» (2003), інших, що відображали розуміння українськими урядами розвитку інформаційної сфери за умов демократичних перетворень суспільства і водночас загроз, які може нести інформаційна сфера для стабільності суспільства в умовах глобалізаційних інформаційних процесів. До цього слід додати й Доктрину інформаційної безпеки України від 2009 року, що свідчило про зростання уваги з боку керівництва держави до проблеми інформаційної безпеки. Втім, в цілому підходи щодо інформаційної не набули системності в аспекті цілісної стратегії, здатної регулювати державну інформаційну політику в усіх сферах суспільних відносин та стримувати можливі загрози в даній сфері.

Зазначене стало сприятливим середовищем підготовки й початку агресії РФ проти України в 2014 році у вимірі гібридної війни, супутнім і водночас самостійним складником якої стала інформаційна, психологічна війна. Протидією гібридній війни у цьому відношенні об'єктивно очікувалось залучення до стримування агресора ресурсів як військового, так й інформаційного характеру, де інформаційний чинник знову ж таки набував чи не найважливішого значення як мотиватор суспільної свідомості і суспільної готовності на стримування агресора.

Конкретизованими кроками в цьому відношенні стали зміни до існуючого законодавства, що актуалізували його значення; розробка низки нових документів законодавчого і нормативно-правового характеру, які набули регуляторного значення в інформаційній сфері. Серед таких, зокрема, Стратегії національної безпеки України (від 2015 і 2020 рр.), Закон України «Про національну безпеку України», Доктрина інформаційної безпеки України, Стратегія кібербезпеки України, Воєнна доктрина України, Закони України «Про інформацію», «Про доступ до публічної інформації», «Про Раду національної безпеки і оборони України, Стратегія інформаційної безпеки, інші акти.

Поява Стратегії національної безпеки від 2015 року зумовлювалась визнанням на політичному рівні докорінних змін у зовнішньому та внутрішньому безпековому середовищі України за умов агресії Росії, необхідності створення нової системи забезпечення національної безпеки України. В документі окреслювались цілі національної безпеки України як реалізації якісно нової державної політики, спрямованої на ефективний захист національних інтересів в економічній, соціальній, гуманітарній та інших сферах, комплексне

реформування системи забезпечення національної безпеки та створення ефективного сектору безпеки і оборони України; визначались напрями державної політики на створення ефективного сектору безпеки і оборони як готовності держави на відбиття зовнішньої агресії у будь-яких формах і проявах (зокрема у формі гібридної війни) [20; 21].

Відповідно до визначеного в СНБ від 2015 р. напрямку вдосконалення законодавства з питань національної безпеки і оборони України Верховна Рада України прийняла Закон «Про національну безпеку України» від 21.06.2018, орієнтований на визначенні сутності національної безпеки та напрямів її забезпечення в умовах агресії РФ.

В Законі України «Про національну безпеку України» від 2018 р.:

– подано визначення національної безпеки України, національних інтересів України, Стратегії національної безпеки України, Стратегії кібербезпеки...

– визначено правову основу державної політики у сферах національної безпеки і оборони, яку становлять Конституція України, Закон України «Про національну безпеку України» та інші закони України, міжнародні договори, а також видані на виконання Конституції та законів України інші нормативно-правові акти;

– окреслено принципи державної політики у сферах національної безпеки і оборони, визначено фундаментальні національні інтереси України [22].

Підґрунтям до зазначеного документу стала Доктрина інформаційної безпеки, затверджена Президентом України 25.02.2017 р.

Метою Доктрини визнано уточнення засад формування та реалізації державної інформаційної політики, насамперед, щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Зазначено, що Доктрина базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

В Доктрині окреслено широке коло пріоритетів державної політики в інформаційній сфері, які охоплюють заходи:

1) щодо забезпечення інформаційної безпеки:

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері...;

2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію;

3) щодо відкритості та прозорості держави перед громадянами;

4) щодо формування позитивного міжнародного іміджу України.

Спеціальним напрямком доктрини стало визначення системи та функціональних повноважень державних структур України у сферах інформаційної безпеки України. Значалось й про науково-аналітичне та експертне забезпечення процесу формування і реалізації державної інформаційної політики, що покладалось на Національний інститут стратегічних досліджень при Президентові України [23].

Супроводними до Доктрини інформаційної безпеки в аспекті реалізації відповідної державної політики стали й деякі інші політико-правові документи, зокрема, Воєнна доктрина України, Стратегія кібербезпеки України, чинні законодавчі акти, які регламентували діяльність виконавчої влади в інформаційній сфері.

Воєнна доктрина України як документ похідного спрямування від Стратегії національної безпеки у вимірі забезпечення воєнної безпеки була затверджена указом Президента України за рішенням Ради національної безпеки і оборони України 24.09 2015 р.

Доктрина:

– визнала Російську Федерацію в якості воєнного противника України, тоді як інформаційну війну Російської Федерації проти України в якості однієї з головних тенденцій, що впливають на воєнно-політичну обстановку в регіоні довкола України;

– визначила сутнісний зміст цілеспрямованого інформаційного (інформаційно-психологічного) впливу з використанням сучасних інформаційних технологій як воєнної загрози з боку Російської Федерації, спрямовану на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин;

– окреслила цілі та основні завдання воєнної політики, що передбачають, зокрема:

▪ удосконалення державної інформаційної політики у воєнній сфері;

▪ попередження та ефективну протидію інформаційно-психологічним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні [24].

Стратегія кібербезпеки України, затверджена указом Президента України від 15.03.2016 р. за рішенням Ради національної безпеки і оборони України:

– окреслила вимогу щодо невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України в умовах агресії РФ;

– визначила правові засади державної політики з кібербезпеки, що формуються з урахуванням Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року» [25].

Варто визнати в аспекті зазначеного й вагомність такого документу, як Стратегія національної безпеки України від 14.09.2020, затвердженого у форматі оновлення нормативно-правової бази інформаційної безпеки після чергових президентських виборів 2019 р. [26].

Показовим елементом Стратегії 2020 р. стала традиційність визнання гібридного характеру впливів Росії проти України з невід’ємним компонентом агресії у формі інформаційної війни, з одного боку, а з іншого – визнання пріоритетом активну та ефективну протидію розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді. «Для відновлення свого впливу в Україні Російська Федерація, продовжуючи гібридну війну, системно застосовує політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби...». І далі: «Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз...», – говорить в документі [26].

Такий підхід поєднується в Стратегії національної безпеки з перспективами ефективного стратегічного планування і кризового менеджменту в усіх сферах державної політики, включаючи систему інформаційної безпеки.

Конкретизованим напрямом реалізації зазначеного стало рішення РНБО «Про Стратегію інформаційної безпеки» (15.10.2024) із введенням в дію відповідного документу за указом Президента України від 28 грудня 2021 року.

Специфікою Стратегії інформаційної безпеки, поряд із визначенням самого поняття («інформаційна безпека»), – окреслення інформаційних загроз, а також інформаційних заходів оборони держави в умовах збройної агресії проти України; стратегічних цілей й напрямів, а також механізмів реалізації Стратегії.

Інформаційна безпека розглядається в документі як «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» [27].

Інформаційна загроза пояснюється в документі як «потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні». Серед важливих ідей документу й визначення інформаційних заходів оборони держави як «сукупності скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, в умовах воєнного або надзвичайного стану щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві».

В документі визначено шляхи реалізації Стратегії, включно з такими напрямками, як «Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини.

Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності...

Підвищення рівня медіакультури та медіаграмотності суспільства...

Забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів, гарантування їх безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту...

Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору, а також відновлення їх права на інформацію, що дає їм змогу підтримувати зв'язок з Україною...

Створення ефективної системи стратегічних комунікацій...

Розвиток інформаційного суспільства та підвищення рівня культури діалогу...» [27].

Визначені напрями (відповідно очікуваних результатів Стратегії) забезпечили достатньо високий рівень захищеності інформаційного поля України від початку широкомасштабної агресії РФ 2022 року, втім, з еволюцією підходів державних структур, де формат забезпечення інформаційної безпеки пов'язувався з лінією на звуження прав громадян в умовах реалій воєнного часу. Зазначене набуло нормативно-правового закріплення з урахуванням Указу Президента України від 24.02.2022 «Про введення воєнного стану в Україні», де, зокрема, йдеться, що «у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану»» [28].

Серед статей Конституції України, на які звертається увага в аспекті обмежень прав і свобод громадян з огляду на проблеми інформаційної безпеки:

стаття 31 («Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції»);

– стаття 32 («Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України»);

– стаття 34 («Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань»);

– стаття 41 («Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності») [19; 12].

До цього варто додати й низку актів законодавчого характеру щодо внесення змін до Кримінального та Кримінального процесуального кодексів України із забезпечення протидії несанкціонованому поширенню забороненої інформації стратегічного значення, зокрема, щодо Збройних Сил України, електронних комунікацій, кіберзахисту і т.і як фактору певних заборон та зростання відповідальності громадян в умовах воєнного або надзвичайного стану [29–31].

Іншим суттєвим підходом в аспекті інформаційної безпеки країни стала тенденція на концентрацію інформаційних ресурсів під контролем держави як засобу стримування й протидії інформаційних загроз в умовах широкомасштабної агресії РФ. На увагу заслуговує Рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», введене в дію Указом Президента України 19.03.2022. В документі наголошується, що «реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UАразом»» [32].

Варто додати в аспекті нормативно-правового забезпечення системи інформаційної безпеки України в умовах війни й Закон України № 2849-IX «Про медіа», який набрав чинності 31 березня 2023 року після підписання Президентом України (13.12.2022). Закон розширив повноваження Національної ради з питань телебачення та радіомовлення щодо реєстрації засобів масової інформації, розробки кодексів (правил) поширення інформації із запровадження можливих санкцій і т.і. [33].

Зазначені документи в сукупності сформували базову платформу забезпечення діяльності державних структур у сфері інформаційної безпеки в умовах воєнного стану. Втім затяжний характер війни з окупацією значної частини території України, використання найновітніх технологій впливу на свідомість в психічний стан людини висувають за необхідне подальші кроки з вдосконалення безпекової політики держави і суспільства в інформаційній сфері. Так, можна погодитись з думкою аналітиків, що сформована в умовах війни нормативно-правова база інформаційної безпеки не позбавлена проблемних аспектів, де поза сферою уваги залишається коло вагомих питань, які потребують врегулювання.

Серед таких:

- гармонізація інтересів держави і суспільства в системі інформаційної безпеки, зокрема, з огляду на гарантування безпеки персональних даних та прав громадян;
- посилення відповідальності як державних, так і недержавних ЗМІ, посадових осіб не тільки за поширення несанкціонованої, а й за об'єктивність і достовірність вагової для суспільства інформації;
- недопущення зловживання свободою діяльності засобів масової інформації на шкоду інтересам держави, а також правам і свободам людини;
- отримання балансу інтересів забезпечення свободи слова та прав і законних інтересів особи, суспільства і держави, їх взаємної відповідальності [13].

Останні положення можуть стосуватись, зокрема, відомого рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», яке, як це справедливо визнається в низці джерел, позбавило можливості опозиційні до влади, втім, проукраїнські канали брати участь у формуванні інформаційного поля держави в умовах війни [12; 13]. Проблематичним у даному відношенні є те, що відімкнення каналів в цифровій мережі Т2 відбулось поза спеціального рішення відповідальних щодо цього органів – Національної ради України з питань телебачення і радіомовлення, Міністерства оборони України (яке вповноважене регулювати режим воєнного стану), РНБО України чи суду.

Варто додати до вищевикладеного й ускладненість ефективної реалізації регуляторного законодавства у сфері інформаційної безпеки в умовах воєнного стану з урахуванням недостатньої системності відповідної бази до початку широкомасштабної агресії рф.

В колі проблемних аспектів:

- незавершеність процесу формування законодавчої бази, представленої на етапі 2021-2022 рр. значним колом політико-правових документів, які мали відношення до сфери інформаційної безпеки. Суттєвим кроком щодо систематизації зазначеного стала Стратегія інформаційної безпеки (2021), втім, документ не знайшов реалізації у форматі відповідного нормативного акту (закону), а також конкретизованих програм діяльності щодо цілей і напрямів реалізації Стратегії;
- відсутність чіткого закріплення на законодавчому рівні механізму координації дій органів державного управління у сфері інформаційній сфері, порядку правового закріплення обсягів відповідальності, а також взаємовідносин державних безпекових структур із іншими органами та відомствами, приватними структурами, віднесеними законодавством до суб'єктів забезпечення національної безпеки України;
- неузгодженість значної частини сформованих за часи незалежності України нормативно-правових актів щодо інформаційної безпеки з новітніми підходами розуміння сутності та шляхів стримування інформаційних загроз.

На порядку денному – як формування цілісної нормативно-правової бази державної політики, орієнтованої на стримування інформаційної агресії, так і оновлення існуючого законодавства з урахуванням загроз інформаційній безпеці в умовах воєнного стану. Актуалізований

формат нормативно-правового забезпечення системи інформаційної безпеки має сприяти при цьому не тільки вдосконаленню існуючого законодавства щодо протистояння інформаційній агресії РФ в умовах війни, а й формуванню платформи стримування інформаційних викликів, зумовлених обставинами повоєнного відродження та розвитку країни.

Список використаної літератури

1. Світова гібридна війна: український фронт: монографія / за заг.ред. В.П. Горбуліна. К.: НІСД, 2017. 496 с.
2. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти. НАПрН України, НДІП, НАН України, Нац. б-ка України ім. В. І. Вернадського. Київ, 2015. 388 с.
3. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
4. Магда Є.В. Гібридна війна : вижити і перемогти. Х. : Віват, 2015. 304 с.
5. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
6. Парахонський Б.О., Яворська Г.М. Онтологія війни і миру: безпека, стратегія, смисл: монографія. Київ: НІСД, 2019. 560 с.
7. Почепцов Г. Гібридна війна: інформаційна складова. *Media Sapiens*. 25.10.2015. URL: <https://ms.detector.media/mediaanalitika/post/14501/2015-10-25-gibrydna-viyna-informatsiyna-skladova/>
8. Алещенко В. Психологічні аспекти інформаційної війни. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2022. № 2(50). С. 27–31. URL: <https://miljournals.knu.ua/index.php/visnuk/article/view/929/874>
9. Артемов В.Ю., Хорошко В.О., Хохлачова Ю.Є., Погорелов В.В. Інформаційно-воєнна безпека як елемент національної безпеки України. *Захист інформації*. 2022. Т. 24, № 1. С. 21-29. URL: <file:///C:/Users/admin/Downloads/INFORMATION+AND+MILITARY+SECURITY+AS+AN+ELEMENT+OF+NATIONAL+SECURITY+OF+UKRAINE.pdf>
10. Залевська І.І., Удренас Г.І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1–2. С. 20 – 26. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/1e9150a5-fe34-42b9-9f26-582b2a89c1ef/content>
11. Кантур О. Досвід іноземних держав у питанні протидії інформаційним впливам Російської Федерації. *Вісник Київського національного університету імені Тараса Шевченка. Державне управління*. 2022. Вип. 2 (16). С. 5-12. URL: https://www.researchgate.net/publication/362449697_Dosvid_inozemnih_derzav_u_pitanni_protidii_informacijnim_vplivam_Rosijskoj_Federacii
12. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. Актуальні проблеми вітчизняної юриспруденції. 2022. № 1. С. 150-155. URL: http://apnl.dnu.in.ua/1_2022/25.pdf
13. Новицька Н. Б., Пунда О. О., Добрянська О. Д. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. Соціологія права. 2022. Вип. 1–2(40–41). С. 71-76. URL: <https://elar.khmnmu.edu.ua/server/api/core/bitstreams/8f9ec4e4-f843-4b9c-b37a-e93d379d7898/content>
14. Онопрієнко С. Функції забезпечення інформаційної безпеки публічного адміністрування в Україні за умов повномасштабної збройної агресії Російської Федерації. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2022. № 2 (50). С. 95–98. URL: <https://miljournals.knu.ua/index.php/visnuk/article/view/944/886>

15. Курінний С. В. Адміністративно-правове забезпечення інформаційної гігієни під час воєнного стану в Україні. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 1 (122). С. 38–43. URL: <https://er.dduvs.edu.ua/bitstream/123456789/11984/1/4.pdf>
16. Смотров Д.В., Л.Браїлко. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*. Серія Право. 2023. Вип. 77, частина 2. С. 121–127. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/284104/278250>
17. Русакевич А. Інформаційна безпека в умовах воєнного стану у аспекті захисту інформаційних прав громадян. *Law. State. Technology*. 2024. Вип. 2. С. 58–61. URL: <https://journals.politehnica.dp.ua/index.php/lst/article/view/603>
18. Лопатченко І.М., Помаза-Пономаренко А.Л., Батир Ю.Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану. *Вісник Національного університету цивільного захисту України*. Державне управління. 2024. Вип. 1(20). URL: <http://repositc.nuczu.edu.ua/bitstream/123456789/20308/1/2Lopatchenko.pdf>
19. Конституція України. Документ 254к/96-ВР, чинний, поточна редакція від 01.01.2020, підстава – 27-IX. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.
20. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015 URL: <http://zakon2.rada.gov.ua/laws/show/287/2015>.
21. Про Стратегію національної безпеки України. Рішення Ради національної безпеки і оборони України від 6 травня 2015 року. Стратегія національної безпеки України. Затверджено Указом Президента України від 26 травня 2015 року N 287/2015. URL: <https://ips.ligazakon.net/document/MUS24689>
22. Про національну безпеку України: Закон України від 21.06.2018 року № 2469-VIII, чинний, поточна редакція від 24.10.2020, підстава – 912-IX. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.
23. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017. Доктрина інформаційної безпеки України. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text>.
24. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24 вересня 2015 № 555/2015. Воєнна доктрина України. URL: <https://zakon.rada.gov.ua/laws/show/555/2015#Text>.
25. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96/2016. Стратегія кібербезпеки України. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#Text>.
26. Про рішення Ради національної безпеки і оборони України 14 вересня 2020 р «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. Стратегія національної безпеки і оборони. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.
27. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Указ Президента України від 28.12.2024. Стратегія інформаційної безпеки. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
28. Про введення воєнного стану в Україні. Указ Президента України від 24.02.2022. URL: <https://zakon.rada.gov.ua/laws/show/64/2022#Text>
29. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації

- про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#n10>
30. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам. URL: <https://zakon.rada.gov.ua/laws/show/2137-20#Text>
 31. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції. Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2110-20#Text>
 32. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану. Рішення РНБО. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-22#Text>
 33. Про медіа. Закон України. Документ 2849-IX, чинний, поточна редакція – Редакція від 11.02.2024, підстава – 3269-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

ON THE ISSUE OF POLITICAL AND LEGAL SUPPORT OF UKRAINE'S INFORMATION SECURITY: FROM DEVELOPMENT TO WARTIME CHANGES

Viacheslav Pashkovkyi

Taras Shevchenko National University of Kyiv,

Faculty of Philosophy,

Volodymyrska str., 60, 01033, Kyiv, Ukraine

The problems of information security are among the most acute in the modern scientific and political discourse of Ukraine. This is due to the importance of the information factor in the overall system of national security, the implementation of the components of which, including military, political, economic, and other dimensions of security, is impossible without information stability and cohesion of society as opposed to the relevant challenges and threats. The article is dealt with the analysis of the specifics and objectively significant directions of formation and development of the regulatory and legal foundations of information security, taking into account the challenges that characterize the relevant sphere of national security of Ukraine. The focus of the article is on determining the trend of approaches to the formation of the regulatory framework for Ukraine's information security from the proclamation of independence to the beginning of the large-scale aggression of the Russian Federation; outlining the specifics of the legislative framework of Ukraine in the field of information security under martial law; identification of problematic aspects and prospects for the development of the regulatory framework for Ukraine's information security, taking into account the challenges and tasks of wartime.

It is stated in the article that the process of improving the political and legal framework of Ukraine in the field of information security should be aimed at harmonizing the interests of the state and society, in particular, with regard to ensuring the security of personal data and the rights of citizens; strengthening the responsibility of both state and non-state media, officials not only for the dissemination of unauthorized, but also for the objectivity and reliability of information that is important for society; prevention of abusing freedom of mass media to the detriment of the interests of the state, as well as human rights and freedoms. Among the problematic aspects that need to be considered is the formation of a coherent regulatory framework for information security, which should summarize the relevant legal developments in the field of information security during the period of Ukraine's independence, as well as challenges and threats to information threats in the conditions of martial law and post-war reconstruction of the country.

Key words: political and legal framework, martial law, information security, Ukraine.