УДК 34:004.056:355.45
DOI https://doi.org/10.32782/2663-5984.2025/1.20

Руснак Ю.І.
Центр воєнно-стратегічних досліджень
Національного університету оборони України

ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

У статті акцентовано увагу на забезпеченні інформаційної безпеки України в умовах російсько-української війни. Метою дослідження є аналіз правових аспектів формування та розвитку нормативно-правової бази України в сфері інформаційної безпеки як ключового елементу в умовах війни російською федерації проти України та з урахуванням досвіду проведення Антитерористичної операції (Операції Об'єднаних сил) на Сході України для розроблення рекомендацій щодо подальшого вдосконалення законодавства в окресленій сфері. Методи дослідження вибрані відповідно до поставленої мети та зумовлені логікою дослідження. Під час написання статті автором застосовано такі методи: системний підхід, історичний метод, порівняльно-правовий, метод аналізу та синтезу та інші. У статті визначено, що розпочата у 2014 році агресія російської федерації, зумовила нові виклики і загрози в інформаційній сфері. Детально аналізується генеза розвитку нормативно-правових актів України у сфері інформаційної безпеки в контексті загострення російсько-української війни та їх адаптації до новітніх викликів гібридної війни й інформаційної агресії. Важливість дослідження еволюції законодавства в зазначеній сфері зумовлена тим, що це дало змогу визначити як історичні виклики формували правові механізми, а також їх здатність адаптуватися до новітніх загроз, зокрема, такі як кібератаки і дезінформація. Окреслене також дало змогу виявити прогалини у законодавстві та дослідити як шляхом прийняття нових нормативно-правових актів відбулось вдосконалення в зазначеній сфері. Також, здійснено аналіз нормативно-правових актів, прийнятих в умовах широкомасштабної агресії російської федерації проти України 24 лютого 2022 року та надано рекомендації щодо вдосконалення законодавчої бази для забезпечення інформаційної безпеки України. Теоретична та практична значущість статті полягає у тому, що автором було здійснено комплексний аналіз ключових нормативно-правових актів, досліджено передумови їх розвитку та становлення. Отримані результати можуть слугувати підґрунтям для подальших досліджень щодо розвитку та вдосконалення законодавства в окресленій сфері.

Ключові слова: *Збройна агресія, гібридні загрози, пропаганда, інформаційна безпека, національна безпека.*

Постановка проблеми. З початком гібридної збройної агресії російської федерації (далі – рф) у 2014 році, перед Україною постали нові виклики у сфері інформаційної безпеки. Рф почала застосовувати широкий арсенал гібридних інструментів, що містило, зокрема, поширення дезінформації і пропаганди серед населення, здійснення кібератак на державні інформаційні ресурси і критичну інфраструктуру, а також, інші форми інформаційного впливу. Через це, виникла необхідність у вдосконаленні існуючої, на той момент, нормативно-правової бази для протидії інформаційним загрозам, з метою забезпечення сталого розвитку інформаційного суспільства, захисту прав і свобод громадян й зміцнення національної безпеки держави.

Втім, внаслідок широкомасштабного вторгнення рф в Україну у лютому 2022 року, ситуація в інформаційному просторі України зумовила вдосконалення не лише існуючих, але й розробки нових механізмів протидії інформаційним загрозам. Широкомасштабна війна 2022 року ознаменувала новий етап інформаційної війни, для якої характерним є: посилення дезінформаційних кампаній, значна ескалація кібератак, застосування нових технологій, розширенням географії проведення інформаційних атак та ін. В результаті цього, питання щодо вдосконалення існуючої нормативно-правової бази в контексті забезпечення інформаційної безпеки зумовлює актуальність обраної теми та потребує подальших досліджень.

Аналіз останніх досліджень і публікацій. Питанню дослідження правових аспектів інформаційної безпеки України присвячена низка досліджень науковців. Так, зокрема в роботі Бес-

палова І. О. [6] розкриваються правові засади інформаційної безпеки під час дії правового режиму воєнного стану, в роботі Валюшко І. О. [12] досліджена трансформація законодавства щодо регулювання інформаційної безпеки України після російського вторгнення.

У роботі Борисова О. Ю. [24], увагу зосереджено на нормативно-правовій базі забезпечення інформаційної безпеки України, де зокрема, виокремлено сучасні проблеми та відправні точки їх вирішення, в дослідженні Новородовського В. [26] розглядається інформаційна безпека України в умовах російської агресії.

Втім, виходячи з окреслених досліджень та в умовах триваючої агресії рф, окреслена тема потребує подальшого ґрунтовного аналізу.

Постановка завдання. Метою статті є аналіз правових аспектів формування та розвитку нормативно-правової бази України в сфері інформаційної безпеки як ключового елементу в умовах війни рф проти України та з урахування досвіду проведення Антитерористичної операції (Операції Об'єднаних сил) на Сході України для розроблення рекомендацій щодо подальшого вдосконалення законодавства в окресленій сфері.

Виклад основного матеріалу. Поняття інформаційної безпеки доцільно визначити як стан захищеності національних інтересів України в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз [1]. Інформаційна безпека держави забезпечується завдяки проведенню єдиної державної політики національної безпеки в інформаційній сфері. Це інтегрована складова національної безпеки, і розглядається як пріоритетна функція держави [2].

За період незалежності, Україні вдалося напрацювати певну законодавчу базу у сфері національної інформаційної безпеки, яка і діяла до початку вторгнення рф в Україну у 2014 році. Однак, як виявилося, існуюча на той період законодавча база не повною мірою була готова до викликів, що постали перед нашою державою в умовах гібридної агресії рф. Вона була не досконалою і не відповідала реальним викликам та умовам, що склалися. Після окупації Автономної Республіки Крим, а згодом і окремих районів Донецької та Луганської областей, рф розгорнула широку кампанію з дезінформації та пропаганди на захоплених територіях, намагаючись маніпулювати суспільною свідомістю в Україні та за її межами.

Виходячи з необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, виникла необхідність кардинальних змін у системі забезпечення інформаційної безпеки України [3]. 28 квітня 2014 року у рішенні Ради національної безпеки і оборони України (далі – РНБО) «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» було запроваджено основний план заходів. 1 травня 2014 року, виконуючий обов'язки Президента України О. Турчинов підписав Указ «Про рішення Ради національної безпеки і оборони України "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України"» № 449/2014 [4].

Відповідно до окресленого Указу передбачалось у тримісячний термін розробити проєкт нової редакції Доктрини інформаційної безпеки України, проєкт Закону України «Про кібернетичну безпеку України», законопроєкти про внесення змін до деяких законів України, зокрема, до Законів України «Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про службу безпеки України», «Про службу спеціального зв'язку та захисту інформації України» та внести їх на розгляд Верховної Ради України.

У травні 2014 року було ініційовано Проєкт Закону «Про засади інформаційної безпеки України» № 4949 [5], яким пропонувалось унормувати терміни «інформаційна безпека», «інформаційна інфраструктура», «забезпечення інформаційної безпеки», «загрози інформаційній безпеці» та низку інших вкрай важливих для суспільства і держави категорій. Проте цей законопроект так і не було втілено в життя [6].

В грудні 2014 року було створено Міністерство інформаційної політики України. При ньому, в процесі спілкування Міністра Ю. Стеця з представниками громадськості створили Експертну Раду, основною метою якої є розробка Стратегії інформаційної політики України, Концепції інформаційної безпеки України та Державної програми розвитку інформаційного простору України [7]. Президент України на прес-конференції 29 грудня 2014 року пояснив доцільність створення Міністерства інформаційної політики необхідністю ефективної контрпропаганди в умовах інформаційної війни [8].

14 січня 2015 року Кабінет Міністрів України прийняв Постанову № 2 «Питання діяльності Міністерства інформаційної політики України»,

якою було утворено Міністерство інформаційної політики України та затверджено Положення про міністерство. Відповідно до окресленої Постанови, основними завданнями Міністерства було визначено:

– забезпечення інформаційного суверенітету України, зокрема, з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів;

– забезпечення здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації [9].

У вересні 2019 року Міністерство інформаційної політики було реорганізоване (з ліквідацією функцій та повноважень). Крім того, варто звернути увагу на Закон України від 5 лютого 2015 року № 159-VIII «Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України» [10], яким було внесено зміни та доповнено Статтею 15^1 Закон України «Про кінематографію» щодо заборони розповсюдження і демонстрування в Україні фільмів, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що створюють позитивний образ працівників держави-агресора, працівників радянських органів державної безпеки, виправдовують чи визнають правомірною окупацію території України, а також забороняється трансляція (демонстрування шляхом показу каналами мовлення) фільмів, вироблених фізичними та юридичними особами держави-агресора. Передбачена частиною першою цієї статті заборона розповсюдження і демонстрування фільмів, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій поширюється на розповсюдження та демонстрування будь-яких фільмів незалежно від країни походження, виробництва після 1 серпня 1991 року.

24 вересня 2015 року була прийнята оновлена Воєнна Доктрина України [11]. У Доктрині відображались ідейні стовпи усієї військово-політичної діяльності держави, крім того, доктрина чітко визначала інформаційну війну рф проти України. Варто зазначити, що в оновленій Воєнній Доктрині України було визначено воєнно-політичні виклики, які можуть перерости в загрозу застосування воєнної сили проти України. Серед них, зокрема: цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований 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 [12].

6 травня 2015 року РНБО України схвалила проєкт нової Стратегії національної безпеки, затвердженої Указом Президента України від 26 травня 2015 року № 287/2015 [13]. Варто зазначити, що у новій Стратегії національної безпеки України було визначено загрози інформаційній безпеці України, а саме: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства, що було відсутнім у Стратегії національної безпеки України від 12 лютого 2007 року [14]. Крім того, у новій Стратегії національної безпеки визначено складові щодо забезпечення інформаційної безпеки.

Варто зазначити, що усі попередні стратегічні документи у сфері безпеки були більш декларативними, аніж практичними. Окреслений документ базувався на науковому підході й до його розроблення долучилися вітчизняні та міжнародні експерти, представники ЄС та НАТО [12].

У 2016 році Указом Президента від 6 червня 2016 року № 240/2016 введено в дію рішення РНБО України «Про Стратегічний оборонний бюлетень України», де зокрема серед потенційних загроз визначено неспроможність ефективно реагувати на зростаючу кількість та потужність кібератак та протистояти кіберзлочинності. Оперативною ціллю 1.5. визначено удосконалення системи кібербезпеки та захисту інформації [15].

Окремо заслуговує на увагу прийняття Стратегії кібербезпеки від 27 січня 2016 року, введеної в дію Указом Президента України від 15 березня 2016 року № 96/2016 [16]. Стратегія кібербезпеки України стала першою спробою нормативного унормування питань кібербезпеки під час активної фази гібридної агресії і сам факт її прийняття став позитивним та важливим з точки зору накопичення відповідного досвіду та створення правового підґрунтя для розбудови національної системи кібербезпеки. Під час визначення структури нової Стратегії було враховано кращі світові практики з розробки стратегій у сфері кібербезпеки. Зокрема, було проаналізовано кібербезпекові стратегії Європейського Союзу, Сполучених Штатів Америки, Великої Британії, Іспанії, Норвегії та інших провідних країн [17].

Стратегія забезпечила підґрунтя для розроблення подальших нормативно-правових актів з питань кібербезпеки та визначила основні засади

та напрями державної політики у цій сфері. Розпорядженням Кабінету Міністрів України почав затверджуватись річний план заходів з її реалізації, включаючи конкретні завдання для органів державної влади, спрямовані на виконання положень Стратегії, вирішення існуючих проблемних питань та розбудову кібербезпекового потенціалу України [18].

Зокрема, відповідно до Розпорядження Кабінету Міністрів України було затверджено такі плани:

Розпорядження Кабінету Міністрів України від 24 червня 2016 р. № 440-р «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України».

Розпорядження Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України».

Розпорядження Кабінету Міністрів України від 11 липня 2018 р. № 481-р «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України».

Також, на підставі ухвалення рішення про Стратегію кібербезпеки 2016 року, Указом Президента України було ухвалено рішення про створення Національного координаційного центру кібербезпеки [19].

Указом Президента України від 14 березня 2016 № 92/2016 затверджено Концепцію розвитку сектору безпеки і оборони України [20]. Серед основних завдань безпеки і оборони було визначено забезпечення інформаційної та кібербезпеки. Також, виконання завдань реформування та розвитку Збройних Сил України передбачало удосконалення системи забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України.

13 лютого 2017 року Президентом України було підписано Указ № 32/2017, яким було введено в дію рішення РНБО України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [21].

Важливим кроком стало введення в дію Указом Президента України від 25 лютого 2017 року № 47/2017 рішення РНБО України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [22]. У Доктрині інформаційної безпеки вказувалось, що застосування рф технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Інформаційна сфера, будучи системоутворюючим фактором життя суспільства, здійснює активний вплив на стан політичної, економічної, оборонної та інших складових безпеки України.

Значення Доктрини інформаційної безпеки як у площині протидії загрозам інформаційній та національній безпеці України, здійснювалось осучаснення векторності діяльності держави у захисті інформаційного простору країни від зовнішньої інформаційної агресії, так і з точки зору вдосконалення нормативно-правового регулювання інформаційної сфери [23]. Також, варто підкреслити той факт, що Доктрину інформаційної безпеки України було затверджено через більш ніж 2,5 роки після початку відкритої збройної агресії з боку рф. При цьому, сама Доктрина не була нормативно-правовим актом, який би створював конкретні правові механізми. Окреслений акт став базовим і призначеним для відображення цілей, «векторів» діяльності держави у даній сфері [24].

Окремо варто звернути увагу, що рф, завдяки соціальним мережам, таким, як «Вконтакте» та «Одноклассники», які були досить поширеними у країнах пострадянського простору, зокрема, і в Україні, формувала через певні спільноти меседжі, спрямовані на дезорганізацію та дезінтеграцію суспільства [25]. Підґрунтям для цього став документ «Стратегія національної безпеки Російської Федерації до 2020 року», у якому чітко зазначено про необхідність поширення «правдивої» інформації для громадян рф та росіян, які проживають закордоном через засоби масової інформації та соціальні мережі. Отже, відбувалося поширення ідей «русского міра», що зумовлювало маргіналізацію певних прошарків суспільства і створювало передумови для розгортання сепаратистських рухів на території іншої країни [26]. Указом Президента України від 15 травня 2017 року № 133/2017 було введено в дію рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», відповідно до якого було заборонено Інтернет провайдерам в Україні надання послуг з доступу користувачам мережі Інтернет до ресурсів сервісів «Mail.ru», «Вконтакте» та «Одноклассники» [27]. Отже, дане рішення РНБО України, яке спрямоване на обмеження відповідних інтернет-ресурсів рф стало відповіддю щодо протидії інформаційній агресії та пропаганді ворога.

Також, варто звернути увагу на прийняття Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [28], у якому визначено правові та організаційні засади захисту життєво важливих

інтересів людини, громадянина, суспільства, держави та національних інтересів у кіберпросторі. До окресленого Закону, законодавцем неодноразово вносились зміни.

У 2018 прийнято Закон України «Про національну безпеку» № 2469-VIII, де зокрема, визначено, що «національна безпека – захищеність … і забезпечення свободи слова та інформаційної безпеки, кібербезпеки та кіберзахисту … при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам» [29].

Указом Президента України від 14 вересня 2020 року № 392/2020 було введено в дію рішення РНБО України від 14 вересня 2020 року «Про Стратегію національної безпеки України» на підставі чого, втратила чинність, стаття 2 Указу Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"» [30]. Стратегія 2020 року стала основою для розробки Стратегії кібербезпеки, Стратегії інформаційної безпеки, Стратегії забезпечення державної безпеки та ін.

Президент України своїм Указом № 447/2021 від 26 серпня 2021 року ввів у дію рішення РНБО України від 14 травня 2021 року «Про Стратегію кібербезпеки України», на підставі якого втратила чинність стаття 2 Указу Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» [31]. Так, у Стратегії кібербезпеки України 2021 року визначено, що рф залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України.

Також, у Стратегії деталізуються перспективні напрями посилення спроможностей національної системи кібербезпеки. Оскільки забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Також пріоритетами забезпечення кібербезпеки України визначені: убезпечення кіберпростору для захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки.

З метою адекватного реагування на поширення гібридних загроз в Україні, Указом Президента України від 28 грудня 2021 року № 685/2021 було введено в дію рішення РНБО України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», на підставі якого втратила чинність стаття 2 Указу Президента України від 25 лютого 2017 року № 47 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"» [32]. Основною загрозою безпеці України у Стратегії визначена рф і проведена нею країною інформаційна політика, і задекларовано тезу про те, що інформаційна політика рф – це загроза не лише для України, але й для інших провідних демократичних держав світу. Також, у Стратегії визначаються завдання та шляхи діяльності держави з метою недопущення кризових явищ у вітчизняному інформаційному просторі, посилення інформаційної безпеки та її складових. Стратегію планується реалізувати до 2025 року. Окремо варто зауважити, що цим декларативним документом визначено 7 важливих перспективних цілей.

16 лютого 2022 року Указом Президента України № 56/2022 було введено в дію рішення РНБО України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» [33]. У ній закріплено основні пріоритетні напрями у сфері державної безпеки. Також у Стратегії зазначається, що об'єктами забезпечення державної безпеки є інформаційна безпека, державна таємниця та службова інформація. Відповідно ці цієї Стратегії, інформаційна безпека – це стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання 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 шляхом 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.

24 лютого 2022 року рф розпочала широкомасштабне вторгнення в Україну, що призвело до

безпрецедентних викликів у сфері інформаційної безпеки. Органами державної влади було вжито низку заходів задля збереження стійкості своєї інформаційної інфраструктури, протидії російській дезінформації та забезпеченні доступу громадян до достовірної інформації.

Так, зокрема, 19 березня 2022 року Президент України підписав Указ, відповідно до якого було введено в дію рішення РНБО України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [34], яким було створено єдину інформаційну платформу стратегічної комунікації – цілодобовий інформаційний марафон «Єдині новини #UA разом». Також встановлено відповідальність за поширення певної інформації в умовах воєнного або надзвичайного стану шляхом внесення змін до Кримінального та Кримінального процесуального кодексів України за: несанкціоноване розповсюдження інформації про направлення, переміщення міжнародної військової допомоги в Україну, рух, переміщення або розміщення Збройних Сил України чи інших військових формувань України; виготовлення та поширення забороненої інформаційної продукції; несанкціоноване поширення 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 [35].

Наразі в Україні функціонує також Центр протидії дезінформації при РНБО України, на сайті якого можна ознайомитись з актуальною інформацією та подіями в цій сфері. Центр протидії дезінформації є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення РНБО України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106 [36]. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [37].

Також, варто зазначити, що ще у 2021 році Президентом України піднімалось питання щодо створення Кіберсил ЗС України. У 2023 та 2024 роках зосереджувалась увага на практичну реалізацію даного питання, втім, в Україні досі немає юридично оформлених Кіберсил ЗС України.

Висновки. Отже, аналіз правових аспектів формування та розвитку нормативно-правової бази України в сфері інформаційної безпеки свідчить, що у період з 2014 до 2022 року було прийнято низку документів щодо забезпечення інформаційної безпеки в умовах гібридної агресії російської федерації та захисту інформаційного простору нашої держави. Завдяки комплексним заходам, Україна змогла частково протидіяти інформаційній агресії російської федерації, захистити свій інформаційний простір та підвищити стійкість суспільства до маніпуляцій та дезінформації. Втім, з початком широкомасштабного вторгнення держави-агресорки в Україну, перед нашою державою постали нові виклики та загрози, що потребують подальших законодавчих змін щодо забезпечення інформаційної безпеки держави.

В сучасних реаліях стрімкими темпами розвиваються і змінюються технології. В результаті цього виникає необхідність у постійному оновленні законодавчої бази задля ефективного реагування на нові виклики. Подальші дослідження окресленої теми варто зосередити на вдосконаленні існуючої нормативно-правової бази, шляхом внесення змін до діючого законодавства та прийняття нового. Серед практичних рекомендацій щодо вдосконалення законодавства із забезпечення інформаційної безпеки варто виокремити такі:

1. Погоджуючись із думкою дослідників, які займались цим питанням, важливим стало б прийняття рамкового Закону «Про інформаційну безпеку», що закріпив би ключові поняття і положення інформаційної безпеки України.

2. Крім того, варто переглянути такий основоположний документ, як Стратегія інформаційної безпеки, реалізація якої спрямована до 2025 року, з урахуванням сучасних загроз в умовах широкомасштабної агресії з боку російської федерації. У новій Стратегії слід звернути увагу на питаннях застосування штучного інтелекту.

3. Окремо потребує уваги також питання важливості ухвалення Закону України «Про Кіберсили Збройних Сил України», прийняття якого дало би змогу ефективніше захищати національні інтереси в інформаційному просторі.

Отже, розширення та вдосконалення законодавчої бази, створення нових інституцій та механізмів, поглиблення співпраці з міжнародними партнерами – це ключові напрями розвитку правового забезпечення інформаційної безпеки в Україні в умовах зростаючої агресії російської федерації.

Список літератури:

1. Шубіна О. В. Державна інформаційна безпека: проблеми визначення концепту. *Держава та права.* 2014. № 3. С. 26–31.

2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision.* 2016. Vol. 2. № 1. С. 27–32.

3. Шаповал Р. В., Клочко В. О. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. *Наше право.* 2014. № 6. С. 5–9.

4. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : Указ Президента України від 01.05.2014 № 449/2014. URL: https://zakon.rada.gov.ua/laws/show/449/2014#Text (дата звернення: 07.11.2024).

5. Про засади інформаційної безпеки України: Проєкт Закону України від 28.05.2014 № 4949. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123 (дата звернення: 10.11.2024).

6. Беспалов І. О. Правові засади інформаційної безпеки під час дії правового режиму воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2024. № 11. URL: https://reicst.com.ua/pmtl/article/view/2024-11-01-05/2024-11-01-05 (дата звернення: 10.11.2024).

7. Відбулось перше засідання Експертної Ради з розробки концепції інформаційної безпеки та з питань розвитку інформаційного простору. *Урядовий портал.* URL: https://www.kmu.gov.ua/news/248043524 (дата звернення: 07.11.2024).

8. Нестеряк Ю. В. Визначення та узагальнення пріоритеті в державної політики України в інформаційній сфері. *Публічне управління та митне адміністрування.* 2015. № 2 (13). С. 98–103.

9. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14.01.2015 № 2. URL: https://zakon.rada.gov.ua/laws/show/2-2015-п#Text (дата звернення: 10.11.2024).

10. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України: Закон України від 05.02.2015 № 159-VIII. URL: https://zakon.rada.gov.ua/laws/show/159-19#Text (дата звернення: 12.11.2024).

11. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України від 24.09.2015 № 555/2015. URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text (дата звернення: 10.11.2024) – втратив чинність.

12. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. *Історико-політичні студії. Збірник наукових праць.* 2017. С. 30-43.

13. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 12.11.2024).

14. Про Стратегію національної безпеки України: Указ Президента України від 12.02.2007 №105/2007. URL: https://zakon.rada.gov.ua/laws/show/105/2007#Text (дата звернення: 11.11.2024) – втратив чинність.

15. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 06.06.2016 № 240/2016. URL: https://zakon.rada.gov.ua/laws/show/240/2016#Text (дата звернення: 13.11.2024) – втратив чинність.

16. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 11.11.2024).

17. Ткачук Н. А. Щодо підготовки нової редакції стратегії кібербезпеки України. Актуальні проблеми управління інформаційною безпекою держави: *зб. тез наук. доп. наук.-практ. конф.* Київ : НА СБУ, 2021. С. 130–132.

18. Ткачук Н. А. Стан та проблемні питання реалізації стратегії кібербезпеки України. *Інформація і право.* 2019. № 1(28). С. 129–134.

19. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 10.11.2024).

20. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14.03.2016 № 92/2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016#Text (дата звернення: 11.11.2024) – втратив чинність.

21. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: Указ Президента України від 13.02.2017 № 32/2017. URL: https://zakon.rada.gov.ua/laws/show/32/2017#Text (дата звернення: 14.11.2024).

22. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 12.11.2024).

23. Савицький В. Т. Інформаційна безпека в системі національної безпеки України. *Університетські наукові записки.* 2017. № 62. С. 195–207.

24. Борисов О. Ю. Нормативно-правова база забезпечення інформаційної безпеки України: сучасні проблеми та відправні точки їх вирішення. *Інформація і право.* 2020. № 4(35). С. 113–118.

25. Світова гібридна війна: Український фронт. Національний інститут стратегічних досліджень. Київ, 2017. 496 с.

26. Новородовський В. Інформаційна безпека України в умовах російської агресії. *Society. Document. Communication. Соціум. Документ. Комунікація.* 2020. № 9. С. 150–179.

27. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 15.05.2017 № 133/2017. URL: https://zakon.rada.gov.ua/laws/show/133/2017#Text (дата звернення: 14.11.2024).

28. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.11.2024).

29. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2469-19#Text (дата звернення: 08.11.2024).

30. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 12.11.2024).

31. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 11.11.2024).

32. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 15.11.2024).

33. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»: Указ Президента України від 16.02.2022 № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення: 16.11.2024).

34. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19.03.2022 № 152/2022. URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text (дата звернення: 16.11.2024).

35. Дорошенко Т. В. Проблемні питання забезпечення інформаційної безпеки держави в умовах повномасштабної агресії. *Наукові перспективи,* 2024. № 4(46). С. 159–169.

36. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text (дата звернення: 16.11.2024).

37. 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, серія «Державне управління».* 2024. № 1(20). С. 14–24.

Rusnak Yu.I. LEGAL ASPECTS OF ENSURING INFORMATION SECURITY DURING THE RUSSIA-UKRAINE WAR

The article focuses on ensuring Ukraine's information security amidst the Russian-Ukrainian war. The aim of the study is to analyze the legal aspects of the formation and development of Ukraine's regulatory framework in the field of information security as a key component in the conditions of the war waged by the Russian Federation against Ukraine. It also incorporates the experience gained during the Anti-Terrorist Operation (Joint Forces Operation) in Eastern Ukraine to develop recommendations for improving the legislative framework in the specified area.

The research methods were selected in line with the study's purpose and determined by its logical structure. The author utilized various methods, including a systemic approach, historical method, comparative legal method, analysis, synthesis, and others.

The article establishes that the aggression initiated by the Russian Federation in 2014 introduced new challenges and threats in the information domain. It provides a detailed analysis of the genesis of the development

of Ukraine's regulatory and legal acts in the field of information security against the backdrop of the escalating Russian-Ukrainian war and examines their adaptation to modern challenges of hybrid warfare and information aggression. The significance of studying the evolution of legislation in this sphere lies in identifying how historical challenges have shaped legal mechanisms and their capacity to adapt to emerging threats, such as cyberattacks and disinformation.

The study also highlights gaps in the legislation and investigates how the adoption of new regulatory and legal acts has contributed to improvements in this area. Additionally, the article analyzes the regulatory and legal acts adopted during the large-scale aggression launched by the Russian Federation against Ukraine on February 24, 2022, and provides recommendations for enhancing the legislative framework to ensure Ukraine's information security.

The theoretical and practical significance of the article lies in the comprehensive analysis of key regulatory and legal acts, as well as the exploration of the prerequisites for their development and establishment. The findings may serve as a basis for further research on the development and improvement of legislation in the specified domain.

Key words: *Armed aggression, hybrid threats, propaganda, information security, national security.*