Шифр «нове покоління»

КОНСТИТУЦІЙНО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПАРАДИГМІ «ВІЙНИ НОВОГО ПОКОЛІННЯ»

ЗМІСТ

ВСТУП 3

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ 6

1.1. Інформаційна безпека як самостійна складова системи національної безпеки України: поняття та зміст 6

1.2. Інформаційна складова гібридної війни 10

РОЗДІЛ 2. КОНСТИТУЦІЙНО-ПРАВОВІ ТА ІНСТИТУЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 15

2.1. Конституційно-правові засади забезпечення інформаційної безпеки в Україні: проблеми та напрями оптимізації 15

2.2. Інституційне забезпечення інформаційної безпеки України на сучасному етапі державотворення України 20

РОЗДІЛ 3. КОНСТИТУЦІЙНЕ ПРАВО НА ТАЄМНИЦЮ КОРЕСПОНДЕНЦІЇ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ 24

ВИСНОВКИ 29

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 31

ВСТУП

Актуальність теми дослідження. Інтенсифікація нових загроз, що постали перед Україною, зумовили необхідність адаптації української системи забезпечення інформаційної безпеки до нових умов гібридного протистояння, що призвели до суттєвої активізації як Української держави в цілому, так у західних урядів для перегляду концептуальних підходів щодо забезпечення інформаційної безпеки, як складової національної безпеки. А реальній втраті суверенітету над частиною території України (анексія Криму, ситуація в зоні бойових дій на Донбасі) під псевдолегітимним виглядом так званих референдумів передувала багаторічна зовнішня інформаційна агресія, котра переросла в повній мірі у відкриту та неприховану інформаційну війну.

Приклад XXI ст. переконливо демонструє і переконує в тому, що зважаючи на ці зовнішньополітичні обставини багато уваги приділяється геополітичному виміру цієї проблеми, тому поряд з юридичними та технічними активізувалися також політологічні та соціально-філософські дослідження на тему інформаційної безпеки, що в підсумку знаходить відображення в дослідженнях закономірностей розвитку інформаційної сфери як системоутворюючого фактора життя сучасного суспільства в цілому і життя кожного члена цього суспільства.

Доктрина інформаційної безпеки 2017 року чітко декларує, що проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. Тому актуальність цієї теми визначається необхідністю захисту прав людини, які відносяться до першочергової області національних інтересів в інформаційній сфері, реалізація яких спрямована на формування «безпечного інформаційного середовища» в Україні.

Мета і задачі дослідження. Метою наукової роботи є з’ясування і аналіз конституційно-правових та інституційних аспектів інформаційної безпеки в

умовах гібридної війни та вироблення на цій основі пропозицій і рекомендацій, які сприятимуть підвищенню ефективності забезпечення інформаційної безпеки в Україні.

Відповідно до визначеної мети поставлені наступні **задачі**:

- розкрити зміст поняття інформаційної безпеки як самостійної складової системи національної безпеки України;
- дослідити інформаційну складову гібридної війни, основними суб'єктами якої є ЗМІ та Інтернет;
- визначити проблеми та напрями оптимізації конституційно-правового забезпечення інформаційної безпеки в Україні;
- охарактеризувати стан інституційного забезпечення інформаційної безпеки України на сучасному етапі державотворенні;
- з'ясувати проблемні питання правового забезпечення конституційного права на таємницю кореспонденції в інформаційному просторі в умовах гібридної війни;
- показати шляхи підвищення ефективності конституційно-правового забезпечення інформаційної безпеки в Україні.

Об'єктом дослідження є інформаційна безпека України.

Предметом дослідження є інформаційна безпека України в умовах гібридної війни.

Методи дослідження. За допомогою історичного методу здійснювалось дослідження формування правових поглядів та ґенезу теорій на поняття інформаційної безпеки (пп. 1.1), діалектичний метод пізнання – дослідження інформаційної безпеки як самостійної складової системи національної безпеки України та гібридної війни як нової форми глобального протистояння (пп. 1.1, 1.2). Порівняльний метод використовувався при дослідженні сукупності заходів конституційно-правового забезпечення інформаційної безпеки в Україні (п. 2.1); метод інтерпретації (тлумачення) використовувався для з'ясування змісту правових норм конституційно-правового механізму забезпечення інформаційної безпеки (п.2.1), структурно-функціональний метод

використовувався для аналізу інституційної бази у сфері інформаційної безпеки України (п.2.2). Соціологічний метод – при проведенні анкетування респондентів, аналізі та узагальненні результатів анкетування (п. 1.2). За допомогою методів правового моделювання та прогнозування було підтверджено висновок про необхідність удосконалення нормативно-правового забезпечення інформаційної безпеки України шляхом розробки та прийняття Інформаційного кодексу та Закону України «Про гарантії права людини таємницю кореспонденції» (пп.2.1, Розділ 3).

Теоретична і практична значущість дослідження. Теоретичні та практичні висновки і положення, обґрунтовані у дослідженні, доповнюють та уточнюють на загальнотеоретичному та практичному рівнях проблематику забезпечення національної безпеки в інформаційній сфері та можуть бути використані у подальших теоретичних і практичних розробках з питання захисту інформаційної безпеки в умовах гібридної війни.

Запропоновані в роботі теоретичні положення та висновки можуть бути рекомендовані для використання у правозастосовній діяльності державних органів та установ, що працюють у сфері інформаційної безпеки та у юридичній практиці – для підвищення рівня правосвідомості й правової культури громадян в площині інформаційної безпеки.

Матеріали даного дослідження можуть бути використані при розробці навчально-методичної літератури з теорії та практики забезпечення національної безпеки у інформаційній сфері. Основні положення та висновки, викладені у дослідженні можуть бути використані в процесі підготовки та прийняття нових нормативно-правових актів та систематизації чинного законодавства, програмно-цільових та стратегічних документів, спрямованих на удосконалення державної політики інформаційної безпеки.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

1.1. Інформаційна безпека як самостійна складова системи національної безпеки України: поняття та зміст

Концептуальні основи інформаційної безпеки ще тільки починають розроблятися та вимагають подальшого опрацювання. Складність висвітлення проблеми інформаційної безпеки до теперішнього часу, пов’язана з відсутністю загальноприйнятого категоріального апарату, що описує цю предметну область. Труднощі у визначенні поняття «інформаційна безпека», на наш погляд, обумовлені ще тим фактом, що феномен інформаційної безпеки наповнюється власним змістом в різних наукових областях: технічній, правовій, психологічній, соціальній, тим самим ще раз підкреслюючи її багатогранну природу. Тому спроби виробити дефініцію робляться постійно, оскільки визначення сутності інформаційної безпеки відноситься до числа проблем, вирішення яких має як теоретичне, так і практичне значення.

У свою чергу, Степанов В. Ю. зазначає, що термін «інформаційна безпека» в нашій державі поки не дістав адекватних наукових розробок. Унаслідок цього, у панівному термінологічному вакуумі, його трактування іноді вражає своєю багатоликістю, а місцями й неадекватністю суті того явища, яке він віддзеркалює. Тому, теоретичне питання щодо термінології знаходить важливе значення внаслідок її застосування [1, с. 27].

Вартує зазначити, що формування інформаційної безпеки викликаний об’єктивними умовами розвитку соціуму. Усвідомлюючи особливості інформаційної безпеки в Україні, що пов’язані, перш за все, з активною інформаційною агресією проти нашої держави, а по-друге, реформуванням самої системи національної безпеки країни, в результаті чого виникають труднощі, що не дозволяють сформулювати досить повне визначення досліджуваного поняття.

Розглянувши основні труднощі, які виникають на шляху вирішення проблеми сутності інформаційної безпеки, перейдемо до розкриття основних

підходів до визначення інформаційної безпеки. З-поміж існуючих концептуальних підходів до трактування інформаційної безпеки спробуємо окреслити сутність цього феномену в рамках енциклопедичного, доктринального та нормативно-правового підходів.

У багатотомній юридичній енциклопедії Ю. С. Шемшученка інформаційна безпека України визначається як один із видів національної безпеки, важлива функція держави [2, с. 714].

Характеризуючи сучасний стан досліджуваної проблеми в доктринальному напрямі, О. Д. Довгань та Т. Ю. Ткачук пишуть наступне: «інформаційна безпека – це стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, в т.ч. захищеність національних цінностей, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних національних цілей та реалізація національних інтересів [3, с. 97].

Дещо в іншому ракурсі трактує інформаційну безпеку В. В. Шемчук, який репрезентує свою позицію крізь призму правовідносин, що виникають під час забезпечення стану захищеності інформаційного простору. За визначенням В. В. Шемчука, інформаційна безпека – це правовідносини, що виникають під час здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства та держави [4, с. 33].

Інша група вчених під інформаційною безпекою розуміють як сукупність засобів забезпечення інформаційного суверенітету України, захисту держави та її громадян від зовнішніх і внутрішніх інформаційних загроз» [5, с. 19]. В цьому ключі розглядає зазначене поняття С.О. Лисенко, вказуючи на державній діяльності з підтримання інформаційної складової національної безпеки, яка охоплює певну частину відокремлених від інших напрямів діяльності держави [6, с. 158]. У рамках даного напряму інформаційна безпека покликана забезпечити захист національних цінностей за допомогою усього арсеналу засобів, що є в розпорядженні держави.

Цікавими з точки зору тематики дослідження є визначення інформаційної безпеки Я. М. Жарковим, М. Т. Дзюбою, І. В. Замаруєвою, які у своєму підручнику «Інформаційна безпека особистості, суспільства, держави» визначають інформаційну безпеку не лише як самостійну складову національної безпеки, а й як складову інших сфер національної безпеки держави, спрямованою на забезпечення національних інтересів у цих сферах [7, с. 31].

Вищевказана думка є справедливою і підтверджується тим, що інформаційна безпека закономірно виходить на перший план у системі національної безпеки, оскільки інформаційна сфера як системоутворюючий фактор життя суспільства активно впливає на стан всіх інших ключових елементів національної безпеки, а саме економічної, екологічної, політичної, воєнної безпеки (та є складовою всього переліченого). Адже, як вірно зазначає В. О. Антонюк, «елементи структури системи національної безпеки, у свою чергу, є складними підсистемами, що взаємодіють між собою окремими аспектами» [8, с. 98].

У дисертаційному дослідженні Т. Ю. Ткачука, зміст категорії «інформаційна безпека», як і «національна безпека» в цілому, розглядається з точки зору діяльнісного підходу, визначаючи її передусім як процес, а не «стан захищеності» [9, с. 73].

Підкреслимо зазначену думку як вузлову в нашому дослідженні. І справді, можна погодитися з цієї точкою зору і примітно вказати, що зміст інформаційної безпеки не можна зводити тільки до рамок стану захищеності – її зміст значно ширший. Це багатогранна область діяльності, яка включає такі ознаки як, рух, тривалість та динаміку. Тому, можна стверджувати, що інформаційна безпека – це процес діяльності державних органів, направлений на попередження та боротьбу загрозам інформаційній сфері, вживання заходів у вигляді сукупності активних дій та засобів інформаційного впливу, які реалізуються і здатні контролюватися тривалий час.

Нормативно-правовий підхід до розуміння інформаційної безпеки представлений в законах та інших нормативних актах України, які регулюють відносини у сфері інформаційної безпеки. Передусім варто вказати, що зміст інформаційної безпеки передбачає широкий комплекс компонентних частин та на сьогодні не має чіткого юридичного визначення у законодавстві.

В Законі України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р. офіційно визнано інформаційну безпеку як невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки [10]. Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» було вперше законодавчо закріплено поняття інформаційна безпека як стан захищеності життєво важливих інтересів людини, суспільства і держави. [11].

Також інформаційна безпека розкривається у Доктрині інформаційної безпеки України від 25 лютого 2017 р. [12] як невід'ємна складова кожної зі сфер національної безпеки і як важлива самостійна сфера забезпечення національної безпеки. Саме ж поняття інформаційної безпеки застосовується у Законі України «Про національну безпеку України» від 21 червня 2018 р. [13], але жодним чином не визначено, що саме мається на увазі під інформаційною безпекою та забезпеченням інформаційної безпеки.

На нашу думку, на сьогодні поняття «інформаційна безпека» як в доктринальному, так і нормативно-правовому підходах є результатом інтеграції змісту понять «складова частина національної безпеки» й «стан захищеності».

На основі аналізу різних підходів до визначення категорії інформаційної безпеки слід зробити висновок про недопустимість суворого дотримання однієї авторської позиції. Інтерпретація указаних формулювань призводить до обрання комплексного підходу до розуміння сутності інформаційної безпеки держави (безпека є, водночас, і станом, і процесом). На нашу думку, інформаційна безпека – це стан та процес захищеності життєво важливих інтересів особи, суспільства та держави, при якому вона, з одного боку, здатна ефективно протистояти дестабілізуючому та неправомірному впливу зовнішніх

і внутрішніх інформаційних загроз, а з іншого – її постійне функціонування не створює інформаційних загроз для елементів самої системи і зовнішнього середовища. Дане визначення в концентрованому вигляді виражає сутність поняття «інформаційна безпека».

Основний зміст поняття «інформаційна безпека» полягає у: 1) вивченні негативних результатів застосування інформаційних технологій для суспільства та дослідження причин їх прояву; 2) у виявленні способів їх подолання, тим самим формуючи безпечний стан інформаційного середовища; 3) створенні оптимальних умов для оптимального функціонування інформаційної інфраструктури та забезпеченні безпеки інформації; 4) захисті суб'єктів інформаційної взаємодії від негативного впливу та виключенні ризиків; 5) задоволенні інформаційної потреби соціальних суб'єктів за допомогою формування безпечного стану інформаційного середовища.

Методологічною основою визначення поняття «інформаційна безпека» має бути віднесення категорії «безпека» не до самої інформації, хоча інформаційна безпека і пов'язана з нею, а до суб'єктів інформаційного середовища – фізичних та юридичних осіб, які беруть участь в інформаційному процесі [14].У підсумку, ґрунтуючись на вищевикладеному аналізі наукових підходів, визначимо суттєвий зміст поняття «інформаційна безпека»: забезпечення безпеки інформації та забезпечення безпеки суб'єктів інформаційної взаємодії від негативного інформаційного впливу.

1.2. Інформаційна складова гібридної війни

«Гібридна війна» – термін, що з'явився в кінці XX століття в США, який позначає введення війни проти будь-якої держави як традиційними (тобто за участю регулярних військових підрозділів, розвідки тощо), так і нетрадиційними способами [15, с. 50].

Гібридну війну називають війною четвертого покоління, «війною, яка сполучає традиційні та нетрадиційні форми, військові та невійськові тактики» [16, с. 88]. Серед основних напрямів невійськового впливу використовуються

всі відомі невоєнні засоби тиску – політичні, економічні, гуманітарні. Але пріоритетним тут, без сумніву, є інформаційний компонент.

У ході гібридної війни в інформаційному полі можливе досягнення таких результатів, як втрата державних територій без пострілів, за використанням однієї тільки дезінформації чи налаштування населення проти державної влади [17, с. 138]. Інформативна невизначеність підкріплюється формуванням певного дискурсу, а точніше системним вилученням з нього дефініцій «агресія», «вторгнення», «окупація». Інформаційне протистояння є першим етапом гібридної війни, яке може перерости в пряме зіткнення і до стану оголошення війни.

На думку О. Я. Лещенка, єдиного визначення терміну «гібридна війна» не існує. Визначення «гібридна війна» відсутнє в міжнародно-правових документах. Не застосовується цей термін й у воєнних доктринах Російської Федерації та Сполучених Штатів Америки [18, с. 54]. Досліджуване явище не є сталим, а досить рухливим, воно не вибудовується в історичному часі як щось зрозуміле, а модифікує та набуває нового вигляду.

Інформаційна складова гібридної війни Російської Федерації проти України є мабуть наймасштабнішою в новітній історії за часом та задіяними ресурсами. Так, у вересні 2014 р. Верховний головнокомандуючий Об'єднаних збройних сил НАТО в Європі генерал Філіп Брідлав назвав її «найдивовижнішим бліцкригом інформаційної війни, який ми колись бачили в історії» [19].

У квітні 2015 р. на парламентській асамблеї НАТО було представлено доповідь Д. Калхи «Гібридна війна: новий стратегічний виклик НАТО?» [20]. У цій доповіді зокрема підкреслюється, що Росія використовує внутрішню слабкість України за рахунок, насамперед, невійськових методів (таких як політичне, інформаційне, економічне залякування та маніпуляції), що дозволило Росії завдяки пропаганді й викривленню фактів побудувати нову віртуальну реальність, де вона виступала гарантом й захисником прав

російськомовних громадян. В інтерпретації Москви використання сили було обумовлено захистом співвітчизників від «звірств» українського уряду.

Враховуючи відсутність єдиного наукового трактування гібридної війни, пропонуємо виділяти певні виміри цього явища через інформаційну складову і розглядати гібридну війну як нову форму глобального протистояння; загальну назву новітньої форми військового конфлікту; нестандартний тип ведення війни, комбінація різних типів і способів впливу на інформаційне суспільство.

У напрямку інформаційного впливу на власних громадян країна-агресор використовує антиукраїнську тематику (а українська проблематика у деяких медійних засобах Російської Федерації іноді досягає 80% загального обсягу інформації) як засіб: 1) підживлення імперського духу росіян, що тримається на ідеях шовінізму і ксенофобії; 2) консолідації російського суспільства перед загрозою зовнішнього ворога – у тому числі України як сателіта США і НАТО; 3) відволікання російських громадян від власних соціально-політичних проблем; 4) залякування населення Російської Федерації негативними наслідками будь-яких виступів проти існуючої влади Кремля («недопущення російського майдану»); 5) мотивації агресивних дій особового складу Збройних Сил Російської Федерації проти України та поповнення різноманітних збройних формувань, що воюють проти України.

На міжнародному рівні антиукраїнська інформаційна пропаганда намагається довести, що Росія не має відношення до війни проти України (Крим – істинно «руська» територія і його приєднання до Російської Федерації – це повернення історичної справедливості, здійсненої на основі волевиявлення кримчан на референдумі 2014 р; на Донбасі Росія не воює) та концентрує увагу на формуванні образу України як: 1) політично нестабільної держави, в яку небезпечно вкладати гроші; 2) країни, де порушуються права людини, здійснюється штучна українізація, ведеться наступ на російськомовне населення; 3) технологічно відсталої та ненадійного економічного партнера, що не дотримується норм міжнародного права; 4) країни, що не готова до вступу до ЄС і НАТО, а природним станом для якої є позаблоковий статус.

Для населення окупованої території Донбасу і у зоні конфлікту антиукраїнська інформаційна діяльність Російської Федерації має на меті культивування ідей про: 1) Україну – країну-агресора, яка розв'язала війну проти народу Донбасу, що повстав проти київської хунти; 2) участь у військових діях на боці Збройних Сил України бандерівців, галичан і американських найманців; 3) історичний органічний зв'язок з Росією, з цінностями «руського миру»; 4) Новоросію як особливу територію південно-східної частини України; 5) економічну самодостатність Донбасу; 6) неприйняття або вороже ставлення до всього українського – держави, історії мови, культури; 7) можливе входження Донбасу до складу України, але на правах особливого статусу територіальної автономії; 8) підкидання у масову свідомість негативних сценаріїв, що здатні самореалізовуватися, та нагнітання катастрофічних настроїв.

Для всього населення, що мешкає на території України основними завданнями інформаційної війни є наступні: 1) формування позитивного і привабливого образу Росії, підживлення ностальгії за СРСР; 2) орієнтація на міф про єдність слов'янських народів, а отже, на євразійський вектор розвитку України; 3) прищеплення цінностей «руського миру»; 4) створення негативного образу України як неуспішної держави із низькими стандартами життя, високим рівнем злочинності і тотальною корупцією; 5) вороже ставлення до власного політичного керівництва як некомпетентного, неукраїнського, корумпованого; 6) розповсюдження недовіри до ідеї євроінтеграції та вступу до НАТО; 7) нав'язування думки про Україну як штучне територіальне утворення, до якого за певними суб'єктивними обставинами були включені Крим, Новоросія, Галичина, Буковина і Центральна частина, що передбачає її не унітарний, а федеративний устрій.

Україна вжила певних заходів щодо протистояння російській інформаційній експансії, однак вони, на погляд фахівців, є певною мірою ситуативними, досить вузько спрямованими і не відповідають значним масштабам російської експансії [21, с. 318].

За даними Київського міжнародного інституту соціології, яке проводилося у лютому 2019 року, з 33% до 38.5% зросла частка тих, хто вважає, що в Україні забагато прокремлівських пропагандистських ЗМІ. На противагу цьому 30% (стільки ж було у лютому 2018 року) бачать в Україні наступ на свободу слова [22]. Тільки протягом п’яти місяців 2018 року Службою Безпеки України виявлено та задокументовано використання російськими спецслужбами 181 інтернет-ресурсу для дестабілізації соціально-політичної ситуації в нашій країні та маніпулювання суспільною свідомістю [23], що є свідченням масштабності кібервійни Російської Федерації проти України.

Загалом за 2019 рік фахівці Служби Безпеки України нейтралізували понад 480 кіберінцидентів та кібератак на органи державної влади та об’єкти критичної інфраструктури. За цей період також припинено функціонування більше ніж 1000 сайтів, що використовувались у злочинних цілях [24].

Для України подолання негативних наслідків дії сучасних інформаційних загроз власними зусиллями є вкрай проблематичним. Більш адекватною відповіддю на сучасні виклики могло б стати її прискорене включення до системи колективної безпеки в Європі шляхом євроатлантичної та європейської інтеграції.

Проте, як вірно зауважує Р.В. Шаповал, необґрунтоване «запозичення» правових норм ЄС та інших розвинених країн є небезпечним явищем для формування правового поля України з питань забезпечення інформаційної безпеки. Адже у цих країнах забезпечення інформаційної безпеки здійснюється на основі сталого функціонування економіки, державних і суспільних інституцій та на базі правових основ демократичного суспільства, що формувалася там багато десятиріч [25, с. 8].

РОЗДІЛ 2. КОНСТИТУЦІЙНО-ПРАВОВІ ТА ІНСТИТУЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Конституційно-правові засади забезпечення інформаційної безпеки в Україні: проблеми та напрями оптимізації

Правова основа забезпечення інформаційної безпеки в теоретичному сенсі – це сукупність різних за юридичною силою права норм, що відносяться до різних галузей і відбивають сутність процесів, що відбуваються в сфері забезпечення інформаційної безпеки, складаючи єдину систему [26, с. 12].

Вихідною точкою для функціонування системи інформаційної безпеки є Конституція України, а також закони України, укази та розпорядження Президента України, міжнародно-правові акти, що пов'язані із забезпеченням як міжнародної, так і національної безпеки, постанови та розпорядження Кабінету Міністрів України, відомчі нормативні акти у формі наказів, директив, положень, правил, інструкцій.

Аналіз змін в законодавчому забезпеченні інформаційної сфери України з погляду її безпеки після агресії Росії зумовлює аналіз відповідної нормативної бази, яка діяла на етапі від 90-х років і до початку російського втручання у 2014 р. і виявила необхідність її подальшого серйозного коригування відповідно до потреб часу. Повинні погодитися з О.О. Золотар, яка пише: «На жаль, не існує Закону України «Про інформаційну безпеку України» незважаючи на об'єктивну потребу такого акту в час, коли Україна знаходиться в стані гібридної війни, за умов якої інформаційна безпека є найбільш атакованою і, водночас, найбільш вразливою» [27, с. 181].

Основним нормативно-правовим актом, що визначає правові засади політики безпеки є Конституція України, яка надає великого значення інформаційній складовій національної безпеки. Так, норма ч. 1 ст. 17 Конституції України встановлює, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [28]. У цьому контексті інформаційна безпека розглядається на одному рівні з

такими невід'ємними ознаками державності, як суверенітет і територіальна цілісність.

Про інформаційну сферу йдеться в інших статтях Основного Закону, зокрема, ст. ст. 31 32, 34, 50 в контексті забезпечення конституційних гарантій права на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції; захисту від втручання в приватне життя; захисту від незаконного поширення конфіденційної інформації, судового захисту права спростовувати недостовірну інформацію та права вимагати її вилучення у зв'язку з цим; права вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір; права вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також права на її поширення.

Конституція України стала основним правовим базисом подальшої нормотворчості в інформаційній сфері. Втім, на думку І.О. Валюшко, ця нормотворчість, поряд з певними позитивами розвитку інформаційного поля, свободи і захисту інформації, не виявила необхідної дієвості в умовах інформаційної війни. Головне, ця нормотворчість не забезпечила реалізацію ст. 17 Конституції, яка ставить інформаційну безпеку до ряду найважливіших функцій держави, таких як захист суверенітету та територіальної цілісності. Відповідно, незабезпечення інформаційної безпеки призвело до втрати частини суверенітету та територіальної цілісності нашої держави [29, с. 32].

До початку збройного конфлікту на Сході України нашій державі вдалося напрацювати певну законодавчу базу у сфері національної інформаційної безпеки, однак, як виявилося вона не стала вирішальним фундаментом для захисту інформаційного простору України від викликів інформаційної агресії і відставала від сучасних реалій.

На реалізацію конституційних норм в Україні прийнято низка законів, а саме: Закон України «Про інформацію» (перший базовий нормативний закон у цій галузі) (1992 р.); Закон України «Про друковані засоби масової інформації (пресу в Україні)» (1992 р.), Закон України «Про авторське право і суміжні

права» (1993 р.), «Про телебачення і радіомовлення» (1993 р.), «Про інформаційні агентства» (1995 р.), Закон України «Про рекламу» (1996 р.), «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» (1997 р.), «Про електронні документи та електронний документообіг» (2003 р.), «Про захист персональних даних» (2010 р.) та ін.

Позитивним зрушенням у формуванні цілісної державної політики щодо інформаційної безпеки було прийняття Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», який, зокрема, передбачав вдосконалення нормативно-правової бази у сфері забезпечення інформаційної безпеки та розробку Інформаційного кодексу України. На переконання зарубіжного фахівця Л. Лессига, саме кодекс в якості норм і правил, створить необхідний формат регулювання електронного середовища [30, с. 89].

Серед інших документів, що стосувалися сфери інформаційної безпеки були Стратегія національної безпеки України (2007), Доктрина інформаційної безпеки України (2009 р.).

З початком російської військової агресії проти України, у якій інформаційна складова почала відігравати ключову роль, розпочалася трансформація національного інформаційного законодавства. Стартовим нормативно-правовим актом у цьому напрямку стало рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року, введене в дію Указом в. о. Президента України від 1 травня 2014 року № 449/2014. Цим рішенням було сформовано цілісний погляд на систему забезпечення інтересів України у сфері інформаційної безпеки, що дало поштовх до майбутніх дій та заходів органами влади щодо переформатування стану справ у цій ситуації. Справедливим було твердження документу про те, що «останнім часом Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через

що намагається маніпулювати суспільною свідомістю в Україні та за її межами» [31].

6 травня 2015 року Рада національної безпеки і оборони України схвалила проект нової Стратегії національної безпеки, яка розрахована до 2020 року [32]. Усі попередні стратегічні акти у сфері інформаційної безпеки мали більш рекомендаційний, аніж практичний характер. Указаний документ базується на науковому підході. До його розроблення долучилися вітчизняні та міжнародні експерти, представники ЄС та НАТО.

В Україні концептуальним документом щодо забезпечення інформаційної безпеки України та протидії російським інформаційним загрозам стала Стратегія кібербезпеки України, яка була введена в дію Указом Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [33].

На основі вищезгаданої Стратегії національної безпеки України була затверджена Доктрина інформаційної безпеки, ухвалена Радою національної безпеки та оборони у грудні 2016 р. і введена в дію Указом Президента П. Порошенка 25 лютого 2017 р. [34].

Основною рисою Доктрини інформаційної безпеки 2017 року, яка відрізняється від попередньої Доктрини (2009 року) є спроба збалансувати повноваження між гілками влади та силових структур у сфері інформаційної безпеки. Основним недоліком Доктрини вважаємо те, що вона не має достатнього правового регулювання потенційного залучення представників усіх секторів громадянського суспільства до заходів забезпечення інформаційної безпеки.

9 травня 2018 року набрав чинності Закон України «Про основні засади забезпечення кібербезпеки України», а 21 червня 2018 року було прийнято Закон України «Про національну безпеку України».

26 липня 2018 року Кабінет Міністрів України схвалив Стратегію інформаційної реінтеграції Донецької та Луганської областей, підготовлену Міністерством інформаційної політики України (МІП) [35]. Це перший

комплексний документ, що визначає інформаційну політику щодо цього непростого питання. Реалізація Стратегії розрахована на період до 2020 року.

На основі вищевикладеного, законодавчу базу України у сфері інформаційної безпеки загалом можна поділити на дві групи. Перша включає концептуальні, базові документи, такі як Доктрини та Стратегії, які визначають основні загрози та тенденції в інформаційній безпеці. Друга група містить Закони України, Укази Президента, рішення РНБО України, які забороняють контент країни агресора на радіо, телебаченні та в Інтернет просторі України.

Як справедливо відзначає О. В. Олійник, особливим недоліком нормативно-правового регулювання інформаційної безпеки України є розпорошення його у численних нормативно-правових актах різної юридичної сили. Причому важливі проблеми нормативно закріплюються підзаконними нормативно-правовими актами. Не менш важливою проблемою для ефективного забезпечення інформаційної безпеки України є неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією [36, с. 133].

Загалом, незважаючи на певну невпорядкованість, неузгодженість та безсистемність українського законодавства у інформаційній сфері, інформаційне законодавство України в останні роки було переглянуто і трансформовано відповідно до нових викликів та загроз в умовах військової агресії. Певні правові акти були прийняті на короткотривалу дію і термін їхньої чинності закінчується у 2020 році. Тому враховуючи той факт, що Україна знаходиться в стані гібридної війни, за умов якої інформаційна безпека є найбільш атакованою і, водночас, найбільш вразливою, є об’єктивна потреба в опрацюванні базового закону – Інформаційного кодексу, який би включав окремий розділ про інформаційну безпеку чи прийнятті спеціального Закону України «Про інформаційну безпеку України», який зможе регламентувати основні засади державної політики, спрямованої на захист інформаційної безпеки людини, суспільства та держави від зовнішніх та внутрішніх загроз.

2.2. Інституційне забезпечення інформаційної безпеки України на сучасному етапі державотворення України

Наразі зберігається дуже розгалужена (при цьому сталою є тенденція до зростання кількості суб'єктів) система залучення державних інституцій з дещо дублюючими та перехрещеними повноваженнями до забезпечення інформаційної безпеки України. З урахуванням положень Конституції України й інших законів та нормативно-правових актів України, якими визначаються повноваження, права та обов'язки, до основних суб'єктів забезпечення інформаційної безпеки відносять Президента України, Кабінет Міністрів України та Верховну Раду України.

Президент України як глава держави, гарант державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, Верховний Головнокомандуючий Збройних Сил України і Голова Ради Національної безпеки і оборони України здійснює загальне керівництво у сферах національної безпеки та оборони України. Президенту України також підпорядковуються Національний інститут стратегічних досліджень, який є базовою науково-дослідною установою аналітико-прогнозного супроводження діяльності Президента України.

У контексті координації функцій забезпечення інформаційної безпеки варто акцентувати на особливому статусі Ради національної безпеки і оборони України як суб'єкта інформаційних відносин, оскільки він є єдиним органом, який має повноваження координувати та контролювати діяльність органів виконавчої влади з реалізації політики інформаційної безпеки України та вносити Президенту України пропозиції щодо її уточнення та ресурсного забезпечення. Окрім цього, при РНБО з 2002 року існує консультативно-дорадчий орган «Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки» [37]. До основних її завдань, зокрема, належить аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики.

Функція Верховної Ради України полягає у напрацюванні законодавчої бази у сфері інформаційної безпеки та забезпеченні відповідного парламентського контролю. Верховна Рада України в межах повноважень, визначених Конституцією України, визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного та воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних Сил України та інших військових формувань, створених відповідно до законів України.

До складу Верховної Ради входять три профільні парламентські комітети: Комітет з питань національної безпеки, оборони та розвідки, Комітет з питань гуманітарної та інформаційної політики, Комітет з питань цифрової трансформації, які виконують завдання щодо підготовки законопроектів з питань розвитку інформаційної сфери та інформаційної безпеки.

Кабінет Міністрів України, керуючись Конституцією країни та іншим вітчизняним законодавством здійснює реалізацію політики інформаційної безпеки України. До інституцій інформаційної безпеки прямо чи опосередковано відносяться міністерства та інші центральні органи виконавчої влади; Державний комітет телебачення і радіомовлення України; Державна служба спеціального зв'язку та захисту інформації України; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України, на які безпосередньо покладається виконання заходів у сфері національної безпеки України.

Місцеві державні адміністрації та органи місцевого самоврядування, відповідно до їхньої компетенції, забезпечують вирішення питань у сфері інформаційної безпеки на регіональному рівні.

Слід звернути увагу на існування значної кількості органів виконавчої влади, які функціонують у сфері забезпечення інформаційної безпеки. В результаті можна стверджувати той факт, що розбудова механізму

інформаційної безпеки відбувається зі значним ухилом в бік органів виконавчої влади.

На основі дослідження їхньої компетенції у сфері інформаційної безпеки В. М. Абакумов стверджує про паралелізм та дублювання функцій окремими органами, що, звісно ж, негативно відображається на результативності їх діяльності. На його думку, необхідно, насамперед, визначити, які органи і за якою ознакою мають належати до органів виконавчої влади, що функціонують у сфері забезпечення інформаційної безпеки (у тому числі у сфері протидії інформаційним війнам), скільки їх має існувати у державі, на яких принципах і за якими ознаками вони мають бути об'єднані в єдину систему держави [38, с.68-69].

Пропонується підпорядкувати сферу інформаційної безпеки одному керуючому органу при Президентові України або Кабінетові Міністрів України з метою виконання чіткого виконання завдань, визначених у Стратегії національної безпеки та Доктрині інформаційної безпеки.

Ще одним важливим кроком у напрямку підвищення стандартів захисту інформаційної безпеки людини вбачається створення інституту інформаційного омбудсмена – як незалежного органу, діяльність якого спрямована на захист прав і свобод людини в інформаційній сфері. Подібна інституція Інформаційного комісара нині існує у Туреччині. Досвід цієї країни свідчить, що інформаційний комісар як окрема незалежна інституція займається питаннями захисту прав громадян, журналістів та громадських активістів у справах з доступу до інформації та забезпечення захисту персональних даних.

Існує також об'єктивна потреба у формуванні громадського інституту контролю за діяльністю іноземних масмедіа, незалежних експертних оцінок маніпулятивних впливів іноземних ЗМІ на українську аудиторію.

Варто відзначити, що 14 січня 2015 року Кабінет Міністрів України ухвалив постанову «Питання діяльності Міністерства інформаційної політики України» [39], відповідно до якої затверджено відповідне Положення про створення Міністерства інформаційної політики України. Вперше за історію

незалежної України, була створена окрема урядова установа, основною метою якої стало формування інформаційної політики України та відбиття інформаційних нападів проти нашої держави.

Окрім цього, у листопаді 2017 року Міністерство інфраструктури України створило генеральний секретаріат цифрової інфраструктури та державне підприємство, яке займається питаннями кібербезпеки. ЄС виділив на цю структуру близько 60 млн. гривень в якості європейського гранту [40].

Як підкреслює В. М. Пастушенко, створене нещодавно Міністерство інформаційної політики за своєю суттю також не вирішить питання належного регулювання інформаційної сфери з боку держави. Започаткування роботи ще одного центрального органу виконавчої влади, ймовірно призведе до чергового дублювання та роззосердження функцій регулювання інформаційним простором та його ресурсами на вищому рівні державного управління [41, с. 60]

Таким чином, зміст організаційно-правових механізмів державної політики щодо забезпечення інформаційної безпеки складається з певної трьохелементної системи, у якій Верховною Радою України визначаються основи інформаційної безпеки, Президентом вирішуються питання щодо визначення конкретних інструментів досягнення цих основ, а на Кабінет Міністрів покладено завдання щодо застосування обраного інструменту впливу на суспільні відносини і проведення в життя передбачених заходів. За допомогою заданої схеми взаємодії вищих органів державної влади в сфері інформаційної безпеки реалізується на практиці конституційний принцип розподілу влад.

РОЗДІЛ 3. КОНСТИТУЦІЙНЕ ПРАВО НА ТАЄМНИЦЮ КОРЕСПОНДЕНЦІЇ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

На постіндустріальному етапі розвитку суспільства удосконалення інформаційно-комунікаційних технологій супроводжується розширенням можливостей їхнього недобросовісного використання, яке створює загрози інформаційній безпеці і може призводити до порушень прав людини. У зв'язку з цим виникає проблема співвідношення інформаційної безпеки і прав людини, перш за все, конституційного права на таємницю листування в інформаційному середовищі, дослідженню якої і присвячений цей розділ.

Водночас, маємо констатувати, що незважаючи на те, що інформаційна безпека традиційно складається з трьох компонентів (безпека людини, суспільства, держави), основна увага дослідників зосереджена лише на двох останніх елементах, в той час як саме людина зазнає чи не найбільше негативних впливів в інформаційному суспільстві (як технологічних так і психологічних). Важливою складовою цієї проблеми є те, що, а ні на науковому, а ні на державному рівні немає чіткого та однозначного розуміння, що власне має захищатись в контексті інформаційної безпеки особи [42, с. 96]. Тож виникає своєрідна дилема: заходи із захисту прав людини в інформаційному суспільстві можуть супроводжуватися власне порушенням цих прав.

Як випливає зі статті 3 Конституції України, «людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю». Підкреслюється, що права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави, а їх утвердження і забезпечення прав і свобод людини є головним обов'язком держави. Конституція України виступає гарантом зазначених положень, тому втрата зв'язку з вищою цінністю – правами людини – для діяльності держави та її органів щодо забезпечення інформаційної безпеки, будь-то правотворча, правоохоронна діяльність, створює ризики для порушення відповідних прав.

Тому будь-яка діяльність держави, в тому числі та, яка спрямована на забезпечення інформаційної безпеки, повинна ґрунтуватися в своїй початковій точці на визнання, дотримання та захисту прав людини.

У державах з демократичними правовими режимами, як правило, встановлений пріоритет прав людини перед забезпеченням національної безпеки. В основі даного підходу лежать положення Резолюції A/RES/66/290, прийнята Генеральною Асамблеєю 10 вересня 2012 р. яка зазначила, що безпека людини заснована на національній відповідальності [43].

Щодо пріоритетності конституційних прав і свобод людини, то тут слід зауважити, що у Доктрині інформаційної безпеки України 2017 р. відображено тенденцію до домінування позиції людини у сфері безпеки, оскільки «до національних інтересів України в інформаційній сфері на перший план віднесено такі життєво-важливі інтереси особи, як: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів».

Однак, коли справа доходить до перелічення загроз національним інтересам та національній безпеці України в інформаційній сфері (ст. 4), то на перше місце виходять інтереси, насамперед, держави, оскільки вони рангуються за наступними сферами: у зовнішньополітичній сфері; у сфері державної безпеки; у воєнній сфері; у внутрішньополітичній сфері. Тобто, декларований у перших статтях пріоритет людини та її прав, інтересів відходить на другий план, коли йдеться про реальні загрози та пріоритети державної політики в інформаційній сфері.

Український дослідниця О. О. Золотар справедливо зазначає, що інформаційна безпека людини не повинна протиставлятись інформаційній безпеці держави та суспільства. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держави, попередження міжнародних

конфліктів чи терористичних актів. Таким чином, має місце конфлікт інтересів різних об’єктів інформаційної безпеки [27, с. 384].

Вважається, що традиційні підходи до вирішення даного конфлікту засновані на домінуванні тієї чи іншої цінності. Важливо зрозуміти, що інформаційна безпека людини не повинна прирівнюватися інформаційній безпеці держави та суспільства. Адже сама людина визнається основною цінністю в Конституції Україні і забезпечення її прав і свобод і є кінцевою метою реалізації функцій держави. Пріоритет прав людини по відношенню до інформаційної безпеки виражається в неприпустимості обмеження свободи вираження поглядів, свободи інформації та ін. На відміну від держав, які утверджують та забезпечують вищу цінність прав людини, в деяких державах така домінанта має обмежений характер зі встановленням необхідного і достатнього контролю над загрозами інформаційній безпеці як правової цінності (Північна Корея).

Забезпечення інформаційної безпеки може бути безпосередньо спрямоване на створення умов для реалізації прав людини. З іншого – заходи щодо забезпечення інформаційної безпеки не повинні призводити до обмеження прав людини і повинні бути відповідні загрозам і наслідків їх прояву. Основними принципами встановлення обмеження права людини при забезпеченні інформаційної безпеки є «встановлення обмеження тільки законом» і «необхідність у демократичному суспільстві». При цьому такий принцип як «необхідність у демократичному суспільстві» є оціночним і застосовується вже після встановлення обмеження.

Кожен, хто знаходиться на території України (її громадяни, іноземці чи особи без громадянства), або ж під її юрисдикцією, має конституційне право на таємницю листування, телефонних розмов, та іншої кореспонденції, закріплене в ст. 31 Конституції України. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з’ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо. Однак, станом на 2019 рік, для України

продовжує залишатися невирішеною проблема забезпечення конституційного права людини на таємницю кореспонденції, особливо в інформаційному середовищі, та враховуючи той факт, що Україна перебуває під постійним інформаційним натиском нерезидентів, який з часом лише посилюється.

Важливо зазначити, що дія Закону України «Про основні засади забезпечення кібербезпеки України» [44] не поширюється на соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсі. А отже, фактично кореспонденція приватних осіб (людей), яка поширюється у зазначеному кіберпросторі, залишається поза захистом (абз.3 та абз.4 ст. 2 Закону України «Про основні засади забезпечення кібербезпеки України»), окрім гарантій закріплених в ч.3 ст. 9 Закону України «Про телекомунікації» № 1280-IV від 18 листопада 2003 р.

Суперечливість дії норм зазначеного закону полягає і в тому, що об'єктами кібербезпеки є конституційні права і свободи людини і громадянина, в тому числі і конституційне право людини на таємницю кореспонденції. То ж, кожна особа, яка фізично перебуває на території України, спілкуючись в кіберпросторі через передачу/прийом її кореспонденції, у разі виникнення кіберзагроз, потребує захисту з боку української держави, виходячи з наданих їй гарантій, закріплених в ст. 31 Конституції України. А тому, виникає проблема реального, а не декларативного, забезпечення конституційного права людини на таємницю кореспонденції, при тому, що, власне, на людину з боку держави, не покладається жодного обов'язку вжити всіх можливих заходів щодо забезпечення інформаційної безпеки кореспонденції, що передається.

Щодо забезпечення конституційного права людини на таємницю кореспонденції в кіберпросторі в Україні, то положеннями ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» законодавчо передбачена державно-приватна взаємодія у сфері кібербезпеки, яка полягає в

наступному: по-перше, у підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі; по-друге, в обміні інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз, кібератак та кіберінцицентів; по-третє, в формуванні ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет.

То ж, пропонується доповнити перелік напрямів державної політики в сфері, пов'язаній в кіберпростором, блоком заходів, спрямованих на реалізацію політики у сфері таємниці кореспонденції, зокрема через: 1) внесення змін до чинного законодавства України (правова реформа у сфері таємниці кореспонденції, а саме шляхом прийняття та реалізації спеціального закону України «Про гарантії права людини таємницю кореспонденції», який враховуватиме міжнародні стандарти в сфері таємниці кореспонденції, в т.ч. ЄС та НАТО); 2) розробку та введення в освітній процес курсу дисципліни (програми) «Інформаційно-правова культура та безпека в Україні», зокрема в кіберпросторі, що проводитиметься для слухачів на трьох рівнях: на першому – для дітей шкільного віку та студентів відповідно у школах та у вищих учбових закладах; на другому – для дорослих (реалізація через соціальну рекламу ЗМІ); на третьому – для дорослих, діяльність яких пов'язана з правом та/або забезпеченням таємниці кореспонденції (через проведення курсів підвищення кваліфікації у вищих учбових закладах).

ВИСНОВКИ

Системний аналіз літературних джерел за темою дослідження показав, що серед сучасних дослідників відсутнє єдине бачення трактування «інформаційної безпеки». Принципово важливим є розуміння інформаційної безпеки не лише як самостійної складової національної безпеки, а й як складову інших сфер національної безпеки держави і від рівня її забезпечення залежить успішне функціонування всіх інших видів безпеки.

Конкретизовано зміст поняття «інформаційна безпека», що розглядається на основі комплексного або інтегрального підходу як: стан та процес захищеності життєво важливих інтересів особи, суспільства та держави, при якому вона, з одного боку, здатна ефективно протистояти дестабілізуючому та неправомірному впливу зовнішніх і внутрішніх інформаційних загроз, а з іншого – її постійне функціонування не створює інформаційних загроз для елементів самої системи і зовнішнього середовища.

Константовано, що інформаційна складова гібридної війни проти України знаходить втілення в декількох напрямках – серед власних громадян країни-агресора; серед міжнародної спільноти; серед населення окупованої території Донбасу і у зоні конфлікту; серед всього населення, що мешкає на території України. Усі перераховані напрями антиукраїнської інформаційної складової гібридної війни тісно пов’язані між собою, забезпечуючи реалізацію стратегічної програми РФ як на локальному, так і на глобальному рівнях.

Аналіз законодавчої бази доводить, що через значну кількість законів та особливо підзаконних нормативних актів у сфері інформаційних відносин, що ускладнює їх пошук; відсутність системної, чіткої та ієрархічної єдності законів, що призводить до суперечливого тлумачення та застосування норм права на практиці; термінологічні розбіжності, що призводять до варіативного розуміння норм, одним із найбільш оптимальних шляхів її вирішення є систематизація та кодифікація інформаційного законодавства. У зв’язку з цим обґрунтовується доцільність та своєчасність проведення упорядкування інформаційного законодавства, зокрема, шляхом прийняття спеціального

Закону України «Про інформаційну безпеку України», а доречніше Інформаційного кодексу, який би відображав основні пріоритети, систему і структуру інформаційного законодавства.

Установлено, що одним із найважливіших питань у сфері розбудови забезпечення інформаційної безпеки в Україні є впровадження системи стратегічного управління. Його основні складники – це система інформаційно-аналітичного забезпечення (джерела інформації, критерії і показники загроз, методики оброблення інформації, моніторинг, документування, банки даних паспортів загроз та антикризових механізмів тощо), система обґрунтування рішень (наукові установи, апарат РНБОУ), система ухвалення рішень (РНБОУ, Президент України, Верховна Рада України), система забезпечення реалізації рішень (Кабінет Міністрів України через стратегії, програми, плани, бюджети). Ці процедури мають бути чітко регламентовані та нормативно закріплені.

У зв’язку зі створенням ряд нових інституцій у сфері інформаційної безпеки, функції яких є дещо розмитими та нечіткими і часто дублюються, пропонуються: здійснити перерозподіл повноважень між органами державної влади та підпорядкувати сферу інформаційної безпеки одному керуючому органу з метою виконання чіткого виконання завдань, визначених у Стратегії національної безпеки та Доктрині інформаційної безпеки; сформувати незалежний інститут інформаційного омбудсмена – як незалежного органу, діяльність якого спрямована на захист прав і свобод людини в інформаційній сфері.

Визначено основні напрями розвитку та удосконалення існуючої нормативно-правової бази з питання конституційного права людини на таємницю кореспонденції. До них належать: гармонізація законодавства України та правових систем ЄС та НАТО у сфері таємниці кореспонденції шляхом розробки та прийняття базового закону України «Про гарантії права людини на таємницю кореспонденції»; створення та введення в освітній процес курсу дисципліни (програми) «Інформаційно-правова культура та безпека в Україні».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Степанов В. Ю. Інформаційна безпека в інформаційній сфері державного управління. *Теорія та практика державного управління*. 2016. Вип. 4. С. 24–28.

2. Юридична енциклопедія : у 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. Київ: Укр. енциклопедія, 1998–1999. Т. 2 : Д – Й. 744 с.

3. Ткачук Т. Ю., Довгань О. Д. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. 2018. № 1 (24). С. 89–103.

4. Шемчук В.В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи. *Вчені записки ТНУ імені В.І. Вернадського*. Том 30 (69). № 4. 2019. С.31–37.

5. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23.

6. Лисенко С. О. Конституційні засади розуміння інформаційної безпеки. *Публічне урядування*. 2016. № 4. С. 154–161.

7. Жарков Я.М., Дзюба М.Т., Замаруєва І.В. Інформаційна безпека особистості, суспільства, держави: підручник. Київ: Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.

8. Антонов В. О. А Конституційно правові засади національної безпеки України: монографія / В. О. Антонов; наук. ред. Ю.С. Шемшученко. Київ: ТАЛКОМ, 2017. 576 с.

9. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір. дис. … д-ра юрид. наук. Ужгород, 2019. 487 с.

10. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. / Офіційний веб-портал Верховної ради України. URL: http://zakon0.rada.gov.ua/laws/show/75/98-вр

11. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V / *Відомості Верховної Ради*. 2007. № 12. Ст. 102.

12. Доктрина інформаційної безпеки України: затв. указом Президента України від 25 лют. 2017 р. № 47/2017. Урядовий кур'єр. 2017. 28 лютого. № 38.

13. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII / *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

14. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво*. № 2/2016. URL: http://www.kbuapa.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf

15. Світова гібридна війна: український фронт: монографія / за заг. ред. В. П. Горбуліна. К. : НІСД, 2017. 496 с.

16. Рущенко І. П., Рущенко Ю. І. Гібридна агресія та громадянський спротив у Харкові 2014 р.: уроки першої фази російсько-української війни. *Український соціум*. 2016. № 3(58). С.88–99.

17. Мосов С. П., Уханова Н. С. Протидія негативним інформаційним впливам на людину і суспільство в умовах гібридної війни. *Інформація і право*. 2018. № 2 (25). С. 134–141.

18. Лещенко О. Я. Трансформація системи цивільного захисту України в умовах сучасних воєнно-політичних конфліктів гібридного типу: дис. … канд. юрид. наук. Київ, 2020. 293 с.

19. John Vandiver. SACEUR: Allies must prepare for Russia «hybrid war» (4 September 2014). URL: https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464

20. Julio Miranda Calha. Hybrid Warfare: NATO's New Strategic Challenge?, NATO Parliamentary Assembly (7 April 2015). URL: https://www.eerstekamer.nl/id/vk3nbmfqmt7x/document_extern/nato_pa_rapport_hybrid_warfare_nato/f=/vk3nbqkjzced.pdf

21. Міжнародна інформаційна безпека: теорія і практика: підручник. Київ: Центр вільної преси, 2016. 418 с.

22. Джерела інформації, медіаграмотність і російська пропаганда: результати всеукраїнського опитування громадської думки : Аналітичний звіт. (Березень 2019 р.). URL: Режим доступу: https://detector.media/doc/images/news/archive/2016/164308/DM- KMIS_Report _05_2019_web.pdf

23. Удосконалення законодавства щодо протидії загрозам національній безпеці в інформаційній сфері необхідне для блокування російських кібератак. URL: https://ssu.gov.ua/ua/news/2/category/301/view/5025#.HWFI8oZe.dpbshttps://ssu.gov.ua/ua/news/2/category/301/view/5025#.HWFI8oZe.dpbs

24. У 2019 році розпочато 339 кримінальних проваджень у сфері інформаційної безпеки. URL: https://detector.media/infospace/article/174215/2020-01-25-u-2019-rotsi-rozpochato-339-kriminalnikh-provadzhen-u-sferi-informatsiinoi-bezpeki-sbu/

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

26. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : автореф. дис. … канд. юрид. наук. Львів, 2019. 20 с.

27. Золотар О. О. Інформаційна безпека людини: теорія і практика. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

28. Конституція України : прийнята 28 черв. 1996 р. № 254/96 ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

29. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. Історико-політичні студії. Серія: Політичні науки : зб. наук. пр. / М-во освіти і науки України, ДВНЗ «Київ. нац.

екон. ун-т ім. Вадима Гетьмана», Ін-т історії укр. сусп-ва ; редкол.: І. Д. Дудко (голова) [та ін.]. Київ : КНЕУ, 2017. № 2. С. 30–43.

30. Lessig L. Code and Other Values of Cyberspace. New York: Basic Books, 1999. 320 p.

31. 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: http://zakon.rada.gov.ua/go/laws/show/449/2014/paran2#n2

32. 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 р. № 287/2015 / Верховна Рада України. Законодавство України. URL: https://goo.gl/OvFRER

33. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016 / Верховна Рада України. Законодавство України. URL: https://goo.gl/LqyZg7

34. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514/2009/ URL: http://www.president.gov. ua/documents/9570. html

35. Про схвалення Стратегії інформаційної реінтеграції Донецької та Луганської областей, підготовлену Міністерством інформаційної політики України: Розпорядження Кабінету Міністрів України від 26 липня 2018 р. № 539-р URL: https://zakon.rada.gov.ua/laws/show/539-2018-%D1%80

36. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство*. 2012. № 3. С. 132-137.

37. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки: Указ Президента України від 22 січня 2002 року N 63/2002. URL: https://zakon.rada.gov.ua/laws/show/63/2002

38. Абакумов В. М. Інституційне забезпечення протидії інформаційним війнам в Україні. *Право і Безпека*. 2010. № 2. С. 65–69.

39. Питання діяльності Міністерства інформаційної політики України: постанова Кабінету Міністрів України від 14 січня 2015 р. № 2 // Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF

40. Кібербезпекою об'єктів критичної інфраструктури опікуватиметься держпідприємство при Мінінфраструктури. URL: https://ua.interfax.com.ua/news/general/465659.html

41. Пастушенко В. М. Проблеми правового регулювання державного управління інформаційною сферою України. *Наукові записки Інституту законодавства Верховної Ради України*. 2015. № 1. С. 59–64.

42. Дубова С.В. До проблеми забезпечення інформаційної безпеки особи в інформаційному суспільстві (методологічні аспекти). Проблеми захисту прав людини в інформаційному суспільстві : матеріали наук.-практ. конф. / 1 квітня 2016 р., м. Київ / Упорядн. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний інститут стратегічних досліджень, 2016. С.96-99.

43. Resolution adopted by the General Assembly on 10 September 2012 URL: https://undocs.org/en/%20A/RES/66/290

44. Про основні засади забезпечення кібербезпеки України : Закон України № № 2163-VIII від 05.10.2017 р. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

АНОТАЦІЯ

Постановка питання про інформаційну безпеку в умовах гібридної війни має особливе значення для України. Не дивлячись на численну кількість наукових праць на цю тему, кількість яких різко збільшилася з 2014 року і продовжує зростати дотепер, значна частина питань теорії та практики забезпечення інформаційної війни все-таки залишається відкритою.

Актуальність теми обумовлена тим, що на сьогодні існує недосконаліть чинного нормативно-правового забезпечення системи інформаційної безпеки в Україні. Це при тому, що кількість прийнятих законів у згаданій сфері переважає понад двадцяти нормативно-правових актів, але більшість з них суперечать один одному. Сучасне українське суспільство потребує якісної нормативно-правової бази у сфері інформаційної безпеки, щоб почувати себе захищеним в інформаційному середовищі хоча б у правовому відношенні.

Об’єктом дослідження є інформаційна безпека України.

Предметом дослідження є інформаційна безпека України в умовах гібридної війни.

Метою наукового дослідження є з’ясування і аналіз конституційно-правового та інституційного забезпечення інформаційної безпеки в умовах гібридної війни та вироблення на цій основі пропозицій і рекомендацій, які сприятимуть підвищенню ефективності забезпечення інформаційної безпеки. Зокрема, в роботі відповідно до визначеної мети поставлено такі завдання: розкрити зміст поняття інформаційної безпеки як самостійної складової системи національної безпеки України; дослідити інформаційну складову гібридної війни, основними суб’єктами якої є ЗМІ та Інтернет; визначити проблеми та напрями оптимізації конституційно-правового забезпечення інформаційної безпеки в Україні; охарактеризувати стан інституційного забезпечення інформаційної безпеки України на сучасному етапі державотворення України; з’ясувати проблемні питання правового забезпечення конституційного права на таємницю кореспонденції в інформаційному просторі в умовах гібридної війни; показати шляхи

підвищення ефективності конституційно-правового забезпечення інформаційної безпеки в Україні.

Як методологічна основа дослідження використані філософські, загальнотеоретичні та спеціальні методи наукового пізнання, застосування яких зумовлюється системним підходом, а саме історичний, діалектичний, порівняльно-правовий, структурно-функціональний, соціологічний, метод інтерпретації та методи правового моделювання та прогнозування.

У науковій роботі здійснено аналіз інформаційної безпеки України у парадигмі «війни нового покоління». У першому розділі систематизовано та проаналізовано науковий, енциклопедичний та нормативний підходи в частині трактування поняття інформаційної безпеки як самостійної складової системи національної безпеки України. Представлено інтегральний або діяльнісний підхід до розуміння інформаційної безпеки, під якою слід розуміти стан та процес захищеності життєво важливих інтересів особи, суспільства та держави, при якому вона, з одного боку, здатна ефективно протистояти дестабілізуючому та неправомірному впливу зовнішніх і внутрішніх інформаційних загроз, а з іншого – її постійне функціонування не створює інформаційних загроз для елементів самої системи і зовнішнього середовища.

Досліджується природа російсько-української «гібридної війни», акцентуючи увагу на інформаційну складову «гібридної війни», яка в рамках воєн четвертого покоління стала однією із визначальних чинників у протистоянні російським інформаційним впливам.

У другому розділі роботи висвітлюються аналіз конституційно-правового забезпечення інформаційної безпеки та система основних державних інституцій України, які покликані формувати та забезпечувати реалізацію політики інформаційної безпеки в Україні. Встановлено, що у правовому регулюванні забезпечення інформаційної безпеки в Україні існує низка організаційних, нормативних, процесуальних проблем, які потребують комплексного опрацювання.

У третьому розділі звернено увагу на невирішеності проблеми забезпечення конституційного права людини на таємницю кореспонденції, особливо в кіберпросторі, враховуючи той факт, що Україна перебуває під постійним інформаційним натиском зовнішньої сторони. Наголошено на проблемі пропорційності і дотримання балансу інтересів при забезпеченні інформаційної безпеки.

Структура й обсяг наукової роботи обумовлені метою, завданнями та предметом дослідження. Робота складається зі вступу, трьох розділів, що поділені на 4 підрозділів, висновків та списку використаних джерел. Список джерел та літератури має 44 найменувань.