

Львівський національний університет імені Івана Франка  
Міністерство освіти і науки України

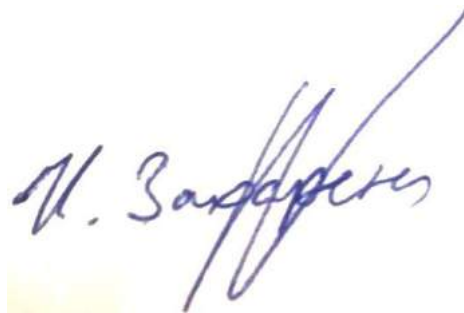
**ЗАХАРЕНКО КОСТЯНТИН ВОЛОДИМИРОВИЧ**

УДК 321.022:323.23

**ІНСТИТУЦІЙНИЙ ВИМІР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ  
УКРАЇНИ: ТРАНСФОРМАЦІЙНІ ВИКЛИКИ, ГЛОБАЛЬНІ  
КОНТЕКСТИ, СТРАТЕГІЧНІ ОРІЄНТИРИ**

Спеціальність 23.00.02 – політичні інститути та процеси

**АВТОРЕФЕРАТ**  
дисертації на здобуття наукового ступеня  
доктора політичних наук

A handwritten signature in blue ink, appearing to read 'K. Zaharenko', is written over a yellow rectangular background.

Львів – 2021

Дисертацією є рукопис.

Роботу було виконано в Національному педагогічному університеті імені М. П. Драгоманова Міністерства освіти і науки України

**Науковий консультант:** доктор політичних наук, професор  
**Дмитренко Микола Андрійович**  
Академія зовнішньої розвідки України,  
головний науковий співробітник

**Офіційні опоненти:** доктор політичних наук, професор  
**Смолянук Володимир Федорович**  
Воєнно-дипломатична академія імені Євгенія  
Березняка, провідний науковий співробітник

доктор політичних наук, доцент  
**Шипунов Геннадій Володимирович**  
Львівський національний університет імені Івана  
Франка, виконуючий обов'язки завідувача  
кафедри теорії та історії політичної науки

доктор політичних наук, доцент  
**Ярош Оксана Богданівна**  
Волинський національний університет імені Лесі  
Українки, завідувач кафедри політології,  
управління та державної безпеки

Захист відбудеться 7 травня 2021 року об 11:00 годині на засіданні спеціалізованої вченої ради Д 35.051.17 Львівського національного університету імені Івана Франка за адресою: 79000, м. Львів, вул. Університетська, 1, ауд. 301, тел. 239-44-62.

З дисертацією можна ознайомитись у Науковій бібліотеці Львівського національного університету імені Івана Франка за адресою: 79601, м. Львів, вул. Драгоманова, 5.

Автореферат розіслано 6 квітня 2021 року.

Вчений секретар  
спеціалізованої вченої ради



В. В. Бунь

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Обґрунтування вибору теми дослідження.** Інформаційна революція спонукає бурхливий розвиток інформаційних потоків, електронних засобів комунікації, інформатики, телематики, створення глобальної інформаційної мережі, яка, за висловом Е. Сміта, перетворилась у «становий хребет сучасної цивілізації». Зросла кількість людей, задіяних у процесах накопичення, обробки, розповсюдження, передачі та обміну інформацією. Інформаційний бум у буквальному розумінні охопив суспільство загалом і окрему особистість зокрема, змінив їх спосіб життя, сформував нові виклики і загрози. Актуальним стало поняття «інформаційної безпеки», забезпечення якої цілком справедливо покладається, насамперед, на державу. Останнє потребує більш глибокого вивчення проблеми змісту та функціональних особливостей державної інформаційної політики, її ролі у створенні та реалізації безпечних інформаційних систем та технологій, а відтак і в створенні додаткових можливостей свободи й доступу до інформаційної діяльності, підтримки розвитку інформаційних ресурсів тощо.

В чому ж полягають фундаментальні витoki та основні детермінанти актуальності проблеми інформаційної безпеки? Формуючи відповідь, насамперед, необхідно підкреслити, що інформаційна революція, що триває вже декілька десятиліть, викликала такі потужні цивілізаційні зрушення у всіх сферах суспільного буття, які важко порівняти з будь-якою іншою епохою. Інформація стала не просто засобом чи зручним способом дії, вона перетворилася для сучасної людини і суспільства на життєвий простір, що містить не тільки нові можливості, але й значні небезпеки. Вплив інформаційної технології і електронних обмінів справляє такий перетворюючий ефект, який не могла викликати навіть промислова революція. Інтернет став таким засобом комунікації, без якого вже не можуть обходитись працівники будь-якої сфери суспільної життєдіяльності. Водночас у новій віртуальній реальності закладено безліч загроз – для індивіда, громади, держави, міжнародних організацій. Інформаційної агресії зазнають важливі основи сучасного суспільного життя – демократія і подальша демократизація, стабільні політичні системи і системи, що модернізуються, локальні культури та нові глобалізовані формати співробітництва та миру. Усе це потребує мобілізації теоретичних зусиль, які мають передувати практиці, визначати детермінанти, ресурси, технології та напрями реалізації цього непростого завдання.

Доповнюється актуалізація дисертаційної роботи і тим фактом, що інформаційна безпека, яка оперує інформацією, безумовно є важливим чи неодмінним знаряддям конструювання сучасної цивілізації. Відповідно, провідні держави світу, усвідомлюючи це, беззаперечно виходять із постулату, що створення інформації та контроль над інформацією та

різними ресурсами й потоками інформації, в тому числі у контексті технологічної модернізації з цього приводу, допомагають їм зберігати своє лідерство і контроль над поточним станом справ. А це ставить на порядок денний проблематику взаємозв'язку інформаційної безпеки та державного суверенітету, який суттєво залежить від різноманітних інформаційних впливів.

Деструктивні та дестабілізуючі інформаційні впливи найперше загрожують вразливим елементам політичної системи. Водночас нерідко цілеспрямовані та регулярні інформаційні атаки самі по собі формують сприятливе для поглинання середовище, коли дієві суб'єкти перетворюються у дезорієнтованих та безпорадних об'єктів політики. Особливо актуальною проблематика інститутів інформаційної безпеки є для нашої країни, суспільство якої та кожен окремих громадянин всі роки незалежності знаходяться під агресивним впливом різних суб'єктів інформаційного простору, як внутрішнього, так і зовнішнього. Для України питання інформаційної безпеки особливо актуалізувалося у зв'язку з гібридною війною, яку розв'язала Росія в останні роки.

Важливі мотиви актуалізації проблематики інформаційної безпеки полягають ще й в тому, що тільки країни з розвинутою інформаційною інфраструктурою здатні ставати конкурентоспроможним суб'єктом сучасного міжнародного глобального середовища. У зв'язку з цим, важливим аспектом дослідження різних вимірів інформаційної безпеки держави і суспільства є визначення рівня інформатизації всіх сфер суспільної життєдіяльності в кожній окремих країні.

***Зв'язок роботи з науковими програмами, планами, темами, грантами.*** Дисертацію виконано в межах комплексної наукової теми кафедри політичних наук «Проблеми політичної модернізації і трансформації: світовий досвід і українські реалії», що входить до тематичного плану науково-дослідних робіт Національного педагогічного університету імені М. П. Драгоманова, науковий напрям «Дослідження проблем гуманітарних наук», затверджений Вченою радою НПУ імені М. П. Драгоманова (протокол № 6 від 26 грудня 2013 р.). Тема дисертації затверджена на засіданні Вченої ради НПУ імені М. П. Драгоманова (протокол № 12 від 29 травня 2014 року).

***Метою дисертаційної роботи*** є концептуальне визначення суб'єктності політичних інститутів, що мають відношення до забезпечення інформаційної безпеки української держави і суспільства, а також аналіз їх розвитку в сучасних умовах, які складаються внаслідок розгортання глобалізаційних процесів та посилення агресивних дій Росії щодо інформаційного поля України.

Для досягнення поставленої мети у роботі послідовно розв'язано наступні ***дослідницькі завдання***:

- охарактеризувати стан дослідження обраної проблеми, основні джерела та детермінанти питань інформаційної безпеки;

- дослідити теоретико-методологічні особливості засад дослідження феномену «інформаційна безпека» у суспільстві, з'ясувати основні параметри цього поняття;
- вивчити параметри українського правового поля регулювання інформаційної безпеки, структурувати сукупність політико-правових актів, діючих в Україні, окреслити ситуативні лакуни, які потребують доопрацювання в світлі існуючих викликів інформаційної безпеки;
- позиціонувати національну нормативну базу інформаційної безпеки відносно міжнародних норм та практики забезпечення інформаційної безпеки;
- концептуальна фіксація глобального характеру проблеми інформаційної безпеки та з огляду на це визначення природи останньої;
- провести концептуально-теоретичний аналіз суб'єкт-об'єктних характеристик інформаційної безпеки держави та суспільства;
- з'ясувати інституційну складову проблеми інформаційної безпеки (визначення ролі державних, партійних, громадських органів, установ, організацій у формуванні інформаційно-безпекових пріоритетів соціуму та держави); окреслити організаційно-управлінських акторів, що безпосередньо впливають на стабілізацію чи дестабілізацію інформаційно-безпекової ситуації в країні;
- аналіз діяльності ЗМІ в контексті забезпечення інформаційної стабільності в державі;
- вивчення можливостей ефективної протидії інформаційно-деструктивним впливам, що мають зовнішні та внутрішні джерела у сучасній Україні.

*Об'єктом дослідження* виступають проблеми інформаційної безпеки України в умовах політичної трансформації, а *предметом дослідження* є державні та недержавні інститути, які функціонально впливають на формування політики інформаційної безпеки України.

**Методи дослідження.** Проведене дослідження базується на використанні загальнонаукових методів: індукція, дедукція, аналіз, синтез, порівняння, абстрагування, узагальнення та формалізація. Також використано спеціальні методи: порівняльний, структурно-функціональний, системний і інституціональний підходи до дослідження. Для вивчення зв'язків та залежностей в умовах процесів глобалізації застосовано методи екстраполяції, верифікації та типології. З допомогою порівняльного методу (аналіз окремого випадку, кростемпоральний та кроснаціональні порівняння) розглянуто та зіставлено параметри нормативно-політичної бази регулювання інформаційної безпеки в Україні та провідних державах світу; інформаційно-безпекову діяльність державних інститутів та політичних партій; позицію засобів масової інформації у сфері інформаційної безпеки. Структурно-функціональний

метод дозволив проаналізувати суб'єкт-об'єктний вимір інформаційної безпеки. Системний метод дозволив вивчити місце та роль державних та недержавних інститутів у забезпеченні інформаційної безпеки держави. Інституційний метод надав можливість через аналіз основних інститутів зрозуміти функціональне забезпечення інформаційної безпеки. Теоретико-методологічною основою дослідження виступив неоінституціоналізм у форматі історичного, соціологічного та теорії раціонального вибору. При опрацюванні теми була також використана низка концептів демократії, які прийнято застосовувати під час вивчення міжінституціональних відносин.

*Наукова новизна отриманих результатів дисертації* полягає, насамперед, у тім, що в ньому з позицій сучасного науково-політологічного дискурсу комплексно проаналізовані основні тенденції процесу формування інформаційної безпеки в трансформаційному суспільстві та місце і роль державних і не державних інститутів у забезпеченні інформаційної безпеки України. У процесі аналізу отримані висновки і результати, які свідчать про розв'язання визначених наукових завдань та характеризуються елементами наукової новизни, авторським концептуальним підходом до проблематики, зокрема:

*Вперше:*

– констатовано, що в системі викликів і ризиків, які постають перед Україною в контексті глобального характеру інформаційної безпеки, ключовим є втрата власної національної ідентичності, державного суверенітету, особливо інформаційного суверенітету, який визнається сьогодні головною ознакою державної самостійності та правосуб'єктності;

– доведено, що в системі інформаційної безпеки важливе місце займає інформаційна безпека нації, яка включає в себе захист неповторних національно-культурних цінностей, історичних традицій, історичної пам'яті, мови, унікальних субкультур;

– встановлено, що рівень інформаційної безпеки визначає стан розвитку політичної, соціально-економічної, оборонної, закордонної та інших компонентів національної безпеки України, а відповідні деструктивні інформаційні впливи проявляються фактично у всіх сферах життя суспільства;

– обґрунтовано, що існуюча інфраструктура державних інститутів інформаційної безпеки України мусить вибудовуватися за принципом стримувань і противаг, відповідно, що державні інститути повинні постійно перебувати під громадським контролем, бути відкритими до комунікації з ЗМІ, прозорими у своїх рішеннях та звітності, зрозумілими для міжнародних партнерів.

*Удосконалено та поглиблено:*

– розуміння, що інформаційна безпека у будь-якому структурно-функціональному вимірі телеологічно має бути орієнтована на захист прав людини і громадянина, на забезпечення повноцінного національно-культурного розвитку певного соціуму та на всебічний захист державного

суверенітету;

- розуміння інформаційної безпеки з точки зору формування єдиного функціонально-життєвого соціального простору творення суттєвих змістів, що визначають такі світоглядно-аксіологічні пріоритети, як патріотизм, гідність, державотворення, загальнолюдські цінності;

- параметри взаємодії ЗМІ та держави, опрацьовано шість моделей: незалежної преси, соціальної відповідальності, демократичного представництва, радянська модель, авторитарна та модель розвитку. З допомогою чотирьох з них на різних історичних етапах можна пояснити ситуацію в Україні. Також доведено, що три моделі дають можливість адекватно характеризувати авторитарні системи правління;

- підхід, згідно якого найбільш вразливе середовище для інформаційних операцій агресивного характеру формується з людей, які є апатичні до політики, пасивні у соціальних справах, нігілістичні, замкнені рамками мінімальних знань та вузьких світоглядних орієнтирів;

- висновок, що визначальною інформаційною загрозою національній безпеці виступає маніпуляція суспільною свідомістю, оскільки це дестабілізуючий вплив і на інформаційну структуру країни, і на її інформаційні ресурси та на суспільство загалом, в тому числі на окрему особистість, як громадянина;

- оцінка, що ефективна інформаційна політика державних структур досить часто вимірюється не лише міжнародними стандартами та правилами, але і спроможністю захищати специфічні національні інтереси, приймати актуальні виклики та долати гострі загрози;

- твердження, що основними формами та умовами колективної протидії маніпулятивним впливам є: просвітницька діяльність; проведення заходів, завдяки яким громадяни могли б навчитися протистояти маніпулюванню; моніторинг діяльності ЗМІ; розвиток у суспільстві конкуруючих мереж розповсюдження інформації; вироблення та популяризація критеріїв оцінки суспільної та політичної відповідальності представників влади.

*Отримали подальшого розвитку:*

- твердження, що одним з ключових вимірів проблематики інформаційної безпеки сьогодні є пошук адекватного балансу між впливами глобального характеру, які ґрунтуються на інтенсифікації переміщення інформації в глобальному інформаційному середовищі та потребами окремих людей і суспільних груп, в тому числі держав, що не є провідними суб'єктами, здатними впливати на глобальні цивілізаційні тенденції та процеси;

- висновок, що великі геополітичні протистояння найчастіше ведуться не на полі головних супротивників, а у просторі вразливих суспільств та нестабільних держав. Неспроможність цих держав давати адекватні інформаційні відповіді кваліфікується як підстава для інформаційної експансії та поступового поглинання, навіть без очевидного застосування

сили;

– положення, згідно якого можливість держави і суспільства протистояти зовнішній інформаційній агресії зумовлюється: проведенням демократичних реформ; зрілим громадянським суспільством; стабільною правовою державою; сформованою демократичною та активістською політичною культурою;

– оцінки, що поняття культури інформаційної безпеки трактується як рівень розвитку людини та суспільства, які характеризуються значимістю забезпечення безпеки життєдіяльності в системі особистісних і соціальних цінностей, безпечної поведінки в повсякденному житті в умовах небезпечних та надзвичайних ситуацій, рівнем захищеності від загроз і небезпек у всіх сферах життєдіяльності. На індивідуальному рівні культура безпеки проявляється у світогляді та зразках поведінки;

– твердження, що кращі безпекові стратегії та практики, які успішно захищають сучасний інформаційний простір, побудовані на трьох визначальних принципах: ієрархічності, державної координованості та взаємодії;

– оцінки, згідно яких перед державною владою з розвитком соціальних мереж постають такі завдання: структуризація віртуальних спільнот у вітчизняних соціальних мережах; усвідомлення їх впливовості та можливостей; пошук та вироблення адекватних реакцій на реальні та потенційні загрози, приховані у віртуальному громадянському просторі; розвиток доступних механізмів державного регулювання цього соціального феномену; слідування демократичним взірцям та традиціям у цій сфері;

– висновок, що фейкові партійні структури або не здійснюють інформаційної діяльності взагалі, або здійснюють пряме та опосередковане інформаційне обслуговування потужних політичних партій. В будь-якому випадку їх діяльність сприяє викривленню інформаційного та політичного просторів держави й чинить негативний вплив на інформаційну безпеку особистості та суспільства;

– підвищення ролі політичної освіти і просвітництва, як змістовної основи вироблення окремими особами, громадянським суспільством, державою імунітету до багатьох загроз, пов'язаних з інформаційно-маніпулятивними впливами різних зовнішніх и внутрішніх суб'єктів.

*Теоретичне і практичне значення отриманих результатів* дисертаційної роботи полягає у тім, що в ньому вперше в політологічній літературі останніх років проаналізовані основні тенденції процесу забезпечення інформаційної безпеки в трансформаційному суспільстві за допомогою різного інструментарію – утвердженню демократичної свідомості й ідеології, інтелектуалізації, інформатизації та прагматизації політичного поля, забезпечення всебічної політологічної та правової освіти широким колам громадськості. Автором виявлені основні зміни в



трансформаційному соціумі та їхні виклики щодо повноцінного формування інформаційно-безпекового порядку денного, актуального як для держави як політичного утворення та суспільства як суспільно-політичного феномену, так і для окремих громадян та їхніх груп. У дисертації проаналізовані також зміна інтересів та потреб політичного класу та особистості трансформаційного суспільства з огляду їхньої експектації стосовно різноманітних вимірів проблематики інформаційної безпеки. Матеріали дисертації можуть бути використані в частині політичного виховання особистості як елемента державної гуманітарної політики та в навчальному процесі при викладанні курсів політології, культурології, спеціалізованих курсів інформаційної, та інформаційно-правової безпеки. На основі дисертаційного тексту може бути підготовлений спеціальний курс для студентів політологічних спеціальностей.

**Особистий внесок здобувача.** Дисертаційна робота є самостійним науковим дослідженням, спрямованим на досягнення мети – концептуального визначення суб'єктності політичних інститутів, які мають відношення до забезпечення інформаційної безпеки української держави і суспільства, а також аналіз їх розвитку в сучасних умовах. Задля цього автором роботи опрацьовано сукупність міжнародних та національних нормативно-правових і політико-правових актів та проаналізовано функціональні аспекти діяльності державних та громадських структур України в царині інформаційної безпеки. Відповідно, особистий внесок здобувача репрезентовано у тексті дисертації, 1 монографії, 21 статті у періодичних фахових виданнях з політичних наук, а також у 10 наукових працях, що засвідчують апробацію матеріалів і додатково відображають наукові результати дисертації. Наукові результати отримані автором самостійно, а усі опубліковані праці за темою дисертації є одноосібними.

**Апробація результатів дисертаційного дослідження.** Основні положення і висновки дослідження оприлюднені на міжнародних і всеукраїнських наукових та науково-практичних конференціях, семінарах, круглих столах, з-поміж яких: Друга міжнародна науково-практична конференція «Управлінські компетенції викладача вищої школи» (28 лютого 2014 р., м. Київ), міжнародна науково-практична конференція «Політика і духовність в умовах глобальних викликів» (2 квітня 2014 р., м. Київ), IV міжнародні Драгоманівські читання: до 180-річчя НПУ імені М. П. Драгоманова (16–17 квітня 2015 р., м. Київ), Одинадцяті юридичні читання «Форма сучасної національної української держави: реалії та перспективи» (21–22 травня 2015 р., м. Київ), міжнародна науково-практична конференція «Формування державної освітньої політики: філософські, теоретичні та прикладні аспекти» (25–26 лютого 2016 р., м. Київ), міжнародна науково-практична конференція «Сутність та перспективи впровадження електронної демократії в Україні» (15

листопада 2016 р., м. Вінниця), Різдвяні педагогічні читання «Новий вчитель для нової української школи» (23–25 грудня 2016 р., м. Київ), науково-практична конференція «Ціннісний дискурс у суспільстві та освіті» (1–2 березня 2018 р., м. Київ), міжнародна наукова конференція «Тринадцять юридичні читання «Українська державність: кризь призму часу (до 100-річчя Української національно-демократичної революції 1917–1921 рр.)»» (24–25 травня 2018 р., м. Київ), наукова конференція «Культурологічна практика в системі підготовки майбутнього вчителя» (5–6 жовтня 2018 р., м. Київ), тиждень філософії в НПУ імені М. П. Драгоманова «Майбутнє філософської освіти в Європі: виклики та перспективи» (14–17 травня 2019 р., м. Київ), науково-практична конференція «Значення культурної практики в освітянському процесі університету» (31 травня – 1 червня 2019 р., м. Київ – м. Новгород-Сіверський), Політологічні читання імені професора Богдана Яроша (14 квітня 2020 р., м. Луцьк). Крім того, положення і результати дисертації неодноразово обговорювались під час засідань й семінарів кафедри політичних наук Національного педагогічного університету імені М. П. Драгоманова.

**Публікації.** За темою дисертації опубліковано 32 наукові праці, серед яких: 1 – одноосібна монографія, 15 – статті у наукових фахових виданнях України з політичних наук, 6 – статті у наукових фахових виданнях з політичних наук, які включені до міжнародних наукометричних баз, 10 – наукові праці, що засвідчують апробацію матеріалів і додатково відображають наукові результати дисертаційної роботи.

**Структура дисертації.** З огляду на об'єкт і предмет, мету та завдання дослідження робота складається із анотацій, вступу, шести розділів, в тому числі десяти підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертаційної роботи – 423 сторінки, серед яких основна частина дисертації – 362 сторінки. Список використаних джерел складається з 481 позиції.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У **«Вступі»** обґрунтовано вибір теми дослідження, зв'язок роботи з науковими планами і темами, визначено мету й завдання, обґрунтовано методологію дослідження, наукову новизну, особистий внесок здобувача, теоретичне й практичне значення отриманих результатів, представлено дані про апробацію дослідження, публікації, структуру та обсяг дисертації.

У першому розділі – **«Історіографічні та теоретико-методологічні особливості та параметри дослідження проблеми інформаційної безпеки в умовах політичної трансформації»** – проаналізовано історію та сучасний стан дослідження обраної проблематики, його зарубіжні та українські контексти, категоріальні та методологічні основи.

У підрозділі 1.1. – *«Стан дослідження й історіографія проблематики інформаційної безпеки в умовах політичної трансформації у зарубіжній та вітчизняній науці»* – проблематика інституційного виміру інформаційної безпеки України, зокрема з погляду трансформаційних викликів, глобальних контекстів і стратегічних орієнтирів розвитку нашої держави на тлі загальносвітових процесів, визначається доволі багатогранною, такою, що потребує історіографічної структуризації.

Головна увага сфокусована на тому, що обрана тематика компонує питання як теоретико-методологічного, так і практично-емпіричного порядків, а також стосується і нашої держави, й інших країн світу. Різносторонні та різні за важливістю й наповненням складові проблематики інформаційної безпеки осмислюються ґрадуально, зокрема у географічному (в зарубіжних і вітчизняних дослідженнях), часовому (в класичних і новітніх розвідках) та джерельному відтинку.

Проблемно-безпекові аспекти політичного життя суспільства простежуються через аналіз масиву фундаментальних доробків, виданих головню до початку 1990-х рр. (Е. Аронсон, М. Балфур, З. Бауман, Х. Бей, Д. Белл, З. Бжезинський, Ж. Бодрійяр, Г. Вайнштейн, У. Дайзард, Р. Дарендорф, Ж. Доменак, А. Ендмюллер, А. Кампен, Г. Кан, М. Кастельс, Е. Кац, П. Лазарфельд, Г. Лассуел, М. Маклюен, Е. Масуда, Г. Міллер, В. Парето, А. Тойнбі, Е. Тоффлер, С. Хантінгтон, Ю. Габермас, Д. Шарп та інші). Інформаційно-безпековий вимір, важливий як для окремої людини, так і спільнот та для людства загалом, позначився і на суттєвому прирості сучасного наукового знання, що у дисертації відмічено на прикладі формування й розвитку спеціалізованих періодичних наукових топ-видань з означеної проблематики.

Питання інформаційної безпеки осмислюються не лише як політологічні, але й як міждисциплінарні, що у підрозділі зауважується на прикладі аналізу відповідних наукових праць в Україні. Вивчаючи актуальні напрями й аспекти інформаційної безпеки, увага зосереджена довкола розвідок політологів, філософів, економістів, соціологів, юристів й інших дослідників, котрі різного часу вивчали її доволі відмінні прояви у сенсі особливостей поступу інформаційного суспільства, комунікації, інституційного дизайну, інформаційного середовища тощо (Л. Абрамов, А. Баранов, Т. Бельська, О. Бойко, В. Брижко, Я. Варивода, В. Горбулін, В. Гурковський, С. Денисюк, М. Дмитренко, О. Дубас, Н. Глебова, Ю. Горбань, В. Григор'єв, В. Гурковський, С. Даниленко, О. Дзьобань, Б. Кормич, В. Ільганаєва, С. Кудрявцева, В. Ліпкан, О. Логінов, Є. Макаренко, М. Присяжнюк, В. Петрик, Т. Пода, В. Попов, Г. Почепцов, Л. Смола, В. Смолянук, О. Степко, А. Чічановський, Г. Шипунов, А. Юричко, С. Ягодзінський, О. Ярош та багато інших).

На підставі структуризації наукових джерел з досліджуваної теми виявлено, що джерельну базу потрібно поділяти на теоретико-методологічну та більшою мірою практично орієнтовану, в тому числі на

кейс інформаційної безпеки в Україні. Загалом констатовано, що проблематика інформаційної безпеки відчутно пов'язана з дослідженням феноменів інформаційного суспільства, інформаційного простору, інформації як такої та національної безпеки держави тощо, однак й досі залишається недостатньою мірою систематизованою, головню в рамках розвитку сучасної політичної науки в Україні, навіть попри актуальність означеного питання в контексті розвитку нашої держави.

У підрозділі 1.2. – *«Ключові поняття, концептуальні та наукові підходи і правові означення як теоретико-методологічна основна дослідження інформаційної безпеки за політичної трансформації»* – розглядаються ключові одиниці дослідження, що дозволяють вести мову про науковий характер обраної проблематики аналізу та обґрунтованість пропонуванних у роботі рекомендацій та висновків.

Проаналізовано категорії, теоретичні підходи й правові означення, які покладені в основу дослідження інформаційної безпеки в умовах політичної трансформації та можуть розвиватися сучасною політичною наукою й надалі. Встановлено, що категорія і феномен інформаційної безпеки, навіть теоретико-методологічно, є надзвичайно багатовимірними, складними та поліморфними, адже їх часто аналізують у рамках різних парадигм, підходів, концептуалізацій і вимірів, а також у широкому та вузькому розумінні. Ця теза підтверджується також через аналіз українського законодавства та практики, які не є достатньо консолідованими. Встановлено, що навіть теоретико-методологічно і регламентаційно означена проблематика потребує подальшого розвитку та систематизації, зокрема зважаючи на вивчення досвіду країн Західної Європи, США, Китаю й інших впливових акторів міжнародної політики.

Виокремлені важливі виміри у розумінні проблематики інформаційної безпеки: державно-управлінський, соціальний, феноменологічний, політико-філософський, комунікаційний. Окремо зауважується й правовий зміст проблеми, що полягає щонайменше в тому, аби чітко окреслити та розмежувати права й обов'язки усіх зацікавлених суб'єктів у цьому просторі: виробників інформаційних технологій, креаторів інформаційних засобів, постачальників інформаційних послуг, власників інформації, користувачів інформації, зрештою держави як визначального регулятора інформаційного ринку. Констатовано, що особливий наголос у цьому контексті потрібно робити на дослідженні інформаційної безпеки, в тому числі у нашій державі, завдяки інструментарію політичної науки.

Сучасна політична наука орієнтує зокрема й це дослідження на аналіз динаміки і статички політичного життя, тож у питаннях інформаційної безпеки політологія розвиває бачення організованих суб'єктів і стихійних чинників, що впливають на цю сферу, дозволяє вивчати проблеми та суперечності, реалії та ризики, пріоритети і виклики. Інформаційна безпека держави, суспільства, громадянина, людини

осмислюється як чинник міжцивілізаційного зближення, конкурентоспроможних комунікацій, правової культури, національної довіри, демократизаційних зрушень. Запропоноване її бачення у локальних, національних, регіональних, міждержавних та глобальних вимірах, при чому кожен з них потребує фахового концептуального розуміння та стратегічного консультування.

У другому розділі – *«Законодавча база України та міжнародні стандарти і практика щодо функціонування інститутів інформаційної безпеки»* – розкрито політико-правову сутність та специфіку інституційних основ інформаційної безпеки.

У підрозділі 2.1. – *«Правове забезпечення інформаційної безпеки в Україні»* – визначено, що з точки зору права інформаційна безпека базується на державній інформаційній політиці, відповідних законах, які врегульовують суперечності, гарантують інформаційну свободу громадян та їхній доступ до інформації в національному інформаційному просторі.

Встановлено, що для нормативно-правового регулювання інформаційної безпеки України властива певна дезорієнтованість, фрагментарність, розпливчастість, недосконалість чинного законодавства, що яскраво виявили анексія Криму Російською Федерацією у 2014 р. та пряма агресія на сході, тривала війна України з маріонетковими структурами, що фінансуються та підтримуються Росією. Складність законодавчого регулювання у інформаційній сфері пов'язується також з тим, що об'єктами такого забезпечення одночасно є особистість, суспільство та держава. Їхні інтереси в інформаційній сфері збігаються лише частково, а забезпечення та регламентація належить до різних структур. Відтак підсумовується, що захист інформаційної безпеки потребує внутрішньої консолідації, об'єднання різних політичних сил, соціальних груп, окремих громадян для вироблення дієвих норм та спільного позиціонування на міжнародній політико-правовій арені.

Окреслюються основні правила щодо діяльності в інформаційній сфері, закладені передусім у Конституції України, а також низці Законів України («Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про звернення громадян», «Про державну таємницю» та багато інших), у податковому, адміністративному, карному, цивільному кодифікованому законодавстві. Особлива значимість відводиться державним документам (концепціям, стратегіям, доктринам), що закладають концептуальні правові виміри інформаційної безпеки, пріоритети розвитку цієї сфери, орієнтири прийняття нових норм та усунення колізій в існуючих.

Загалом правова політика України в інформаційній сфері охарактеризована як така, що ще за багатьма ознаками залишається декларативною, розпорошеною, змістовно невизначеною, несистемною, бюрократизованою. Великий вплив на неї мають закріплена система

фінансово-промислових інтересів, застарілих комунікацій, інерційних суспільних мас. Однак на шляху до демократії, європейської інтеграції, у боротьбі з російською агресією, ця політика зазнає помітних реформ. Стверджується, що вирішення складних тактичних завдань і необхідність швидкого реагування на вкрай небезпечні інформаційні виклики, що часом загрожують цілісності країни та суб'єктності держави, збагачує безцінним досвідом українське суспільство, консолідує довкола спільних цілей та стратегічних орієнтирів, які потенційно стануть важливою основою якісного політико-правового забезпечення інформаційної безпеки громадян, соціуму, держави. Висловлюється застереження, що цей унікальний досвід неодмінно варто враховувати також і у контексті загальноєвропейського, аналізуючи потенціал вітчизняної політико-правової системи.

Підрозділ 2.2. – «*Міжнародні норми та практика забезпечення інформаційної безпеки*» – описує політико-правовий, а відтак і праксеологічний змісти проблематики, через які розпізнається повнота можливостей, що дозволяють сучасним державам і міжнародній спільноті загалом захищати свій інформаційний простір від актуальних викликів глобалізованого світу.

Проблеми правового регулювання інформаційних відносин в Україні розглядаються як пов'язанні не лише з інформаційною безпекою держави, але й з можливостями її швидкої подальшої інтеграції у міжнародну спільноту демократичних, модернізованих країн. При цьому зауважується, що демократичні країни сьогодні вигідно відрізняються ширшими можливостями, розвинутішими правовими механізмами реалізації національних інтересів, в тому числі й в інформаційній сфері. Проведений аналіз засвідчив, що і норми, і практики забезпечення інформаційної безпеки тут передусім орієнтовані на збереження інформаційного суверенітету, на пріоритет національних інтересів, охорону й захист інформації, контроль за порядком використання національних інформаційних ресурсів, а також поширення національних цінностей у глобалізованому світі.

Водночас осмислюються й міжнародні здобутки у забезпеченні інформаційної безпеки політико-правовими засобами, зокрема міжнародно-правові основи, закріплені ООН: суверенна рівність держав у використанні інформаційних ресурсів, недопустимість інформаційної інтервенції, ворожої пропаганди, поширення деструктивної інформації, незастосування сили і використання інструментів інформаційного впливу проти територіальної цілісності держав, превентивна дипломатія за допомогою інструментів інформаційного впливу, визначеність меж національного інформаційного простору, свобода слова та вільного обігу інформації, незалежності і плюралізму міжнародних мас-медіа, заборона цензури, захист конфіденційності інформаційних ресурсів, культурна самобутність в інформаційній діяльності тощо. Йдеться про відповідний

комплекс політичних, економічних і соціокультурних принципів, важливих для міжнародного порозуміння.

Уніфіковані норми щодо правового регулювання міжнародної інформаційної безпеки визначаються як необхідність нашого часу, сучасного суспільства, що характеризується всеохоплюючою глобалізацією і потужними антиглобалізаційними рухами, зростанням гострих протистоянь між ними, в тому числі й в інформаційному просторі, порушенням територіальної цілісності й інформаційного суверенітету держав, поєднанням конвенційних і не конвенційних засобів сучасної війни, зрештою дрібними кіберзлочинами та масштабними хакерськими атаками, масованим інтелектуальним піратством тощо.

Третій розділ – *«Глобальний характер та суб'єкт-об'єктні виміри інформаційної безпеки»* – присвячений особливостям глобалізованого світу, які позначаються на можливостях безпекових інститутів продуктивно взаємодіяти як на безкордонних просторах сучасності, так і всередині національних політичних систем.

Підрозділ 3.1. – *«Глобальний характер інформаційної безпеки: інституційні можливості та ризики»* – акцентує на тому, що сьогодні важливо розуміти як позитивні, так і негативні прояви глобалізованого цифрового світу, постійно розширювати горизонти залучення високих технологій в політичний процес, але й прогнозувати і попереджати потенційні небезпеки, які можуть паралельно змінювати політичну картину світу.

Категорія інформаційної безпеки розглядається як така, що має глобальний характер, а тому й потребує аналізу в системі глобального (світового) інформаційного простору. Визначивши основні переваги та ризики інтенсифікації трансферу та руху інформації у глобалізованому комунікативному просторі та в умовах інформаційної революційності, доведено неможливість повноцінного використання нових переваг, що з'являються в інформаційному суспільстві, без забезпечення адекватного рівня інформаційної безпеки. Можливості швидких інформаційних обмінів, отримання завдяки новим інформаційним технологіям нових знань, розвиток соціальних та індивідуальних форм творчості на основі оперування великими масивами інформації можуть бути нівельованими через некоректне або ж злочинне використання нових технологій навіювання, маніпулювання та інформаційні диверсії. Стверджується, що одним із ключових завдань сучасної науки є пошук адекватних шляхів для глобального стійкого балансу між розвитком інформаційних технологій та вдосконаленням механізмів інформаційного захисту. Саме глобальний характер інформаційної цивілізації, через який перед людиною і суспільством постають додаткові виклики та загрози інформаційній безпеці, змінює сучасні наукові та практичні підходи до неї.

Розглянувши ключові деструктивні зовнішні та внутрішні інформаційні впливи як основні джерела загострення інформаційної

небезпеки, доведено їх особливу гостроту в умовах глобальної цивілізації. Вказується, що сьогодні жодна держава чи національне суспільство не в змозі адекватно відповісти на ті виклики, що породжує глобальний інформаційний простір. Проте, якщо держави-лідери здатні займати в цьому просторі активницьку позицію, то такі трансформаційні суспільства як Україна, автоматично перетворюються на об'єкти інформаційної агресії з боку могутніх суб'єктів глобалізованого світопорядку. Серед рекомендацій дослідження – врахування такої специфіки глобальних інформаційних реалій у вибудовуванні стратегії інформаційної національної безпеки України. В умовах, коли в країні все ще розвиваються основи демократично-правової державності, громадянського суспільства, протистояти зовнішнім і внутрішнім деструктивним інформаційним впливам можна виключно спираючись на досвід та ресурсно-технологічну допомогу більш значних суб'єктів сучасного глобального геополітично-інформаційного простору.

У підрозділі 3.2. – *«Суб'єкт-об'єктні виміри інформаційної безпеки у контексті впливовості та партнерства політичних інститутів»* – йдеться про характеристики об'єктів, на яких спрямована безпекова діяльність, та її суб'єктів – людей та соціальних інститутів, які її забезпечують.

Класифікувавши контрольовані та неконтрольовані інформаційні обміни, визначено кілька принципів побудови ефективної системи державної інформаційної безпеки. Зокрема, державі рекомендується розробити нормативно-правову базу та задіяти управлінсько-адміністративні механізми для реалізації певної програми контролю за інформацією, що переміщується в національному інформаційному просторі. Тільки тоді коли контрольовані обміни будуть превалювати над неконтрольованими, можна констатувати певний рівень інформаційної безпеки держави, суспільства і людини. При цьому зауважується, що державний контроль за інформаційною сферою не повинен порушувати ключові права і свободи громадян. Демократичне ж забезпечення прав громадян на отримання і передачу інформації вбачається надійним підґрунтям для системи державного контролю над інформаційною сферою. Відтак перші кроки розбудови стратегії забезпечення інформаційної безпеки в Україні розглядаються невіддільно від широких демократизаційних перетворень, зокрема розвитку та активізації реального і дієвого громадянського суспільства, яке не може існувати без сильної правової держави.

Проаналізувавши основні види та напрями збудження інформаційної небезпеки, серед яких особливо підкреслені спеціальні інформаційні операції, інформаційна агресія, інформаційна війна тощо, проілюстровано складність протистояння таким агресивним діям в умовах сучасного глобалізованого світу. Зауважується, що технологічна сфера глобально-інформаційної цивілізації забезпечує високий рівень транспарентності



інформаційного простору, що дозволяє потенційним суб'єктам інформаційної агресії вільно використовувати свою перевагу в технологічному і ресурсному потенціалі. Суб'єктами інформаційної агресії відтак визначені саме країни-лідери, що ставлять перед собою глобальні геополітичні завдання, або ж транснаціональні корпорації, успіх яких залежить від маніпулювань з глобальним інформаційним полем. Для тих же держав та соціальних спільнот, що стають об'єктами інформаційної агресії, рекомендується діяти на випередження і профілактично (передусім, підняття рівня освіченості та громадянської активності населення). Підкреслюється, що освічені громадяни, які опираються на демократично-правові державні інституції, здатні ефективно протистояти інформаційно-психологічним впливам, що чиняться під час інформаційних операцій чи воєн.

Суб'єкт-об'єктні характеристики інформаційної безпеки осмислюються як такі, що мають багатоплановий й різнорівневий характер, який варто враховувати при оцінках впливовості різних інститутів та визначенні стратегічних орієнтирів ефективного партнерства між ними. Системоутворюючим суб'єктом інформаційної безпеки вважається держава, але її діяльність у демократичних країнах не може повною мірою забезпечити багатоаспектні інтереси й потреби об'єктів у цій сфері. Простежується тенденція і необхідність до залучення у забезпеченні інформаційної безпеки країни недержавних суб'єктів, а також різноманітних колективів, етнонаціональних утворень, комерційних структур тощо.

У четвертому розділі – *«Інформаційно-безпекова діяльність державних інститутів та політичних партій»* – до певної міри реалізується структурно-функціональний аналіз окремих інститутів та загалом системи інформаційної безпеки, визначаються ролі державних і партійних структур у цій системі.

У підрозділі 4.1. – *«Інформаційно-безпекова діяльність державних інститутів: єдність культурного та політичного факторів»* – аналізується інформаційна безпека держави, що відіграє провідну роль в забезпеченні життєво важливих інтересів будь-якої країни.

Метою забезпечення інформаційно-безпекової діяльності державних інститутів означено створення розгалуженого та захищеного інформаційного простору, захист національних інтересів держави в умовах формування світових інформаційних мереж, захист економічного потенціалу країни від неправого застосування інформаційних і комунікаційно-технологічних ресурсів, втілення на практиці прав людини й громадян, інститутів та держави на продукування та використання відповідної інформації. Держава розглядається як визначальний колективний суб'єкт інформаційної безпеки, що здійснює функції у цій сфері через органи влади.

Окреслена комплексна інформаційно-безпекова діяльність держави, яка повинна передбачити правові, організаційно-економічні, технологічні, політичні, а також ціннісно-культурні методи роботи, що доповнюють та увиразнюють зміст один одного. Стверджується, що держава через низку політичних інституцій здійснює заходи для забезпечення інформаційної безпеки та є головним агентом збереження стабільної рівноваги та впровадження прогресивних змін у перехідному суспільстві. Держава у цій сфері аналізується як така, що за різних обставин може як наближати, так і віддаляти перспективу інформаційного суспільства (перешкоджати громадській ініціативі, обмежувати творчий та інтелектуальний порив у цьому напрямку). Державні інститути визначають правові рамки інформаційного простору, але як і будь-які інші можуть й (не)свідомо порушувати відповідні норми в обличчі окремих державних службовців чи й цілих організацій.

Суперечлива роль держави вбачається ще тому, що вона виявляє та знешкоджує зовнішні інформаційні атаки, але нерідко й у її структурах окремі іноземні агенти реалізують пріоритети і стратегії інших держав. Відтак підсумовується, що існуюча інфраструктура державних інститутів інформаційної безпеки України мусить вибудовуватися за принципом стримувань і противаг, також державні органи повинні постійно перебували під громадським контролем, відкриті до комунікації зі ЗМІ, прозорі у своїх рішеннях і звітності, зрозумілі для міжнародних партнерів.

У підрозділі 4.2. – *«Роль політичних партій на шляху розвитку стратегії інформаційної безпеки у демократичному суспільстві»* – тема безпекових функцій політичних інститутів розвивається та поглиблюється на рівні аналізу розмаїття партійних завдань у сучасному інформаційному суспільстві.

Визначивши зміст категорії «інформаційна безпека» як різновиду національної безпеки, яка націлена на забезпечення прав і свобод всіх учасників інформаційної діяльності, місце та роль у цьому процесі політичних партій стверджується як беззаперечна. Зазначається, що політичні партії, популяризуючи певну ідеологію, здійснюючи агітаційно-просвітницьку роботу, беручи участь у діяльності органів влади, активно впливають на інформаційний простір країни і як наслідок стають активними суб'єктами інформаційної безпеки. Специфіка позиціонування політичної партії у інформаційному просторі держави і суспільства окреслюється як самостійний предмет безпекового напрямку. Розглядаються типові шляхи такого позиціонування, яке відбувається за допомогою різноманітних ЗМІ й обумовлено тим, що будь-яка політична партія повинна бути зв'язуючою ланкою між владою та громадянським суспільством.

Підкреслюється, що зв'язок сучасної політики та інформаційних технологій формує ряд дискусійних питань, вирішення яких залежить і від рівня розвитку партійної системи в країні. Партійну змагальність

запропоновано до певної міри розуміти як змагання технологій: та партія, що має доступ до кращих технологій, здійснила якісніший кадровий відбір фахівців, що здатні вирішувати складні завдання сучасного цифрового суспільства, цілком може сподіватися на електоральну підтримку. Сучасні технології цілком спроможні розвивати та сприяти як демократичним партійним ідеологіям, так і популістським передвиборчим обіцянкам, що однаково відчутно позначається на стані національної безпеки.

Зазначено, що особливу роль інформаційна діяльність рухів відіграє під час значних суспільних трансформацій, наприклад, перехід від тоталітаризму або авторитаризму до демократії, коли опозиційних партій, ще немає (тоталітаризм) або їх діяльність є значно обмеженою (авторитаризм). Інформаційна діяльність партій і рухів в умовах демократії створює підґрунтя для її розвитку, є запобіжником від руху назад до автократії, своєрідним форпостом громадянського суспільства, одним з призначень яких є безпека особи й суспільства, зокрема й у інформаційному її прояві. Стверджується, що партії та рухи беруть доволі активну участь у виробленні стратегії інформаційної безпеки у демократичній державі (йдеться як про урядові, так і опозиційні сили). Натомість у країнах з нестійкими демократіями стратегія інформаційної безпеки є прерогативою лише урядових сил.

У п'ятому розділі – *«Громадянське суспільство та засоби масової інформації у системі інформаційної безпеки»* – розкрито потенціал сучасних теорій соціальної комунікації та транзитологічних моделей, у яких вбачаються численні позиції для поновлення теоретичних і прикладних дискусій про потенціал умовно нових і старих інститутів у розбудові інформаційного суспільства.

У підрозділі 5.1. – *«Консолідуючий потенціал громадянського суспільства у системі інформаційної безпеки та чинники його дестабілізації»* – виявлено, що інформаційне споживання в Україні все ще мало пов'язане з інформаційною продукцією, виробленою громадським сектором, незалежними аналітичними центрами, просвітницькими, культурними організаціями і професійними об'єднаннями громадян. Одночасно вказується на потенціал громадянського суспільства, що доведено подіями помаранчевої Революції та Революції гідності, тенденцію його подальшого зростання, в тому числі й в безпековій сфері.

Зауважується, що громадські ініціативи зі своєчасного, достовірного, об'єктивного інформування могли би поступово долати загальну атмосферу нігілізму, корумпованості, примітивності, а нерідко й безпорадності чи дезорієнтованості в українському суспільстві. Однак у загальному масиві інформації сучасного суспільства такі якісно нові, модернізовані формати донесення важливих сенсів громадськими організаціями все ще поодинокі. Нові інформаційно-комунікативні технології для появи та утвердження сучасних віртуальних громадсько-політичних спільнот зробили значний внесок, забезпечивши їх такими

важливими механізмами як інтерактивність, низька витратність, мультимедійність, асинхронність, глобальність, анонімність. Широкі можливості інформаційних і комунікаційних процесів в глобалізованому світі привносять також широкі загрози, в тому числі й для громадянського суспільства, і для держави.

Висловлено застереження, що перебільшувати загрози громадянського суспільства і при цьому недооцінювати його можливостей для системи інформаційної безпеки все ж не варто, особливо в умовах демократизації. Ці суперечливі тенденції пов'язані між собою. Часто саме зі стихійних рухів, не до кінця усвідомлених громадських активностей, не формалізованих об'єднань громадян зростають дієві та ефективні соціально значущі проекти інформаційного простору. Громадський сектор може як посилювати соціально-політичний дисбаланс (через окремі зацікавлені у дестабілізації групи), так і виступити у ролі зв'язкового каналу, що поєднуватиме розірвані інформаційні простори. Підсумовується, що якісний рівень поінформованості населення все ще потребує особливої уваги усіх зацікавлених у захисті національних інтересів суб'єктів політики.

Встановлено роль інститутів громадянського суспільства, що володіють відчутним рівнем консолідуючого потенціалу в системі інформаційної безпеки. Громадські ініціативи осмислюються як такі, що володіють винятковим прикладом солідаризованої дії, що може мати і реальний, і віртуальний вимір, об'єднувати людей зі спільними цінностями й інтересами заради сучасних загальнонаціональних та навіть загальнолюдських міжнародних орієнтирів безпеки та розвитку.

Підрозділ 5.2. – *«Засоби масової інформації як інститути інформаційної безпеки: проблеми (не)залежності та (без)відповідальності»* – визначає суперечливу сутність медіа у сучасній системі інформаційної безпеки.

З'ясовано, що основи правового регулювання ЗМІ в Україні були закладені у перші роки української державності. Зокрема у відповідності з нормами міжнародного права з 1990-ті рр. були прийняті основні нормативно-правові акти, що регулюють основні види ЗМІ, видавничу справу та рекламу, захищають авторське право та суспільну мораль та встановлюють порядок висвітлення ЗМІ діяльності органів влади та самоврядування в Україні. Водночас відносно недавно законодавчо унормовано систему суспільного телебачення і радіомовлення, хоча процес становлення суспільного мовлення в Україні тільки розпочався, а також потребує законодавчого регулювання діяльність інтернет-ЗМІ, які за розміщення неперевіреної або недостовірної інформації сьогодні фактично не можливо притягати до відповідальності.

Осмислюються і набувають подальшого розуміння шість нормативних моделей взаємодії ЗМІ та держави: модель незалежної преси, модель соціальної відповідальності, модель демократичного

представництва, радянська модель, авторитарна і модель розвитку. Орієнтиром для сучасної України визначена саме комплексна демократична модель соціальної відповідальності, втілення в життя якої залежить від успішного запровадження системи суспільного мовлення, що буде фінансуватись суспільством та асоціюватись у громадян з правдою, чесністю, простотою, нейтральністю.

Акцентується, що не лише держава, однак й самі ЗМІ здатні нести відповідальність ЗМІ за інформаційну безпеку суспільства. Проаналізовані відповідні положення, що закладені у міжнародних та національних етичних кодексах журналістів. В Україні через існування тривалий час кількох таких кодексів, уявлення про відповідальність журналіста перед суспільством не були конкретизовані. Аналізується й об'єднаний Етичний кодекс українського журналіста, що вимагає від останнього служити інтересам суспільства, розповсюджуючи правдиву та об'єктивну інформацію, запобігаючи фальсифікаціям і усім виявам дискримінації. Сумлінне слідування вітчизняних журналістів цим принципам та належний громадський контроль за їх дотриманням визначені важливою запорукою забезпечення інформаційної безпеки українського суспільства.

Узагальнюється, що проблематика інформаційної безпеки індивіда, суспільства, держави і навіть світового співтовариства часто залежить від того, який шлях пройшли та якої якості набули у цьому процесі засоби масової інформації. Виокремлені орієнтири на цьому шляху (як глобальні тенденції, так і національна специфіка), але універсальними критеріями для оцінки функціонування ЗМІ як інститутів інформаційної політики та інформаційної безпеки названа їхня незалежність і відповідальність.

Шостий розділ – *«Стратегічні орієнтири протидії зовнішнім і внутрішнім інформаційно-дестабілізаційним впливам в умовах гібридної війни»* – переглядає представлений раніше системний аналіз окремих інститутів та загалом системи інформаційної безпеки у сучасному дослідженні, що видається не повним без врахування можливостей аксіологічної аналітики, тобто вивчення етичних, культурних, моральних, ціннісних суб'єктів і об'єктів політики, які задають динаміку та визначають загальні межі інформаційних перетворень у кожному конкретному суспільстві чи громаді.

Інформаційна безпека осмислюється у контексті викликів сучасної демократизації і політичної модернізації, тобто як вид безпеки національної, орієнтованої на демократичні права і свободи людини мати вільний доступ до інформації, на створення і впровадження безпечних інформаційних технологій, на вільну журналістську діяльність, на захищені права інтелектуальної власності, на орієнтування у глобальному просторі можливостей інформаційного суспільства тощо. Однак сучасні українські реалії вносять корективи до дослідницьких політологічних стратегій, зокрема передбачають розгляд можливих диверсій у цю сферу. Українське суспільство за багатьма вимірами – інституційними, політико-

правовими, ціннісно-культурними – виявилось невідповідним до протидії внутрішнім і зовнішнім інформаційно-деструктивним впливам. Водночас інформаційна війна, яку розгорнув агресор проти України, зобов'язує до активної, цілеспрямованої, стратегічної протидії атакам і війнам в інформаційному полі, а відповідній проблематиці відведений окремий розділ дисертацій.

Пропонована проблематика умовно розподілена на окремі аспекти: 1) диверсифікація джерел інформації; 2) відкритість інформаційного простору та контроль за доступністю інформації; 3) протидія маніпулятивним впливам (засоби, технології, можливості); 4) підризна діяльність російських ЗМІ та завдання протидії їм. Підкреслюється, що правове інформаційне поле, суспільне мовлення, державницька доктрина складають інтегральну основу для суспільства, солідаризують його. Однак в Україні все ще спостерігається фрагментарне бачення стратегії розвитку держави, суперечливе наповнення спільного інформаційного простору, незавершеність формування законодавчої бази інформаційного суспільства. Загальна ситуація у сфері інформаційної безпеки охарактеризована як неоднозначна: тактика влади щодо захисту журналістів, забезпечення свободи слова та розвитку інформаційного простору в Україні неодноразово змінювалася, була часто залежною від виборчих циклів, зовнішньополітичних декларацій, культури владної діяльності тієї чи іншої елітарної групи. Водночас системі у цій сфері протягом усіх років незалежності не вистачає прозорих механізмів та єдиних для усіх підходів.

Розглядаються й інші причини, що негативно позначаються на інформаційному просторі: протистояння різних політичних сил в Україні, дискредитація політичних супротивників, репутаційні зазіхання, іміджеві стратегії, партійний брендинг, негласні внутрішньопартійні заборони – усе це складає підґрунтя для продукування обмежених, спотворених, ангажованих інформаційних продуктів. Вказані обмеження пов'язані не лише з політичними маніпуляціями, але й зі специфікою масової свідомості як такої. Загалом можливості для скорочення доступу до правдивих відомостей визначаються як такі, що однаково зумовлені і політичною кон'юнктурою, і специфікою масової свідомості, й історичними традиціями кожного конкретного суспільства. Умовна ж прозорість, доступність інформаційного доквілля є важливою метою політичної модернізації та усіх суб'єктів демократизаційних процесів.

Утаємниченість, бюрократизм, системні обмеження, тотальний контроль в інформаційній сфері перехідного суспільства розглядаються як чинники, що ускладнюють загальнополітичну ситуацію та посилюють суспільну напругу. Дзеркально доповнює несприятливу для демократичного розвитку ситуацію також зростаюча зовнішня інформаційно-психологічна експансія, яку переживає сучасне українське суспільство. Першочергові заходи з протидії таким загрозам вбачаються в

асиметричних рішеннях, зокрема й диверсифікації джерел інформації, відкритість інформаційного простору загалом. Останній, а також контроль за доступністю інформації теж розглядаються важливими інструментами протидії інформаційним загрозам. Відкритість уможливується через глобальне подолання відстаней від інформатора до споживача інформаційного продукту, через оновлення комунікаційних можливостей (комп'ютеризації, телефонізації, інтернету), а також через демократизаційні процеси у сучасному світі. Відкритість змінює поведінку і світогляд людини, економіку підприємства та інформаційну культуру, соціальну структуру суспільства та інституції держави, публічну політику і державне управління.

При цьому зауважується, що така відкритість потребує і певного контролю, чітко визначених правил політико-правових механізмів. Загалом в основі боротьби проти зовнішніх і внутрішніх інформаційних впливів та дестабілізаторів, у розрізі зміцнення безпеки в інформаційній сфері в Україні, передусім, вбачаються такі заходи: узгодження вітчизняного законодавства в інформаційній сфері з європейськими стандартами, а також здійснення контролю за безумовним його дотриманням; активний розвиток інформаційних технологій та забезпечення державою умов для розвитку інформаційної інфраструктури; активізація формування громадянського суспільства, сприяння втіленню принципу безумовної правової рівності всіх учасників процесу інформаційної взаємодії незалежно від їх політичного, соціального та економічного статусу.

Стверджується, що така стратегія сприятиме тому, що обмеження доступу до інформації стане винятком із загального принципу відкритості інформації та здійснюватиметься тільки на основі законодавства. Виключно законними засобами держава здатна забезпечити захист суспільства від неправдивої, перекрученої і недостовірної інформації, захистити національні інтереси. Запозичення досвіду провідних країн світу в інформаційній сфері, раціоналізована кадрова політика, активна співпраця з міжнародними структурами щодо протидії інформаційному тероризму, хакерству можуть суттєво змінити баланс сил в інформаційній війні, яку нині розгорнув агресор проти України.

## **ВИСНОВКИ**

У висновках сформульовано теоретичні положення, що характеризуються новизною та мають практичне значення. Відтак після визначення основних джерел, витоків і детермінант актуальності питань інформаційної безпеки були розглянуті й порівняні різні дискурсивні традиції та методи означення категорій «інформаційної безпеки», що розповсюджені в українському і зарубіжних філософсько-політичних дискурсах. Цілісно проаналізувавши інформаційну безпеку в

інформаційній політиці України та впливових країн світу, ми можемо зробити деякі взаємопов'язані висновки з приводу основних принципів наших досліджень з цього питання та теоретичних та методологічних принципів.

*По-перше*, розглянувши та систематизувавши основні джерела та детермінанти питань інформаційної безпеки, у дослідженні було якісно відображено актуальність і багатовимірність концептуальних та теоретичних розвідок й аналізу цього питання у сучасній філософії, політології та дискурсі національної безпеки. При цьому, головним фактором, який визначає актуальність питань інформаційної безпеки, є значне збільшення інформаційного потоку та комунікацій у глобальному масштабі. Таке зростання призвело до багатьох проблем і викликів у галузі національної безпеки, що вимагає постійних досліджень та пошуків. Інформаційне втручання на регіональному геополітичному рівні додає інших важливих небезпек. У той же час з інформаційними викликами стикаються всі – громадяни, суспільні групи, держави, людство тощо. Це спричиняє надзвичайну важкість концептуальних і теоретичних досліджень з питань інформаційної безпеки. У нашій роботі одним із базових методів, котрі були застосовані, є комплексний системний підхід, на підставі якого ми провели загальне і структурне дослідження питань інформаційної безпеки, з якими стикаються людство, суспільство і країна, в тому числі на прикладі України. Багатосуб'єктність у галузі інформації та безпеки визначає складність, важливість та актуальність дослідження проблеми з точки зору політичної науки та аналізу політичної безпеки.

*По-друге*, встановлено, що у сучасній політичній науці та політичному дискурсі, розглядаючи основні принципи та стандарти, які визначають поняття «інформаційна безпека» у суспільстві, підкреслено надзвичайну розмаїтість і багатогранність цих категорій. Українські та зарубіжні науковці із цього питання визначили зміст категорії інформаційної безпеки, обговорили такі аспекти, як роль глобальної цивілізації, національна безпека та національна оборона, інформаційні та технічні параметри в рамках визначення безпеки, а також важливість інформаційної безпеки для кожної людини чи конкретної соціальної групи людей. Зважаючи на різноманітність методів, ключовою теорією і методологічним принципом нашого дослідження став принцип системності, що базується на всебічному, структурному і функціональному аналізі категорії «інформаційна безпека» та розглядає її окремішній, соціальний, національний і глобальні виміри. З огляду на це, особливої важливості набув комплексний фактор чи фактори, які поєднують інформаційну безпеку країни та суспільства із інформаційною, психологічною і світоглядно-феноменологічною безпекою людини й соціальних груп. На підставі теоретичних і методологічних засад вивчення питань інформаційної безпеки, ми дефініювали це поняття як різновид національної безпеки, що має на меті забезпечити вільний доступ до інформації, створення та впровадження захищених і цілком безпечних



інформаційних технологій та захист прав інтелектуальної власності й інформаційної свободи для всіх учасників.

*По-третє*, внутрішня і міжнародна експертиза українського інформаційного законодавства свідчить, що воно відповідає європейським стандартам/вимогам. Однак, прийняті норми поки що мало відображаються у суспільно-політичних реаліях: відчутні недоліки загальної культури дотримання встановлених норм як політичними суб'єктами, інститутами державної влади різних рівнів так і широкими масами громадян. Окрім того ознаками правового унормування інформаційного простору України виступають: фактична відсутність правового регулювання функціонування в країні міжнародних інформаційних систем, серед яких Інтернет, відтак й труднощі діяльності для Інтернет- ЗМІ та загрози від окремих з них; суперечливі трактування у нормативно-правовому забезпеченні діяльності ЗМІ загалом; відсутність дієвих норм сприяння економічно незалежним медіа; не врегульований статус конфіденційної інформації. Одночасно говорячи про формування правових основ і гарантій міжнародної інформаційної безпеки, слід визнати, що наразі можна засвідчити різні позиції провідних держав сучасності щодо розуміння новітніх потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства.

*По-четверте*, уніфіковані норми правового регулювання міжнародної інформаційної безпеки стають необхідністю нашого часу, що характеризується всеохоплюючою глобалізацією та потужними антиглобалізаційними рухами, зростанням гострих протистоянь між ними, в тому числі й у інформаційному просторі; порушенням територіальної цілісності і інформаційного суверенітету держав, поєднанням конвенційних і не конвенційних засобів сучасної війни; зрештою дрібними кіберзлочинами та масштабними хакерськими атаками, масованим інтелектуальним піратством. Особливий вплив на необхідність продовження напрацювання спільних стандартів регулювання міжнародної інформаційної безпеки мали інформаційна агресія Російської Федерації під час анексії Криму і фактичної війни в окремих частинах Донецької і Луганської областей, яка була спрямована не лише на громадян України, але і по відношенню до громадян Росії і цілого світу.

*По-п'яте*, провівши порівняльний аналіз питань інформаційної безпеки в контексті інформаційної політики України і впливових країн світу, було доведено потребу конструювання систематичної стратегії формування інформаційної та безпекової політики України. Сьогодні в нашій країні не існує системи інформаційної безпеки, що відповідає сучасним цивілізаційним і геополітичним викликам. Тому насправді управління безпекою інформації потрібно посилити у всіх сферах: в нагляді, організації та управлінні й інформаційних технологіях. Але спочатку існує дуже гостра необхідність у формулюванні чіткої стратегії трансформації сектору інформаційної безпеки країни та національного й

громадянського суспільства. Ця стратегія повинна ґрунтуватися на міцній концепції, теорії, науці і практиці та формуватися у рамках національної політичної науки та дискурсу. А тому вивчення багатьох аспектів національної, соціальної та людської інформаційної безпеки є надзвичайно актуальним і важливим завданням, яке сьогодні стоїть перед науковою спільнотою в нашій державі. Окрім новітніх викликів та реалій, що не врегульовані або не передбачені існуючим законодавством, не одне десятиріччя існують проблеми інформаційного простору, що потенційно становлять ризики і для інформаційної безпеки нашої держави. Серед них ми можемо виділити: 1) проблеми створення суспільного мовлення та приналежності засобів масової інформації фінансово-промисловим олігархічним групам; 2) проблеми законодавчого регулювання інформаційної діяльності в мережі Інтернет і поширення інформації у соціальних Інтернет-мережах; 3) проблеми авторського права за умов поширення Інтернет-технологій та ідентифікації джерел.

*По-шосте*, провівши деталізований концептуально-теоретичний аналіз суб'єкт-об'єктних характеристик інформаційної безпеки держави і соціуму, виділено декілька ключових активних груп, що визначають таку суб'єктність. До них насамперед відносяться держані органи, відповідальні за забезпечення інформаційної безпеки, політичних акторів національного поля (партії, лідери, активні лобістські групи тощо), громадські організації, асоціації, інституції, засоби масової інформації. При цьому, на нашу думку, суб'єкт-об'єктні відносини у системі інформаційної безпеки великою мірою залежать від діяльності державних структур загалом, а у контексті пропонованої проблематики – від інститутів інформаційної безпеки, які функціонують в системі державного управління й адміністрування. Держава задає загальну динаміку та правила роботи на інформаційному ринку країни, встановлює норми та обмеження для розвитку інформаційної демократії, захищає інформаційний простір не лише від загалом атак, але й конкретних суб'єктів інформаційного маніпулювання. У державній системі координат інформаційної безпеки кожен суб'єкт політики має знайти своє місце, якщо дбає про збереження цілісності країни, суверенітет держави, соціально-політичний розвиток суспільства, до якого належить.

*По-сьоме*, доведено, що власне на державу покладається головна відповідальність по забезпеченню інформаційної безпеки та координації зусиль всіх суб'єктів, причетних до імплементації функцій захисту інформаційного простору. Визначено, що існуюча інфраструктура державних інститутів інформаційної безпеки України мусить вибудовуватися за принципом стримувань і противаг, важливо також, щоб державні органи постійно перебували під громадським контролем, були відкриті до комунікації зі ЗМІ, прозорі у своїх рішеннях та звітності, зрозумілі для міжнародних партнерів. В процесі аналізу партійної діяльності в контексті проблематики інформаційної безпеки, слід зазначити, що інформаційна безпека країни залежить від того, чиї інтереси

представляє і захищає та чи інша політична партія, бо в її інформаційній політиці відображаються і пов'язуються інтереси країни, народу та партії. В цьому аспекті детально проаналізовано особливості діяльності державницьких та опозиційних політичних партій і рухів в інформаційному та технологічному вимірі, а також їхній вплив на безпеку особистості, держави та суспільства. Констатовано, що в Україні не існує спільного політичного розуміння відповідальності за інформаційну безпеку нації, держави, соціуму, а політичні сили готові жертвувати загальноукраїнськими інтересами заради досягнення тимчасових вузькопартійних цілей в процесі боротьби за владні, посадові повноваження. Перелік важливих та життєво необхідних для суспільства і політичної системи функцій, які покладаються на державу як суб'єкта інформаційної політики, є досить великим. Це і збереження інформаційного суверенітету держави, і попередження безконтрольного впливу на інформаційний простір, і захист та гарантії усім суб'єктам інформаційних відносин, і забезпечення прав людини та громадянина. Дії окремих державних органів чи посадовців можуть мати негативний інформаційний вплив на суспільство; шкоди завдає і неповна, невчасна, недостовірна комунікація державних діячів зі суспільством; поширеним є явище нерационального застосування інформаційних технологій, порушення конфіденційності в держструктурах тощо. Рациональне та адекватне позиціонування держави на інформаційному ринку також може бути ускладнене відсутністю стратегічних пріоритетів і визначень у цій сфері, зрощуванням приватних інтересів окремих зацікавлених сторін із державними, надмірною електоральною залежністю (популізмом) високопосадовців, або ж навпаки – ігноруванням зв'язків з громадськістю, залежністю від іноземних суб'єктів тощо. Тобто йдеться на загал про комплекс проблем, пов'язаних з виробленням політики і її виконанням, що впливає на стан захищеності суспільства.

*По-восьме*, здійснивши загальний аналітичний огляд особливостей законодавчого врегулювання діяльності ЗМІ в Україні, а також визначивши ключову роль засобів масової інформації у розповсюдженні правдивої чи неправдивої інформації як чинник інформаційної безпеки суспільства й держави, доведено, що на особливу увагу заслуговує проблема фундаментальної відповідальності ЗМІ за інформаційну безпеку суспільства. В цьому контексті, ілюструється, що ЗМІ, будучи продуктом індустріального суспільства, в епоху інформаційного суспільства набувають нових якостей та характеристик. Мультимедійність, інтерактивність, можливість зворотного зв'язку та навіть діалог між великою кількістю користувачів, персоналізація, відсутність посередників, позагеографічність або позапросторовість інформаційно-комунікативних технологій перетворюють ЗМІ на доволі значущий чинник формування особистих позицій громадян і розвитку суспільства та демократичного життя. Водночас зростають маніпулятивні можливості ЗМІ та збільшуються ризики деструктивного впливу ЗМІ на перебіг суспільних

процесів. Об'єктивна потреба у посиленні демократичного представництва і контролю через ЗМІ з одного боку, та запобіганні утвердження медіакратії (влади ЗМІ) з іншого боку, зумовлюють необхідність здійснення цілеспрямованої державної політики в інформаційній сфері, однією з важливіших складових якої є забезпечення інформаційної безпеки суспільства. Одночасно варто виокремити і проблемні результати діяльності ЗМІ: формування «масової» людини, розрив соціальних контактів, дезінтеграція суспільства, витіснення традицій, заміщення прямих контактів кібер-комунікаціями, байдужість, некритичність, дезорієнтованість, надмірна емоційність та навіть агресивність. Наявність одночасно багатьох джерел інформації, попри усі переваги на практиці досить часто виявляє лише доступ до суперечливих та взаємовиключних суджень.

*По-дев'яте*, визначивши протидію різноманітним інформаційно-дестабілізаційним впливам в зміцненні інформаційної безпеки держави чи суспільства ключовим завданням всіх відповідальних суб'єктів в цій сфері, сформульовані головні пріоритети, що постають перед всіма сторонами, що впливають на рівень інформаційної безпеки української держави і соціуму. Такими завданнями, зокрема, ми окреслили: 1) диверсифікацію джерел інформації; 2) відкритість інформаційного простору та контроль за доступністю інформації; 3) протидію маніпулятивним впливам (засоби, технології, можливості); 4) адекватний захист та відповідь на підривної діяльність російських засобів масової інформації і завдання боротьби з ними інформаційних інститутів в Україні. Необхідно, щоб ініціативи держави та наддержавних інституцій щодо кібер- та інформаційної безпеки були достатньо розвинутими. Вони можуть носити різний характер – від антитерористичних дій спеціальних служб із правом застосування насильства до захисту вітчизняного мовного та культурного простору. Проте, для України важливо взяти на озброєння принаймні ті з них, які дозволять адекватніше відповідати на виклики інформаційної безпеки в умовах недомінантних умов у власному інформаційному просторі. Крім того, важливо встановити чітку ієрархію інформаційно-безпекових принципів та цінностей (наприклад унормувати поняття, класифікувати та конкретизувати інформаційні загрози, вирішити дилему свободи розповсюдження інформації та запобіганні деструктивним інформаційним впливам), виробити чіткі норми та інструкції для органів безпеки, систематизувати правовий корпус в галузі інформаційних відносин та ієрархію державних інституцій, що їх забезпечують, а не створювати нові установи з повноваженнями, що дублюють одне одного. Тільки за умов чіткого визначення ключових пріоритетів інформаційної безпеки на державному рівні, а також при нагальній розробці дієвих механізмів її забезпечення, у України з'явиться шанс на ефективну протидію зовнішнім та внутрішнім небезпекам інформаційної дестабілізації. Цим і зумовлена значна актуальність та важливість дослідницьких результатів, представлених в даному дисертаційному дослідженні.

**СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ***Наукові праці, в яких опубліковані основні наукові результати дисертації:**Монографія:*

1. Захаренко К. Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток. Київ: Вид-во НПУ імені М.П. Драгоманова, 2017. 389 с.

*Наукові статті:*

2. Захаренко К. Глобальна природа інформаційної безпеки // Політологічний вісник. 2015. Вип. 79. С. 181–189.
3. Захаренко К. Держава як суб'єкт інформаційної безпеки суспільства // Політологічний вісник. 2015. Вип. 78. С. 86–96.
4. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки // Нова парадигма. 2015. Вип. 127. С. 40–53.
5. Захаренко К. Роль громадських організацій і рухів у формуванні національної інформаційної безпеки // Гілея: науковий вісник: зб. наук. пр. 2016. Вип. 115. С. 426–430.
6. Захаренко К. Информационная безопасность в системе глобального информационного пространства // Strategic. Vaku. 2017. № 3–4 (21–22). С. 223–234.
7. Захаренко К. Інформаційні впливи як джерела загострення інформаційної небезпеки // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 126. С. 331–336.
8. Захаренко К. Партії і політичні рухи в інформаційному вимірі сучасної держави // Гілея: науковий вісник: зб. наук. пр. 2017. Вип. 116. С. 285–289.
9. Захаренко К. Засоби масової інформації як необхідний елемент розвитку інформаційного суспільства // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 132. С. 250–254.
10. Захаренко К. Протидія маніпулятивним впливам (засоби, технології, можливості) // Гілея: науковий вісник: зб. наук. пр. 2018. Вип. 137. С. 181–189.
11. Захаренко К. Стратегія формування ефективної системи державної інформаційної безпеки // Гілея: науковий вісник. 2018. Вип. 131. С. 268–272.

12. Захаренко К. Теоретичні засади дослідження інформаційної безпеки // Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 2 (4). С. 107–116.
13. Захаренко К. Диверсифікація джерел інформації в контексті інформаційної безпеки // Політикус. 2019. № 1. С. 5–9.
14. Захаренко К. Інформаційна безпека суспільства як предмет правового регулювання // Гілея: науковий вісник: зб. наук. пр. 2019. Вип. 148. С. 26–31.
15. Захаренко К. Категорія інформаційної безпеки у вітчизняному політологічному дискурсі // Вісник Львівського університету. Серія філос.-політолог. студії. 2019. Вип. 23. С. 158–165.
16. Захаренко К. Міжнародний досвід інформаційної безпеки // Сучасне суспільство: політичні науки, соціологічні, культурологічні науки. 2019. Вип. 1 (17). С. 95–109.
17. Захаренко К. Особливості формування ефективної державної інформаційної політики // Політичне життя. 2019. №3. С. 71–76.
18. Захаренко К. Правовий супровід інформаційної безпеки суспільства // Держава і право. 2019. Вип. 83. С. 128–138.
19. Захаренко К. Специфіка позиціонування політичної партії в інформаційному просторі держави і суспільства // Держава і право. 2019. Випуск 85. С. 338–348.
20. Захаренко К. Чинники здійснення державної інформаційної політики України // Регіональні студії. 2019. № 17. С. 15–19.
21. Захаренко К. Відповідальність засобів масової інформації в системі інформаційної безпеки суспільства // Політикус. 2019. № 5. С. 4–9.
22. Захаренко К. Відкритість інформаційного простору та контроль за доступністю інформації // Вісник Прикарпатського університету. Політологія. 2020. Вип. 14. С. 46–55.

*Наукові праці, що засвідчують апробацію матеріалів та додатково відображають наукові результати дисертації:*

23. Захаренко К. До питання про розвиток національної системи інформаційної безпеки: досвід сусідів // Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія. 2018. Вип. 50. С. 176–189.
24. Захаренко К. Засоби масової інформації як інструмент та механізм розвитку інформаційного суспільства // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2018. Вип. 39. С. 79–87.

25. Захаренко К. Засоби масової інформації як чинник розвитку суспільства // Вісник Інституту розвитку дитини. Серія: Філософія, педагогіка, психологія. 2015. Вип. 38. С. 29–36.
26. Захаренко К. Категорія «інформаційної безпеки» у вітчизняному науковому дискурсі // Гуманітарний вісник державного вищого навчального закладу «Переяслав-Хмельницький державний педагогічний університет ім. Г. С. Сковороди». Серія: Філософія. 2015. Вип. 37. С. 106–117.
27. Захаренко К. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі // Гуманітарний вісник ЗДІА. 2018. Випуск 72. С. 44–52.
28. Захаренко К. Місце політичних партій в системі інформаційної безпеки // Політологічні читання імені професора Богдана Яроша : зб. наук. пр. / за заг. ред. В.І. Бортнікова, О.Б. Ярош, Я.Б. Яроша. Луцьк: Вежа-Друк, 2020. Вип. 9. С. 44–49.
29. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки // Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Серія: Філософія. 2017. Вип. 48 (1). С. 212–219.
30. Захаренко К. Проблеми консолідації суб'єктів інформаційної безпеки // Проблеми соціальної роботи: філософія, психологія, соціологія. 2018. № 1(11). С. 36–43.
31. Захаренко К. Проблеми формування ефективної державної інформаційної політики // Науковий часопис НПУ імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2016. Вип. 36. С. 202–209.
32. Захаренко К. Розвиток системи інформаційної безпеки: досвід зарубіжних країн // Вища освіта України. 2018. № 3. С. 71–77.

## АНОТАЦІЯ

***Захаренко К. В.* Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. – Кваліфікаційна наукова праця на правах рукопису.**

Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.02 – політичні інститути та процеси. – Національний педагогічний університет імені М. П. Драгоманова, Львівський національний університет імені Івана Франка, Львів, 2021.

Резонансне дослідження з позицій сучасного політологічного дискурсу комплексно аналізує основні тенденції процесу формування інформаційної безпеки в трансформаційному суспільстві, зокрема інституційний вимір такого процесу, роль державних і неурядових інститутів у забезпеченні інформаційної безпеки України. Проблема

інформаційної безпеки осмислюється на трьох визначальних напрямках: у світлі трансформації українського суспільства загалом та його політичної системи; у контексті глобалізації сучасного світу; у стратегічному баченні – як перспектива розвитку політичних інститутів, відносин і процесів, що забезпечують демократичні зміни та безпеку України загалом. Серед основних ризиків, які постають перед Україною, розглядається загроза втрати інформаційного суверенітету. Значиму роль відведено інформаційній безпеці нації, зокрема таким її структурним компонентам: захист неповторних національно-культурних цінностей, історичних традицій, історичної пам'яті, мови, унікальних субкультур тощо.

Серед авторських пропозицій важливі ті, що стосуються існуючої інфраструктури державних інститутів інформаційної безпеки України. Інформаційно-безпекова діяльність політичних партій в Україні визначена суперечливою. Стверджується, що у сучасній системі інформаційної безпеки значима роль відведена громадянському суспільству і засобам масової інформації. В умовах гібридної війни стратегічні орієнтири протидії зовнішнім і внутрішнім інформаційно-дестабілізаційним впливам осмислюються через: 1) впровадження кращих безпекових практик, які успішно захищають сучасний інформаційний простір та побудовані на трьох визначальних принципах (ієрархічності, державної координованості та взаємодії); 2) підвищення ролі політичної освіти і просвітництва (змістовної основи вироблення імунітету до багатьох загроз, пов'язаних з інформаційно-маніпулятивними впливами); 3) подальший розвиток культури інформаційної безпеки.

Інституційне розуміння формування інформаційно-безпекового порядку денного може зацікавити державних діячів, громадських активістів, партійних лідерів, політичних експертів, консультантів, аналітиків. Матеріали дослідження можуть бути корисними для програм з громадянської та політичної освіти, інформаційної гігієни, при викладанні політичних наук, а також загалом у визначенні подальших орієнтирів розвитку державної гуманітарної політики.

*Ключові слова:* інформаційна безпека, політичні інститути, політична трансформація, політична модернізація, інформаційна стратегія, інформаційний суверенітет, глобалізація.

## АННОТАЦІЯ

***Захаренко К. В. Институциональное измерение информационной безопасности Украины: трансформационные вызовы, глобальные контексты, стратегические ориентиры. – Квалификационный научный труд на правах рукописи.***



Диссертация на соискание ученой степени доктора политических наук по специальности 23.00.02 – политические институты и процессы. – Национальный педагогический университет имени М. П. Драгоманова, Львовский национальный университет имени Ивана Франко, Львов, 2021.

Исследование с позиций современного политологического дискурса комплексно анализирует основные тенденции процесса формирования информационной безопасности в трансформационном обществе, в частности институциональное измерение такого процесса, роль государственных и неправительственных институтов в обеспечении информационной безопасности Украины. Проблема информационной безопасности осмысливается на трех главных направлениях: в свете трансформации украинского общества и его политической системы; в контексте глобализации современного мира; в стратегическом видении – как перспектива развития политических институтов, отношений и процессов, обеспечивающих демократические перемены и безопасность Украины в целом. Среди основных рисков, стоящих перед Украиной, рассматривается угроза потери информационного суверенитета. Значимая роль отведена информационной безопасности нации, в частности таким ее структурным компонентам: защита уникальных национально-культурных ценностей, исторических традиций, исторической памяти, языка, уникальных субкультур и тому подобное.

Среди авторских предложений важные, касающиеся существующей инфраструктуры государственных институтов информационной безопасности Украины. Информационная деятельность политических партий в системе безопасности Украины определена противоречивой. Утверждается, что в современной системе информационной безопасности значимая роль отведена гражданскому обществу и средствам массовой информации. В условиях гибридной войны стратегические ориентиры противодействия внешним и внутренним информационно-дестабилизирующим воздействиям осмысливаются через: 1) внедрение лучших практик безопасности, которые успешно защищают современное информационное пространство и построены на трех главных принципах (иерархичности, государственной скоординированности и взаимодействия); 2) повышение роли политического образования и просвещения (содержательной основы выработки иммунитета к многим угрозам, связанных с информационно-манипулятивными действиями) 3) дальнейшее развитие культуры информационной безопасности.

Институциональное понимание формирования повестки дня в системе информационной безопасности может заинтересовать государственных деятелей, общественных активистов, партийных лидеров, политических экспертов, консультантов, аналитиков. Материалы исследования могут быть полезными для программ гражданского и

политического образования, информационной гигиены, при преподавании политических наук, а также в целом в определении дальнейших ориентиров развития государственной гуманитарной политики.

*Ключевые слова:* информационная безопасность, политические институты, политическая трансформация, политическая модернизация, информационная стратегия, информационный суверенитет, глобализация.

## ABSTRACT

***Zakharenko K. V. Institutional Dimension of Information Security of Ukraine: Transformational Challenges, Global Contexts and Strategic Landmarks. – Qualifying scientific research on the rights of a manuscript.***

Dissertation on acquisition of the scientific degree of the Doctor of Political Science in specialization 23.00.02 – Political Institutions and Processes. – National Pedagogical Dragomanov University, Ivan Franko National University of Lviv, Lviv, 2021.

From the perspective of modern political discourse, the given research provides a comprehensive analysis of the trends in forming information security in a transformational society, including the institutional dimension of such process and the role of the state and non-governmental institutions in ensuring information security of Ukraine. The problem of information security is considered in three defining directions: in the light of the transformation of the Ukrainian society as a whole and its political system; in the context of globalization of the modern world; in the strategic vision – as a prospect for the development of political institutions, relations and processes that ensure democratic change and security of Ukraine in general.

Historiographical and theoretical-methodological features of the study of the information security issues under political transformation are revealed through the coordination of key concepts, conceptual approaches, legal definitions, retrospectives, etc. It is emphasized that the level of information security determines the state of development of other components of national security of Ukraine, and the corresponding destructive informational influences are manifested in virtually all spheres of society.

The dissertation analyzes the legal framework of Ukraine and international standards for the functioning of information security institutions. At the same time, it is emphasized that the effective information policy of state bodies is often measured not only by international standards and rules, but also by the ability to protect specific national interests, accept current challenges and overcome acute threats. Geopolitical confrontations are viewed as those that are mostly conducted not in the field of the main opponents but in the space of vulnerable societies and unstable states.

The chosen problematics of the research are of a global character and belong to subject-object dimensions. In the system of risks facing Ukraine in the context of the global nature of information security, the main threat is that of losing its information sovereignty, and hence the associated national identity and state sovereignty, i.e., the key features of state independence and legal personality. Among the key issues is the further search for an adequate balance between global impacts, which are based on the intensification of information movement in the global information environment, and the needs of individuals and social groups, including states that are not leading actors in influencing global civilizational tendencies and processes. Therefore, in the information security system in general, a significant role is given to the information security of the nation, in particular the following structural components: protection of unique national and cultural values, historical traditions, historical memory, language, unique subcultures and more.

Among the author's proposals and recommendations of most importance are those related to the existing infrastructure of Ukrainian governmental institutions of information security, which should be built on the principle of checks and balances, in which state institutions should be under public control, open to communication, transparent in their decisions and reporting and understandable to international partners. At the same time, it is emphasized that the government faces a number of relatively new tasks with the development of social networks (e.g., structuring virtual communities in domestic social networks; comprehending their impact and opportunities; finding and developing adequate responses to real and potential threats hidden in the virtual civic space; developing available mechanisms of state regulation of this social phenomenon; following democratic patterns and traditions in the relevant field). The information and security activities of political parties in Ukraine are quite contradictory.

It is argued that civil society and the media play a significant role in the modern information security system. The thesis is that the most vulnerable environment for aggressive information operations is formed of ordinary people who are apathetic to politics, passive in social affairs, nihilistic, closed to the extent of minimal knowledge and narrow worldviews is consistently substantiated. The defining information threat to national security is the manipulation of public consciousness, i.e., creating a destabilizing impact on the information structure of the country and its information resources and society as a whole.

Strategic guidelines for counteracting external and internal information and destabilizing influences in a hybrid war are studied herein through: 1) introduction of best security practices that successfully protect the modern information space and are based on three defining principles (hierarchy, state coordination and interaction); 2) increasing the role of political education and

enlightenment (i.e., the substantive basis for the development of individuals, civil society, the state of immunity to many threats associated with information and manipulative influences); 3) further development of information security culture (such level of human and social development which is characterized by the importance of life safety in the system of personal and social values, safe behavior in everyday life in dangerous and emergency situations, the level of protection from threats and dangers in all spheres of life), etc.

The provided theoretical analysis of the trends in the process of information security in a transformational society is of practical importance, and it highlights the need to attract and develop various tools to establish democratic consciousness and ideology, intellectualization, informatization and pragmatization of the political field, providing comprehensive political and legal education. Institutional understanding of the formation of the information and security agenda may be of interest to statesmen, public activists, party leaders, political experts, advisers and analysts. The research materials may be useful for programs in civic and political education, information hygiene, in teaching political science and also in determining the guidelines for the development of the state of humanitarian policy.

*Keywords:* information security, political institutions, political transformation, political modernization, information strategy, information sovereignty, globalization.



Підписано до друку 05.06.2021 р. Формат 60x84/16.  
Папір офсетний. Гарнітура Times.  
Обл.-вид. арк 1,5  
Наклад 100 прим. Зам. № 091  
Віддруковано з оригіналів.

---

Видавництво Національного педагогічного університету  
імені М.П. Драгоманова. 01601, м. Київ-30, вул. Пирогова, 9  
Свідоцтво про реєстрацію № 1101 від 29.10.2002.  
(044) 239-30-26.