МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

Шемчук Віктор Вікторович

УДК 342+007(100)+340.5

КОНСТИТУЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ ДЕРЖАВ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ

спеціальність 12.00.02 – конституційне право; муніципальне право
(081– Право)

Автореферат
дисертації на здобуття наукового ступеня
доктора юридичних наук

Ужгород – 2020

Дисертацією є рукопис.
Роботу виконано в Таврійського національного університету імені В.І. Вернадського Міністерства освіти і науки України.

Науковий консультант – доктор юридичних наук, професор,
Заслужений юрист України
Федоренко Владислав Леонідович,
директор Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України.

Офіційні опоненти: доктор юридичних наук, професор,
Заслужений юрист України
Бисага Юрій Михайлович,
завідувач кафедри конституційного права та порівняльного правознавства
ДВНЗ «Ужгородський національний університет»;

доктор юридичних наук, професор
Дешко Людмила Миколаївна,
професор кафедри конституційного права Інституту права Київського національного університету ім. Т. Г. Шевченка;

доктор юридичних наук, доцент
Зозуля Олександр Ігорович,
завідуючий науковим сектором порівняльного конституційного та муніципального права Науково-дослідного інституту державного будівництва та місцевого самоврядування НАПрН України.

Захист відбудеться 18 грудня 2020 року о «11» годині на засіданні спеціалізованої вченої ради Д 61.051.07 ДВНЗ «Ужгородський національний університет» за адресою: 88000, м. Ужгород, вул. Капітульна, 26, каб. 45.

З дисертацією можна ознайомитися в науковій бібліотеці ДВНЗ «Ужгородський національного університет» (м. Ужгород, вул. Університетська, 14).

Автореферат розісланий 17 листопада 2020 року

Вчений секретар
спеціалізованої вченої ради…….Р. М.Фрідманський

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми дослідження. З часу проголошення незалежності України, а надалі й прийняття Конституції України правники здійснюють пошук і обґрунтування оптимальної моделі розбудови держави як суверенної і незалежної, демократичної, соціальної, правової держави. Реалізація такої моделі можлива лише в державі, в якій суверенітет поширюється на всю її територію в межах існуючого кордону, а національна безпека забезпечується в усіх сферах життєдіяльності суспільства та держави, включаючи інформаційну безпеку.

Несистемність підходів до законодавства у сфері інформаційної безпеки призводить до тиражування великої кількості нормативно-правових актів різної юридичної сили, які фрагментарно врегульовують суспільні відносити у сфері інформаційної безпеки та її забезпечення. Прикметно, що законодавче визначення інформаційної безпеки міститься лише в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» № 537-V від 09.01.2007 р. Зокрема, згідно зі ст. 13 цього Закону інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання й порушення цілісності, конфіденційності та доступності інформації.

У Законі України «Про національну безпеку України» № 2469-VIII від 21.06.2018 зміст інформаційної безпеки не розкривається, вона лише визнається одним із напрямів державної політики у сфері національної безпеки і оборони. Так само і в Законі України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998. інформаційна безпека називається невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки, але саме поняття не деталізується.

Відзначимо, що останніми роками у науковців пожвавився інтерес до цієї проблематики. На тлі загострення реальної військової загрози територіальній цілісності України, непорушності її державних кордонів та реальній загрозі національній безпеці включаючи інформаційну безпеку України. Це знайшло своє відображення у значній кількості наукових досліджень, результатом яких стали надруковані праці учених-конституціоналістів і інших правознавців.

На сьогодні вітчизняні вчені-конституціоналісти (Ю. Барабаш, К. Бєляков, Ю. Бисага, О. Бориславська, Ю. Волошин, Л. Дешко, О. Зозуля, Т. Костецька, А. Крусян, О. Марцеляк, О. Нестеренко В. Нестерович, М. Савчин, А. Селіванов, В. Серьогін, О. Скрипнюк, О. Совгиря, В. Федоренко, О. Фрицький, В. Шаповал, В. Шатіло, Ю. Шемшученко та ін.) досліджували окремі аспекти конституційно-правового забезпечення інформаційної безпеки в Україні. До того ж, у 2016–2020 роках посилився інтерес українських вчених і експертів до досліджень феноменології т.з. «гібридної війни» (В. Горбулін, А. Дорошкевич, О.

Жайворонок, О. Литвиненко, Є. Магда, С. Максимов, Г. Сасин, Т. Черненко та ін.), інформаційних воєн (В. Алещенко, Ю. Горбань, Г. Почепцов, Є. Скулиш, П. Ткачук і ін.), проблем інформаційної безпеки в Україні (І. Боднар, О. Довгань, А. Гальчинський, В. Ліпкан, А. Марущак, і ін.), у тому числі й у кіберпросторі (М. Грайворонський, П. Демченко, І. Сопілко та ін.).

Враховуючи порівняльно-правовий характер дослідження проблем конституційно-правового захисту інформаційної безпеки у дослідженні використані наукові здобутки таких зарубіжних учених як Д. Белл, П. Берман, Ш. Блек, Н. Вейнсток, Р. Ведгвуд, Дж. Голдсміс, Дж. Деллапінна, П. Дракер, Т. Стоун'єр, М. Кастельс, Х. Макгрегор, Й. Масуда, К. Мей, Х. Піррітт, Е. Тоффлер, Ф. Уебстер, П. Келлер, Л. Кемп, М. Кіттіманн, В. Кляйнвехтер, Й. Курбалії, Л. Лессіг, Е. Пакард, П. Поланскі, Д. Пост, Дж. Райденберг, Дж. Роджерс, А. Туцці, Л. Солам, М. Таунс, П. Френзісі, П. Шварц, Дж. Харт, М. Чанг та ін.

Разом із тим комплексних досліджень проблем теорії та практики конституційно-правового забезпечення інформаційної безпеки сучасних держав світу, в порівняльно-правовому аспекті, до сьогодні в Україні та за кордоном не проводилось. Натомість потреба в належному теоретико-методологічному забезпеченні конституційно-правових засад інформаційної безпеки України, із використанням наукових здобутків зарубіжних держав, насамперед держав-учасниць ЄС, а також напрацювання пропозицій щодо вдосконалення відповідної правотворчої та правозастосовної практики зберігає свою актуальність.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження відповідає «Концепції вдосконалення суддівства для утвердження справедливого суду в Україні відповідно до європейських стандартів», яка затверджена Указом Президента України 10 травня 2006 року за № 361/2006, Стратегії реформування державного управління України на період до 2021 року, затвердженій Розпорядженням Кабінету Міністрів України 24 червня 2016 року за № 474-р, Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки, затвердженій Указом Президента України 20 травня 2015 року за № 276/2015, Пріоритетним напрямам розвитку правової науки на 2016–2020 роки, затвердженим Постановою загальних зборів Національної академії правових наук України 3 березня 2016 р., Стратегії сталого розвитку «Україна – 2020», затвердженій Указом Президента України 12 січня національного університету імені В.І. Вернадського «Феномен гібридної війни в сучасному соціокультурному та геополітичному контекстах» номер державної реєстрації (0117U004667).

Мета і завдання дослідження. *Метою* дисертаційної роботи є розроблення теоретико-методологічних та конституційно-правових засад забезпечення інформаційної безпеки, як важливої функції сучасних держав у

трансформаційний період, а також напрацювання пропозицій удосконалення його механізмів у сучасних умовах.

Для досягнення зазначеної мети слід вирішити такі *завдання:*

– обґрунтувати теоретико-методологічні основи конституційно-правового забезпечення інформаційної безпеки;

– ґрунтуючись на методології системного підходу, охарактеризувати ґенезу наукових досліджень інформаційного суспільства та інформаційної безпеки;

– розкрити онтологічний, гносеологічний та аксіологічний аспекти підходів до вивчення функцій держави в сучасних умовах;

– розкрити систему інформаційної безпеки: поняття і правову природу, співвідношення інформаційної безпеки держави та інформаційної війни;

– дати поглиблену інтерпретацію співвідношення інформаційної безпеки з деякими іншими видами безпеки;

– визначити основні принципи забезпечення державою інформаційної безпеки у контексті новел законодавства;

– розкрити особливості правового регулювання забезпечення інформаційної безпеки як однієї з найважливіших функцій держави;

– охарактеризувати європейську модель забезпечення інформаційної безпеки сучасних держав;

– визначити ознаки американської моделі забезпечення інформаційної безпеки сучасних держав;

– проаналізувати азійську модель забезпечення інформаційної безпеки сучасних держав;

– узагальнити позитивний зарубіжний досвід реалізації функції забезпечення інформаційної безпеки сучасних держав;

– визначити загрози інформаційній безпеці: проблеми визначення та подолання;

– обґрунтувати шляхи наповнення новим змістом інституційної складової забезпечення інформаційної безпеки української держави та її удосконалення в сучасних умовах;

– окреслити напрями удосконалення механізмів забезпечення інформаційної безпеки держави: теоретичний та законодавчий виміри;

– надати пропозиції щодо напрямів удосконалення нормативно-правової складової механізму забезпечення інформаційної безпеки української держави.

Об'єктом дослідження є суспільні відносини, що виникають у процесі конституційно-правового забезпечення інформаційної безпеки сучасних держав.

Предметом дослідження є конституційно-правове забезпечення інформаційної безпеки сучасних держав.

Методи дослідження. Розв'язання поставлених завдань здійснено з використанням пізнавального потенціалу системи філософських, загальнонаукових та спеціальних методів. Історичний підхід сприяв виявленню закономірностей розвитку та динаміки формування інформаційної безпеки як

явища, її поняття і правової природи, співвідношення інформаційної безпеки держави та інформаційної війни (підрозділ 2.1); аналіз та синтез дав можливість визначити ознаки, сутність і зміст особливостей правового регулювання забезпечення інформаційної безпеки як однієї з найважливіших функцій держави (підрозділ 2.4). За допомогою форми аналізу – систематизації – визначено співвідношення інформаційної безпеки з деякими іншими видами безпеки (підрозділи 2.2). Структурно-функціональний метод застосований під час характеристики забезпечення державою інформаційної безпеки (підрозділ 2.3). Порівняльно-правовий метод використано для визначення напрямів удосконалення правових засад зарубіжного досвіду реалізації функції забезпечення інформаційної безпеки сучасних держав (підрозділи 3.1; 3.2; 3.3). Методи лінгвістичного аналізу і тлумачення правових норм сприяли виявленню прогалин та інших недоліків законодавства, виробленню пропозицій щодо вдосконалення нормативно-правової складової механізму забезпечення інформаційної безпеки української держави (підрозділи 1.1; 4.3). Системний підхід дав змогу сформулювати теоретичне обґрунтування необхідної діалектичної єдності загальної системи функцій держави у сучасних умовах та механізмів забезпечення інформаційної безпеки держави у сфері публічно-правових відносин як її складника (підрозділи 1.2; 4.1; 4.2).

Нормативну основу роботи становлять Конституція України, закони України, міжнародно-правові акти, ратифіковані Україною, що визначають особливості забезпечення інформаційної безпеки держави, рішення Європейського суду з прав людини тощо.

Наукова новизна одержаних результатів полягає в тому, що у дисертаційному дослідженні уперше на засадах методології системного підходу з урахуванням сучасних новел законодавства та міжнародних стандартів сформовано теоретико-методологічні та правові засади конституційно-правового забезпечення інформаційної безпеки сучасних держав та обґрунтовано нові підходи до розв'язання наявних проблем. Результатами дослідження, що містять наукову новизну, є таке:

уперше:

– на основі порівняльно-правового аналізу міжнародно-правових актів та національного законодавства України, зарубіжного законодавства і досвіду обґрунтовано концептуальний підхід, за яким державна політика у сфері забезпечення інформаційної безпеки України має розглядатись як самостійна функція або підфункція, що становить передумову реалізації державної інформаційної політики України, захисту інформаційних прав і свобод людини та громадянина, захисту інформаційного суверенітету держави і загалом інформаційного простору;

– досліджено світові моделі забезпечення інформаційної безпеки та сформовано пропозиції й рекомендації щодо удосконалення нормативного регулювання інформаційної безпеки української держави в умовах євроінтеграції, інтервенції та розвитку глобального інформаційного простору;

– доведено доцільність застосування концептуальних підходів вітчизняних та зарубіжних авторів до питання інформаційної безпеки держави за допомогою створення спеціального, національного, колегіального органу із захисту персональних даних – Національної комісії із захисту персональних даних. Її формування слід здійснити на засадах оптимізації, економічної доцільності, якісного технічного та кадрового забезпечення та широких повноважень. Основними завданнями цього органу мають бути: захист прав громадян у сфері персональних даних, регулювання захисту персональних даних, контроль та с

а – сформульовано, що сучасний негативний стан інформаційної безпеки держави обумовлений стрімким розвитком інформаційно-комунікаційних технологій, відкритим доступом до інформаційних ресурсів, які постійно модернізуються, діджиталізація, а також створення, розповсюдження та маніпулювання інформацією, у протистояннях між державами та агресії з боку терористичних організацій, широким застосуванням методів інформаційно-психологічного впливу шляхом використання інформаційних і комп'ютерних т

е – обґрунтовано доцільність внесення змін до існуючих міжнародно-правових стандартів, Конституції України, Законів України «Про національну безпеку України» 2018 р., «Про Концепцію Національної програми інформатизації» 1998 р., «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» 2007 р., Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України», затвердженого Указом Президента України 2017 р. та інших н

а – запропоновано першочергові заходи протидії інформаційним впливам РФ змістом яких є розгортання модернізованої системи контрпропагандистської діяльності для ефективної протидії реалізації проекту «руський мір». Основним компонентом якої є розроблення національної ідеї з урахуванням сучасних викликів та приділення уваги захисту релігійних цінностей та українських н

– аргументовано необхідність розробки та впровадження Кодексу про інформацію та інформаційну безпеку України, обов'язковими розділами якого мають бути: загальні положення (розкриваються основні поняття, сфера дії, визначаються суб'єкти, засади тощо); розділ присвячений інформації, доступу до неї та її захисту; розділ, що регулює ІКТ та інформаційну інфраструктуру в державі; розділ про кіберпростір; розділ щодо стратегії інформаційної безпеки; окремі розділи

– запропоновано розробити комплексний нормативний акт щодо проведення спеціальних інформаційних операцій за зразком американської доктрини

удосконалено:

– пізнавальні підходи до встановлення сутності інформаційної функції, яка відноситься до основних функцій держави і становить сформований у сучасних умовах основний напрям її діяльності в інформаційній сфері, значення правового регулювання якого зумовлено об'єктивними процесами глобального та національного інформаційного розвитку, безпосередньо виражає і предметно конкретизує сутність сучасної держави – досягнення демократії, розвиток громадянського інформаційного суспільства, глобальних інформаційно-к

о – положення щодо базової досліджуваної категорії – «інформаційна б езпека», що дозволяє виокремити різні підходи до розуміння її природи і змісту, у найбільш поширеними з них є: діяльнісний (безпека як процес, її забезпечення, в здатність держави ефективно здійснювати функції у даній сфері), статичний (безпека як стан захищеності інформаційного простору, інформації, к інформаційного суспільства і система відповідних гарантій тощо), комплексний а

б – наукову позицію щодо Доктрини інформаційної безпеки України що д озволяє встановити її техніко-юридичні недоліки, а саме: змістовні повторення, в загальні формулювання, дублювання положень інших нормативно-правових а ктів;

м – пріоритетні напрями державної політики у сфері забезпечення к інформаційної безпеки України: захист життєво важливих інтересів особистості, с суспільства та держави від внутрішніх і зовнішніх загроз; захист суверенітету, т підтримка політичної та соціальної стабільності, територіальної цілісності е України; захист критичної інформаційної інфраструктури; забезпечення р розвитку інформаційно-комунікаційних технологій; забезпечення участі У

к – підхід до об'єктів механізму забезпечення інформаційної безпеки у (найзагальнішому розумінні у вигляді предметів, явищ, процесів та осіб, на які б здійснюється інформаційний вплив та щодо яких здійснюються заходи із є забезпечення безпеки, які поділяються на соціальні особа, суспільство, держава, х їх інтереси, права та свідомість) та технічні (інформація, інформаційна й

е – положення щодо забезпечення інформаційної безпеки України, в умовах к ібридної агресії РФ, коли вкрай важливе значення має чітка регламентація р проведення інформаційних операцій у мирний та воєнний час;

м – наукові погляди щодо проблематики інформації та інформаційного і суспільства, інформаційної політики держави та інформаційних прав людини і к громадянина, інформаційної безпеки, кірбербезпеки, інформаційної війни та р національного та глобального інформаційного простору тощо;

у

р *дістали подальшого розвитку:*

о – ряд визначень, зокрема визначення поняття «інформаційна безпека», як у стан захищеності життєво важливих інтересів людини, суспільства і держави, що р

а

й

п

запобігає нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та д
о – положення щодо конституційно-правових та інші засад, особливостей с
дійснення цієї функції держави у національному і міжнародному масштабі тощо;
у – механізм забезпечення інформаційної безпеки як регламентовану з
аконодавством діяльність уповноважених суб’єктів, спрямовану на охорону та з
ахист інформаційної сфери особи, суспільства та держави від зовнішніх і в
н
у – напрями вдосконалення нормативно-правового забезпечення у
інформаційної безпеки на основі аналізу зарубіжного досвіду;
т – пропозиції стосовно формування нормативно-правової складової р
механізму забезпечення інформаційної безпеки від визначення організаційної б
удови цього механізму, регулювання діяльності його суб’єктів та забезпечення з
в
ф **Практичне значення одержаних результатів** полягає в тому, що с
формульовані в дисертації теоретичні положення, пропозиції та рекомендації с
прияти муть формуванню теоретико-методологічних та правових засад в
ирішення адміністративними судами спорів у сфері публічно-правових в
ідносин. Одержані результати можуть бути використані та використовуються:
п – *у науково-дослідній сфері* – як фундамент для розв’язання та подальшого і
дослідження проблематики забезпечення інформаційної безпеки держави й
(Довідка Науково-дослідного центру правового забезпечення державотворення і
та безпеки ТНУ імені В.І. Вернадського № 1/20-01 від 30.09.2020);
з – *у правотворчості* – внесення змін і доповнень до значної кількості й
ормативно-правових актів України, зокрема лягли в основу законопроекту «Про в
внесення змін до деяких законів України щодо посилення відповідальності за в
вчинені правопорушення у сфері інформаційної безпеки та боротьби з к
іберзлочинністю» (номер 2133а від 19.06.2015) та Закону України «Про основні у
засади забезпечення кібербезпеки України» (
Стратегії кібербезпеки України б
езпеки України (https://zakon.rada.gov.ua/laws/show/47/2017#Text) які р
озглядалися Комітетом з питань правоохоронної діяльності та були р
екомендовані для розгляду Верховною радою України (Акт впровадження н
аукових розробок дисертаційного дослідження від 06.07.2020 р. № 04-27/12-
н
о
н
у – *у навчальному процесі* – під час вивчення навчальних дисциплін: н
«Конституційне право», «Адміністративне право», «Трансформація національної
я
я
н
я

правової безпеки», «Інформаційне право», «Захист інформації та інформаційна безпека» «Порівняльне адміністративне право», «Міжнародне інформаційне право», «Міжнародне право» (довідка впровадження результатів дисертаційного дослідження в навчальний процес Навчально-наукового гуманітарного інституту Т

а **Особистий внесок здобувача.** Викладені в дисертації наукові положення, висновки й рекомендації, що виносяться на захист, одержані здобувачем рамостійно. Ідеї та розробки співавторів у дисертації не використані.

і **Апробація результатів дисертації.** Ключові теоретичні напрацювання й рекомендації оприлюднені в тезах доповідей і наукових повідомлень на наукових с науково-практичних семінарах та конференціях, а також у процесі виконання міжнародних проектів: Стан дотримання прав людини в умовах сучасності: теоретичні та практичні аспекти (м. Київ, 22 березня 2018 р.); Сучасна війна: гуманітарний аспект (Харківський національний університет Повітряних сил імені Івана Кожедуба, 31 травня – 1 червня 2018 року); Виклики політики безпеки: історія і сучасність (18–-19 жовтня 2018 р.); Політико-правова доктрина державного суверенітету в умовах глобалізації (26 жовтня 2018 р.); Стан та перспективи реформування сектору безпеки і оборони України (Управління державної охорони України в Київському національному університеті імені Тараса Шевченка); Деокупація і реінтеграція інформаційного простору Криму: міжнародно-правові та медіакомунікативні інструменти (Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка 18 квітня 2019 р.); Верховенство права як гарантія конституційного ладу (м. Київ, 5 грудня 2019 р.).

л **Публікації.** Основні теоретичні й практичні положення дисертаційного дослідження відображено в одноособовій монографії, одній колективній монографії, 25 статтях, опублікованих у вітчизняних та міжнародних фахових виданнях з юридичних наук, 23 з яких – одноособові, 2 – у співавторстві, а також у 11 тезах доповідей і повідомлень, оприлюднених на міжнародних наукових і науково-практичних конференціях, круглих столах, семінарах, конгресах.

Структура дисертації. Дисертація складається зі вступу, чотирьох розділів, які містять тринадцять підрозділів, кожен із яких завершується проміжним висновком. Також у дисертації міститься загальний висновок, де підсумовано результати дисертаційного дослідження та список використаних джерел. Робота відповідає змісту, містить анотацію, має список умовних позначень та посилання на використані джерела. Загальний обсяг дисертації становить 448 сторінок, у тому числі основного тексту – 371 сторінка. Список використаних джерел налічує 651 найменування.

и

т

ОСНОВНИЙ ЗМІСТ РОБОТИ

е У **вступі** обґрунтовано актуальність теми дисертації; висвітлено ступінь наукової дослідженості вибраної для аналізу проблематики, зв’язок із науковими програмами, планами, темами; визначено мету й завдання, об’єкт і предмет,

і

м

е

методологічні основи дослідження; розкрито наукову новизну та практичне значення одержаних результатів; наведено відомості про особистий внесок здобувача, апробацію результатів і публікації, а також структуру й обсяг роботи.

Розділ 1 «Доктринальні джерела дослідження інформаційного суспільства, інформаційної безпеки та функцій держави» складається з двох підрозділів і присвячений з'ясуванню фундаментальних проблем, пов'язаних з розвитком **інформаційного суспільства**, а також оцінюванню сучасного стану досліджень, що спрямовані на їх розв'язання.

У підрозділі 1.1 *«Генеза наукових досліджень інформаційного суспільства та інформаційної безпеки»* наведено огляд досліджень проблематики інформаційного суспільства та інформаційної безпеки, виділено групи праць за предметно-тематичним критерієм, зокрема ті, що висвітлюють сутність та зміст понять «інформаційне суспільство», «інформаційна безпека».

Підтримано думку про те, що механізм забезпечення національної безпеки визначається специфічним видом правових механізмів, який має особливу, складну природу, що зумовлена самою сутністю категорії національної безпеки. Зміст даного механізму розкривається через єдність його комплексних елементів: систему, яка включає в себе конституційні норми та конкретизуючі норми поточного конституційного законодавства, процесуальні акти, правовідносини (правова основа) і цілеспрямовану діяльність (сукупність узгоджених дій їх форм, методів, способів, засобів) органів державної влади, до компетенції яких входить вирішення питань щодо забезпечення безпеки людини і громадянина, держави і суспільства, структур громадянського суспільства (органів місцевого самоврядування, громадських організацій, політичних партій), що мають на меті реалізацію й захист національних інтересів (інституційний механізм).

Застосування системного підходу та критичний аналіз наукового доробку вчених, які займалися розробленням окремих аспектів інформаційного суспільства і зокрема інформаційної безпеки, дали змогу визначити проблематику, яка залишилися поза науковою увагою. Закцентовано увагу на тому, що порушення прав людини не тільки погіршують становище самої людини в суспільстві, а й негативно впливають на функціонування інших компонентів системи національної безпеки, внаслідок чого остання стає більш уразливою і, відповідно, менш надійною. Права людини необхідно вважати головним об'єктом національної безпеки України, оскільки лише на основі безпеки особи можна планувати і вживати заходів із забезпечення безпеки більш складних соціальних систем, таких як суспільство і держава, та створювати умови для забезпечення національної безпеки загалом.

У підрозділі 1.2 *«Аналіз підходів до вивчення функцій держави у сучасних умовах»* висвітлено сучасні методологічні підходи до *вивчення функцій держави у сучасних умовах*, використані вченими у вітчизняній юридичній науці для їх пізнання. Наголошено, що серед складників методології дослідження зазначеної проблематики чільне місце посідають онтологія, гносеологія та аксіологія як

вчення, спираючись на які вдалося розкрити визначення поняття державних функцій, їх системи та класифікації, пов'язані з такими фундаментальними категоріями теорії держави і права як сутність держави, її соціальне призначення та сервісна роль. Саме функціональна характеристика визначає сильну державу та ефективну державність. З огляду на зміну уявлень щодо основних ознак держави та характеристик сучасної державності взагалі істотно уточнено зміст понять, за допомогою яких розкривається теорія функцій сучасної держави і, передусім, саме визначення поняття «функція держави».

Констатується загалом єдність та статичність наукового пізнання досліджуваного явища, що не сприяє ґрунтовному переосмисленню існування наведеного феномена в контексті трансформації цінностей, об'єктом яких є людина. Наголошено, що науковці намагаються певною мірою поєднати найсуттєвіші, на їхню думку, ознаки або атрибути функцій сучасної держави як складного соціального організму, які раніше досліджувалися переважно в межах окремих підходів. Акцентовано увагу на тому, що сучасні тенденції розвитку держав, міждержавного співробітництва засвідчують про поступову деполяризацію суспільства, підкреслюють необхідність зміщення акцентів у розумінні функцій держави у сторону зумовленості їх суспільними потребами і належного закріплення й реалізації прав людини. Активізація розбудови громадянського та інформаційного суспільства зумовлюють перерозподіл функцій держави, власне державними залишаються лише її невід'ємні функції, які громадянське суспільство самостійно здійснювати не здатне (забезпечення суверенітету держави, безпеки суспільства, зовнішньополітична функція і т.д.).

Розділ 2 «Концептуальні підходи до розуміння інформаційної безпеки та правові засади її регулювання» складається з чотирьох підрозділів і присвячений дослідженню поняття і правової природи інформаційної безпеки аналізу принципів забезпечення державою інформаційної безпеки, а також вивченню співвідношення інформаційної безпеки держави та інформаційної війни.

У підрозділі 2.1 *«Інформаційна безпека: поняття і правова природа. Інформаційна безпека держави та інформаційна війна»* розкрито теоретичні підходи до категорій «інформаційна безпека», «інформаційна безпека держави» та «інформаційна війна». Систематизація наукових пошуків у напрямі формування підходів до цих явищ за формально-юридичною ознакою дає змогу говорити про єдність та однорідність форми, якщо таким поняттям позначається діяльність у сфері публічно-правових відносин. Наголошується на ознаках форми, що визначають її особливості та формують її юридичну унікальність у контексті єдності зі змістом.

Інформаційна війна здійснюється у формі інформаційного протиборства як системи цілеспрямованих дій для створення інформаційної переваги за допомогою руйнування інформації, інформаційних систем протилежної сторони, при цьому одночасно відбувається процес захисту власної інформації та інформаційних систем.

Отже, на нашу думку, інформаційна війна – це суспільно-політичне явище, яке в політичному аспекті є продовженням домінуючих ідеологічних засад державної політики, що здійснюється за допомогою комплексу засобів інформаційно-технологічної індустрії, механізмів інформаційно-психологічного впливу на суспільство всередині держави чи населення країн-конкурентів в умовах політичного (воєнно-політичного, економічного) конфлікту з метою формування у соціальному аспекті єдності суспільства, визначення його ідентичності та інформаційного захисту світоглядних цінностей, а також деморалізації та фрагментації населення, силової компоненти держав-противників у межах глобального інформаційного простору.

Інформаційна війна як явище деструктивно впливає на розвиток інформаційних суспільств, інформаційну безпеку людини, держави і суспільства та одночасно сприяє розвитку практично всіх пріоритетних сфер життєдіяльності, у т. ч., через вплив маніпулятивних технологій, що використовуються в інформаційних війнах, на світову політику тощо. Світові тенденції розвитку державно-правових явищ потребують не тільки удосконалення форм і методів організації та здійснення влади, й нових стратегій забезпечення національної інформаційної безпеки. З огляду на це, важливо удосконалити правові основи протидії та запобігання інформаційним війн, негативного інформаційно-психологічного впливу на національному рівні в Україні. Для цього важливо вивчати як зарубіжний досвід, так і відповідні доктринальні та нормативні джерела з метою пошуку оптимальних шляхів виходу з тих ситуацій, в яких опинилось українське суспільство в останні роки.

Таким чином, існують різні підходи до таких багатогранних категорій, як «інформаційна безпека», «інформаційна війна». Водночас, враховуючи системне зростання загроз і протиправних намірів супротивників, інших держав, важливо їх виявляти, запобігати їм та своєчасно протидіяти, захищати національні інтереси й цінності, включаючи інформаційну безпеку, інформаційний суверенітет і т. д.

У зв’язку з цим, на наше переконання, пріоритетним має стати власне комплексне розуміння сутності та гарантій забезпечення інформаційної безпеки держави, враховуючи функціональні аспекти національної безпеки та специфіку інформаційної сфери, національного і світового інформаційного простору, можливі потенційні загрози інформаційних воєн та інших викликів.

У підрозділі 2.2 «*Співвідношення інформаційної безпеки з деякими іншими видами безпеки*», з огляду на проаналізовані в попередніх підрозділах нашого дослідження природу і сутність інформаційного суспільства та інформаційної безпеки, а також функції держав, спрямовані на їх забезпечення, закцентовано увагу на тому, що очевидною є потреба вивчення основоположних теоретичних і законодавчих засад їх правового регулювання. Йдеться, зокрема, про принципи забезпечення інформаційної безпеки як однієї з найважливіших функцій держави.

Як відомо, категорія «забезпечення» є складною й багатогранною, оскільки включає чимало складових, починаючи від створення умов і регулювання, завершуючи реалізацією, охороною і захистом, відновленням або сприянням відновленню у випадку порушення. Тому важливо дослідити та виокремити особливості власне принципів забезпечення державою інформаційної безпеки як основоположних засад усієї системи її забезпечення, визначити підходи до класифікації та власне виокремити різновиди таких принципів, їх значення тощо.

На наше переконання, відмінними тенденціями правового регулювання об'єктів інформаційної сфери є тенденції сутнісного і предметно-функціонального характеру. Так, об'єкти інформаційної інфраструктури одночасно використовуються в різних просторових вимірах, існуюча на глобальному рівні інформаційна інфраструктура складається з взаємопов'язаних інфраструктурних елементів на внутрішньодержавних і наднаціональному рівнях. Сама інформаційна сфера відзначається транскордонним характером тощо.

У підрозділі 2.3 *«Принципи забезпечення державою інформаційної безпеки»* визначено функціональний аспект міжнародно-правового регулювання інформаційної сфери загалом та інформаційної безпеки зокрема, який зумовлений здійсненням регулятивного впливу, спрямованого на впорядкування міжнародних інформаційних відносин, свободи інформації, а саме – можливості збирати, обмінюватися, поширювати й використовувати інформацію; інтегративну чи координуючу функцію, метою якої є прийняття уніфікованих міжнародних стандартів в інформаційній сфері.

Таким чином, аналіз існуючої міжнародно-правової основи цієї сфери демонструє необхідність звернення уваги уповноважених суб'єктів на доволі загальні тенденції регламентації питань інформаційної безпеки, розроблення та прийняття міжнародно-правових стандартів забезпечення інформаційної безпеки, створення дієвих інструментів їх реалізації.

У підрозділі 2.4 *«Особливості правового регулювання забезпечення інформаційної безпеки як однієї з найважливіших функцій держави»* на основі здійсненого аналізу стану правового регулювання забезпечення інформаційної безпеки на рівні національного законодавства України відзначено певну непослідовність і подекуди несистемність. Проте, останніми роками ця ситуація дещо виправилась на краще і демонструє активнішу участь держави в реалізації однієї з найважливіших її функцій, а саме – забезпечення інформаційної безпеки держави. Ця функція, безумовно, пов'язана з реалізацією інших функцій Української держави, визначених органів публічної влади. Надалі ми зупинимось на їх діяльності, виокремленні перспективних напрямів удосконалення в сучасних умовах.

Разом з тим, національне законодавство України потребує подальшого узгодження з існуючими міжнародно-правовими актами універсального й регіонального рівнів у сфері інформаційної безпеки, імплементації існуючих

міжнародно-правових стандартів у законодавство і практику його реалізації. На наш погляд, доцільно також активізувати міжнародну правотворчу діяльність України у цій сфері, що посилить вплив нашої держави у міжнародних правових відносинах, сприятиме удосконаленню правового регулювання забезпечення інформаційної безпеки.

Розділ 3 «Зарубіжний досвід реалізації функції забезпечення інформаційної безпеки сучасних держав» складається з трьох підрозділів, у яких досліджено моделі забезпечення інформаційної безпеки сучасних держав. У глобальному аспекті порівняння систем правового забезпеченні інформаційної безпеки в Україні, європейських та азійських країнах, країнах Північної Америки визначено й доведено пріоритетні, реальні та неприйнятні моделі для подальшого вдосконалення системи інформаційної та кібербезпеки Української держави.

У підрозділі 3.1 *«Європейська модель забезпечення інформаційної* безпеки сучасних держав» з'ясовано моделі інформаційної безпеки європейських країн, що засновуються на відповідному законодавстві Європейського Союзу (ЄС) та національному законодавстві держав-учасниць. Головними актами ЄС у сфері захисту інформаційного простору є: Закон ЄС «Про ENISA (*Агентство Європейського Союзу з питань кібербезпеки*) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку)» від 17.04.2019 р. (Закон «Про ENISA та сертифікацію»), Директива про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива NIS) від 06.07.2016 р., Регламент (ЄС) 2016/679 Європейського парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб стосовно оброблення персональних даних та про вільне переміщення таких даних і скасування Директиви 95/46 / ЕС (Загальні положення про захист даних) (англ. *General Data Protection Regulation,* GDPR) та ін.

Сфера можливостей. ЄС відіграє ключову роль у заохоченні та підтримці розвитку потенціалу у сфері кіберзахисту державних і приватних структур у державах-членах, а також самих європейських інститутів, спираючись на європейські ноу-хау. Він також може надавати підтримку у сфері підготовки та навчання, що створює синергію і запобігає дублюванню потенціалу.

Отже, кібербезпека охоплює всі заходи безпеки, які можуть бути прийняті для захисту від атак у цифровому просторі. Неухильне зростання складності й інтенсивності кібератак призвело до того, що останніми роками більшість розвинутих країн підвищили стійкість та прийняли національні стратегії кібербезпеки. Зокрема, у Франції діє Національна кіберстратегія від 2011 року, Національна стратегія цифрової безпеки від 2015 року, а також Міжнародна стратегія Франції щодо цифрових технологій від 2017 року. Зазначені документи доповнюються Білими книгами, Оборонним оглядом та оглядом стратегії кіберзахисту. Захист інтернет-середовища Франції здійснюють такі державні органи, як ANSSI, CERT, COSSI, Міністерство оборони, COMCYBER та

Міністерство внутрішніх справ. Кібербезпека розглядається Францією як національний пріоритет, який нині стосується кожного з її громадян.

Німецька модель забезпечення інформаційної безпеки держави діє на підставі Конституції ФРН, федеральних законів та законів земель, рішень конституційних судів, наднаціонального законодавства та відповідних підзаконних нормативно-правових актів.

Так, відповідно до параграфа 1 статті 5 Конституції ФРН, кожен має право на свободу вираження і поширювання своєї думки усно, письмово і за допомогою образотворчих засобів, безперешкодно отримувати інформацію з усіх загальнодоступних джерел. Гарантується свобода друку і свобода передавання інформації за допомогою радіо і кіно. Цензура не здійснюється.

У 2009 р. Конституцію ФРН було доповнено статтею 91с, яка заклала основу для співпраці федерального уряду та урядів земель в області інформаційних технологій. Це положення є широким з урахуванням постійного прогресу інформаційних технологій і його зростаючого значення для державного управління. Воно включає в себе фактичні та юридичні аспекти такої співпраці. Закріплена можливість узгодження стандартів для їх одноманітного застосування для забезпечення сумісності і вимог безпеки при обміні даними.

Базовим законом у сфері інформаційної безпеки Німеччини є Закон «Про посилення безпеки систем інформаційних технологій» (Закон про безпеку ІТ) від 25.07.2015р. Закон відводить Федеральному відомству з безпеки у сфері інформаційних технологій (нім. BSI) центральну роль у захисті критично важливих інфраструктур у Німеччині. При цьому під критичними інфраструктурами розуміють об’єкти, установки або їх частини, які належать до секторів енергетики, інформаційних технологій і телекомунікацій, транспорту і дорожнього руху, охорони здоров’я, водопостачання, харчування, фінансів і страхування. Такі об’єкти мають велике значення для функціонування спільноти, тому що їх зупинка або погіршення роботи призведе до значного дефіциту поставок або створить загрози для громадської безпеки.

У підрозділі 3.2 *«Американська модель забезпечення інформаційної безпеки сучасних держав»* наголошено на тому, що у Сполучених штатах Америки інакше врегульовано проблему забезпечення інформаційної безпеки, аніж в європейських країнах. Так, усвідомлення Сполученими Штатами масштабності впливу цифрових технологій на всі процеси у державі та світі, зумовило детальну регламентацію забезпечення безпеки у кіберпросторі. У цьому напрямі важливу організаційну функцію відіграють Національна стратегія безпеки, Національна стратегія кібербезпеки, військові стратегії та доктрини.

Захист інтернет-простору США здійснюється у таких аспектах: захист американського народу, Америки та американського способу життя, забезпечення процвітання Америки, збереження миру методом примусу, посилення американського впливу.

Забезпечення інформаційної безпеки США здійснюється і на військовому рівні, зокрема шляхом проведення інформаційних операцій. Такі операції є

засобами інформаційної війни, а їх проведення здійснюється на підставі відповідних доктрин, стратегій та військових програм. Метою інформаційної операції може бути електронна боротьба, мережеві комп'ютерні операції, військові операції інформаційної підтримки, дезінформація противника, безпека операцій.

У підрозділі 3.3 *«Азійська модель забезпечення інформаційної безпеки сучасних держав»* проаналізовано азійську модель забезпечення інформаційної безпеки сучасних конституційних держав, яка розглядається на прикладі Китайської Народної Республіки (КНР) та Російської Федерації (РФ). Віднесення російської системи забезпечення інформаційної безпеки до азійської моделі зумовлено наявністю тенденцій до запозичення РФ китайського досвіду регулювання інформаційної безпеки та кіберпростору.

Китайська модель забезпечення інформаційної безпеки засновується на тотальному контролі державою її інформаційного простору, що суперечить європейським практикам у цій сфері, і, відповідно, вважається негативним прикладом інформаційної державної політики.

Державний контроль і цензура запроваджені і в китайському онлайн-просторі. Це зумовлено, насамперед тим, що в Китаї найбільша кількість інтернет-користувачів у світі – 802 млн користувачів і 42% світових транзакцій електронної торгівлі надходять з цієї країни. У зв'язку з цим у КНР реалізується проект «Золотий щит» (англ. The Golden Shield Project), який ще називають Великий китайський фаєрвол, програма фільтрації інтернет-контенту в КНР. Цей проект був впроваджений у 2003 р. Ця програма охоплює такі напрями, як система управління трафіком, система інформування про правопорушення, система управління безпекою, інформаційна система моніторингу, система контролю виходу і введення.

«Золотий щит» є одним з 12 ключових проектів КНР у сфері електронного уряду, іменованих «золотими». Іншими «золотими» проектами є: «Золота митниця» (для іноземних торгів), «Золоті мости» (для загальноекономічної інформації), «Золоті фінанси» (для управління фінансами), «Золота картка» (для електронних валют), «Золота вода» (для інформації про водні ресурси), «Золоте сільське господарство» (для сільськогосподарської інформації), «Золота якість» (для контролю якості), «Золоте оподаткування» (для оподаткування) і т. ін.

Проект «Золотий щит» передбачає обмеження доступу до низки іноземних сайтів, веб-сторінки фільтруються по кодовим словам, пов'язаним з національною безпекою та з чорним списком сайтів. Сайти, які розміщені у Китаї, повинні проходити реєстрацію у Міністерстві промисловості та інформаційних технологій. Крім того, в Китаї діє армія блогерів, які за винагороду позитивно висловлюються в чатах, блогах і на форумах про державну політику Китаю.

Прикметно, що досвід КНР щодо інтернет-цензури вивчає та починає імплементувати у своє законодавство РФ, тому російську модель забезпечення інформаційної безпеки відносять до азійської моделі.

Російська модель інформаційної безпеки засновується на розумінні властивостей інформаційного суспільства, процесі цифрової трансформації та спрямованості на захист інформаційної інфраструктури та інтересів держави в умовах інформаційного середовища. Правові засади цієї моделі закріплені у Конституції РФ, федеральному законодавстві, у низці підзаконних нормативно-правових актів та міжнародних документах.

Контент-аналіз Конституції РФ свідчить про відсутність у її тексті поняття «інформаційна безпека», лише застосовується термін «державна безпека». Конституційні положення про право на інформацію та заборону цензури мають засадниче значення насамперед для інформаційної безпеки особи.

Важливе місце в правовому забезпеченні інформаційної безпеки РФ посідає Федеральний Закон «Про інформацію, інформаційні технології та про захист інформації» від 27.07.2006 р. № 149-ФЗ (Закон про інформацію). Він визначає засади правового регулювання у трьох напрямах: реалізація права на інформацію, застосування інформаційних технологій та захист інформації.

У контексті реалізації права на інформацію цей закон визначає основні поняття у цій сфері, закріплює статус інформації як об'єкта правовідносин, установлює критерії її класифікації, називає суб'єктів інформації та описує їх компетенцію. Особлива увага приділяється порядку поширення інформації окремими володільцями інформації та організаторами її поширення.

Для організаторів поширення інформації в мережі Інтернет установлено низку додаткових обов'язків щодо зберігання інформації на території РФ, за невиконання яких передбачена адміністративна відповідальність – накладення адміністративного штрафу на громадян у розмірі від трьох тисяч до п'яти тисяч рублів; на посадових осіб – від тридцяти тисяч до п'ятдесяти неоподатковуваних мінімумів доходів громадян; на юридичних осіб – від восьмисот тисяч до одного мільйона рублів.

Зокрема, організатор поширення інформації в мережі Інтернет зобов'язаний зберігати на території РФ:

1) інформацію про факти прийому, передачі, доставки та (або) оброблення голосової інформації, письмового тексту, зображень, звуків, відео чи інших електронних повідомлень користувачів мережі Інтернет й інформацію про користувачів протягом одного року з моменту закінчення здійснення таких дій;

2) текстові повідомлення користувачів мережі Інтернет, голосову інформацію, зображення, звуки, відео, інші електронні повідомлення користувачів мережі Інтернет до шести місяців з моменту закінчення їх прийому, передачі, доставки та (або) оброблення. Порядок, терміни та обсяг зберігання зазначеної в цьому підпункті інформації встановлює Уряд РФ.

Зазначені норми були внесені у Закон про інформацію 06.07.2016 р. «пакетом Ярової» та анонсувалися як заходи протидії тероризму й забезпечення громадської безпеки, але на практиці викликали дискусію щодо обмеження права на свободу вираження поглядів, права на інформацію та суттєвого зменшення свободи в Інтернеті.

Наприклад, конфлікт державних органів з великими ІТ-компаніями зумовив обов'язок організаторів поширення інформації в Інтернеті надавати Федеральній службі безпеки РФ інформацію, яка необхідна для декодування електронних повідомлень їх користувачів.

У Доктрині інформаційна безпека РФ розуміється як стан захищеності особистості, суспільства і держави від внутрішніх і зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини і громадянина, гідні якість і рівень життя громадян, суверенітет, територіальна цілісність і стійкий соціально-економічний розвиток Російської Федерації, оборона й безпека держави.

Водночас забезпечення інформаційної безпеки роз'яснюється як здійснення взаємопов'язаних правових, організаційних, оперативно-розшукових, розвідувальних, контррозвідувальних, науково-технічних, інформаційно-аналітичних, кадрових, економічних та інших заходів з прогнозування, виявлення, стримування, запобігання, відбиття інформаційних загроз і ліквідації наслідків їх прояву.

Національні інтереси РФ в інформаційній сфері розділені на такі групи:

1. Гарантування та захист прав і свобод людини та громадянина (право на інформацію, право на приватність при використанні ІТ, інформаційна підтримка демократичних інститутів).
2. Стабільне функціонування інформаційної інфраструктури (критично важливі об'єкти інформаційної інфраструктури та мережа електрозв'язку) як у мирний час, так і воєнний період.
3. Розвиток ІТ та електронної промисловості.
4. Участь у побудові мережі міжнародної інформаційної безпеки.
5. Інформування громадськості, серед іншого і міжнародної, про офіційні позиції з важливих питань у державі та світі та про державну політику РФ.
6. Використання ІТ для забезпечення національної безпеки у сфері культури.

У Доктрині наводиться достатньо широкий аналіз сучасного стану інформаційної безпеки РФ та основних загроз для неї. Виходячи з концепції Доктрини, загрози інформаційної безпеки РФ можна розділити та такі види: загрози конституційним правам і свободам людини і громадянина у сфері інформаційної діяльності та культурного життя, загрози індивідуальній, колективній та громадській свідомості; загрози ІТ мережам та засобам; загрози інформаційному забезпеченню політики держави; кіберзлочинність та терористична діяльність; загрози розвитку вітчизняної індустрії інформації.

Значна увага приділяється загрозам інформаційному простору в аспекті військово-політичних та дестабілізуючих цілей. Наприклад, зазначається, що одним з основних негативних чинників, що впливають на стан інформаційної безпеки, є нарощування низкою зарубіжних країн можливостей інформаційно-технічного впливу на інформаційну інфраструктуру у військових цілях.

Одночасно з цим посилюється діяльність організацій, що здійснюють технічну розвідку щодо російських державних органів, наукових організацій і підприємств оборонно-промислового комплексу. Розширюються масштаби використання спеціальними службами окремих держав засобів здійснення інформаційно-психологічного впливу, який спрямований на дестабілізацію внутрішньополітичної та соціальної ситуації в різних регіонах світу і призводить до підриву суверенітету й порушення територіальної цілісності інших держав. В цю діяльність втягуються релігійні, етнічні, правозахисні та інші організації, а також окремі групи громадян, при цьому широко використовуються можливості інформаційних технологій.

Варто звернути увагу на те, що РФ обрала стратегію протидії зазначеному інформаційно-психологічному впливу через посилення державного регулювання інформаційного простору та обмеження права на інформацію й права конфіденційності в Інтернеті. Такий підхід діаметрально протилежний підходу, що застосовує ЄС для боротьби з недостовірними новинами («фейками»).

Отже, розглянута модель інформаційної безпеки РФ засновується на жорсткому державному регулюванні інформаційного простору та обмеженні доступу та свободи в онлайн-середовищі, також наявна тенденція до подальшого ізолювання національного сегмента Інтернету. У вказаних аспектах така модель набуває спільних ознак з китайськими державними проектами інформаційної безпеки та все більше протиставляється моделям забезпечення інформаційної безпеки західних країн.

Розділ 4 «Механізми забезпечення інформаційної безпеки сучасних держав і перспективи їх удосконалення» складається з чотирьох підрозділів, в яких розкрито перспективні напрями використання позитивного зарубіжного досвіду та наповнення новим змістом питань інформаційної безпеки сучасних держав і перспективи їх удосконалення та окрім науково-теоретичної складової, акцентовано увагу на наявні проблеми забезпечення інформаційної безпеки й запропоновано шляхи їх вирішення, зокрема в Українській державі.

У підрозділі 4.1 *«Механізми забезпечення інформаційної безпеки держави: теоретичний та законодавчий вимір»* здійснено дослідження та аналіз наукових поглядів щодо сутності таких базових понять у сфері інформаційної безпеки як «забезпечення інформаційної безпеки», «механізм забезпечення інформаційної безпеки» та «система забезпечення інформаційної безпеки», наголошено на відсутності усталеного підходу до визначення вказаних категорій.

За таких умов, з одного боку, існує широкий простір для відповідних теоретико-правових пошуків, які в цілому випадку часто призводять до збільшення дискусійних питань та протиставленні наукових позицій. Зокрема, в монографіях та дисертаційних дослідженнях забезпечення інформаційної безпеки тлумачиться і як діяльність, і як сукупність чи система заходів, і як соціальний феномен, і як соціально-правовий механізм, і як коло процесів і явищ тощо.

Така варіативність поглядів на забезпечення інформаційної безпеки зумовлює й низку різноманітних визначень механізму та системи такого забезпечення. Наприклад, механізм забезпечення інформаційної безпеки розглядається як: система державно-правових інституцій; система з власною структурою; система різних засобів; сукупність державних органів, громадських структур, заходів, важелів та способів дій.

Ми під системою забезпечення інформаційної безпеки пропонуємо розуміти комплексний механізм реалізації інтересів в інформаційній сфері; сукупність механізмів та суб'єктів; сукупність органів, зв'язків, інструментів та технологій; систему різних заходів тощо.

Як бачимо, у цьому напрямі досліджень серед авторів немає узгодженої позиції щодо змісту та співвідношення категорій «механізм» та «система». Так, в одних наукових працях, де автори розглядають механізм забезпечення інформаційної безпеки крізь призму системи або, навпаки, можна говорити про фактичне ототожнення цих категорій. В інших же працях автори прямо зазначають про необхідність розрізнення цих двох понять, але не розкривають їх співвідношення.

З іншого боку, різноманітність трактувань базових понять у сфері інформаційної безпеки породжує концептуальну невизначеність реалізації державної функції щодо забезпечення інформаційної безпеки як на теоретичному, так і на законодавчому рівнях. У зв'язку з цим знижується загальна ефективність реалізації зазначеної функції держави та ускладнюється її вдосконалення.

Таким чином, на підставі вищевикладеного ми запропонували розглядати механізм забезпечення інформаційної безпеки як регламентовану законодавством діяльність уповноважених суб'єктів, спрямовану на охорону та захист інформаційної сфери особи, суспільства та держави від зовнішніх і внутрішніх загроз, удосконалення заходів інформаційної протидії та боротьби.

Наведена дефініція охоплює ключові елементи механізму забезпечення інформаційної безпеки: об'єкт, суб'єкт, загрози, напрями, заходи.

Об'єкти механізму забезпечення інформаційної безпеки у найзагальнішому розумінні – це предмети, явища, процеси та особи, на яких здійснюється інформаційний вплив та щодо яких застосовуються заходи із забезпечення безпеки. Їх можна розподілити на соціальні (особа, суспільство, держава, їх інтереси, права та свідомість) та технічні (інформація, інформаційна інфраструктура, інформаційні технології тощо).

У підрозділі 4.2 *«Загрози інформаційній безпеці: проблеми визначення та подолання»* здійснено аналіз деяких нормативно-правових актів, який демонструє відсутність на законодавчому рівні поняття «загроз інформаційній безпеці держави». Тому варто звернутись до доктринальних джерел, енциклопедичних та інших наукових видань. Найширше загрози інформаційним ресурсам розглядають як потенційно можливі випадки природного, технічного або антропогенного змісту, які можуть спричинити небажаний вплив на

інформаційну систему, а також на інформацію, що зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом як уразливість. Саме за наявності уразливості як певної характеристики системи і відбувається активізація загроз. А самі загрози за своєю суттю відповідно до теорії множин є невичерпними, а отже, й не можуть бути піддані повному описові у будь-якому дослідженні.

До загроз інформаційній безпеці системі управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій у роботі самого обладнання. Через їх чисельність відповідно до загальної класифікації загроз національній безпеці, виокремлюють загрози інформаційній безпеці за різними критеріями.

За джерелами походження: природного походження (масове руйнування через природні катаклізми каналів зв'язку); техногенного походження (аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів системи управління національною безпекою тощо); антропогенного походження (помилковий запуск програми, (не)навмисне допущення через недотримання правил безпеки роботи в Інтернеті інсталяції закладок тощо).

За характером реалізації: реальні (активізація шляхів дестабілізації є неминучою і не обмежена часом і простором); потенційні (шляхи дестабілізації можливі за певних умов середовища функціонування органів публічної влади); здійснені (загрози втілені у життя); уявні (умовні чи схожі з існуючими, але такими не є).

За ступенем гіпотетичної шкоди: загроза (явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері і створюють небезпеку для системи управління національною безпекою, життєзабезпечення її системостворюючих елементів); небезпека (безпосередня дестабілізація функціонування системи управління національною безпекою).

За ймовірністю реалізації: вірогідні (за виконання певного комплексу умов обов'язково настануть., наприклад, оголошення атаки інформаційних ресурсів, що передує власне атаці); неможливі (за виконання певного комплексу умов ніколи не настануть, переважно мають більш декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякувальні); випадкові (за виконання певного комплексу умов протікають по-різному, їх аналізують за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах).

За рівнем детермінізму: випадкові (загрози, які можуть трапитися або не трапитися – загрози хакерів дестабілізувати інформаційні системи органів влади); закономірні (загрози стійкого, повторювального характеру, зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки, – численні атаки хакерів на офіційні сайти ФБР, ЦРУ США).

Цей перелік, звісно, можна продовжувати, але очевидний такий висновок. Так, поняття «загрози» розглядають переважно абстрактно або спрощено, подекуди звужено, відірвано від контексту поняття «інформаційна безпека» і майже не пов'язано з контекстом родового поняття «загроза».

Загрози інформаційній безпеці України ми розглядаємо як детермінуючі фактори, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в інформаційній сфері, організацію та функціонування національного інформаційного простору загалом. Вони мають або можуть мати широкомасштабне значення, пов’язані з ризиками і небезпеками в інших сферах.

У підрозділі 4.3 *«Проблеми і напрями удосконалення нормативно-правової складової механізму забезпечення інформаційної безпеки української держави»* проведений науковий аналіз Доктрини інформаційної безпеки України дозволив нам встановити її техніко-юридичні недоліки, а саме: змістовні повторення, загальні формулювання, дублювання положень інших нормативно-правових актів. Крім того, виявлено й концептуальні недоліки цього доктринального документа: застосування вузького підходу до об’єктів механізму забезпечення інформаційної безпеки особи; наявність суперечностей та дублювання положень у переліку національних інтересів в інформаційній сфері; допущення повторень, неповноти переліку, термінологічної невизначеності при виділенні загроз інформаційній безпеці держави; викладення помилкового аналізу ситуації у сфері інформаційної безпеки держави; відсутність положень про спеціальні інформаційні операції.

Для забезпечення інформаційної безпеки України, особливо в умовах війни та гібридної агресії РФ, вкрай важливе значення має чітка регламентація проведення інформаційних операцій у мирний та воєнний час.

Тому існує нагальна потреба розробити комплексний нормативно-правовий акт щодо проведення спеціальних інформаційних операцій. На наш погляд, нормативно-правовий акт про інформаційні операції слід розробити за зразком американської доктрини «Інформаційні операції» (JP 3-13).

Нормативно-правова складова механізму забезпечення інформаційної безпеки конституційної держави Україна виконує низку завдань: від визначення організаційної будови цього механізму, регулювання діяльності його суб’єктів і до забезпечення законності його функціонування.

Основним напрямом удосконалення нормативно-правової складової такого механізму вважаємо систематизацію, яка дає змогу вирішити проблему термінологічної неузгодженості, усунути протиріччя між актами різної юридичної сили та забезпечить єдність нормативно-правового поля.

Видається доцільним також запропонувати розробити Кодекс про інформацію та інформаційну безпеку України, обов’язковими розділами якого мають бути: загальні положення (розкриваються основні поняття, сфера дії, визначаються суб’єкти, засади тощо); розділ, присвячений інформації, доступу до неї та її захисту; розділ, що регулює ІКТ та інформаційну інфраструктуру в

державі; розділ про кіберпростір; розділ щодо стратегії інформаційної безпеки; окремі розділи стосовно інформаційної безпеки особи, суспільства та держави.

У підрозділі 4.4. *«Інституційна складова забезпечення інформаційної безпеки української держави та її удосконалення в сучасних умовах»* з'ясовано вектор удосконалення конституційного та правового врегулювання проблемних питань, запропоновано реальні механізми для реформування існуючих механізмів та інституцій, запропоновано конкретні заходи для швидкого й ефективного нормотворення та усунення існуючих проблем.

Так, у законодавстві України регламентовані загрози національній безпеці України на сучасному етапі розвитку нашого суспільства і держави існують у зовнішньополітичній сфері, у сфері державної безпеки, у воєнній сфері та сфері безпеки державного кордону України, у внутрішньополітичній сфері, в економічній сфері, у соціальній та гуманітарній сферах, у науково-технологічній сфері, у сфері цивільного захисту, в екологічній сфері, в інформаційній сфері.

Безпосередньо детермінують посягання на інформаційну безпеку, так само як і на державний суверенітет, територіальну цілісність держави, України такі загрози, як претензії з боку інших держав світу, глобалізація світових відносин і зосередження важелів впливу на світові процеси в руках окремих осіб або груп, прояв сепаратизму і намагання автономізації за етнічною ознакою окремих регіонів України. Усі інші загрози національній безпеці України можуть прямо й не створювати небезпеки посягання, але тією чи іншою мірою підривають ці фундаментальні цінності держави та суспільства.

Слід підкреслити, що загрози інформаційній безпеці держав виходять за межі географічних їх кордонів, посягають на національний інформаційний простір, але можуть мати транскордонні чи глобальні негативні наслідки.

Отже, необхідність подальшого вивчення і розроблення чіткого поняття «загроза» є нагальною і має бути спрямована на формування ефективної й реальної системи моніторингу та управління загрозами, іншими ризиками для інформаційної безпеки держави.

З метою запобігання й протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання сучасної держави, з огляду на відповідні функції і завдання полягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, запобігати інформаційним конфліктам та оперативно їх долати. Враховуючи активну глобалізацію інформаційно-комунікаційних мереж, важливо не тільки державам, а й міжнародним організаціям долучатись до співпраці в напрямі протидії різноманітним видам інформаційної агресії.

ВИСНОВКИ

У дисертаційному дослідженні здійснено комплексну наукову розробку теоретико-методологічних та правових засад забезпечення інформаційної безпеки як функції сучасних держав. На основі порівняльно-правового аналізу міжнародно-правових актів та національного законодавства України, зарубіжного законодавства і досвіду виокремлено ряд моделей забезпечення інформаційної безпеки, а також їх особливості. Сформульовано пропозиції та рекомендації щодо удосконалення забезпечення інформаційної безпеки Української держави в умовах євроінтеграції, інтервенції та розвитку глобального інформаційного простору. Висновки, пропозиції та рекомендації щодо наукового й прикладного використання отриманих результатів вирішення наукової проблеми підтверджують актуальність теми. Основні ідеї дослідження такі:

1. Обґрунтовано теоретико-методологічні основи конституційно-правового забезпечення інформаційної безпеки та визначено, що активізація досліджень в інформаційній сфері в Україні в останніми роки зумовлена різними чинниками і факторами. Так, зокрема, спочатку прослідковувався науковий інтерес до проблематики інформації та інформаційного суспільства, згодом до інформаційної політики держави та інформаційних прав людини і громадянина, зрештою, і до інформаційної безпеки, кібербезпеки, інформаційної війни та і

н

ф Головним напрямом у реалізації функції держави із забезпечення інформаційної безпеки є захист інформаційної сфери особи та її прав у ній, але на сьогодні в системі центральних органів державної виконавчої влади України немає органу, відповідального за забезпечення інформаційної безпеки особи. У зв’язку з цим пропонуємо створити спеціальний, національний, колегіальний орган із захисту персональних даних – Національну комісію із захисту персональних даних. Її формування слід здійснити на засадах оптимізації, економічної доцільності, якісного технічного та кадрового забезпечення й широких повноважень. Основними завданнями цього органу мають бути: захист прав громадян у сфері персональних даних, регулювання захисту персональних даних, контроль та санкції, інформування та освіта.

2. Ґрунтуючись на методології системного підходу, охарактеризовано генезу наукових досліджень інформаційного суспільства та інформаційної безпеки, які зумовлені багатьма обставинами, тенденціями й закономірностями. Зокрема, акцентовано увагу на тому, що стрімкий розвиток інформаційно-комунікаційних технологій, доступ до інформаційних ресурсів, які постійно модернізуються, діджиталізація, а також створення, розповсюдження та маніпулювання інформацією, у протистояннях між державами та агресії з боку терористичних організацій застосовуються методи, засновані на інформаційних та комп’ютерних технологіях й інформаційно-психологічному впливі, електронних засобах масової інформації тощо. Використовуються різноманітні заходи, серед яких пропаганда, провокації, поширення неправдивої інформації «фейків», кібератаки,

н

ф

о

р

крадіжки персональної інформації та її поширення, розпалювання конфліктів у соціальних мережах або інформаційної (гібридної) війни, що має прихований і тривалий характер.

Розгляд інституційної складової механізму забезпечення інформаційної безпеки держави дає змогу встановити чотири спеціальних суб'єкти (Міністерство культури та інформаційної політики, Мінцифри, Держспецзв'язку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації) та чотири суб'єкти зі спеціальними повноваженнями щодо реалізації функції держави із забезпечення інформаційної безпеки (Міністерство оборони України, Міністерство закордонних справ України, Служба безпеки України, Департамент кіберполіції Національної поліції України).

3. Розкрито онтологічний, гносеологічний та аксіологічний аспекти підходів до вивчення функцій держави в сучасних умовах. Підкреслено, що загрози в інформаційній сфері стосуються інтересів людини, суспільства держави та світової спільноти. Тому жодна держава, включаючи Україну, не може стояти осторонь цих проблем. І серед напрямів їх діяльності таким чином виокремилась інформаційна функція держави або взагалі самостійна група функцій держави в інформаційній сфері. Інформаційна функція належить до основних функцій держави і становить сформований у сучасних умовах основний напрям її діяльності в інформаційній сфері, значення правового регулювання якого зумовлено об'єктивними процесами глобального та національного інформаційного розвитку, безпосередньо виражає і предметно конкретизує сутність сучасної держави – досягнення демократії, розвиток громадянського інформаційного суспільства, глобальних інформаційно-комунікативних технологій.

Головним напрямом у реалізації функції держави із забезпечення інформаційної безпеки є захист інформаційної сфери особи та її прав у ній, але на сьогодні в системі центральних органів державної виконавчої влади України немає органу, відповідального за забезпечення інформаційної безпеки особи. У зв'язку з цим пропонуємо створити спеціальний, національний, колегіальний орган із захисту персональних даних – Національну комісію із захисту персональних даних. Її формування слід здійснити на засадах оптимізації, економічної доцільності, якісного технічного та кадрового забезпечення й широких повноважень. Основними завданнями цього органу мають бути: захист прав громадян у сфері персональних даних, регулювання захисту персональних даних, контроль та санкції, інформування та освіта.

4. Розкрито систему інформаційної безпеки: поняття і правову природу, співвідношення інформаційної безпеки держави та інформаційної війни. Поряд з інформаційною функцією держави досліджено інформаційно-виховну функцію, інформаційно-комунікативну функцію держави, функцію забезпечення інформаційної безпеки тощо. Загалом проаналізовані нами монографічні, дисертаційні дослідження, інші наукові праці засвідчують неоднозначний підхід

авторів до функцій держави в інформаційній сфері. Слід підкреслити значний внесок у їх вивчення значної кількості сучасних учених – представників різних галузей юридичної науки (теорії держави і права, конституційного права, адміністративного та інформаційного права, цивільного і господарського права, міжнародного права), а також ряду інших галузей вітчизняної й зарубіжної науки. Насамперед, відзначимо наукові здобутки на цьому шляху О. Тихомирова, А. Пазюка, Т. Ткачука та багатьох інших вчених.

5. Надано поглиблену інтерпретацію співвідношення інформаційної безпеки з деякими іншими видами безпеки. Зважаючи на те, що перед вченими постало чимало питань, насамперед, стосовно доцільності виокремлення напряму державної політики у сфері забезпечення інформаційної безпеки України як самостійної функції або під функції, визначено, що функція забезпечення інформаційної безпеки становить передумову реалізації державної інформаційної політики України, захисту інформаційних прав і свобод людини та громадянина, захисту інформаційного суверенітету держави й загалом інформаційного простору.

6. Визначено основні принципи забезпечення державою інформаційної безпеки у контексті новел законодавства. Всебічний аналіз базової досліджуваної категорії – «інформаційна безпека» – дає можливість виокремити різні підходи до розуміння її природи і змісту. Найбільш поширеними з них є: діяльнісний (безпека як процес, її забезпечення, здатність держави ефективно здійснювати функції у цій сфері), статичний (безпека як стан захищеності інформаційного простору, інформації, інформаційного суспільства і система відповідних гарантій тощо), комплексний або змішаний (безпека як стан і процес).

7. Розкрито особливості правового регулювання забезпечення інформаційної безпеки як однієї з найважливіших функцій держави. Правове регулювання інформаційної безпеки в Україні, реалізація функції забезпечення інформаційної безпеки держави здійснюються на основі існуючих міжнародно-правових стандартів, Конституції України, Законів України «Про національну безпеку України» 2018 р., «Про Концепцію Національної програми інформатизації» 1998 р., «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» 2007 р., Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України», затвердженого Указом Президента України 2017 р., значної кількості інших нормативно-правових актів.

Так, згідно з існуючим законодавчим визначенням, інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Разом з тим, за ст. 17 Конституції України забезпечення інформаційної безпеки визнано однією з найважливіших функцій держави, справою всього Українського народу. Слід зазначити, що її реалізація, як і власне інформаційна безпека, мають міжгалузеву природу, що відображається у значному комплексі форм і методів, рівнів здійснення. Розкрито конституційно-правові та інші засади, особливості здійснення цієї функції держави в національному й міжнародному масштабі тощо.

З огляду на сучасний стан загроз інформаційній безпеці, удосконалено пріоритетні напрями державної політики у сфері забезпечення інформаційної безпеки України:

а) захист життєво важливих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз;

б) захист суверенітету, підтримка політичної та соціальної стабільності, територіальної цілісності України;

в) захист критичної інформаційної інфраструктури;

г) забезпечення розвитку інформаційно-комунікаційних технологій;

ґ) забезпечення участі України в міжнародній системі інформаційної безпеки.

Узагальнено позитивний зарубіжний досвід реалізації функції забезпечення інформаційної безпеки сучасних держав. Ґрунтовне вивчення зарубіжного досвіду реалізації функції забезпечення інформаційної безпеки сучасних держав дає змогу порівняти різні моделі забезпечення інформаційної безпеки. По-перше, європейська модель забезпечення інформаційної безпеки ґрунтується на профільному законодавстві ЄС, національних актах держав-учасниць. Основоположними документами ЄС у цій сфері є Закон ЄС «Про ENISA (Агентство Європейського Союзу з питань кібербезпеки) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013, Директива NIS від 06.07.2016 р. та Регламент захисту персональних даних (GDPR) та інші.

9. Охарактеризовано європейську модель забезпечення інформаційної безпеки сучасних держав. Моделі інформаційної безпеки Франції та Німеччини є ефективними, відповідають сучасним викликам та загрозам, які стоять перед національною безпекою цих країн. Їх розвинутість забезпечується ґрунтовним аналізом та стратегічними підходами, професійністю кадрів та усвідомленням провідної ролі найсучасніших ІКТ та інновацій. Головними суб’єктами захисту інформаційного та цифрового середовища Франції виступають Національне агентство безпеки інформаційних систем (ANSSI), CERT, COSSI, Вища рада аудіовізуальних засобів, Національна Комісія із захисту даних та свобод, Директорат з розвитку засобів масової інформації, Міністерство оборони, COMCYBER та Міністерство внутрішніх справ. У ФРН інформаційний захист держави насамперед здійснюється Федеральним відомством з безпеки в сфері інформаційних технологій (BSI), Національним центром кіберзахисту, відділом

інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки Бундесверу.

10. Визначено ознаки американської моделі забезпечення інформаційної безпеки сучасних держав. Американська модель забезпечення інформаційної безпеки засновується на Конституції США, більш ніж 500 федеральних законів та законів штатів, а також на низці стратегій та військових програм. Основними органами в системі забезпечення інформаційної безпеки США виступають: Агентство національної безпеки, Департамент внутрішньої безпеки, Міністерство оборони, Агентство з питань кібербезпеки та безпеки інфраструктури, Агентство оборонних інформаційних систем тощо. Система захисту американського кіберпростору ґрунтується на принципі багатосторонньої моделі управління Інтернетом, засадах відкритого, функціонально сумісного, надійного і безпечного Інтернету, принципі інвестування передових технологій, розвитку кадрового потенціалу та економічної обґрунтованості.

11. Проаналізовано азійську модель забезпечення інформаційної безпеки сучасних держав. Зокрема визначено, що китайська модель інформаційної безпеки є прикладом негативної державної політики у сфері інформації, адже заснована на тотальному державному контролі та цензурі. У КНР діє програма «Золотий щит». За її допомогою здійснюється маніпулювання громадською думкою, інтернет-цензура та контроль за ІТ компаніями та користувачами. Закон про кібербезпеку КНР несе ризики для компаній, які працюють у сфері ІКТ, в аспекті комерційного шпіонажу, кіберзлочинності та залежності від китайських спецслужб. У свою чергу, модель забезпечення інформаційної безпеки РФ засновується на державному патерналізмі та консерватизмі, що означає постійне посилення державного контролю за виробниками ІКТ та інформаційним простором країни, попри декларацію тріади інтересів держави, суспільства та особи в інформаційному середовищі. Основними законодавчими актами РФ у цій сфері є Федеральний Закон «Про інформацію, інформаційні технології та про захист інформації» та Доктрина інформаційної безпеки РФ. Головними суб'єктами реалізації інформаційної політики є Мінкомзв'язку та Роскомнагляд. Саме останній має широкі повноваження по блокуванню сайтів та акаунтів, порушенню адміністративних справ проти ІТ компаній та організаторів поширення інформації, відкликанню ліцензій у ЗМІ, теле- та радіокомпаній, веденню реєстрів інформації тощо.

12. Обґрунтовано шляхи наповнення новим змістом інституційної складової забезпечення інформаційної безпеки української держави та її удосконалення в сучасних умовах. Загалом різноманітність трактувань базових понять у сфері інформаційної безпеки породжує концептуальну невизначеність щодо реалізації функції держави із забезпечення інформаційної безпеки як на теоретичному, так і на нормативно-правовому рівнях. Для ефективної реалізації та вдосконалення цієї функції законодавцю варто визначитися з концепцією механізму забезпечення інформаційної безпеки держави. Пропонуємо

розглядати механізм забезпечення інформаційної безпеки як регламентовану законодавством діяльність уповноважених суб'єктів, спрямовану на охорону та захист інформаційної сфери особи, суспільства та держави від зовнішніх і внутрішніх загроз та удосконалення заходів інформаційної протидії та боротьби. Наведена дефініція охоплює ключові елементи механізму забезпечення інформаційної безпеки: об'єкт, суб'єкт, загрози, напрями, заходи. Об'єкти механізму забезпечення інформаційної безпеки у найзагальнішому розумінні – це предмети, явища, процеси та особи, на які здійснюється інформаційний вплив та щодо яких здійснюються заходи із забезпечення безпеки. Їх можна розділити на соціальні (особа, суспільство, держава, їх інтереси, права та свідомість) та технічні (інформація, інформаційна інфраструктура, інформаційні технології тощо).

Аналіз Доктрини інформаційної безпеки України дає змогу встановити її техніко-юридичні недоліки, а саме: змістовні повторення, загальні формулювання, дублювання положень інших нормативно-правових актів. Крім того, виявлено й концептуальні недоліки цього доктринального документа: застосування вузького підходу до об'єктів механізму забезпечення інформаційної безпеки особи; наявність суперечностей та дублювання положень у переліку національних інтересів в інформаційній сфері; допущення повторень, неповноти переліку, термінологічної невизначеності при виділенні загроз інформаційній безпеці держави; викладення помилкового аналізу ситуації у сфері інформаційної безпеки держави; відсутність положень про спеціальні інформаційні операції.

13. Визначено загрози інформаційній безпеці: проблеми визначення та подолання. Для забезпечення інформаційної безпеки України в умовах гібридної агресії РФ вкрай важливе значення має чітка регламентація проведення інформаційних операцій у мирний та воєнний час. Тому існує потреба в розробленні комплексного нормативного акту щодо проведення спеціальних інформаційних операцій. На наш погляд, нормативно-правовий акт про інформаційні операції слід розробити за зразком американської доктрини «Інформаційні операції» (JP 3-13).

Нормативно-правова складова механізму забезпечення інформаційної безпеки конституційної держави Україна виконує низку завдань: від визначення організаційної будови цього механізму, регулювання діяльності його суб'єктів та до забезпечення законності його функціонування. Основним напрямом удосконалення нормативно-правової складової цього механізму вважаємо систематизацію, яка дасть можливість вирішити проблему термінологічної неузгодженості, усунути протиріччя між актами різної юридичної сили та забезпечить єдність нормативно-правового поля.

14. Окреслено напрями удосконалення механізмів забезпечення інформаційної безпеки держави на теоретичному та законодавчому вимірі. Видається доцільним розробити Кодекс про інформацію та інформаційну безпеку України, обов'язковими розділами якого мають бути: загальні положення

(розкриваються основні поняття, сфера дії, визначаються суб'єкти, засади тощо); розділ, присвячений інформації, доступу до неї та її захисту; розділ, що регулює ІКТ та інформаційну інфраструктуру в державі; розділ про кіберпростір; розділ щодо стратегії інформаційної безпеки; окремі розділи стосовно інформаційної безпеки особи, суспільства та держави.

Аналіз законопроекту про протидію дезінформації як напряму удосконалення нормативно-правової складової механізму забезпечення інформаційної безпеки держави свідчить про неприйнятність доповнень КК України новими складами злочинів у сфері дезінформації, з огляду на велику кількість ризиків для зловживань, переслідувань та цензури. Водночас пропонуємо внести в законодавство України зміни і доповнення щодо закріплення порядку реалізації права на забуття в Інтернеті.

Першочерговим заходом протидії інформаційним впливам РФ має стати модернізована система контрпропагандистської діяльності. Компонентами ефективної протидії реалізації проекту «руський мір» вважаємо розроблення національної ідеї з урахуванням сучасних викликів та приділення уваги захисту релігійних цінностей та українських національних традицій. Велика популярність соціальних мереж і блогосфери, їх активне використання з метою пропаганди, дезінформації чи втручання в політичні процеси держави зумовлюють необхідність установити засади їх правового регулювання. Зокрема, видається важливим розпочати суспільне обговорення можливостей регулювання діяльності з ведення блогів політичної тематики. На наш погляд, перспективним є механізм оподаткування онлайн-медіа ресурсів та діяльності, пов'язаної з їх використанням, а також державного нагляду за діяльністю політичних блогерів, які мають велику аудиторію (від 100 тис. підписників) тощо.

За результати дослідження сформульовано пропозиції і рекомендації стосовно внесення змін і доповнень до значної кількості нормативно-правових актів України, напрямів, форм і методів діяльності відповідних суб'єктів реалізації функції держави із забезпечення інформаційної безпеки.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Монографії

1. Шемчук В.В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльний аналіз: монографія: Київ: Ліра-К, 2020. 351с.
2. Ткачук П.П., Гула Р.В., Сивак О.І., Щурко О.М., Шемчук В.В. Інформаційна війна і національна безпека: монографія. Львів.: НАСВ, 2015. 265 с.

Статті в наукових фахових виданнях України з юридичних наук, у т. ч. тих, які зареєстровані у міжнародних наукометричних базах

1. Шемчук В. В. Конституційно-правові засади розвитку інформаційного суспільства в Україні. *Науковий вісник Національної*

академії внутрішніх справ. 2018. № 3. С. 133–144. URL:http://nbuv.gov.ua/UJRN/Nvknuvs_2018_3_13.
2. Шемчук В. В. Інформаційна функція та її місце в системі функцій сучасної держави. *Вчені записки Таврійського національного університету імені В.І.Вернадського. Серія: «Юридичні науки».* 2018. Т. 29(68), № 4. С. 39–45. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_4_9.
3. Шемчук В.В. Соціально-правова природа інформаційного суспільства. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: «Юридичні науки».* 2018. Т. 29(68). № 3. С. 109–113. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_3_21.
4. Шемчук В.В. Комплекс наукових підходів визначення сутності інформаційного протиборства в сучасних умовах. *Науково-практичний журнал «Наше право».* 2018. №1. С.117–121.
5. Шемчук В.В. Теоретико-правові засади дослідження інформаційної безпеки. *Науково-практичний журнал «Європейські перспективи».* 2019. №2. С.5–11.
6. Шемчук В. В. Тенденції і напрями міжнародно-правового регулювання інформаційної сфери. *Вісник Південного регіонального центру Національної академії правових наук України.* 2019. № 19. С. 106–114. URL: http://nbuv.gov.ua/UJRN/vprc_2019_19_17.
7. Шемчук В.В. Захист інтернет-середовища як складова інформаційної безпеки держави: досвід Франції. *Науковий вісник УжНУ. Серія «Право».* 2019. №57. С.49-53.
8. Шемчук В.В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктриний законодавчої основи. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: «Юридичні науки»*. 2019. Т. 30 (69). № 4. С. 31–37. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2019_30(69)_4_8.
9. Шемчук В.В. Концептуальні підходи розуміння інформаційної війни в сучасному світі. *Вчені записки Таврійського національного університету ім. В.І.Вернадського. Серія: «Юридичні науки».* Том 30 (69). № 3. 2019. С.29–35.
10. Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Електронне наукове фахове видання «Порівняльно-аналітичне право».* 2019. № 2. С.34–40.
11. Шемчук В.В. Основні напрями міжнародного співробітництва у сфері кібербезпеки. *Вчені записки Таврійського національного університету імені В.І.Вернадського. Серія: «Юридичні науки»*. 2018. Т. 29(68). № 2. С. 125–130. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_2_24
12. Шемчук В.В. Принципи забезпечення інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України.* 2018. № 4. С. 50–56. URL: http://nbuv.gov.ua/UJRN/Nzizvru_2018_4_10.
13. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки Таврійського національного університету*

імені В. І. Вернадського. Серія: «Юридичні науки». 2018. Т.29 (68). № 6. С. 119–124. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_6_23.

14. Шемчук В.В. Проблеми концептуального визначення свободи інформації. *Міжнародний науковий журнал «Верховенство права».* 2019. №1. С.36–41. (Кишинев, Молдова).

15. Шемчук В.В. Глобальне інформаційне суспільство: основні підходи та сутнісні характеристики. *Міжнародний науковий журнал «Верховенство права».* Кишинев, Молдова, 2019. № 2. С. 177–183.

16. Шемчук В.В. Роль і значення інформаційної функції держави у сучасних умовах. *The scientific heritage.* 2019. No 33. URL: file:///C:/Users/user/Downloads/1602489241118224.pdf (Угорщина).

17. Шемчук В.В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. *Філософські та методологічні проблеми права.* 2019. № 1. С. 51–59. URL: http://nbuv.gov.ua/UJRN/Fmpp_2019_1_8.

18. Shemchuk V. National cyber strategy of the United States of America: experience for Ukraine. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник НАВС.* 2019. №.4. С.31–37.

19. Шемчук В.В. Економічна та інформаційна безпека держави: правові аспекти співвідношення. *Актуальні проблеми держави і права.* 2019. Вип. 83. Одеса. С. 253–259.

20. Шемчук В.В. Азіатська модель забезпечення інформаційної безпеки сучасних держав. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2019. Вип. 4. С. 67–80. URL: http://nbuv.gov.ua/UJRN/Vlduvs_2019_4_8.

21. Шемчук В.В. Загрози інформаційній безпеці: проблеми визначення і подолання. *Експерт: парадигми юридичних наук і державного управління.* 2020. №1. С.285–296.

22. Шемчук В.В. Проблеми визначення свободи інформації і її реалізація на тимчасово окупованій території України. *Ukrainian journal of inetnational law.* 2019. №2. С. 46–49.

23. Шемчук В.В. Комунікативна чи інформаційна функція сучасної держави. Visegrad Journal on Human Rights.2019. №4. (Т.1). С. 182-187.

Тези конференцій, які засвідчують апробацію матеріалів дисертації:

1. Шемчук В.В. Інформаційне протиборство та кіберзлочинність як основні загрози безпеці держави. *Інформаційна агресія Російської Федерації проти України: матер. наукового семінару, 25 жовтня 2018 р.* Харківський національний університет Повітряних Сил імені Івана Кожедуба. Харків, 2018. С. 33-35. URL: http://www.hups.mil.gov.ua/nauka/konferencii-kursantiv-ta studentiv/informacijna-agresiya-rf-proti-ukraini/

2. Шемчук В.В. Інституційний механізм забезпечення інформаційної безпеки України та сталого розвитку інформаційного суспільства. *Стан та перспективи реформування сектору безпеки і оборони України: Матеріали міжнародної*

науково-практичної конференція, 30 листопада 2018 року. С. 560–562. URL: http://www.indo.knu.ua/index.php/ua/.
3. Шемчук В.В. Проблеми впорядкування термінологічного апарату у сфері інформаційної безпеки. *Українська мова в юриспруденції: стан, проблеми, перспективи: матеріали XV Всеукр. наук.-практ. конф. (Київ, 28 листопада 2019 р.).* Київ : Нац. акад. внутр. справ, 2019. Ч. 1. С. 234–236.
4. Шемчук В.В. Конституційна та правова держава в умовах сучасних реформ: теоретичні і практичні проблеми. *Верховенство права як гарантія конституційного ладу: Матер. науково-практичного круглого столу (м. Київ, 5 грудня 2019 р.).* Київ. 2019. С.179–181.
5. Шемчук В.В. Засади забезпечення прав людини в умовах кіберзагроз. *Стан дотримання прав людини в умовах сучасності: теоретичні та практичні аспекти: Матеріали VIII Всеукраїнської науково-практичної конференції (м. Київ, 22 березня 2018 р.)*. Київ. 2018. С. 424–426.
6. Шемчук В.В. Концепція «мережецентричної війни» та її застосування при веденні бойових дій. *Сучасна війна: гуманітарний аспект. Матер. науково-практичної конференції (Харківський національний університет Повітряних сил імені Івана Кожедуба, 31 травня – 1 червня 2018 року).* Харків. 2018. С. 90–96.
7. Шемчук В.В. Проблеми забезпечення національного інформаційного суверенітету в умовах агресії Російської Федерації. *Невідкладні заходи з протидії російській агресії в Криму: політичні, юридичні, економічні, управлінські та соціальні аспекти: матеріали науково-практичної конференції (4 вересня 2018 р., м. Київ).* Представництво Президента України в АРК. Київ-Одеса. Фенікс. 2018. С. 160–164.

АНОТАЦІЇ

Шемчук В.В. Конституційно-правове забезпечення інформаційної безпеки

Дисертація на здобуття наукового степеня доктора юридичних наук зі спеціальності 12.00.02 – конституційне право; муніципальне право (081 — Право). – Державний вищий навчальний заклад «Ужгородський національний у

н Дисертацію присвячено дослідженню теоретичних і практичних питань ізабезпечення інформаційної безпеки як функції сучасних держав. На основі норівняльно-правового аналізу міжнародно-правових актів та національного законодавства України, зарубіжного законодавства і досвіду виокремлено ряд моделей забезпечення інформаційної безпеки, а також їх особливості. Сформульовано пропозиції та рекомендації щодо удосконалення забезпечення інформаційної безпеки Української держави в умовах євроінтеграції, інтервенції та розвитку глобального інформаційного простору.

е Головним напрямом у реалізації функції держави із забезпечення інформаційної безпеки є захист інформаційної сфери особи та її прав у ній, але на сьогодні в системі центральних органів державної виконавчої влади України

Ужгород, 2020.

немає органу, відповідального за забезпечення інформаційної безпеки особи. Тому пропонуємо створити спеціальний національний, колегіальний орган із захисту персональних даних – Національну комісію із захисту персональних даних. Її формування слід здійснити на засадах оптимізації, економічної доцільності, якісного технічного та кадрового забезпечення й широких повноважень. Основними завданнями цього органу мають бути: захист прав громадян у сфері персональних даних, регулювання захисту персональних даних, контроль та санкції, інформування та освіта.

Першочерговим заходом протидії інформаційним впливам РФ має стати модернізована система контрпропагандистської діяльності. Компонентами ефективної протидії реалізації проекту «руський мір» вважаємо розроблення національної ідеї з урахуванням сучасних викликів та приділення уваги захисту релігійних цінностей та українських національних традицій. Велика популярність соціальних мереж і блогосфери, їх активне використання з метою пропаганди, дезінформації чи втручання в політичні процеси держави, зумовлюють необхідність установити засади їх правового регулювання. Зокрема, видається важливим розпочати суспільне обговорення можливостей регулювання діяльності з ведення блогів політичної тематики. На наш погляд, перспективним є механізм оподаткування онлайн-медіа ресурсів та діяльності, пов'язаної з їх використанням, а також державного нагляду за діяльністю політичних блогерів, які мають велику аудиторію (від 100 тис. підписників) тощо.

За результати дослідження сформульовано пропозиції і рекомендації стосовно внесення змін і доповнень до значної кількості нормативно-правових актів України, напрямів, форм і методів діяльності відповідних суб'єктів реалізації функції держави із забезпечення інформаційної безпеки.

Ключові слова: *безпека, інформаційна безпека, інформаційне право, інформаційні правовідносини, загрози, інформаційна політика, інформаційне законодавство, конституційне право, кібербезпека, кіберзагрози, порівняльний аналіз, євроінтеграція.*

Шемчук В.В. Конституционно-правовое обеспечение информационной безопасности современных государств: сравнительно-правовой анализ**.** – **Рукопись.**

Диссертация на соискание ученой степени доктора юридических наук по специальности 12.00.02 – конституционное право; муниципальное право (081 - право). – Государственное высшее учебное заведение «Ужгородский национальный университет», Ужгород, 2020.

Диссертация посвящена исследованию теоретических и практических вопросов обеспечения информационной безопасности как функции современных государств. На основе сравнительно-правового анализа международно-правовых актов и национального законодательства Украины, зарубежного законодательства и собственного опыта выделены ряд моделей

обеспечения информационной безопасности, а также их особенности. Сформулированы предложения и рекомендации по совершенствованию обеспечения информационной безопасности Украинского государства в условиях евроинтеграции, интервенции и развития глобального информационного пространства.

Главным направлением в реализации функции государства по обеспечению информационной безопасности является защита информационной сферы человека и его прав в ней, но сегодня в системе центральных органов исполнительной власти Украины отсутствует орган, ответственный за обеспечение информационной безопасности личности. В связи с чем предлагаем создать специальный национальный, коллегиальный орган по защите персональных данных – Национальную комиссию по защите персональных данных. Ее формирование следует осуществить на основе оптимизации, экономической целесообразности, качественного технического и кадрового обеспечения и широких полномочий. Основными задачами этого органа должны быть: защита прав граждан в сфере персональных данных, регулирования защиты персональных данных, контроль и санкции, информирование и образование.

Первоочередной мерой противодействия информационным воздействиям РФ должна стать модернизированная система контрпропагандистской деятельности. Компонентами эффективного противодействия реализации проекта «русский мир» считаем разработку национальной идеи с учетом современных вызовов и уделение внимания защите религиозных ценностей и украинских национальных традиций. Большая популярность социальных сетей и блогосферы, их активное использование в целях пропаганды, дезинформации или вмешательства в политические процессы государства предопределяет необходимость установления основ их правового регулирования. В частности, представляется важным начать общественное обсуждение возможностей регулирования деятельности по ведению блогов политической тематики. На наш взгляд, перспективным является механизм налогообложения онлайн-медиа ресурсов и деятельности, связанной с их использованием, а также государственного надзора за деятельностью политических блогеров, имеющих большую аудиторию (от 100 тыс. подписчиков), и др.

Анализ Доктрины информационной безопасности Украины позволил установить ее технико-юридические недостатки, а именно: содержательные повторения, общие формулировки, дублирование положений других нормативно-правовых актов. Кроме того, обнаружены и концептуальные недостатки этого доктринального документа: применение узкого подхода к объектам механизма обеспечения информационной безопасности личности; наличие противоречий и дублирования положений в перечень национальных интересов в информационной сфере; допущение повторений, неполноты перечня, терминологической неопределенности при выделении угроз информационной безопасности государства; изложения ложного анализа

ситуации в сфере информационной безопасности государства; отсутствие положений о специальных информационные операции.

Для обеспечения информационной безопасности Украины, в условиях гибридной агрессии РФ крайне важное значение имеет четкая регламентация проведения информационных операций в мирное и военное время. Поэтому существует потребность в разработке комплексного нормативного акта о проведении специальных информационных операций. На наш взгляд, нормативно-правовой акт об информационных операции следует разработать по образцу американской доктрины «Информационные операции» (JP 3-13).

Нормативно-правовая составляющая механизма обеспечения информационной безопасности конституционного государства Украина выполняет ряд задач: от определения организационного строения этого механизма, регулирования деятельности его субъектов и к обеспечению законности его функционирования. Основным направлением совершенствования нормативно-правовой составляющей указанного механизма считаем систематизацию, которая позволит решить проблему терминологической несогласованности, устранить противоречия между актами различной юридической силы и обеспечить единство нормативно-правового поля.

По результатам исследования сформулированы предложения и рекомендации по внесению изменений и дополнений к значительному количеству нормативно-правовых актов Украины, направлений, форм и методов деятельности соответствующих субъектов реализации функции государства по обеспечению информационной безопасности.

Ключевые слова: *безопасность, информационная безопасность, информационное право, информационные правоотношения, угрозы, информационная политика, информационное законодательство, конституционное право, кибербезопасность, киберугрозы, сравнительный анализ, евроинтеграция.*

Shemchiuk V. V. Constitutional and legal support of information security of modern states : The doctoral dissertation for Doctor in Law scientific degree on a specialty 12.00.02 - Constitutional law; Municipal law (081 - Law). - State Higher Educational Institution “Uzhhorod National University”, Uzhhorod, 2020.

The dissertation is dedicated to the study of theoretical and practical issues related to information security as a function of modern states. Based on the comparative legal analysis of both international legal acts and national legislation of Ukraine, foreign legislation and experience, several information security models as well as their features are identified. The suggestions and recommendations for improving the information security of the Ukrainian state in the context of European integration, intervention and development of the global information space have been stated.

The main area in the implementation of the information security state function is the protection of the information field of a person and his or her rights in it, but today

:

co

there is no body responsible for information security in the system of central bodies of state executive power of Ukraine. Therefore, we propose to establish a specialized, national, collegial body for personal data protection - the National Commission for Personal Data Protection. Its establishment should be carried out based on optimization, economic feasibility, quality technical and personnel support as well as wide powers. The main tasks of this body should be as follows: protection of the rights of citizens in the field of personal data, regulation of personal data protection, control and sanctions, information and education.

A priority measure to counteract Russia's informational influences should become a modernized system of counter-propaganda activities. We believe that the development of a national idea taking into account modern challenges and focusing on the protection of religious values and Ukrainian national traditions should be the components of effective counteraction to the implementation of the "Russkyi Mir" project. The great popularity of social networks and the blogs, their active use for propaganda, misinformation or interference in the political processes of the state, lead to the necessity of the establishment of their legal regulation principles. In particular, it is essential to start a public discussion on the possibilities of regulating political blogging. In our point of view, the mechanism of taxation of both online media resources and activities related to their use, as well as state supervision over the activities of political bloggers, having a large audience (from 100 thousand subscribers), etc., seems the most advanced.

According to the study results, the suggestions and recommendations concerning changes and amendments to a large number of legal acts of Ukraine as well as areas, forms and methods of the activities of relevant state bodies in the field of provision of state functions on information security have been stated.

Keywords:

Підписано до друку 16.11.2020. Формат 60x90/16. Папір офсетний.
Друк цифровий. Умовн. друк. арк. 1,8. Тираж 100 прим. Зам. № 2/16-11.
Видавництво УжНУ «Говерла».
88000, м. Ужгород, вул. Капітульна, 18.
Телефон +38 (095) 212 7679