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

Кваліфікаційна наукова праця

на правах рукопису

Шемчук Віктор Вікторович

УДК 342.5: 351.862.4

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

Спеціальність 12.00.02 – конституційне право; муніципальне право
(081 — Право)

Подається на здобуття наукового ступеня **доктора юридичних наук**

за спеціальністю 12.00.02 — конституційне право; муніципальне право (081 — Право)

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ В.В. Шемчук

Науковий консультант:

доктор юридичних наук, професор

Федоренко Владислав Леонідович

Ужгород – 2020

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACERT – Армійський центр реагування на загрози інформаційної безпеки США

ANSSI, Agence nationale de le sécurité des systèmes d'information – Національне агентство безпеки інформаційних систем Франції

BSI, Bundesamt für Sicherheit in der Informationstechnik – Федеральне відомство з безпеки в сфері інформаційних технологій Німеччини

CISA, The Cybersecurity and Infrastructure Security Agency – Агентство з питань кібербезпеки та безпеки інфраструктури» США

CSA, Conseil supérieur de l'audiovisuel – Вища рада аудіовізуальних засобів

COSSI, Centre Opérationnel de la Sécurité des Systemes d'Information – Оперативний центр безпеки інформаційних систем Франції

CNIL, Nationale Informatique et Libertés – Національна Комісія захисту даних та свобод

Cyber-AZ, Cyber-Abwehzentrum – Національний центр кіберзахисту Німеччини

DDM, Direction du developpement des medias – Директорат з розвитку засобів масової інформації

DINUM, La direction interministérielle du numérique – Міжвідомче управління з цифрових технологій

DISA, Defense Information Systems Agency – Агентство оборонних інформаційних систем (Міністерства оборони США

DISIC, Direction interministerielle des systemes d'information et de communication – Міжвідомчий директорат з питань інформаційних систем та зв'язку

ENISA, European Network and Information Security Agency – Агентство Європейського Союзу з питань кібербезпеки

FISMA – Федеральний закон США «Про управління інформаційною безпекою» 2014 р.

GDPR, General Data Protection Regulation – Загальний регламент про захист даних

JTF-CNO1, Joint Task Force for Computer Network Operations – Об'єднаний центр забезпечення роботи комп'ютерних мереж США

MISO, Military Information Support Operations – військові операції

NCCIC – Національний центр кібербезпеки та інтеграції комунікацій США

NIS, Network and Information Security Directive – Директива мережевої та інформаційної безпеки

NPPD, National Protection and Programs Directorate – ініціатива Національного захисту та управління програмами

NIST – Національний інститут стандартів і технологій США

NSA / CSS – Агентство національної безпеки/ Центральна служба безпеки США

NSC – Рада національної безпеки США

OMB, Office of Management and Budget – Офіс управління та бюджету США

SGDSN, Secretariat general de la defense et de la securite nationale – Генеральний секретаріат оборони та національної безпеки

SGG, Secretariat general du gouvemement – Генеральний секретаріат уряду Франції

US-CERT, Computer Emergency Response Team – Команда екстреного реагування на кіберінциденти США

АРК – Автономна Республіка Крим

ВКРЕ – Всесвітня конференція з розвитку електрозв'язку

ВОІВ – Всесвітня організація інтелектуальної власності

ВСІТ – Всесвітній конгрес інформаційних технологій

ГА ООН – Генеральна Асамблея ООН

ГІ – Глобальна інформаційна інфраструктура

Держспецзв'язок – Адміністрація Державної служби спеціального зв'язку та захисту інформації України

ЄвроДІГ – Європейський регіональний форум з управління Інтернетом

ЄКПЛ – Європейська конвенція про захист прав людини та основоположних свобод

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

ЗМІ – засоби масової інформації

ЗМК – засоби масової комунікації

ІБ – інформаційна безпека

ІКТ – інформаційно-комунікаційні технології

Інфосфера – інформаційна сфера

ІО – інформаційні операції

Кабмін, Уряд – Кабінет Міністрів України

Кібербезпека – кібернетична безпека

КК України – Кримінальний кодекс України;

КНР – Китайська Народна Республіка

Міносвіти – Міністерство освіти і науки України

Мінцифри – Міністерство цифрової трансформації України

Мін'юст – Міністерства юстиції України

ОБСЄ – Організація з безпеки та співробітництва в Європі

ОЕСР – Організація економічного співробітництва та розвитку

ООН – Організація Об'єднаних Націй

ПАРЄ – Парламентська Асамблея Ради Європи

РЄ – Рада Європи

РНБО – Рада національної безпеки і оборони України

Роскомнагляд – Федеральна служба по нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій РФ

СБУ – Служба безпеки України

РФ – Російська Федерація

СНД – Співдружність незалежних держав

Стратегія – Стратегія національної безпеки України, введена у дію Указом Президента № 287/2015 від 26.05.2015 р.

США – Сполучені Штати Америки

ФБР – Федеральне бюро розслідувань США

ФКК – Федеральна комісія з комунікацій США

ФУІ – Форум з управління Інтернетом

ЦГДІ – Цільова група з дослідження Інтернету

ШОС – Шанхайська організація співробітництва

ЮНЕСКО – Організація Об’єднаних Націй з питань науки, культури і освіти.

ВСТУП

Актуальність теми дослідження. З моменту проголошення незалежності України, а потім – прийняття Конституції України правники здійснюють пошук оптимальної моделі розбудови держави як суверенної і незалежної, демократичної, соціальної, правової держави. Реалізація такої моделі можлива лише в державі, де суверенітет поширюється на всю її цілісну і недоторкану територію в межах існуючого кордону.

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 визнається одним із напрямів державної політики у сфері національної безпеки та оборони. Так само і в Законі України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 р. інформаційна безпека називається невід’ємною частиною політичної, економічної, оборонної та інших складових національної безпеки, але саме поняття не деталізується.

Відзначимо, що останніми роками пожвавився інтерес до цієї проблематики. Це стало особливо помітно на тлі загострення глобального протистояння супердержав, реальної військової загрози територіальній цілісності України, непорушності її державних кордонів, непохитності її конституційного ладу, загрозам національній безпеці через військову інтервенцію, війни з Росією та анексією значної частини української території. Це знайшло своє відображення у значній кількості наукових досліджень, результатом яких є надруковані праці вчених різних галузей сучасної науки.

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» (А. Дорошкевич, В. Горбулін, О. Жайворонок, О. Литвиненко, Є. Магда, С. Максимов, Г. Сасин, Т. Черненко, Г. Яворська та ін.), інформаційних війн та інших форм інформаційного протиборства (В. Алещенко, В. Бебек, Ю. Горбань, І. Грабчук, Р. Гула, Д. Коваль, С. Любарський Я. Малик, Г. Почецов, В. Сербін, Є. Скулиш, О. Сивак, П. Ткачук, В. Хорошко, О. Щурко та ін.), проблем інформаційної безпеки в Україні (О. Баранов, О. Довгань, Д. Безуглий, І. Боднар, І. Валюшко, А. Гальчинський, М. Дмитренко, М. Желіховський, О. Зозуля, Н. Камінська, Б. Кормич, Ф. Медвідь, В. Ліпкан, О. Логінов, Ю. Максименко, Є. Мануйлов, Л. Наливайко, А. Нашинець-Наумова, О. Семченко, В. Петрик, П. Біленчук, Л. Борисова, І. Неклонський, О.Дзьобань, В. Богуш, О. Юдін, О. Сорокін, Т. Перун, В. Пилипчук, О. Ніщименко, О. Олійник, Г. Ситник, О. Тихомиров, Т. Ткачук, В. Фатхутдінов, А. Шумка та ін.).

Спочатку дослідники вдавались до вивчення переважно проблематики національної безпеки (В. Барчук, В. Горбулін, Ю. Ірхін, І. Каріх, А. Рубан, М. Пендюра, З. Чуйко, А. Ковальчук, В. Антонов, С. Чумаченко та ін.), меншою мірою, зокрема, до прийняття спеціального законодавства, кібернетичної безпеки та кіберпростору (М. Грайворонський, П. Демченко, Д. Дубов, І. Діордіца, М. Ожеван, Н. Савінова, І. Сопілко та ін.).

За останні десятиріччя вивчаються різноманітні аспекти становлення та функціонування інформаційного суспільства національного або міжнародного масштабу (Д. Андреєв, О. Задорожній, В. Кір'ян, О. Кирилюк, В. Скалацький, Н. Кушакова-Костицька, М. Гуцалюк, М. Дімчогло, В. Залізняк, І. Кисарець, О. Копан, Б. Кормич, П. Матвієнко, Г. Несвіт, А. Новицький та ін.); державної інформаційної політики та національного інформаційного суверенітету (І. Арістова, В. Горовий, О. Джураєва, О. Джус, В. Попик, А. Селіванов, Д. Севрюков, О. Скрипнюк, Л. Рябовол, В. Ковтун, Н. Пархоменко, Є. Стрельцов); проблеми розвитку інформаційного права та інформаційного законодавства (К. Череповський, В. Цимбалюк, В. Гавловський, В. Гриценко, А. Марущак, М. Швець, Р. Калюжний, П. Мельник та ін.).

З-поміж досліджень, присвячених правам та свободам людини і громадянина, сучасних закономірностей їх розвитку і механізмів забезпечення, охорони й захисту, прослідковуються тенденції до виокремлення інформаційних прав і свобод людини і громадянина, прав людини онлайн (В. Брижко, К. Бєляков, А. Іщенко, Л. Вакарюк, Т. Костецька, А. Марущак, В. Політанський, О. Золотар, О. Марцеляк, А. Олійник, О. Фрицький, Т. Проценко, В. Нестерович, К. Полетило, Н. Ткачук, В. Федоренко та ін.).

Окремо доцільно виокремити акцент дослідників на питаннях захисту персональних даних, інформаційних баз даних, доступу до інформації, інформації з обмеженим доступом, публічної та інших видів інформації (В. Баскаков, І. Берназюк, І. Кушнір, Л. Рудник, О. Нестеренко, Є. Теплюк, А. Пазюк, О. Волох, І. Забара, О. Стрельченко та ін.).

На нашу думку, згадані вище пріоритетні напрями сучасних наукових досліджень базуються на ґрунтовних теоретичних працях, концептуальних методологічних та інших розробках. Звісно, навряд чи можливо всебічно вивчити, враховуючи різноманітні сутнісні ознаки, критерії класифікації, об'єктно-суб'єктні характеристики, джерельну основу, функціональні та інші аспекти без здобутків учених – представників теорії держави і права, філософії права. Тут варто відзначити науковий доробок О. Балинської, С. Бобровник, Б. Бабіна, М. Баймуратова, І. Біласа, С. Бостана, С. Головатого, С. Гусарєва, М. Костицького, М. Козюбри, В. Забігайла, О. Лощихіна, Н. Оніщенко, О. Петришина, Н. Пронюк, Т. Подорожньої, О. Скакун, О. Тихомирова, О. Фатхутдінової, Н. Шаптали, А. Шевченка та інших учених.

Функції сучасної держави неодноразово розглядали представники різних галузей вітчизняної й зарубіжної науки. Водночас варто підкреслити, що основні напрями забезпечення національної, інформаційної, економічної, екологічної та інших видів безпеки поступово утвердились як об'єкти міжгалузевого, міждисциплінарного наукового аналізу. Цьому сприяли і виклики сучаснго цивілізаційного розвитку, в тому числі гібридні.

Підтримуємо позиції деяких науковців у контексті становлення вітчизняного й зарубіжного конституціоналізму, першочергових завдань щодо забезпечення конституційного ладу, територіальної цілісності й непорушності державних кордонів України, забезпечення прав і свобод людини і громадянина, принципів правової незалежної, демократичної унітарної і соціальної держави. Такі завдання конституційної держави зумовлюють необхідність дослідження засад і механізму її конституційної безпеки, конституційних деліктів і конституційної відповідальності, деяких інших конституційних та інших правових інститутів, галузей. Відзначимо значну існуючу основу для подальших розвідок на цьому шляху, зокрема, науковий доробок М. Гультая, Ю. Барабаша, Ю. Бауліна, А. Головіна, В. Городовенка, А. Селіванова, І. Сліденка, Ю. Волошина, Я. Берназюка, М. Оніщука, В. Демиденка, В. Кампа, А. Колодія, Н. Мяловицької, І. Магновського, Р. Губаня,

О. Ярмиша, О. Батанова, А. Крусян, П. Мартиненка, О. Совгирі, В. Шаповала, А. Янчука та інших дослідників.

Безумовно, не можна не згадати вагомого внеску зарубіжних учених у становлення вітчизняної доктринальної основи в цій сфері, особливо таких 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.

Стрімке реформування, оновлення законодавства, логіка попередніх наукових досліджень та інтереси практики зумовили актуальність потреби розвитку теоретико-методологічних та правових засад конституційно-правового забезпечення інформаційної безпеки сучасних держав, науковим «базисом» для якого є праці зазначених учених.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження відповідає «Концепції вдосконалення судівства 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 року, Стратегії сталого розвитку «Україна - 2020», затвердженій Указом Президента України 12 січня 2015 року за №5/2015, комплексній науково-дослідній темі Таврійського 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 генезу 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 дає 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 (підрозділ 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 в сучасних умовах та механізмів забезпечення інформаційної безпеки держави у сфері публічно-правових відносин як її складника (підрозділи 1.2;

Нормативну основу роботи становлять Конституція України, закони України, міжнародно-правові акти, ратифіковані Україною, що визначають особливості забезпечення Аінформаційної 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 санкції, інформування та освіта;

– 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 технологіях, а також електронних засобів масової інформації тощо;

– 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 нормативно-правових актів;

– 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 національних традицій;

– 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 стосовно інформаційної безпеки особи, суспільства та держави;

– запропоновано розробити комплексний нормативний акт щодо проведення спеціальних інформаційних операцій за зразком американської доктрини «Інформаційні операції» (JP 3-13);

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-комунікативних технологій;

– положення щодо базової досліджуваної категорії – «інформаційна безпека», що дозволяє 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 даній сфері), статичний (безпека як стан захищеності інформаційного простору, інформації, інформаційного суспільства і система відповідних гарантій тощо), комплексний або змішаний (безпека як стан і процес);

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

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

– підхід до об’єктів механізму забезпечення інформаційної безпеки у найзагальнішому розумінні у вигляді предметів, явищ, процесів та осіб, на які здійснюється інформаційний вплив та щодо яких здійснюються заходи із забезпечення безпеки, які поділяються на соціальні особа, суспільство, держава, їх інтереси, права та свідомість) та технічні (інформація, інформаційна інфраструктура, інформаційні технології тощо);

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

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

дістали подальшого розвитку:

– ряд визначень, зокрема визначення поняття «інформаційна безпека», як стан захищеності життєво важливих інтересів людини, суспільства і держави, що 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 доступності інформації;

– положення щодо конституційно-правових та інші засад, особливостей здійснення цієї функції держави у національному і міжнародному масштабі тощо;

– 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;

– напрями вдосконалення нормативно-правового забезпечення інформаційної безпеки на основі аналізу зарубіжного досвіду;

– пропозиції стосовно формування нормативно-правової складової механізму забезпечення інформаційної безпеки від визначення організаційної будови цього механізму, регулювання діяльності його суб'єктів та забезпечення законності його функціонування.

Практичне значення одержаних результатів полягає в тому, що сформульовані в дисертації теоретичні положення, пропозиції та рекомендації сприятимуть формуванню теоретико-методологічних та правових засад вирішення адміністративними судами спорів у сфері публічно-правових відносин. Одержані результати можуть бути використані та використовуються:

– *у науково-дослідній сфері* – як фундамент для розв'язання та подальшого дослідження проблематики забезпечення інформаційної безпеки держави (Довідка Науково-дослідного центру правового забезпечення

державотворення та безпеки ТНУ імені В.І. Вернадського № 1/20-01 від

– *у правотворчості* – внесення змін і доповнень до значної кількості нормативно-правових актів України, зокрема лягли в основу законопроекту «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю» (номер 2133а від 19.06.2015) та Закону України «Про основні засади забезпечення кібербезпеки України» (https://zakon.rada.gov.ua/laws/show/2163-19#Text), використано при підготовці Стратегії кібербезпеки України (https://zakon5.rada.gov.ua/laws/show/96/2016#Text) та Доктрини інформаційної безпеки України (https://zakon.rada.gov.ua/laws/show/47/2017#Text) які розглядалися Комітетом з питань правоохоронної діяльності та були рекомендовані для розгляду Верховною радою України (Акт впровадження н

а – *у навчальному процесі* – під час вивчення навчальних дисциплін: у«Конституційне право», «Адміністративне право», «Трансформація кнаціональної правової безпеки», «Інформаційне право», «Захист інформації та іінформаційна безпека» «Порівняльне адміністративне право», «Міжнародне інформаційне право», «Міжнародне право» (довідка впровадження результатів дисертаційного дослідження в навчальний процес Навчально-наукового куманітарного інституту Таврійського національного університету імені В.І. Вернадського № 167/267 від 29.10.2020).

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

о **Апробація результатів дисертації.** Ключові теоретичні напрацювання й рекомендації оприлюднені в тезах доповідей і наукових повідомлень на наукових і науково-практичних семінарах та конференціях, а також у процесі

к
20

д

виконання міжнародних проектів: Стан дотримання прав людини в умовах сучасності: теоретичні та практичні аспекти (м. Київ, 22 березня 2018 року); 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 року); Політико-правова доктрина державного суверенітету в умовах глобалізації (26 жовтня 2018 року); Стан та перспективи реформування сектора 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 року); Верховенство права як гарантія конституційного ладу (м. Київ, 5 грудня 2019 року).

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, у якому 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 417 сторінок, у тому числі основного тексту – 362 сторінки. Список використаних джерел налічує 684 найменування.

РОЗДІЛ 1.
ДОКТРИНАЛЬНІ ДЖЕРЕЛА ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ФУНКЦІЙ ДЕРЖАВИ

Розвиток Світу – еволюція сучасних суспільств, держав, міжнародних організацій і всього світового співтовариства – неможливий і вже практично не уявляється без інформаційно-комунікаційних технологій, Інтернету, соціальних мереж, мессенджерів тощо. Вони сприяють оперативному пошуку, накопиченню, обробленню, поширенню та збереженню величезних масивів інформації, збереженню її конфіденційності, впорядкуванню доступу до неї, але навіть і їх потужності обмежені. Не завжди вдається належним чином захистити, власне, інформацію, суб'єктів інформаційних відносин, гарантувати інформаційну безпеку на національному, наднаціональному чи міжнародному рівнях. Внаслідок цього виникають різного роду конфлікти, в тому числі збройні протистояння міжнародного й неміжнародного характеру, інформаційні та гібридні війни, інші форми спротиву і протидії.

Безумовно, держави взяли на себе зобов'язання щодо запобігання і протидії загрозам і викликам, порушенням прав людини і громадянина в інформаційній сфері, забезпечення доступу до інформації в різних галузях, розвитку інформаційної інфраструктури.

Конституційна та інша законодавча регламентація функцій держави, функціонально-компетенційних характеристик відповідних органів державної влади та місцевого самоврядування в Україні підкреслюють важливість таких напрямів суспільної діяльності, як захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки, додержання критеріїв безпечної екології екологічної і підтримання екологічного балансу на території України, збереження генофонду нації та Українського народу і т. д.

Таке широке коло завдань та обов'язків держави потребує не лише

належного правового врегулювання, а й ефективних механізмів їх реалізації, моніторингу та системного удосконалення. Це, звісно, неможливо забезпечити без ґрунтовної теоретичної основи, науково-експертної діяльності, імплементації до національного законодавства існуючих міжнародних норм і стандартів, вивчення та впровадження кращого з відповідного зарубіжного досвіду.

Генеза наукових досліджень інформаційного суспільства та інформаційної безпеки

Широкий спектр відносин, що визначають предмет та об’єкт нашого дослідження, змушує проаналізувати основні наукові здобутки вітчизняних і зарубіжних учених стосовно розвитку інформаційного суспільства, інформаційної безпеки в контексті розвитку національної безпеки, її різновидів, а також функцій держави та відповідних нормативних, інституційних механізмів їх забезпечення.

Останніми роками пожвавився інтерес до цієї проблематики. Це стало особливо помітно на тлі загострення глобального протистояння супердержав, реальної військової загрози територіальній цілісності України, непорушності її державних кордонів, непохитності її конституційного ладу, загрозам національній безпеці через військову інтервенцію, війни з Росією та анексією значної частини української території. Це знайшло своє відображення у значній кількості наукових досліджень, результатом яких є надруковані праці вчених різних галузей сучасної науки.

Так, агресія Росії відновила науковий інтерес українських вчених до теми гібридної війни (А. Дорошкевич, В. Горбулін, О. Жайворонок, О. Литвиненко, Є. Магда, С. Максимов, Г. Сасин, Т. Черненко, Г. Яворська та ін.), інформаційних війн та інших форм інформаційного протиборства (В. Алещенко, В. Бебек, Ю. Горбань, І. Грабчук, Р. Гула, Д. Коваль, С. Любарський Я. Малик, Г. Почецов, В. Сербін, Є. Скулиш, О. Сивак, П. Ткачук, В. Хорошко, О. Щурко та ін.), проблем інформаційної безпеки в Україні (О. Баранов, О. Довгань, Д. Безуглий, І. Боднар, І. Валюшко, А. Гальчинський, М. Дмитренко, М. Желіховський, О. Зозуля, Н. Камінська, Б. Кормич, Ф. Медвідь, В. Ліпкан, О. Логінов, Ю. Максименко, Є. Мануйлов, Л. Наливайко, А. Нашинець-Наумова, О. Семченко, В. Петрик, П. Біленчук, Л. Борисова, І. Неклонський, О.Дзьобань, В. Богуш, О. Юдін, О. Сорокін, Т. Перун,

В. Пилипчук, О. Ніщименко, О. Олійник, Г. Ситник, О. Тихомиров, Т. Ткачук, В. Фатхутдінов, А. Шумка та ін.).

Спочатку дослідники вдавались до вивчення переважно проблематики національної безпеки (В. Барчук, В. Горбулін, Ю. Ірхін, І. Каріх, А. Рубан, М. Пендюра, З. Чуйко, А. Ковальчук, В. Антонов, С. Чумаченко та ін.), меншою мірою, зокрема, до прийняття спеціального законодавства, кібернетичної безпеки та кіберпростору (М. Грайворонський, П. Демченко, Д. Дубов, І. Діордіца, М. Ожеван, Н. Савінова, І. Сопілко і т. д.).

За останні десятиріччя вивчаються різноманітні аспекти становлення та функціонування інформаційного суспільства національного або міжнародного масштабу (Д. Андреєв, О. Задорожній, В. Кір'ян, О. Кирилюк, В. Скалацький, Н. Кушакова-Костицька, М. Гуцалюк, М. Дімчогло, В. Залізняк, І. Кисарець, О. Копан, Б. Кормич, П. Матвієнко, Г. Несвіт, А. Новицький та ін.); державної інформаційної політики та національного інформаційного суверенітету (І. Арістова, В. Горовий, О. Джураєва, О. Джус, В. Попик, А. Селіванов, Д. Севрюков, О. Скрипнюк, Л. Рябовол, В. Ковтун, Н. Пархоменко, Є. Стрельцов); проблеми розвитку інформаційного права та інформаційного законодавства (К. Череповський, В. Цимбалюк, В. Гавловський, В. Гриценко, А. Марущак, М. Швець, Р. Калюжний, П. Мельник та ін.).

З-поміж досліджень, присвячених правам та свободам людини і громадянина, сучасних закономірностей їх розвитку і механізмів забезпечення, охорони й захисту, прослідковуються тенденції до виокремлення інформаційних прав і свобод людини і громадянина, прав людини онлайн (В. Брижко, К. Бєляков, А. Іщенко, Л. Вакарюк, Т. Костецька, А. Марущак, В. Політанський, О. Золотар, О. Марцеляк, А. Олійник, О. Фрицький, Т. Проценко, В. Нестерович, К. Полетило, Н. Ткачук, В. Федоренко та ін.).

Окремо доцільно виокремити акцент дослідників на питаннях захисту персональних даних, інформаційних баз даних, доступу до інформації,

інформації з обмеженим доступом, публічної та інших видів інформації (В. Баскаков, І. Берназюк, І. Кушнір, Л. Рудник, О. Нестеренко, Є. Теплюк, А. Пазюк, О. Волох, І. Забара, О. Стрельченко та ін.).

На нашу думку, згадані вище пріоритетні напрями сучасних наукових досліджень базуються на ґрунтовних теоретичних працях, концептуальних методологічних та інших розробках. Звісно, навряд чи можливо всебічно вивчити, враховуючи різноманітні сутнісні ознаки, критерії класифікації, об'єктно-суб'єктні характеристики, джерельну основу, функціональні та інші аспекти без здобутків учених – представників теорії держави і права, філософії права. Тут варто відзначити науковий доробок О. Балинської, С. Бобровник, Б. Бабіна, М. Баймуратова, І. Біласа, С. Бостана, С. Головатого, С. Гусарєва, М. Костицького, М. Козюбри, В. Забігайла, О. Лощихіна, Н. Оніщенко, О. Петришина, Н. Пронюк, Т. Подорожньої, О. Скакун, О. Тихомирова, О. Фатхутдінової, Н. Шаптали, А. Шевченка тощо.

Функції сучасної держави неодноразово розглядали представники різних галузей вітчизняної і зарубіжної науки. Водночас, варто підкреслити, основні напрями забезпечення національної, інформаційної, економічної, екологічної та інших видів безпеки поступово утвердились як об'єкти міжгалузевого, міждисциплінарного наукового аналізу. Цьому сприяли і виклики сучаснго цивілізаційного розвитку, в тому числі гібридні.

Підтримуємо позиції деяких науковців у контексті становлення вітчизняного і зарубіжного конституціоналізму, першочергових завдань щодо забезпечення конституційного ладу, територіальної цілісності й непорушності державних кордонів України, забезпечення прав і свобод людини і громадянина, принципів правової незалежної, демократичної унітарної і соціальної держави. Такі завдання конституційної держави зумовлюють необхідність дослідження засад і механізму її конституційної безпеки, конституційних деліктів і конституційної відповідальності, деяких інших конституційних та інших правових інститутів, галузей. Відзначимо значну існуючу основу для подальших розвідок на цьому шляху, зокрема, науковий

доробок М. Гультая, Ю. Барабаша, Ю. Бауліна, А. Головіна, В. Городовенка, А. Селіванова, І. Сліденка, Ю. Волошина, Я. Берназюка, М. Оніщука, В. Демиденка, В. Кампа, А. Колодія, Н. Мяловицької, І. Магновського, Р. Губаня, О. Ярмиша, О. Батанова, А. Крусян, П. Мартиненка, О. Совгирі, В. Шаповала, А. Янчука і т. д.

Безумовно, не можна не згадати вагомого внеску зарубіжних учених у становлення вітчизняної доктринальної основи у цій сфері, особливо таких 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.

Спробуємо зупинитись на ключових положеннях і висновках низки існуючих досліджень у цій сфері.

Зокрема, цікава праця з конституційного права на тему *«Конституційно-правові засади національної безпеки України*», підготовлена В. Антоновим (Київ, 2017). У ній розкрито теоретико-правові та методологічні засади національної безпеки, систему національної безпеки України та її конституційно-правовий вимір, конституційно-правові аспекти системи забезпечення національної безпеки Української держави, а також проблеми такого забезпечення. З-поміж основних теоретичних, методологічних та практичних висновків, сформульованих за результатами цього дослідження, виокремимо такі:

– використання поняття «безпека» свідчить про те, що не існує безпеки відокремлено від життєдіяльності людини і що категорія безпеки детермінована усіма об'єктивними і суб'єктивними чинниками життя людини, суспільства і держави. Саме тому безпека набуває змістовного вираження тільки у зв'язку з конкретними чинниками цієї життєдіяльності;

– для категорії національної безпеки як специфічного конституційно-правового інституту забезпечення безпеки людини є найважливішою конституційно-правовою засадою, визначальною для регламентації відносин у цій сфері;

– національна безпека в Україні за своєю суттю є системним об'єктом конституційно-правового регулювання. Це система відносно самостійних і взаємопов'язаних елементів, головною метою яких є захист життєво важливих прав і свобод людини та громадянина, інтересів суспільства і держави від внутрішніх і зовнішніх загроз;

– єдиним державно-правовим механізмом, який охоплює всі елементи системи національної безпеки, призначеним для ефективної реалізації цільових установок вказаної системи шляхом виконання функцій щодо захисту життєвих інтересів особи, суспільства і держави в межах повноважень, визначених чинним законодавством, є механізм забезпечення системи національної безпеки. Він виступає як найважливіша підсистема в системі національної безпеки. Її призначення полягає в організованій державою взаємодії державних органів, посадових осіб, громадських організацій і окремих громадян, спрямованій на убезпечення особи, суспільства й держави від внутрішніх і зовнішніх загроз;

– функціонування системи національної безпеки здійснюється в рамках державної безпекової політики, відповідно до якої прогнозуються, плануються, організовуються і здійснюються заходи безпекового характеру (доктрини, стратегії, концепції і програми), спрямовані на захист національних інтересів України. Центральне місце в безпековій політиці належить забезпеченню встановленого ст. 48 Конституції України права громадян на достойний життєвий рівень для себе і своєї сім'ї, оскільки внутрішні суперечності соціально-економічного розвитку України та глобальні світові кризові явища провокують цілу низку реальних і потенційних загроз в економічній і соціальній сферах та створюють небезпеку життєвим інтересам суспільства, самому його існуванню і т. д. [118, с. 536-540].

Прикметно, що в монографії «Конституційно-правові засади національної безпеки України» проаналізовано розвиток і становлення основних етапів загальної теорії національної безпеки і відзначено, що кожний з цих етапів був наповнений своїм змістом, який віддзеркалює особливості розвитку суспільства та державності і має лише йому притаманні риси. Так, перший етап накопичення відповідних знань та ідей щодо проблеми безпеки завершується на початок XIII ст. коли ще не приділялося належної уваги питанню створення необхідних умов для безпеки особистості. Простежується теологічне сприйняття проблеми забезпечення безпеки особи. Разом з тим зароджується також реалістичне трактування безпеки в контексті забезпечення добробуту як мети особи, суспільства і держави. Напрацювання концептуальних засад національної безпеки дало можливість ученим сформулювати основи загальної теорії безпеки, зокрема, визначити основний постулат внутрішньої безпеки нації, який полягає в захисті державою життєво важливих інтересів особистості.

Формування та становлення ідей і поглядів на проблему безпеки особистості, суспільства та держави створили теоретичне підґрунтя для обґрунтування двох моделей безпеки особистості: ліберальної та соціалістичної.

Сучасний етап розвитку загальної теорії національної безпеки бере свій початок у XX ст. Раніше домінуючі політологічні праці присвячені національній безпеці у нових реаліях: поява і застосування зброї масового ураження, що зумовило переосмислення ролі воєнної сили та умов її застосування, а також розвиток інформаційного суспільства і пов’язаних з цим світових процесів глобалізації, доповнюються працями, підготовленими в межах юридичної науки, економічної та історичної, військової, технічної, науки державного управління (державне управління у сфері державної безпеки та охорони громадського порядку), а також інформацієзнавства, комунікацієзнавства, безпекознавства тощо.

Ми погоджуємося, що забезпечення національної безпеки держави постає як одна з найважливіших умов реалізації стратегічної мети – розбудови

України як суверенної, незалежної, демократичної, соціальної, правової держави. Власне, тому діяльність влади в Україні повинна спрямовуватися на збереження стабільності та контрольованість політичних і соціально-економічних процесів. Важливу роль у цьому відіграє духовна сфера життєдіяльності суспільства як об'єкта системи національної безпеки, наявність національної ідеї для консолідації громадянського суспільства, виваженої гуманітарної політики.

Разом з тим постає чимало питань, які потребують додаткового роз'яснення, визначення аспектів їх співвідношення. Зокрема, В. Антонов серед однопорядкових категорій визначає державну політику у сфері національної безпеки, безпекову політику, правову політику держави з питань національної безпеки і оборони України, гуманітарну політику тощо [118, с.171].

Водночас автор наголошує, що непростими залишаються і внутрішні виклики національній безпеці. Агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, неефективність системи забезпечення національної безпеки, корупція та недосконаліть системи державного управління, витратна економічна модель та економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення, викривлення демократичних процедур, що штучно стримують процеси кадрового оновлення державних органів, зумовлюють слабкість, а подекуди й неспроможність держави виконувати свої функції, насамперед у сфері захисту прав і свобод людини і громадянина, зростаючу недовіру до держави з боку суспільства.

На десятиріччя раніше підготовлено кандидатську дисертацію *З. Чуйко на тему «Конституційні основи національної безпеки України»* (Харків, 2008) також за спеціальністю 12.00.02 (конституційне право). У ній підкреслюється, що національну безпеку і державну безпеку неприпустимо ототожнювати, а

тим більше підміняти національну безпеку державною безпекою, оскільки вони співвідносяться як ціле і частина. Поняття «національна безпека» охоплює значно ширше коло об'єктів, має міждисциплінарний, міжгалузевий характер та дозволяє об'єднати всі відомі види безпеки, які забезпечує держава.

Авторка пріоритетними структурними елементами національної безпеки залежно від конкретних сфер людської життєдіяльності вважає державну, економічну, енергетичну, екологічну, інформаційну, соціальну, політичну, науково-технологічну та воєнну безпеку. Нормативно-правове забезпечення складових національної безпеки за функціональною ознакою має бути незалежним від політичної ситуації та відображати гостроту реальних проблем і їх значення для розвитку країни. Це потребує ретельного моніторингу та аналізу наявних загроз, урахування потенціалу країни та зарубіжного досвіду в цих сферах суспільних відносин.

Механізм забезпечення національної безпеки визначається специфічним видом правових механізмів, який має особливу, складну природу, що зумовлена самою сутністю категорії національної безпеки. Зміст такого 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 і захист національних інтересів (інституційний механізм) [646, с.15].

Важко не погодитися з тим, що мають бути чітко розмежовані повноваження між Кабінетом Міністрів України, Президентом України, Верховною Радою України та Радою національної безпеки і оборони України

щодо діяльності у сфері національної безпеки. Разом з тим виникають питання: чи справді на початку XXI ст., на відповідному етапі вітчизняного державотворення, його сутнісною характеристикою була цілеспрямована діяльність органів державної влади та інститутів громадянського суспільства щодо захисту національних інтересів від різного роду загроз та забезпечення таких умов для існування людини, держави і суспільства, які гарантували можливість їх всебічного прогресу?

Звісно, практична значимість деяких положень того часу змінилася, певні пропозиції отримали відповідне законодавче оформлення, у будь-якому випадку порушені питання є актуальними і в умовах сьогодення закладено основи для подальших наукових досліджень.

Наступна праця, на яку варто звернути увагу – дисертація *В. Барчука* на тему *«Уповноважений Верховної Ради України з прав людини як суб'єкт забезпечення національної безпеки України*» **(**за спеціальністю 12.00.02 – конституційне право, Київ, 2006). Тут визначено поняття «безпека людини» як стан забезпечення (закріплення, реалізації, охорони, захисту та відновлення) життєво важливих інтересів людини, за яким відбувається її існування і розвиток в умовах впливу внутрішньодержавних і зовнішньодержавних загроз. Це складовий елемент національної безпеки.

Порушення прав людини не тільки погіршує становище самої людини в суспільстві, а й негативно впливає 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 [129].

В. Барчук визначив основне призначення інституту омбудсмана як дієвого фактора національної безпеки України, який полягає в тому, що він розв'язує конфлікти державних та індивідуальних інтересів (аспект

ефективного забезпечення національної безпеки). Його діяльність має місце на кожній із стадій забезпечення прав людини, і визначена з огляду на це вагомість для забезпечення національної безпеки України.

Іншим значимим суб'єктом національної безпеки України є Служба безпеки України, що проводить свою діяльність у безпосередній і опосередкованій формах: по-перше, СБУ безпосередньо забезпечує охорону і захист прав людини від правопорушень; по-друге, створює умови для реалізації людиною власних прав (захищаючи, наприклад, державний суверенітет, конституційний лад, територіальну цілісність і т. д.) і виступає таким чином необхідним елементом юридичного механізму реалізації прав людини. Особливість діяльності Уповноваженого Верховної Ради України з прав людини щодо контролю за дотриманням прав людини Службою безпеки України зумовлює визначення принципів та основних напрямів взаємодії між омбудсманом і Службою безпеки України. Йдеться, зокрема, про: спрямованість взаємодії на забезпечення прав та свобод людини; законність; надання пріоритету договірним засобам над адміністративними методами реагування під час розв'язання конфліктів; застосування найбільш ефективного методу; цілеспрямованість співпраці; своєчасність; взаємодопомога у вирішенні конкретних питань; ієрархічність компетенції; гласність; співпраця у правотворчості; постійне вдосконалення форм співробітництва. Напрямами такої взаємодії є: 1) обмін інформацією; 2) використання спільних можливостей для забезпечення прав людини тощо.

Доцільно, на наш погляд, виокремити також дослідження, присвячене конституційно-правовим засадам забезпечення економічної безпеки у контексті розбудови системи національної безпеки України. Йдеться про дисертацію на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.02 – конституційне право; муніципальне право. *М. Завидняка* на тему *«Конституційно-правові засади забезпечення економічної безпеки України» (Ужгород, 2016).* Тут підкреслено, що Конституція України визначає засади правової визначеності, поваги до прав

людини, обмеження свободи розсуду у діяльності публічної адміністрації у правовому регулюванні економічної безпеки. Особливе значення має співвідношення законодавчого регулювання із підзаконними нормативними актами, оскільки з питань економічної безпеки окремі підзаконні правові акти можуть носити характер з обмеженим доступом, що пов'язано зі специфікою проведення оперативно-розшукових заходів та негласної слідчої діяльності, що необхідно для досягнення легітимних цілей – забезпечення державного суверенітету, економічного добробуту та національної безпеки.

Механізм забезпечення економічної безпеки з точки зору конституціоналізму полягає в юридичних засобах обмеження свободи розсуду в ухваленні рішень спецслужбами та органами безпеки держави, які в такій якості виступають органами публічної адміністрації, а також юридичної визначеності правил і процедур, застосування яких підлягає демократичному контролю на рівні громадських організацій, парламенту, глави держави, а також міжнародних установ, юрисдикцію яких визнано Україною [236, с.13].

Методологія аналізу системи забезпечення економічної безпеки має охоплювати законодавство як систему законів та регуляторних актів, відповідну судову практику, дані аналітичних матеріалів та пропозиції до чинного законодавства з боку наукових установ, вищих навчальних закладів, незалежних аналітичних центрів, а також громадських об'єднань, які спеціалізуються на питаннях економічної безпеки. Автором аргументовано, що з точки зору конституціоналізму економічна безпека полягає в забезпеченні стабільних правил економічної діяльності таким чином, щоб її суб'єкти могли планувати свою діяльність на майбутнє, з метою забезпечення сталого розвитку суспільства і держави, додержання прав і свобод людини та національних економічних інтересів. Такі цілі досягаються шляхом додержання вимог верховенства права у ході ухвалення актів законодавства та здійснення регуляторної політики у сфері економічної безпеки [236, с.13].

Конституційні механізми забезпечення сталого розвитку національної економіки полягають у стимулюванні державою виробництва товарів із

високим ступенем доданої вартості, тобто з багатоступінчастими циклами переробки. Забезпечення належного рівня оплати праці можна досягти шляхом упровадження дерегуляторної політики держави, розширення свободи колективних трудових договорів та соціального партнерства, а також шляхом зниження оподаткування з одночасним забезпеченням гарантій свободи економічної діяльності та прав працівників [236, с.13].

Автор зазначив, що порівняльний аналіз різних типів економічних систем (ліберальних, ліберально-демократичних, соціальних, перехідних та етатистських) свідчить про різний ступінь забезпечення економічних свобод. Досягнення зрілого ступеня економічних свобод є важливим для сталого розвитку економічних систем, які, як правило, стикаються з обмеженістю ресурсів та неповнотою інформації, що не дає змоги будувати якихось далекосяжних планів. Тому вільна конкуренція при відкритості комунікацій дає змогу збалансувати економічну систему та гарантувати мінімальний рівень економічних свобод, які критично важливі для сталого розвитку суспільства. Для цього потрібні незалежні суди, доброчесна аудиторська служба та контроль за публічними фінансами, задовільне функціонування бірж із метою визначення реальних цін на ринку товарів, послуг і капіталів, а також належне функціонування правил і процедур. Структура економічної системи зумовлена ступенем її відкритості-закритості, а також співвідношенням зовнішніх та внутрішніх аспектів її функціонування. Структура національної економічної системи зумовлює також функції економічної безпеки. Показники національної економіки лише засвідчують ті обставини, що держава має вживати неухильних заходів щодо лібералізації режиму відкриття та закриття підприємств, спрощення відповідних адміністративних процедур та фіскальних процедур, підвищення рівня споживання населення, яке б забезпечувало гідний рівень життя людини та сталий розвиток суспільства, що об’єктивно збільшує ВВП і забезпечує самодостатність національної економіки [236, с.13-14].

До системи принципів забезпечення економічної безпеки належать: а) принцип правової соціальної держави; б) принцип свободи економічної діяльності; в) принцип справедливості; г) право на незалежний і безсторонній суд; д) принцип додержання вимог публічного економічного порядку; е) принцип пропорційності.

Встановлено, що функціональний аспект економічної безпеки в Україні має три проблемні складові: 1) значна зарегульованість економіки, що має наслідком низький рівень економічних свобод і низьку ділову активність; 2) гіпертрофоване значення важкої металургії та продукції з низьким ступенем технологічної переробки; 3) анексія Російською Федерацією Криму та підтримка і керівництво незаконними парамілітарними структурами в окремих районах Донецької і Луганської областей, що порушило цілісність національної економічної системи України. Виходом із ситуації є конституційні гарантії свободи підприємницької діяльності, обмеження монополізму та забезпечення національних економічних інтересів на зовнішніх ринках через збалансований баланс експортно-імпортних операцій та гарантії свободи договорів на цих ринках [236, с.13-14].

Забезпечення економічної безпеки в системі поділу влади здійснюється через спеціалізацію, диференціацію та раціоналізований розподіл повноважень між різними їх носіями з метою реалізації засад сталого розвитку національної економіки та виявлення, попередження й усунення потенційних і реальних загроз поступальному її розвитку. Виходячи із цього та з функціональної точки зору всі органи влади наділяються повноваженнями на основі конституції і законів, які визначають основні напрями діяльності в окремій галузі державної діяльності [236, с. 13 -14].

Обґрунтовано, що Конституція України визначає засади правової визначеності, поваги до прав людини, обмеження свободи розсуду в діяльності публічної адміністрації у правовому регулюванні економічної безпеки. У системі правового регулювання економічної безпеки розробка концепцій, програм розвитку у певних галузях публічного управління має змішаний

характер, оскільки вони можуть визначати напрями розвитку законодавства та відповідної адміністративної практики у сфері економічної безпеки. Особливе значення тут має співвідношення законодавчого регулювання з підзаконними нормативними актами, оскільки з питань економічної безпеки окремі підзаконні правові акти можуть мати характер з обмеженим доступом, що пов'язано зі специфікою проведення оперативнорозшукових заходів та негласної слідчої діяльності, що необхідно для досягнення легітимних цілей – забезпечення державного суверенітету, економічного добробуту та національної безпеки [236, с.13-14].

Наступними цікавами працями є монографії та відповідні дисертації, зокрема, *Н. Кушакової-Костицької «Право на інформацію в інформаційну епоху (порівняльне дослідження)» (Київ, 2018), «Філософсько-правові засади становлення і розвитку інформаційного суспільства в Україні» (Київ, 2019).* В останній дисертаційній роботі на здобуття наукового ступеня доктора юридичних наук, підготовленій за спеціальністю – філософія права, розкрито закономірності, які обумовили стрімкий та невпинний прогрес інформаційно-комунікаційних технологій та їх вплив на філософські, правові, соціальні, економічні, політичні, етично-моральні, культурно-освітні та інші виміри життєдіяльності соціуму. Особливу увагу приділено захисту права на отримання достовірної та своєчасної інформації як одного з основоположних прав людини і громадянина та перспективам трансформації інформаційного суспільства у суспільство знань [344, с.39-40].

Авторка охарактеризувала ступінь проникнення інформаційних технологій у всі галузі життєдіяльності соціуму та зазначено, що духовна сфера за відсутністю сучасної, зрозумілої загалу, адекватної вимогам часу ідеології поступилася споживанню та матеріальним інтересам. Це означає, що гуманітарна сфера відіграє, за відсутністю практичного сенсу та порівняно з фундаментальною наукою й технологіями, все меншу роль у суспільстві, зокрема, філософія все більше стає певною абстракцією. А відтак, доцільним

є розвиток нових підходів і загальнонаукових методологій, серед яких інформаційний підхід видається найбільш дієвим і витребуваним [344, с.3].

Інформаційне суспільство визначається як постіндустріальний (інтелектуальний) етап розвитку соціальної організації, протягом якого суспільство формується під впливом інтелектуальних технологій, основою яких є інформація і знання, отримання, оброблення, засвоєння, використання та передавання яких здійснюється за допомогою телекомунікацій і комп'ютерів. Процес утворення цього типу соціальної організації необхідно досліджувати з точки зору не тільки економічних процесів, а й щодо виникнення нових тенденцій в соціальній і духовній сферах.

Н. Кушакова-Костицька вважає серйозною проблемою сучасного інформаційного суспільства виникнення нового понятійного апарату, певні зміни і диференціювання вже сталих термінів, пов'язаних з його функціонуванням. Не принциповою стає відмінність у змісті понять «інформація» – «дезінформація» – «дифамація», «інформування» – «доносництво» (яке в будь-якому випадку недоцільно заохочувати).

Відзначається, що однією з ознак інформаційного суспільства є також розвиток права в напрямі створення та переважання етичних норм і кодексів замість законодавчо закріплених норм поведінки. Доволі дискусійною видається позиція щодо того, що чим вищий рівень суспільної моралі, рівень суспільної свідомості, тим менше потреби у юриспруденції як такої, тобто спостерігається тенденція саморегулювання суспільних відносин, зокрема правовідносин, і на рівні національного інформаційного простору, і на рівні глобального [344, с. 46].

Н. Кушакова-Костицька зазначає ознаки інформаційного суспільства останнім часом набули широкого розповсюдження у всесвітньому масштабі, хоча його гегемоністський характер і не ґрунтується на відповідних теоретикометодологічних засадах у розумінні класичної філософії. Констатується, що глобальна інформаційна цивілізація є рівнем розвитку світового співтовариства), характерною ознакою якої слід вважати зростання

ролі інформації в соціальній життєдіяльності. Її кількісно-якісні показники відображають рівень загальної культури суспільства стосовно вироблення, сприймання й раціонального використання інформації для задоволення матеріальних і соціальних потреб громадян. Інформаційному суспільству притаманне переважання виробництва інформаційного, а не матеріального продукту. Відповідно, починає докорінно саме виробництво – продукт його стає більш інформаційно ємним за рахунок інновацій, дизайну і маркетингу. Основним стратегічним ресурсом такого суспільства є знання, тобто інформація, що проникає в усі сфери життєдіяльності соціуму та кореспондує з поняттям «інформаційна сфера» [344, с.].

Поряд з цим, підкреслюється гегемоністський характер сутності та змісту поняття «інформаційне суспільство», яке останнім часом набуло значного поширення у всесвітньому масштабі. Зокрема, глобальна інформаційна цивілізація — це рівень розвитку глобального суспільства (світового співтовариства), що визначається зростанням ролі інформації як продукту соціальної діяльності людей, за якісними характеристиками якої вимірюється рівень загальної культури суспільства щодо здатності виробляти, сприймати й раціонально застосовувати відомості, дані, знання для потреб життєдіяльності.

Беззаперечно, що для становлення і розвитку інформаційного суспільства, регулювання його засад, інститутів і механізмів важливу роль відіграє нова галузь права – інформаційне право, яке іноді трактують і як віртуальне право, оскільки предметом його дослідження є насамперед закономірності функціонування віртуального простору та віртуальні взаємовідносини між суб’єктами, які діють у цьому просторі.

Розвиваючи вищевикладені положення, відзначимо, що попри це, сьогодні очевидно, що трансформація інформаційного суспільства в суспільство знань, у тому числі й в Україні, не відбувається, оскільки серед основних перепон на цьому шляху стоїть насампереред недостатній рівень культури значної частини ІТ-користувачів, не завжди використання досягнень

науки і техніки призводить до інтелектуального прогресу людства. Іноді інформаційно-комунікаційні технології стають причиною або засобом кібератак, інформаційних воєн чи інших форм протистояння, інтервенцій тощо.

Одним з останніх актуальних досліджень є докторська дисертація *І. Діордіци на тему «Адміністративно-правове регулювання кібербезпеки України» (Запоріжжя, 2018).* Тут визначаються загалом основні загрози кібернетичній безпеці України: використання кіберпростору у воєнних цілях, створення іншими державами кібервійськ, кіберпідрозділів у традиційних родах військ; розроблення іноземними державами нових видів зброї кібернетичного характеру; існування в інших країнах планів наступальних та розвідувальних військових операцій у кіберпросторі; освоєння іноземними спеціальними службами методів розвідувально-підривної діяльності у кіберпросторі, методів маніпулювання суспільною свідомістю за допомогою кіберпростору; можливість втягування України у збройні конфлікти чи у протистояння з іншими державами через використання національного сегмента кіберпростору; спроби втручання у внутрішні справи держави (інформаційна інтервенція) з використанням соціальних мереж, поширення в національному сегменті кіберпростору культу насильства, жорстокості, порнографії; активізація проявів кібертероризму; поширення кіберзлочинності; критична залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції, поширення фактів включення у програмно-технічні засоби прихованих шкідливих функцій; зростання ризиків виникнення надзвичайних ситуацій техногенного характеру через зниження рівня захищеності об’єктів критичної інформаційної інфраструктури держави.

На думку згаданого автора, нагальною є проблема створення інформаційних військ України. Така необхідність зумовленами поширюючими загрозами кібербезпеки, тим паче, що в глобальному відкритому суспільстві, яким є інформаційне суспільство, кібернетична (інформаційна) інтервенція може мати не лише глобальні наслідки, а й

безпосередньо полягати в діях, що характеризуватимуться глобальними ознаками: можливістю спільної участі в інтервенції необмеженої кількості суб'єктів, які значно віддалені один від одного щодо одного об'єкта або щодо необмеженої кількості об'єктів одночасно. Аналогічно, можливе одночасне вчинення кіберзлочинів з метою інтервенції до великої кількості об'єктів або одного надважливого, у т. ч. стратегічного об'єкта. Оскільки робити це можливо й поза кордонами на будь-якій відстані, то підвищена загроза кібернетичної безпеки стає безперечною [208, с. 2-8].

Слід підкреслити, що в дослідженні на тему «Адміністративно-правове регулювання кібербезпеки України» ототожнено декілька категорій, зокрема, кібернетична (інформаційна) інтервенція, кібернетична (інформаційна) безпека тощо. На наш погляд, вони потребують уточнення і розмежування, вивчення аспектів співвідношення тощо.

Інші праці представляють не менший науковий інтерес. Йдеться про *монографію на тему «Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір» (Київ, 2018) та дисертаційне дослідження «Правове забезпечення інформаційної безпеки в умовах євроінтеграції України*» (Ужгород, 2019), підготовлені Т. Ткачуком. Серед важливих теоретичних інновацій у них запропоновано включити до об'єктів правового забезпечення інформаційної безпеки України національні інтереси, цінності, цілі та надбання в інформаційній сфері. До інших важливих наукових досягнень належать розроблені критерії оцінювання негативного впливу загроз на стан інформаційної безпеки України, якими автор вважає деструктивні трансформації національних цінностей в інформаційній сфері, що дає змогу створити правове підґрунтя відповідної методологічної бази, а також класифіковано національні цінності та національні цілі в інформаційній сфері, аргументовано доцільність їх законодавчого закріплення.

Введено в доктрину інформаційного права термін «національні надбання в інформаційній сфері», під яким автор розуміє сукупність унікальних інформаційних продуктів, що мають виняткове суспільне,

економічне, військове та інше значення для реалізації національних цілей в інформаційній сфері [610, с. 377]. Він підкреслює, що реалізація національних інтересів в інформаційній сфері, визначених Доктриною інформаційної безпеки України, буде дієвою в разі законодавчого визначення національних цінностей і зумовлених ними національних інтересів.

До національних цінностей в інформаційній сфері віднесено: а) матеріальний добробут населення (у т. ч. на основі розвитку ІКТ); б) інформаційну захищеність людини, суспільства, держави; в) духовність, доступність віросповідання, запобігання релігійному фанатизму та екстремізму; г) мову; ґ) культуру інформаційних відносин; д) свободу інформації, захищеність інформаційних прав людини, доступ до інформації, нейтралізацію негативних інформаційних впливів та ін.

До національних цілей в інформаційній сфері Т. Ткачук відносить такі: а) покласти край спотворенням поглядів людей на навколишній світ і самих себе (духовна безпека); б) забезпечити впровадження інформаційних технологій у військову сферу та забезпечити їх захист (військова безпека); в) прискорити розроблення та впровадження новітніх ІКТ у суспільно-економічну сферу (економічна безпека); г) досягти належного рівня культури інформаційних відносин (соціальна безпека); ґ) створити загальнодержавні інформаційні системи для постійного моніторингу стану навколишнього середовища (екологічна безпека); д) сприяти інтеграції національної інформаційної інфраструктури зі світовою інфраструктурою; е) посилити захист інформаційних прав людини; є) вжити термінових заходів для створення позитивного іміджу держави в умовах інформаційної глобалізації [611, с. 99].

Загалом погоджуючись із потребою ефективного законодавчого врегулювання суспільних відносин, що виникають у досліджуваній сфері, визначення правових засад організації та координації дій суб’єктів забезпечення інформаційної безпеки України, розроблення пріоритетних напрямів державної політики у сфері інформаційної безпеки, у згаданих вище

працях можна побачитиі й чимало суперечливих позицій. Йдеться, зокрема, про визначення основних цілей державної політики України у сфері забезпечення інформаційної безпеки: а) захист інформаційного суверенітету держави в сучасних умовах глобалізації та інтернаціоналізації процесів в інформаційній сфері; б) забезпечення інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами; в) реалізація конституційних прав і свобод громадян, суспільства і держави на інформацію.

Постають у цьому контексті питання, пов'язані з відмінностями глобалізацією та інтернаціоналізацією процесів в інформаційній сфері; що таке інформаційна достатність, і чи доцільно виокремлювати конституційні права і свободи громадян, суспільства і держави на інформацію? Адже аналіз положень Конституції України та інших держав демонструє дещо інші тенденції.

Т. Ткачук для ефективного правового забезпечення інформаційної безпеки України запропоновано проаналізувати законодавчі акти, положення, норми, які регламентують різні аспекти забезпечення інформаційної безпеки, консолідувати загальні правові норми у ЗУ «Про інформаційну безпеку України». Підтверджена гіпотеза, що даний закон може стати одним із базових при кодифікації вітчизняного законодавства у сфері інформації та створенні Інформаційного кодексу України, а також стати основою для керівних документів державної політики в інформаційній сфері та процесу стратегічного планування забезпечення інформаційної безпеки України [611, с. 29].

Автор зазначає, що забезпечення інформаційної безпеки України є визначальним напрямом державної політики, від якого залежатиме існування держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві. Визначено в роботі основні цілі державної політики України у сфері забезпечення інформаційної безпеки: а) захист інформаційного суверенітету держави в сучасних умовах глобалізації

та інтернаціоналізації процесів в інформаційній сфері; б) забезпечення інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами; в) реалізація конституційних прав і свобод громадян, суспільства і держави на інформацію. Т. Ткачук обґрунтував, що основна мета державної політики у сфері забезпечення інформаційної безпеки України – це управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів. 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 інформаційнокомунікаційних технологій; ґ) забезпечення участі України в міжнародній системі інформаційної безпеки [611, с. 30].

У дослідженні *О. Золотар «Правові основи інформаційної безпеки людини» (Київ, 2018)* обґрунтовано, що інформаційна безпека людини водночас є й станом, і процесом, оскільки виступає невід'ємною частиною життя, в якому людина постійно перебуває під дією конкретних інформаційних впливів. При цьому різні категорії осіб перебувають у неоднакових умовах стосовно можливості реалізації своїх прав і свобод в інформаційній сфері, що визначає ступінь їхньої захищеності в інформаційному суспільстві, види й інтенсивність небезпек, що їм загрожують. Авторське бачення структури інформаційної безпеки людини передбачає виокремлення інформаційно-психологічної, інформаційно-технологічної (елементом якої є кібербезпека людини) та інформаційно-правової складових. Остання визначається закріпленим на національному та міжнародному рівнях інформаційно-правовим статусом людини, тобто

обсягом прав і свобод в інформаційній сфері, а також гарантіями їх реалізації [251].

Авторка встановила, що формування інформаційного суспільства не лише підвищило значення існуючих і появу нових інформаційних прав людини, а й змінило змістовне наповнення усіх прав і свобод людини, а також її обов'язків, в напрямку посилення і ускладнення інформаційної складової кожного з них [251, с. 3].

На основі аналізу міжнародного досвіду виявлено дихотомію проблеми міжнародної інформаційної безпеки та інформаційної безпеки людини як складової інституту прав людини в міжнародному праві. Не слід заперечувати, що правове та організаційне забезпечення інформаційної безпеки людини лише на національному рівні є недостатнім з огляду на глобалізацію, інтенсивні транскордонні інформаційні процеси, трудову міграцію, «е-комерцію», втрату ідентичності та ще цілу низку соціальних процесів, що виникають у зв'язку зі становленням глобального інформаційного суспільства.

Таким чином, інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, спрямована на реалізацію прав і законних інтересів людини в кожній сфері життєдіяльності. Елементами системи інформаційної безпеки вбачаються: 1) правова та наукова (доктринальна) основа; 2) об'єктно-суб'єктний склад, тобто об'єкти інформаційної безпеки, а також система органів (підрозділів), що здійснюють забезпечення; 3) політика інформаційної безпеки; 4) засоби і способи забезпечення інформаційної безпеки [251, с. 4-5]. Безумовно, насамперед, системний підхід є необхідною умовою для визначення загроз, а також пошуку оптимальних шляхів їх нейтралізації.

Автор дослідив політику держави у сфері інформаційної безпеки людини. Також, наголосив на необхідність утворення на рівні незалежного органу держави Уповноваженого з інформаційної безпеки людини, діяльність якого має бути спрямована на реалізацію політики держави щодо забезпечення інформаційної безпеки людини, в тому числі захист прав і свобод людини в

інформаційній сфері, зокрема, права на доступ до публічної інформації та захист персональних даних. Враховуючи специфіку справ, що пов'язані з порушенням інформаційних прав і свобод громадян, обґрунтовано доцільність створення спеціалізованого суду - Вищого інформаційного суду, запропонував віднести до його підсудності справи, що стосуються порушення прав людини на доступ до інформації, захисту персональних даних, дифамації, а також щодо реалізації прав громадян на участь у політичному житті, пов'язані з використанням інструментів електронної демократії [251, с. 6].

Загалом, автор зазначає, що необхідною умовою ефективної реалізації державної політики щодо інформаційної безпеки людини є проведення фундаментальних та прикладних наукових досліджень [251, с. 8].

Загалом значна кількість праць, включаючи дисертаційні, підготовлені представниками науки адміністративного права в Україні. Згадаємо, наприклад, ті, які пов'язані з вивченням аспектів розвитку інформаційного суспільства, інформаційної безпеки, інформаційної політики: І. Арістова «Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади» (Харків, 2002); Б. Кормич «Організаційно-правові основи політики інформаційної безпеки України» (Харків, 2004); О. Логінов «Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади» (Київ, 2005); Т. Субіна «Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України» (Ірпінь, 2010); В. Абакумов «Правове регулювання протидії інформаційним війнам в Україні» (Запоріжжя, 2011); В. Кір'ян «Правові засади розвитку інформаційного суспільства в Україні» (Київ, 2013); І. Сопілко «Правові засади державної інформаційної політики України» (Київ, 2014); Ю. Бурило «Правове регулювання інформаційної діяльності у сфері господарювання» (Київ, 2014); О. Климентьєв «Інформаційна функція Української держави» (Київ, 2014); М. Савюк «Адміністративно-правові засади інформаційного суспільства» (Київ, 2016); А. Нашинець-Наумова «Інформаційна безпека: питання правового

регулювання» (Київ, 2017); О. Головко «Інформаційно-правова політика України у сфері безпеки людини у медіа просторі» (Київ, 2018); Т. Перун «Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні» (Львів, 2019) та інші.

Прикметно, що не тільки учені – адміністративісти вивчають згадані питання, а також і цивілісти, криміналісти та інші науковці. Наприклад, відзначимо роботи О. Кохановської «Цивільно-правові проблеми інформаційних відносин в Україні» (Київ, 2006); О. Кулініч «Інформація з обмеженим доступом як об'єкт цивільних прав» (Одеса, 2006); Н. Савінової «Кримінально-правова політика забезпечення інформаційного суспільства в Україні» (Львів, 2013); О. Горпинюк «Кримінально-правова охорона інформаційного аспекту приватності в Україні» (Львів, 2011), В. Шаблистого «Теоретико-прикладні засади кримінально-правового забезпечення безпеки людини в Україні» (Харків, 2016); М. Кравцової «Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ» (Харків, 2016); О. Ващук «Антроподжерельна невербальна інформація в кримінальному провадженні: криміналістичні засади» (Одеса, 2018) та багато інших.

Не можна не згадати ґрунтовні теореретичні дослідження, підготовлені представниками науки теорії держави і права, що стосуються засад інформаційного суспільства, національної та інформаційної безпеки. Так, відзначимо дослідження М. Пендюри «Національна безпека України в контексті сучасних європейських геополітичних трансформацій (Київ, 2006); Ю. Максименко «Теоретико-правові засади забезпечення інформаційної безпеки України» (Київ, 2007); О. Присяжнюк «Основи концепції правового регулювання інтернет-відносин в Україні: (загальнотеоретичні аспекти)» **(**Харків, 2007); О. Тихомирова «Забезпечення інформаційної безпеки як функція держави» (Київ, 2011); Л. Арнаутової «Правове забезпечення інформаційної політики сучасної України в аспекті процесів європейської інтеграції» (Київ, 2014) тощо.

Зокрема, праці О. Присяжнюк вперше в українській юридичній літературі з позицій загальної теорії держави і права комплексно сформульовано засади та основні елементи концепції правового регулювання суспільних відносин, пов'язаних з використанням всесвітньої комп'ютерної мережі «Інтернет». Враховуючи значення інформації та комп'ютерної мережі як найбільшого у світі інформаційного середовища в становленні, розвитку та функціонуванні інформаційно-правового суспільства як наступника громадянського суспільства, обґрунтовується теза про визнання права людини на інформацію в якості однієї з найвищих сучасних соціальних цінностей. Отже, реалізація цього права людини на Інтернет повинна регламентуватися в Україні виключно законами.

Цікавою є позиція щодо сформульованої дефініції поняття «право віртуального простору» як сукупності юридичних норм – загальнообов'язкових, формально визначених правил поведінки, які встановлюють правовий статус учасників мережі «Інтернет», регулюють окремі види інформаційного обігу в цій мережі, що здатні впливати на життя, безпеку, здоров'я та майно людини, суверенітет, громадський порядок, безпеку та оборону держави. На підставі аналізу змісту норм права, що регулюють діяльність учасників мережі «Інтернет» у США, країнах Європейського Союзу та СНД, обґрунтовано, що право віртуального простору (інтернет-право) є комплексним полісистемним міжгалузевим правовим інститутом, який, подібно будь-яким іншим міжгалузевим правовим інститутам, має власний предмет правового регулювання, але, на відміну від галузей права, йому не притаманні власні методи правового регулювання суспільних відносин.

О. Присяжнюк пропонує доповнити загальновизнану в теорії права класифікацію видів об'єктів правовідносин на матеріальні та ідеологічні таким якісно новим видом об'єктів правовідносин, як інформаційний. Виходячи з аналізу особливостей охоронної правозастосовчої діяльності, яка виникає у зв'язку з неправомірними діями учасників мережі «Інтернет», певне програмне забезпечення, яке використовує держава з метою обмеження або заборони

доступу до тієї чи іншої інформації протиправного характеру, що розміщена на сайтах у цій мережі, повинно розглядатися як якісно новий вид державного примусу [468, с.2-3].

Пропозиція ж прийняття в Україні Основ законодавства з використання українського сегмента мережі «Інтернет», викладена більше як десять років тому, так і не втілилась у реальність.

Деяким іншим працям, присвяченим теоретичному аналізу здійснення функцій держави, в тому числі стосовно забезпечення інформаційної безпеки, а також її гарантування, приділимо увагу в наступних підрозділах длслідження.

Водночас прослідковується певний інтерес до вивчення інформаційної сфери, інформаційного суспільства та інформаційної безпеки в рамках міжнародного права.

Тут відзначимо насамперед серію праць, в тому числі аналітичного характеру, навчальні посібники, монографію та відповідні дисертаційні дослідження А. Пазюка. Його кандидатська робота *«Міжнародно-правовий захист права людини на приватність персоніфікованої інформації» (Київ, 2004)* і докторська дисертація *«Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти)» (Київ, 2016)* послідовно і системно засвідчують актуальність порушеної проблематики та широкомасштабно її розкривають, виходячи з аналізу правотворчої і правозастосовної практики держав і міжнародних організацій у цій сфері, вітчизняних і зарубіжних доктринальних здобутків.

Викладені у першій роботі пропозиції були враховані при підготовці Закону України «Про захист персональних даних» 2010 року внесенні змін і доповнень до значної кількості інших нормативно-правових актів України.

В іншій роботі розкривається поняття інфосфери – системи суспільних інформаційних відносин, які здійснюють суб’єкти права за допомогою використання існуючої на національному та глобальному рівнях інформаційної інфраструктури. Вона не обмежена ані фізично, ані у

правовому сенсі територіальними кордонами суверенних держав, оскільки складається із взаємопов'язаних інфраструктурних елементів на наднаціональному рівні. А розвиток міжнародно-правового регулювання інформаційної сфери зумовлений її транснаціональним характером, що випливає із взаємозв'язку внутрішньодержавної інформаційної інфраструктури з глобальною. Тому до основних функцій міжнародного права в інформаційній сфері відносять: 1) *координуючу* – щодо вироблення єдиних правил поведінки в інформаційній сфері на міждержавному рівні; 2) *регуляторну* – спрямовану на впорядкування міжнародних інформаційних обмінів між невладними акторами (фізичними та юридичними особами приватного права) транснаціональних інформаційних відносин; 3) *забезпечувальну* – щодо дотримання державами (як первинними суб'єктами міжнародного права) «правил відповідальної поведінки» в інформаційній сфері в цілому та в кіберпросторі зокрема; 4) *охоронну* – з підтримання міжнародного правопорядку в інформаційній сфері та покарання його порушників [441]. Виконання сприяє соціальному прогресу, розвитку глобального інформаційного суспільства.

А. Пазюк виокремлює міжнародне регіональне (панєвропейське) право в інформаційній сфері, що випереджає в розвитку міжнародне інформаційне право на універсальному рівні, з огляду на досягнутий рівень уніфікованості підходів на національному рівні та безпосередній вплив права Європейського Союзу, ефективне використання інструментів «м'якого» права у формі рекомендацій та резолюцій. Міжнародне інформаційне право є комплексною галуззю, з огляду на те, що вона становить систему міжнародно-правових норм, які виходять з різних базових галузей міжнародного (публічного) права і об'єднані єдиним предметом регулювання.

З-поміж основних напрямів правового регулювання і співробітництва дослідники переважно відзначають інформаційний контент, інформаційну і комунікаційну діяльність; використання обмежених інформаційних ресурсів (радіочастотний спектр, телефонні ресурси, доменні імена в Інтернеті;

забезпечення інформаційної безпеки, використання інформаційно-комунікаційних технологій в інтересах людства, запобігання та подолання наслідків стихійних явищ тощо.

Концепція права на комунікацію охоплює питання «доступу та участі», розглядаючи індивіда не лише як споживача інформаційного продукту, одержувача повідомлень від засобів масової інформації, а й як активного учасника суспільної комунікаційної діяльності, що є взаємодією і взаємовпливом у двосторонньому напрямі. Виходячи з результатів діяльності ЮНЕСКО і Ради Європи у сфері розвитку комунікаційної складової свободи інформації, відзначено потребу вивчення концепцій «вільного потоку інформації», «нового світового інформаційного і комунікаційного порядку», «нових комунікаційних стратегій», принципів «доступу та участі», що забезпечують участь громадськості в прийнятті рішень публічними інституціями. Отже, доступ до Інтернету розглядається як нова парадигма права на комунікацію, значущий спосіб реалізації прав, свобод та участі в демократії; у законодавстві Європейського Союзу – це зафіксована універсальна (загальнодоступна) послуга, що гарантується кожному якісно і за доступною ціною стверджувати, що свобода інформації є фундаментом демократичного суспільства і особистої свободи людини [441].

На нашу думку, право на свободу інформації включає широкий спектр можливостей для кожної людини і громадянина, проте повинні бути зафіксовані й інструменти контролю за дотриманням установлених меж правововового регулювання, запобігання виникненню загроз інформаційній безпеці та ефективній протидії.

Продовжується викладення цікавих і необхідних пропозицій, пов’язаних з удосконаленням основ функціонування інформаційного суспільства, у кандидатській дисертації *О. Кирилюк на тему «Міжнародно-правове забезпечення розвитку глобального інформаційного суспільства» (Київ, 2016).* Тут підкреслено трансформуючий вплив глобального інформаційного суспільства, під яким розуміється не просто нова суспільна формація, а вся

повнота правовідносин (правопорядок), що виникають в інформаційній сфері, а також унікальне поєднання демократичних інституцій, політичних режимів, сприятливого для інновацій середовища та активного і структурованого громадянського суспільства, що виникли та розвиваються в рамках глобального та інклюзивного кіберпростору, в якому відсутні фізичні кордони.

За авторським визначенням «кіберпростору» – це специфічне середовище, в межах якого на основі використання Інтернету та відповідних інформаційно-комунікаційних технологій здійснюється обіг товарів та послуг, відбувається комунікація та реалізація прав людини, ведеться боротьба за розподіл сфер впливу та формуються власні механізми управління глобальним інформаційним суспільством [287, 74].

Сучасний стан їх правового регулювання відзначається до певної міри нормативним індетермінізмом, що зумовлює необхідність вдосконалення класичних правових концепцій суверенітету, кордонів, громадянства, територіальності та юрисдикції з метою відображення еволюційних змін, викликаних розвитком інформаційних суспільств, включаючи глобальне. Водночас можна виокремити два основні типи інституційних моделей, у рамках яких відбувається формування політики та стандартів управління глобальним інформаційним суспільством. Перша модель ґрунтується на традиційному міждержавному механізмі, прикладом якого може бути співпраця в рамках ООН, а в основі іншої моделі лежить принцип багатосторонньої участі, що передбачає залучення різноманітних недержавних суб’єктів [287, 57].

Не слід заперечувати зростаючу роль міжнародних судових установ, зокрема Європейського суду з прав людини та Суду ЄС, у процесах стандартоутворення інформаційних відносин, практика формує основи правозастосування в аспекті розширювального тлумачення чинних міжнародно-правових норм. Разом з тим, на наш погляд, важливо уніфікувати стандарти захисту і транскордонної передачі персональних даних та кібербезпеки, прав людини онлайн, інформаційного простору і

правовопорядку. Це можливо за умови застосування єдиної системи цінностей (зокрема, пріоритет безпеки чи вільного обміну інформацією), відмови від категоричності формулювань та надання мінімальних обов'язкових гарантій.

О. Кирилюк підкреслює визнання безпеки необхідною передумовою стабільності та передбачуваності розвитку глобального інформаційного суспільства, тому роль міжнародного права полягає у створенні ефективних нормативних рамок та закріпленні належних гарантій безпеки інфраструктури, безпеки власне правовідносин, що виникають в інформаційній сфері. Крім того, потребують збалансування питання приватності та забезпечення кібербезпеки, що відзначаються компліментарним характером. Правовий режим безпеки кіберпростору повинен бути універсальним за своєю природою, оскільки йдеться про такі ключові для людства цінності, як міжнародний мир та стабільність. Фрагментація правового регулювання може привести до посилення регіональної співпраці, але це вирішує проблеми боротьби з кіберзлочинністю та забезпечення кібербезпеки, оскільки останні є глобальними явищами і потребують відповідного універсального механізму регулювання.

Відзначимо, що проблематика інформаційного суспільства та інформаційної політики, а ще частіше – інформаційної безпеки, досліджується не лише в різних галузях юридичної науки, а й не обходить стороною інші галузі вітчизняної науки.

Наприклад, варто відзначити деякі праці, підготовлені в межах науки державного управління, політичної науки, філософської науки та деяких інших, а саме:

О. Литвиненко «Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії)» (Київ, 1997);

К. Данилішина «Американський чинник в процесі інформаційної глобалізації» (Одеса, 2004);

В. Гурковського «Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки» (Київ, 2004);

В. Скалацького «Інформаційне суспільство: сучасні теорії та моделі (соціально-філософський аналіз)» (Київ, 2006);

М. Каращук «Інформаційна влада як чинник демократизації сучасного суспільства» (Київ, 2006);

Г. Камаралі «Становлення та розвиток інформаційної цивілізації» (Донецьк, 2007);

Л. Євдоченко «Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації» (Львів, 2011);

О. Зозулі «Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства» (Київ, 2017);

В. Антонюк «Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України» (Київ, 2017);

А. Головки «Громадянське суспільства як суб'єкт протидії загрозам національній безпеці в інформаційній сфері» (Київ, 2018);

О. Твердохліб «Формування та розвиток інформаційних державно-управлінських ресурсів України» (Київ, 2012);

І. Валюшко «Інформаційна безпека України в контексті російсько-українського конфлікту» (Миколаїв, 2018) та ін.

Зокрема, звернемо увагу на останню дисертаційну роботу з політичної науки, де на основі своєрідного підходу інформаційна безпека визначається фактором ефективного функціонування держав, важливою складовою національної безпеки. Тут визначено основні методи інформаційної війни Кремля, серед яких: маніпуляції в інформаційному просторі України, особливо у східних областях з метою трансформації мислення, ідеології, переконань, поглядів, сприйняття, культурної самобутності, національної ідентичності, історичної пам'яті; пропаганда та дезінформація; поширення за кордоном викривленої інформації та відвертої брехні про Україну тощо.

На переконання авторки, з початком російської військової агресії проти України розпочалася трансформація національного інформаційного законодавства, і питання інформаційної безпеки стало відображатися на

законодавчому рівні доктрин та стратегій, нових законів. Законодавство у сфері інформаційної безпеки України відзначається високою динамікою в останні кілька років, а в поєднанні із реструктуризацією системи національної безпеки може створити дієвий механізм стримування зовнішньої інформаційної агресії. Та реалії сьогодення засвідчують дещо інші тенденції й наслідки [155, 4].

Авторка зазначає , що у сучасних умовах інформаційної війни Росії поряд з існуючими інститутами інформаційної безпеки в Україні з'явилося ряд інституцій, покликаних забезпечити надійне та ефективне впровадження інформаційної політики держави. Однак, це викликає проблему великої кількості державних органів у сфері інформаційної безпеки, що часто призводить до дублювання їх функцій. Дана проблема потребує додаткового вивчення та опрацювання з урахуванням досвіду європейських країн. Разом з тим, в основі їх діяльності має бути ефективна координація між собою; налагодження системи діалогу між державою та суспільством; гнучка взаємодія з освітніми закладами; розробка навчальних програм із метою підвищити культуру використання інформації та формування навиків критичного оцінювання інформації [155, 12].

В умовах трансформаційних процесів у сфері інформаційної безпеки України, безумовно, посилюється важливість ролі дипломатії у вимірі інформаційної безпеки, діяльності українських ЗМІ як інструментів інформаційної безпеки, їх внутрішніх і зовнішніх завдань, а також роль освіти, недержавних та релігійних організацій у забезпеченні інформаційної безпеки в умовах конфлікту.

Поряд з дисертаційними та іншими монографічними дослідженнями, з огляду на загостреність та фрагментарність наукової розробленості комплексної проблематики, пов'язаної з інформаційною безпекою, тривалий час з'являються і колективні публікації вітчизяннх учених. Відзначимо, наприклад, деякі з них:

«Правові засади інформаційної безпеки України» за редакцією П. Біленчука (Харків, 2018);

«Світова гібридна війна: Український фронт» за загальною редакцією В. Горбуліна (Харків, 2017);

«Гібридна війна: in verbo et in praxi» за загальною редакцією Р. Додонова (Вінниця, 2017);

«Інформаційна війна і національна безпека» П.П. Ткачука, Р.В. Гули, О.І. Сивака, О.М. Щурко, В.В. Шемчука (Львів, 2015);

«Інформаційне суспільство: філософсько-правовий вимір» В.Г. Пилипчука, О.П. Дзьобань (Ужгород, 2014);

«Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій» О.С. Онищенка, В.М. Горового, В.І. Попика та ін. (Киїїв, 2011);

«Побудова націєцентричного культурно-інформаційного простору як шлях подолання соціальної конфліктності та солідаризації суспільства» відповідальні редактори М. Жулинський, А. Кравченко (Київ, 2017);

«Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід» за загальною редакцією С. Чернова та ін. (Запоріжжя, 2017) і т. д.

Підготовлено також значну кількість аналітичних доповідей з порушеної нами і згаданими вище дослідниками проблематики [176, 591, 521, 215], відбувається активний науковий дискурс у рамках міжнародних і всеукраїнських конференцій, семінарів і форумів тощо. Значна кількість публікацій навчального, науково-методичного і довідникового характеру також з’являлась і продовжує з’являтись на теренах України, завдання яких – розкрити теоретичні, методичні, галузеві та прикладні аспекти інформаційної безпеки. Так, виокремимо, зокрема, такі:

«Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» (Київ, 1999);

Нижник Н.Р., Ситник Г.П., Білоус В.Т. «Національна безпека України (методологічні аспекти, стан і тенденції розвитку)»: навчальний посібник за загальною редакцією П.В. Мельника, Н.Р. Нижник (Ірпінь, 2000);

Богуш В.М., Кривуца В.Г., Кудін А.М. «Інформаційна безпека: термінологічний навчальний довідник» за редакцією В.Г. Кривуци (Київ, 2004);

Харченко Л.С., Ліпкан В.А., Логінов О.В. «Інформаційна безпека України: глосарій» за загальною редакцією Р.А. Калюжного (Київ, 2004);

Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. «Інформаційна безпека України в умовах євроінтеграції»: навчальний посібник (Київ, 2006);

Кормич Б.А. «Інформаційна безпека: організаційно-правові основи»: навчальний посібник (Київ, 2008);

«Організація захисту інформації з обмеженим доступом»: підручник за загальною редакцією Є.Д. Скулиша (Київ, 2011);

«Менеджмент інформаційної безпеки»: підручник у 2 частинах за загальною редакцією Є.Д. Скулиша (Київ, 2013);

«Забезпечення інформаційної безпеки держави»**:** підручник за загальною редакцією О.А. Семченка та В.М. Петрика (Київ, 2015) тощо.

Отже, протягом останніх років активно до вивчення проблематики національної безпеки, інформаційної безпеки, еконономічної безпеки, екологічної безпеки, кібербезпеки, так само як й інформаційного суспільства, інформаційної політики, вдаються сучасні науковці, представники різних галузей сучасної вітчизяноної науки. Категорії «інформаційне суспільство», «інформаційна політика», «інформаційна безпека» відзначаються міждисциплінарним характером, тому розробляються вченими за напрямами різних наук: права, політології, історії, військової науки, управління, технічної науки тощо. У таких дослідженнях автори використовують численні підходи до розуміння природи і сутності згаданих явищ, розкривають їхній еволюційний характер, особливості тощо.

Розкриття природи, сутнісних характеристик та особливостей інформаційного суспільства, інформаційної політики, інформаційної безпеки спирається на сукупність методів наукового пізнання (діалектичний, аналізу і синтезу, системно-функціональний, порівняльний, історичний тощо). Використання різноманітних методологічних засобів та підходів дає змогу всебічно дослідити державно-правову реальність, простежити вплив правових норм на соціально-політичну дійсність і, навпаки, політичних, соціально-економічних та інших суспільних процесів – на національне законодавство, міжнародно-правові стандарти, краще зрозуміти їх феномени в сучасних умовах глобального інформаційного суспільства.

Аналіз підходів до вивчення функцій держави в сучасних умовах

Вивчення державно-правових явищ дає змогу виокремити певні тенденції й закономірності, що пов'язані насамперед з їх стабільністю та водночас динамікою, модернізацією. Еволюційне розуміння такого феномена, як «функції держави», зумовлено системним, порівняльним, діяльнісним та деякими іншими методологічними підходами. Використання історико-правового методу дало можливість багатьом сучасним дослідникам прослідкувати становлення та розвиток функцій держави на різних історичних періодах, зробити узагальнення та виокремлити позитивні й подекуди негативні результати такого еволюційного шляху функцій держави.

Власне через цей інститут можна проаналізувати різні аспекти державно-правової дійсності, організаційно-структурних або функціонально-діяльнісних проявів держави. Йдеться про її органи, посадових осіб, апарат держави, механізм держави, правовий вплив, ефективність механізму правового регулювання, правотворчий і правозастосовний процеси, з'ясувати реальні завдання і стан реалізації державної правової політики тощо.

Проблематика теорії функцій держави була в центрі уваги учених-державознавців ще з XIX ст. Функціональні характеристики держави вивчали українські та зарубіжні дослідники М. Байтін, С. Бобровник, У. Годвін, С. Гусарєв, О. Джураєва, Л. Дюгі, Г. Єллінек, Л. Каск, М. Кельман, Б. Кістяківський, М. Ковалевський, В. Копєйчиков, М. Коркунов, С. Котляревський, П. Лодій, О. Лощихін, В. Нерсесянц, П. Новгородцев, А. Нормантас, В.Оксамитний, В. Погорілко, М. Палієнко, Л. Петражицький, П. Рабінович, О. Скакун, О. Тихомиров, О. Фатхутдінова, Є. Фомицький, М. Чорноголовкін, В. Чхиквадзе, Г.. Шершеневич та інші. Як бачимо, це переважно представники ліберального напряму в державознавстві, теоретики анархізму, лібертаризму та інших напрямів правової думки.

Деякі сучасні дослідники підкреслюють, що наукове пізнання держави, виявлення її якісного стану в кожний конкретний період, шляхів розвитку,

обов’язково передбачає дослідження її функцій, що являють собою найважливіші якісні характеристики та орієнтири вдосконалення власне держави як особливої організації публічної влади, так і суспільства в цілому. Тому теоретико-правове дослідження держави та ефективності сучасної державності пов’язане насамперед з функціональною роллю держави в суспільстві настільки наскільки ефективно вона виконує свої функції [367].

Як відомо категорію «функція» запровадив німецький дослідник Г. Лейбніц для визначення залежності одних процесів або їх змін від інших (у математиці розуміється як залежність однієї величини від інших).

Різні її інтерпретації можна зустріти в політико-правовій думці, але часто використовуються звичні для теорії держави і права взаємопов’язані поняття «завдання», «цілі» та «функції» держави. При цьому категорія «функція» знаходить власне відображення і трактування у соціології як роль, яку певний соціальний інститут (або окремий соціальний процес) виконує щодо потреб суспільної системи більш високого рівня організації або інтересів класів, які її утворюють, соціальних груп та індивідів [146].

Відомий учений В. Нерсесянц трактує державу як живий організм, а її функції пов’язує з формами життєдіяльності такого організму (формами діяльності, що відображають її смислову сутність) [404 , с. 69].

Л. Каск присвятив свою увагу побудові зумовленої об’єктивними факторами моделі функцій держави, підкреслюючи взаємозв’язок і відносність понять «функція держави» і «структура держави», обґрунтовуючи підхід, за якого функції держави не ототожнюються ні з напрямами, ні зі сторонами державної діяльності й виражаються через зміст цієї діяльності [284, 5–16].

Можна зустріти позицію, коли, описуючи функціональну спрямованість держави, раніше використовували категорії цілі та завдання держави. Наукові дискусії точились, по суті, стосовно того, що в сучасній юридичній науці позначається функціями держави. І дослідникам удалося

сформулювати низку положень щодо функціональної характеристики держави, і це є незаперечним досягненням теорії держави і права.

У кінці XIX ст. на функціональний аспект дослідження держави звертали увагу Б. Чичерін та М. Коркунов, визначаючи не лише поняття й природу функцій держави, а й підходи до їх класифікації. Зокрема, вони поділяли функції держави на внутрішні та зовнішні відповідно до напрямів здійснюваної державою політики. Актуальною і дискусійною для теорії держави цього періоду була й проблема визначення цілей і завдань держави, а відтак – виділення тих функцій, які повинна виконувати держава для досягнення цілей, що стоять перед нею (М. Покровський та ін.). Згодом характерним було розширення сфери діяльності держави, що, як правило, пов'язувалося з демократизацією держави й суспільства, відповідними реформами, поступовим залученням населення до управління справами держави тощо.

Теоретики права визначають переважно функції держави передусім у контексті основних напрямів її діяльності. Як стверджував В. Копєйчиков, поняття «функція держави» пов'язано із втіленням сутності та соціальної спрямованості, завдань і цілей держави [598, с. 65]. Водночас, на переконання В. Оксамитного, функції держави спрямовані на вирішення завдань, що стоять перед державою на різних етапах розвитку, за допомогою спеціальних форм і методів їх реалізації; при цьому розподіл функцій на основні та неосновні є умовним [426, с. 222].

Нарешті, П. Рабінович зазначає, що вони розкривають соціальну сутність і призначення держави в суспільстві, при цьому основні функції, на відміну від неосновних, безпосередньо характеризують її соціальну сутність і призначення [529, с. 37].

Сучасні наукові 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 уточнюється зміст понять, за допомогою яких розкривається теорія функцій сучасної держави і, передусім, саме визначення поняття «функція держави».

Не дивлячись на те, що не спостерігається усталений єдиний підхід до розуміння функцій держави, а також, навпаки, численними є підходи та визначення цтого поняття, жодне з них не може претендувати на всеосяжність, належне відображення сутнісних характеристик і змісту категорії «функція держави». На думку О. Лощихіна, найбільш прийнятним є визначення поняття функцій держави як основних, постійних напрямів і видів діяльності держави, зумовлених об'єктивними потребами суспільного розвитку, внутрішніми й зовнішніми завданнями, в яких виражаються і конкретизуються сутність та соціальне призначення держави.

На його думку, таке формулювання оптимально віддзеркалює основні моменти в розумінні функцій держави на сучасному етапі. По-перше, воно відображає соціальну спрямованість діяльності сучасної держави та орієнтує цей суб'єкт на досягнення головної мети – забезпечення прав особи, її честі й гідності, вирішення найважливіших питань життєдіяльності людини та різних соціальних груп, інституціоналізацію громадянського суспільства в умовах глобальних суспільно-політичних трансформацій. По-друге, розкриває зміст діяльності держави та її динамічну спрямованість. По-третє, відображає місце держави в політичній системі суспільства як первинного суб'єкта, однак вторинної, субсидіарної щодо особистості й громадянського суспільства інституції. У роботі показано, що сучасний етап розвитку вітчизняного державознавства під впливом низки факторів характеризується певними змінами у використанні функціонального підходу. Зокрема, значно розширюється й поглиблюється розуміння соціального призначення держави, відкидається жорсткий зв'язок між змінами соціально-класових характеристик держави, її функцій тощо [367, с. 37].

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. Саме таку позицію відстоює, зокрема, В. Волинець. На його переконання, «функції держави – це динамічна характеристика держави, об'єктивно необхідні, юридично визначені, забезпечені правом та наповнені соціально значущим змістом основні напрями діяльності держави, в яких конкретизуються її цілі й завдання, відображаються її сутнісні характеристики» [169, с. 234].

О. Тихомиров відзначає, що визначення функцій держави лише як основних напрямів її діяльності є достатньо суперечливим, оскільки неможливо встановити чітку межу між основною й неосновною, більш важливою і менш важливою діяльністю держави. Крім того, класифікуючи функції держави, багато авторів розділяють їх за соціальним призначенням (або за значенням) на основні й неосновні (додаткові), що суперечить самому визначенню функцій держави. Тому доповнення «основні» повинно використовуватися лише в розгляді структурного зрізу функцій держави. Майже кожну основну в структурному аспекті функцію можна розділити на складові, які називають додатковими (неосновними) функціями [602].

Натомість, кожну додаткову функцію відносно її складових також можна вважати основною. Таким чином, функції держави організовуються в ієрархічну структуру, на вершині якої виявляється найбільш загальна функція. Такою функцією в сучасних державах є, зокрема, забезпечення національної безпеки, а додатковими щодо неї − забезпечення територіальної цілісності, конституційного ладу, прав і свобод громадян, науково-технічного потенціалу, високого рівня життя населення, інформаційної безпеки тощо [602].

Однак єдиного загальновизнаного підходу немає й дотепер, оскільки поняття «функція держави» є складним, багатогранним та різноплановим, що не дає можливості викласти його в лаконічному доступному формулюванні, зумовлює плюралізм підходів дослідників до інтерпретації функцій держави і

доцільність їх подальшого осмислення в контексті сучасних перетворень держави і суспільства.

Сучасна наука, залежно від того, в чиїх соціальних інтересах здійснюються функції держави, поділяє їх на загальносоціальні та функції захисту групових інтересів. Загальносоціальні функції − це довготривалі, спрямовані на задоволення інтересів суспільства в цілому, всіх його верств, напрями діяльності держави. Функції захисту групових інтересів являють собою такі напрями діяльності держави, що спрямовані на вираження і задоволення інтересів певних соціальних сил − правлячих угруповань, за якими стоять верстви населення, що становлять соціальну базу здійснення державної влади.

Сучасні тенденції розвитку держав, міждержавного співробітництва засвідчують про поступову деполяризацію суспільства, підкреслюють необхідність зміщення акцентів у розумінні функцій держави в сторону зумовленості їх суспільними потребами і належного закріплення й реалізації прав людини. Активізація розбудови громадянського та інформаційного суспільства зумовлює 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.).

Серед класичних (традиційних) критеріїв класифікації функцій держави відомі такі, як територіальна спрямованість діяльності держави, соціальне значення, період існування (здійснення) функцій та сфери суспільного (державного) життя.

Відповідно виокремлюють такі основні групи:

− внутрішні функції, що характеризують основні напрями діяльності, мету і завдання держави і здійснюються всередині країни, в межах території держави і є вираженням її внутрішньої політики;

− зовнішні, що здійснюються за територіальними межами держави, розкривають специфіку її інтересів, спрямованість діяльності в міжнародному

спілкуванні, виражаються у відносинах з іншими державами, державоподібними утвореннями та міжнародними організаціями. У цих функціях знаходить своє втілення зовнішня політика держави.

Це загальноприйнята класифікація функцій держави за сферами її діяльності. Внутрішні, і зовнішні функції держави взаємопов'язані між собою, діють у певній єдності, доповнюючи одна одну.

У свою чергу, за критерієм відносної значущості функцій держави їх розділяють основні, що розкривають соціальну сутність держави, та неосновні – ті, які їх доповнюють [391, с.131,139].

Що стосується різновекторних сфер життєдіяльності людини і суспільства, то підкреслимо доцільність виокремлення таких груп функцій:

1) політичні – формування і здійснення внутрішньої політики держави; створення сприятливих умов для реалізації народовладдя; встановлення офіційних дипломатичних, консульських та інших відносин з державами і міжнародними організаціями; оборонна діяльність держави, що передбачає захист економічними, дипломатичними та військовими засобами її суверенітету й території;

2) соціальні – створення сприятливих умов для усунення конфліктів і суперечок між різними верствами населення, реалізації права на працю, освіту, достатній життєвий рівень, охорону здоров'я тощо;

3) економічні – вплив на сферу виробничих відносин шляхом підтримки і розвитку всіх форм власності; торгово-економічних відносин з іноземними державами, створення і забезпечення функціонування системи оподатковування, бюджетної системи, інновацій тощо;

4) екологічні – охорона й забезпечення раціонального використання природних ресурсів, забезпечення екологічної безпеки суспільства, поліпшення екологічного стану планети, запобігання та ліквідація наслідків екологічних катастроф світового масштабу;

5) культурні – забезпечення консолідації етнічної нації, формування загальної для всієї країни культури, сприяння розвитку культури всіх народів,

які проживають на території держави, встановлення і розвиток культурних зв'язків з іншими державами; підтримка науки, освіти, мистецтва, фізичної культури й спорту; охорона культурної спадщини;

6) правоохоронні – контроль за дотриманням норм права, попередження і протидія злочинності, притягнення до юридичної відповідальності винних у правопорушеннях, забезпечення реалізації й захисту прав і свобод людини та громадянина, сприяння забезпеченню регіонального і міжнародного правопорядку, боротьба з міжнародними злочинами, запобігання виникненню міжнаціональних і міждержавних конфліктів;

7) інформаційні – забезпечення обміну інформацією в межах країни, сприяння інформатизації суспільства та участь у розвитку світового інформаційного простору з метою забезпечення вільного обміну інформацією, захисту інформаційних прав і свобод людини й громадянина, забезпечення інформаційного суверенітету та інформаційної безпеки тощо.

З-поміж інших видів функцій держави додатково виокремлюють ідеологічну та оборонну, правозахисну та інші.

Такий перелік функцій держави не є вичерпним, можливо навіть дискусійним, потребує уточнення й перегляду. Фундаментальні функції держави поступово втрачають домінуюче значення своєї територіальної спрямованості.

Т. Грицай виокремлює захист суспільної моралі як функцію сучасної держави, зокрема її теоретико-правові аспекти. Відзначено, що функції держави є неодмінним джерелом структурування державного механізму та основою для інституціоналізації функцій органів державної влади, тісно пов'язані з правом, яке виступає ключовим упорядковуючим, стабілізуючим, обмежуючим та регулюючим чинником як у їх конституюванні, так і в їх реалізації, взаємно детерміновані з правами людини і характеризуються наявністю чисельних взаємозв'язків та взаємодій, що загалом забезпечує гуманістичний зміст і спрямованість демократичної правової соціальної держави. У сучасному

суспільстві об’єктивна тенденція до збільшення кількості функцій держави шляхом розщеплення існуючих та виникнення нових таких функцій. Їх розвиток не має сталого лінійнго характеру, а зумовлюється складним комплексом дії різнопланових об’єктивних і суб’єктивних, внутрішніх і зовнішніх, постійних і тимчасових чинників [193].

Деякі дослідники розвиток теорії функцій держави у вітчизняній науці пов’язують з трьома основними етапами:

становлення теоретичних знань щодо функцій держави у політико-правовій науці з давніх часів – до початку XX ст.;

радянський період, коли сформувалася й утвердилася марксистсько-ленінська теорія держави та права;

від початку 90-х років XX ст., коли відбувається переосмислення традиційного вчення про функції держави, предметом дослідження стає аналіз наукових поглядів на функції держави, в тому числі тих, які були сформовані у дорадянській юридичній науці.

Звертаючи увагу на деякі недоліки радянської теорії функцій держави, автори наукових праць стверджують, що дослідження поняття функцій, їх системи та механізму реалізації були і в цілому залишаються методологічною базою для сучасних досліджень функціональних аспектів української державності, проблем державотворення та правотворення, модернізації держави й суспільства. Водночас деякі позиції потребують певного коригування, оскільки вчення про державні функції розвивалося переважно в рамках теорії соціалістичної держави; теорія держави та права могла існувати та розвиватися виключно як марксистсько-ленінська. Звідси абсолютизація класової природи держави та її функцій, економічний детермінізм, перебільшення творчих можливостей соціалістичної держави та одночасне применшення аналогічної ролі держави в інших соціально-політичних системах тощо. Тобто ідеологічна заангажованість окремих теоретичних позицій очевидна та навряд чи може сприяти подальшим дослідженням функціональної ролі сучасної держави [367, с. 32].

На думку С. Сунєгіна, сучасні реалії потребують переосмислення оцінок функціональної характеристики держави шляхом зміщення акцентів з розгляду їх зовнішньої атрибутики (наприклад, опис відповідних напрямів діяльності держави, визначення концептуальних шляхів розвитку й удосконалення функцій держави тощо) на суб'єктний, внутрішньо-змістовний рівень їх здійснення, тобто на ціннісно-смислову систему координат, яка панує в суспільстві та якою керуються безпосередні суб'єкти здійснення функцій держави.

Основоположними цінностями функцій держави він визначає насамперед відповідні норми та принципи традиційної моралі, за допомогою яких діяльність держави в особі уповноважених органів державної влади не може обмежуватися лише утилітарними прагненнями, не кажучи вже про суто особисті інтереси конкретних посадових осіб державних органів, а спрямовується на створення міцних солідарних засад розвитку будь-якої соціальної взаємодії, завдяки яким загальний успіх стає необхідною передумовою або обов'язковою умовою досягнення особистого блага та щастя [589, с. 269–277].

Далі відстоюється точка зору, згідно з якою незважаючи на те, що здійснення функцій держави регламентується за допомогою права, його норм і принципів, не всі аспекти конкретних напрямів діяльності держави можуть бути врегульовані правом. Останнє пов'язано з тим, що здійснення державної влади, а відтак і функцій держави, завжди відбувається шляхом волевиявлення конкретних суб'єктів, що об'єктивно не піддається всеохоплюючому правовому контролю. У зв'язку з цим невиправданою слід визнати постановку питання про повне підкорення держави праву, оскільки завжди були й залишатимуться в майбутньому системні хвороби державного апарату (наприклад, бюрократизм, корупція, службові проступки і злочини тощо), які пов'язані насамперед із низькою моральною свідомістю осіб, уповноважених на виконання завдань і функцій держави, а отже, з падінням авторитету морально-релігійних принципів організації суспільного життя та втратою ними у зв'язку з цим свого справжнього регулятивного потенціалу [589, с.

269–277]. Крім того, здійснення державних функцій неможливе без адміністративного, законодавчого, судового розсуду, без необхідності оперативно випереджати правове регулювання нових суспільних відносин, а отже, без дії або належного впливу таких соціальних регуляторів як мораль, релігія, традиції тощо.

Навіть якщо держава формально проголошує та нормативно (юридично) закріплює ціннісний або ідеологічний плюралізм, її діяльність, виражена або об'єктивована у повноваженнях органів державної влади та їх посадових осіб, завжди зорієнтована на конкретновизначену систему цінностей, які мають нерозривний об'єктивно-суб'єктивний вимір. З цього випливає, що цінність предметної діяльності, зокрема функцій держави, має осмислюватися або досліджуватися крізь призму аналізу тих суб'єктивних ціннісних пріоритетів, що спрямовують та визначають людські дії, вчинки, поведінку в цілому.

Незважаючи на те, що розумові здібності, освіта і професійний досвід становлять фундамент здійснення будь-якої інтелектуальної діяльності, особливо тієї, яка пов'язана з виконанням завдань і функцій держави, а також визначають широту й глибину відповідного пізнавального інтересу, вони можуть проявлятися лише через стан внутрішнього, морально-духовного світу людини, який повинен бути на високому рівні, що забезпечує можливість індивіда виходити за межі самого себе, свого життя та інтересів, тобто звичайних меж своєї особистості. Саме внутрішня моральна інтенція надає справжнє значення, позитивну якість та найвищу вартість іншим людським якостям і соціальним цінностям, зокрема розуму, таланту, здібностям, волі, науці, мистецтву, промисловості тощо, спрямовуючи їх на досягнення певного ідеалу чи абсолютного призначення. У протилежному випадку особа, уповноважена на виконання функцій держави, професійно використовуватиме визначені у законодавстві владні повноваження лише з метою задоволення особистих інтересів, прив'язаних здебільшого до її біологічної природи [589, с. 269–277].

Отже, конкретний зміст функцій держави як основних напрямів її діяльності пов'язаний з практичною реалізацією значного обсягу повноважень, якими наділені відповідні органи державної влади, а у випадку делегованих повноважень – також й інші суб'єкти. Іншими словами, лаконічна програмна формула поняття «функції держави» деталізується у процесі діяльності суб'єктів владних повноважень, за допомогою якої забезпечується необхідний нормативно-організуючий вплив на суспільство, а також реальне втілення в соціальне життя законності та правопорядку. Останнє випливає з того факту, що реалізація функцій держави здійснюється за допомогою діяльності системи уповноважених органів державної влади, внаслідок якої досягаються цілі та завдання держави, пов'язані з упорядкуванням суспільних відносин, забезпеченням належних умов для гармонійного розвитку людини і громадянина, охорони й захисту їх прав, свобод і законних інтересів тощо.

У той же час не слід ототожнювати чи змішувати такі категорії як «функції держави» і «функції органів державної влади» або «повноваження органів державної влади», оскільки останні мають конкретний характер та спрямовані на вирішення чітко визначених цілей і завдань державної влади. Так само не є тотожніми «функції держави» та «функції права». Водночас, на наш погляд, вивчення особливостей природи і сутнісних характеристик останньої категорії, як і їх співвідношення, можуть становити предмет окремих самостійних досліджень.

Зупинимось на деяких наукових працях, зокрема дисертаційних дослідженнях, де ґрунтовно, системно розкривається ця тематика.

Наприклад, у роботі *О. Джураєвої «Функції сучасної держави» (Одеса, 2006)* охарактеризовано сучасну державу з урахуванням її статики та динаміки, комплексно досліджено і з'ясовано поняття та сутність сучасної держави, природу та сутність функцій сучасної держави як загальнотеоретичних категорій, їх основні ознаки. Авторка чітко проводить розрізнення між функціями держави, державними послугами та державною

політикою. Тут визначено вплив глобалізації та персоніфікації на функції сучасної держави, а також розглядаються деякі з таких функцій [204, с.20].

Доволі дискусійним є висновок про те, що у зв'язку з невизначеністю соціальних ситуацій, з якими має справу сучасна держава, її функції значною мірою починають набувати пошуково-експериментального характеру. Отже, функції сучасної держави стають дедалі більш координаційними, рекомендаційними. Зазначено, що при цьому не виключаються елементи адміністрування, особливо у сфері здійснення податкової і митної політики. Прикметно, що О. Джураєва розмежовує поняття «державні послуги», яке деякою мірою схоже за змістом, а також за суб'єктами їх виконання з функціями держави:

1) державна послуга делегована, а державна функція – ні (за винятком установлених окремим переліком функцій, що можуть, у деяких випадках, передаватися саморегулюючим організаціям;

2) згідно з етимологією слова під «послугою», переважно, розуміються дія, вчинок, що надає користь, допомогу іншому, також це діяльність підприємств, організацій та окремих осіб, що виконується для задоволення чиїхось потреб, обслуговування, служіння і т. ін. [204, с. 20].

Можна погодитися, що з-поміж низки важливих проблем сучасної правової політики є звільнення держави від надлишкових функцій шляхом їх законодавчого переведення до сфери державних послуг. Правова політика покликана визначити, які державні функції не можуть бути передані іншим суб'єктам, іншими словами, необхідно інвентаризувати державні функції.

Наступною науковою працею, яка представляє інтерес у рамках нашого дослідження, є дисертація *О. Климентьєва «Інформаційна функція Української держави» (Київ, 2014).* Він присвятив значну увагу проблемам інформаційної функції як різновиду основних функцій Української держави. Авторська позиція відображається у розв'язанні конкретних правових проблем, пов'язаних із формуванням, розвитком та правовим регулювання інформаційної функції держави.

У згаданій роботі визначено поняття «функції держави» як опосередковані метою ефективного розвитку держави, зумовлені пріоритетами реалізації першочергових завдань державної політики, основні напрями її діяльності у внутрішній та зовнішній сферах, що виражають її реальну роль, форму, сутність і соціальне призначення в певній сфері життєдіяльності. Також сформульовано алгоритм дослідження інформаційної функції держави та її склад як сукупність таких елементів: мета, завдання, суб'єкти, об'єкти, форми та види, способи та засоби (ресурси та фактори), напрями державної політики [292, с. 21].

Важливо, що певна увага приділяється класифікації інформаційних функцій держави, зокрема, основні їх групи та підгрупи виділяються на підставі таких критеріїв:

– сфера інформаційних відносин – інформаційна безпека, розвиток інформаційного суспільства, е-урядування, інформатизація, телекомунікації та зв'язок, захист прав і свобод людини;

– об'єкти реалізації життєво важливих національних інтересів – особи, суспільства, держави;

– суб'єкти реалізації і склад – одноособові й колективні;

– термін дії – постійні й тимчасові;

– походження – державні й недержавні;

– характер компетенції – загальні й спеціальні;

– за локалізацією – секторальні, державні, міждержавні, наддержавні;

– пріоритетність – пріоритетні, основні, забезпечувальні;

– форма визнання – відкриті, латентні.

Дозволимо не погодитись із твердженням, що оскільки сутність інформаційної функції держави полягає в забезпеченні людині та громадянину права на доступ до інформації, інформаційної відкритості та ін., оптимальною для її реалізації є демократична унітарна республіка. Важаємо, що здійснення інформаційної функції держави можливе і необхідне за будь-якої форми

державного устрою, інших форм сучасної держави. Водночас, певні особливості здійснення інформаційної функції держави, напрями її функціонування зумовлені впливом елементів тієї чи іншої форми держави на процес її здійснення.

Так само видається недоцільним прийняття спеціального законодавчого акта, який закріплював би дефініцію інформаційної функції держави та визначав основні способи її здійснення, як і необхідність закріплення інформаційної функції держави в майбутньому Інформаційному кодексі. Навряд чи можливо нормативно врегулювати забезпечення реалізації інформаційної функції держави у двох нормативно-правових актах.

Багато науковців виокремлюють розуміння поняття інформаційної функції Української держави в широкому та вузькому значенні. У першому випадку, висловлювалася думка про можливість виокремлення в межах інформаційної функції двох похідних функцій: функції інформаційного забезпечення діяльності держави та інформаційно-комунікативної функції. Остання більше відповідає сучасному етапу розвитку глобального інформаційного суспільства.

Слід зазначити, що інформаційна функція характерна не лише для держави чи суспільства, вона стосується і права. Таку позицію підтримує низка вітчизняних і зарубіжних учених (І. Антошина, О. Макеєва, Є. Корж, Н. Оніщенко, А. Червяковський та ін.). Зокрема, в роботі *І. Антошиної «Інформаційна функція українського права» (Одеса, 2015)* підкреслюється специфіка інформаційної функції права як основи правової інформованості в Україні. Її результатом є правова інформованість особистості та українського суспільства в цілому, як сукупність достовірних знань про діюче право та способи його реалізації в конкретних відносинах [120, с. 20].

О. Макеєва зазначає, що інформаційна функція права полягає у доведенні до громадян правової інформації, впливає на правосвідомість особи та на формування правової культури суспільства. Механізм реалізації інформаційної функції права – це система правової інформації, суб’єктів,

об’єктів і юридичних засобів правового інформування, що сприяє підтриманню інформаційної цілісності правової системи. Реалізація цієї функції права втілюється у забезпеченні режиму доступу громадян і посадових осіб до правової інформації, виявляється в таких формах: інформаційно-психологічній, виховній та соціальній. Безумовно, подальше наукове дослідження проблем інформаційної функції права та її вплив на правову культуру суспільства необхідне для утвердження принципу верховенства права, ефективної правотворчої і правозастосовчої діяльності, забезпечення законності і правопорядку в суспільстві. Від ефективності інформаційного впливу права залежить рівень правової культури суспільства [373, с. 47–51].

На думку О. Остапенка, **с**еред великої кількості зовнішніх та внутрішніх функцій Української держави інформаційна функція посідає особливе місце. Однією з її особливостей є ефективна організація розвитку інформаційного суспільства, що сприяє впровадженню е-урядування. Інформаційно-правові відносини є складовим елементом інформаційної функції держави. Вони впливають на:

1) сутність та зміст інформаційної функції держави;

2) ознаки, що характеризують інформаційну функцію держави, взаємопов’язані та взаємообумовлені з ознаками інформаційно-правових відносин (наявність регулятивних, охоронних та спеціалізованих норм права, наявність суб’єктів, які реалізують інформаційну функцію держави);

3) середовище формування інформаційної функції держави;

4) методи та засоби реалізації інформаційної функції держави [437].

С. Кухтик у роботі «Трансформація держави під впливом глобалізації (теоретико-правовий аспект)» (Київ, 2015) обґрунтовує взаємопов’язаність усіх функцій держави. Нині складно провести межу між внутрішніми та зовнішніми напрямами діяльності держави, саме тому в класифікації функцій держави вживаються терміносполучення «переважно зовнішні», «переважно внутрішні» та «змішані». Наводяться приклади модернізації зовнішніх

функцій держави в контексті глобалізаційних викликів, зокрема функції оборони.

За таких умов можна відзначити як позитивні, так і негативні риси такого впливу. До першої групи таким чином належить те, що держави: обмінюються досвідом у сфері здійснення оборонних заходів; постачають одна одній зброю, військову техніку тощо; вступають у міжнародні організації, альянси з метою підвищення власної обороноздатності. Водночас негативними рисами впливу глобалізаційних процесів на функцію оборони є такі: виникнення міжнаціональних, міжетнічних конфліктів, почастішання випадків прояву сепаратизму, екстремізму тощо [343, с. 60].

В. Сало у дисертації «*Внутрішні функції держави в умовах членства в Європейському Союзі*» (Харків, 2008) дослідив процес становлення теорії функції держави, розкриваючи поняття й ознаки функції держави, принципи взаємодії ЄС і держав-членів стосовно реалізації функцій держави. З-поміж основних внутрішніх функцій держав-членів ЄС найбільш поширеними є функції охорони та захисту прав і свобод людини та громадянина, економічні та соціальні функції тощо [550, с. 22].

Разом з тим, видається не зовсім точним відзначення специфіки функціонування держав за умов членства в ЄС як наддержавній організації влади. На наш погляд, і це підтверджується численними науковими працями, ЄС становить особливе наднаціональне утворення, держави-члени якого здійснюють власні зовнішні та внутрішні функції, проте не в тому обсязі, який існував до моменту набуття членства в цьому утворенні. Для Європейського Союзу властиві також виключно його функції і завдання, вивчення яких є доцільним в умовах відносин асоціації з Україною та перспективного її членства.

У докторській дисертації *Л. Наливайко «Державний лад України: поняття, система, гарантії» (Харків, 2010)* проаналізовано теоретико-правові проблеми становлення та розвитку сучасного перехідного за змістом державного ладу України й розкрито теоретико-правові основи «функцій

держави» за умов переходу України до демократичної моделі державного ладу. Вона вважає, що функції держави – це об'єктивно необхідні, взаємопов'язані напрями та види її діяльності, спрямовані на реалізацію її завдань, досягнення відповідної мети в конкретних формах за допомогою спеціальних методів, які виражають сутність, соціальне призначення держави, роль та місце її в суспільстві на конкретному етапі розвитку [399, с. 40].

Авторка провела класифікацію, розкрила теоретико-правовий зміст об'єктних функцій держави на сучасному етапі, форми та методи їх реалізації. Ключовим при цьому є підхід до визначення сутності генези та структури механізму Української держави як інституціонального елемента державного ладу.

Окрім праць, присвячених виключно теоретичним засадам функцій держави, активно в сучасній юриспруденції вивчаються окремі функції держави, форми їх здійснення тощо.

Так, *О. Лощихін у роботі «Теоретико-правові характеристики економічної функції сучасної держави» (Київ, 2010)* розкриває діалектику взаємодії держави, суспільства й економіки як об'єктивної основи формування економічної функції держави. Проаналізовано економічні інтереси сучасної держави та правові проблеми їх реалізації в контексті організації економічного ладу суспільства. Автор дослідив основні чинники становлення та правові проблеми реалізації економічної політики як пріоритетного напряму економічної діяльності сучасної держави [367].

Звісно, на сьогодні немає єдиного підходу до розуміння функцій держави; а за багатоманітності визначень поняття, жодне не може претендувати на всеохопність, адекватне відображення сутності та змісту категорії «функція держави». На думку згаданого дослідника, найбільш прийнятним є визначення поняття функцій держави як основних, постійних напрямів і видів діяльності держави, зумовлених об'єктивними потребами суспільного розвитку, внутрішніми й зовнішніми завданнями, в яких виражаються і конкретизуються сутність та соціальне призначення держави [367].

Безперечно, наявний взаємозв'язок між економічними правами та свободами людини і громадянина й процесами реалізації економічної функції держави.

Схожу проблематику вивчає *О. Варич у роботі «Економічні функції сучасної держави: природа, зміст, тенденції розвитку в Україні» (Київ, 2006).* Тут звернуто увагу на природу та сутність функцій держави як загальнотеоретичної категорії. Підкреслюється вплив держави на економічну сферу, їх взаємозв'язок, а також проблеми меж втручання та напрямів взаємодії держави й суспільства, методи державного регулювання економічних відносин, зміст економічних функцій держави, принципи та форми їх здійснення [156, с. 20].

У свою чергу, *В. Тисянчин* підкреслює еволюцію підходів до розуміння ролі держави для економічної системи суспільства, в тому числі в кризові періоди. У його дисертації *«Правові форми здійснення економічної функції держави: теоретичні і практичні аспекти» (Львів, 2011)* з'ясовано співвідношення економічної функції й економічних завдань держави, досліджено правотвірну форму проведення економічної функції держави, основні проблеми та визначено напрями удосконалення виконавчої діяльності в Україні в економічній сфері, зокрема правовий інструментарій антикризової діяльності публічної влади України за умов світової фінансово-економічної кризи [600, с.16].

Згодом у роботі *С. Мельничук «Правові форми реалізації функцій сучасної держави Україна» (Київ, 2019)* обґрунтовано основні концептуальні положення щодо правових форм реалізації функцій сучасної держави Україна як цілісного процесу. Тому сформована пізнавальна конструкція, яка дала змогу дослідити це явище в контексті трансформації суспільства. Обґрунтовано необхідність здійснення постійного моніторингу правових форм реалізації функцій сучасної держави Україна, зокрема правотворчої, інтерпретаційно-правової, правозастосовної, внаслідок чого можна виявити проблеми їх здійснення та запропонувати основні засоби розв'язання [388].

У нещодавніх дослідженнях, окрім економічної функції, приділяється увага також фіскальній функції держави. Тому звернемося до праць Д. Носікова «Фіскальна функція сучасної держави: теоретико-правовий аспект» (Харків, 2016) та Є. Дуліби «Фіскальна функція держави: адміністративно-правовий аспект» (Дніпро, 2019). У першій з них зроблено висновок про те, що фіскальна функція є складовою частиною економічної функції держави і складається з трьох підфункцій: податкової, митної та бюджетно-штрафної. Фіскальна функція держави є її іманентною ознакою на всіх етапах історичного розвитку. А фіскальна політика в цілому, як і всі її елементи, реалізується через правову політику держави, виступаючи різновидом останньої за сферою реалізації [415, с. 20].

Серед інших функцій сучасної держави активно вивчаються екологічна, соціальна, правоохоронна, правозахисна та деякі інші.

Наприклад, В. Вашкович розглядає соціальну функцію держави, що не є органічним напрямом діяльності держави і виникає на певному етапі її історичного розвитку. Зміст цієї функції в широкому розумінні передбачає її визначення як діяльності держави, що покликана забезпечити соціальний захист, соціальне забезпечення, охорону здоров'я та нормальні умови життя для всього населення. Для громадянина соціальна функція держави виступає в якості соціальних стандартів життя або соціальних норм і нормативів. У державотворчих процесах соціальна функція держави повинна мати своє відображення в структурно-організаційному та інструментальному аспектах: з одного боку, держава повинна створити достатні структури в механізмі держави та інші органи публічної влади, а з іншого – вона повинна наділити їх достатнім інструментарієм (можливістю видавати акти, укладати договори тощо), а також інтегрувати до реалізації цієї функції інших суб'єктів, у тому числі й суб'єктів приватного права, так само наділяючи їх правовими інструментами у здійсненні соціальної функції [158, с. 2].

Здійснення цієї функції перестає бути виключно прерогативою держави та її органів. Не дивлячись на те, що переважна більшість

повноважень, які реалізуються на виконання соціальної функції, залишаються і будуть залишатися у сфері діяльності держави, частину з них держава розподіляє між органами місцевого самоврядування та приватними суб'єктами. Тому обґрунтовується поняття «приватизація соціальної функції держави», що може здійснюватися через делегування повноважень недержавним утворенням, а також через надання цих повноважень. Шляхом надання повноважень держава включає до їх компетенції такі повноваження, якими до цього вони не володіли, або передає від одного владного суб'єкта до іншого.

Видається, з-поміж згаданих вище функцій держави чимало уваги приділено саме правоохоронній функції. Так, Й. Горінецький розкриває теоретичні й практичні аспекти правоохоронної функції держав Центральної Європи. Цю функцію держави розглянуто як самостійний і пріоритетний напрям державної політики, основною метою якого є захист за допомогою юридичних засобів принципів конституційного ладу та права загалом (зокрема, прав, свобод і законних інтересів людини та громадянина, зміцнення законності та правопорядку), що одночасно виступає правовою формою досягнення інших цілей суспільства держави [186, с.20].

Р. Шай дослідив теоретико-практичний аспект правоохоронної функції правової держави. Із позицій теорії держави і права розглянуто наукові підходи щодо природи права та його ролі у формуванні й функціонуванні держави. Відзначено еволюцію функцій держави в процесі розвитку суспільства, роль і місце правоохоронних органів у правовій державі через розкриття природи та сутності правоохоронної діяльності, а правопорядок і законність розглянуто як важливі ознаки правової держави. Тобто правоохоронні органи є суб'єктом реалізації правоохоронної функції правової держави через координацію правоохоронної діяльності у правовій державі [649, с. 20].

Виокремлено пенітенціарну функцію демократичної правової держави та роль громадянського суспільства в механізмі її реалізації у праці

О. Романенка. Зокрема, на підставі аналізу загальнотеоретичного поняття «функція держави» він дійшов висновку, що для розгляду будь-якого напряму державної діяльності як функції держави, необхідно, щоб у ньому відображалась та предметно конкретизувалася сутність та соціальне призначення держави, її цілі та завдання. З урахуванням того, що в теорії держави процес появи нових функцій, трансформації або зникнення вже існуючих найчастіше пов'язують із динамічністю завдань, які ставляться перед державою і відображають потреби суспільства, зроблено висновок, що постановка питання щодо можливості існування тієї чи іншої функції держави потребує передусім визначення суспільних потреб і відповідних до них завдань держави. Тому автор доводить, що однією із суспільних потреб є забезпечення безпеки суспільства, включаючи злочинні посягання. Це дає підстави стверджувати, що одним із завдань, яке стоїть перед державою, є забезпечення безпеки суспільних відносин, за рахунок чого забезпечуватиметься захист інтересів особи, суспільства і, безумовно, самої держави від злочинних посягань.

Розділяємо точку зору О. Романенка стосовно того, що держава (механізм держави) та інститути громадянського суспільства розглядаються як складові елементи єдиного механізму, діяльність якого спрямована на створення умов для реалізації потреб й інтересів людини. З одного боку, держава створює умови для розвитку громадянського суспільства і нормативно обмежує своє втручання в діяльність його інститутів, а з другого – інститути громадянського суспільства утримуються від вчинення дій, заборонених нормами права, і спрямовують свою діяльність на задоволення потреб та інтересів громадян. Для кожного історичного етапу і сфери суспільних відносин обґрунтовуються підстави, які обумовлюють об'єктивну необхідність участі інститутів громадянського суспільства в реалізації основних напрямів діяльності держави. Так, участь інститутів громадянського суспільства в реалізації пенітенціарної функції держави обумовлена

загальними об’єктивними закономірностями виникнення держави та її взаємодією з громадянським суспільством [538, с. 21].

На нашу думку, участь інститутів громадянського суспільства в реалізації інших функцій держави обумовлена, окрім згаданих загальних об’єктивних закономірностей розвитку держави, органів влади, потребою взаємодії з населенням, здійсненням громадського контролю, розвитком інформаційно-комунікаційних технологій, становленням і забезпеченням безпеки національного та світового правового порядку, захистом прав і свобод людини і громадянина тощо.

Поряд з цим, наше завдання передбачає з’ясування не тільки проблемних питань, пов’язаних з поняттям чи класифікацією функцій держави, їх аналізу, а й вивчення природи відносно нової функції сучасної держави – інформаційної. Також можна зустріти виокремлення додатково функції забезпечення інформаційної безпеки, інформаційно-виховної, комунікативної та інших схожих функцій. Це зумовлює необхідність визначення їх місця в системі існуючих функцій держави.

Різноманітні аспекти здійснення функцій держави в інформаційній сфері стали предметом уваги науковців. Йдеться про серію наукових праць *І. Дороніна* (*монографії* «*Теоретико-правові основи реалізації функцій держави в інформаційній сфері», «Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки» й ін.),* дослідження *І. Колодій «Адміністративно-правове забезпечення інформаційної безпеки банківських установ в Україні» (Київ, 2014),* монографію *О. Тихомирова «Забезпечення інформаційної безпеки як функція сучасної держави» (Київ, 2014)* та ін.

В останньому випадку здійснено теоретико-правове осмислення забезпечення інформаційної безпеки як функції сучасної держави; сформовано методологічний підхід, який дає змогу розглядати забезпечення інформаційної безпеки як своєрідну діяльність, одним з основних, але не єдиним суб’єктом якої є держава. Структуровано зміст цієї діяльності, охарактеризовано її елементи в контексті становлення інформаційного суспільства й розбудови

правової держави. Надано правову інтерпретацію інформаційної безпеки та визначено загальні гарантії її забезпечення в правовій сфері [602].

Сучасний стан, значущість і перспективи розвитку інформаційного простору, невиправдані сподівання на ефективність саморегуляції Інтернету та інших глобальних інформаційних мереж доводять необхідність виваженого державного впливу в інформаційній сфері на національному й міжнародному рівнях, особливо стосовно забезпечення інформаційної безпеки. Ця необхідність додатково посилюється новітніми проблемами інформаційної безпеки − захистом інформаційного суверенітету держави, забезпеченням безпеки в кібернетичній сфері, зокрема протидією кіберзлочинності й кібертероризму, захистом критичної кібернетичної інфраструктури держави та іншими [602, с. 6].

Такі відомі учені як М. Байтін та І. Сенякін, В. Нерсесянц раніше не виокремлювали інформаційну функцію держави в самостійну. В останніх вітчизняних публікаціях В. Волинця, С. Глазунової, О. Климентьєва, Т. Костецької, Ж. Павленко та інших авторів активізувалось питання не лише про її виокремлення, а й про її особливості забезпечення, відмінності від інших функцій держави тощо.

Інформаційна функція держави стала об’єктом наукових досліджень порівняно недавно, оскільки за радянських часів інформаційна діяльність держави розглядалася правознавцями в контексті політико-правового забезпечення існуючої ідеології [683, с. 66 – 69].

На користь виокремлення інформаційної функції держави запропоновано такі аргументи. Інформатизація сучасного суспільства передбачає проникнення інформаційних технологій практично в усі сфери суспільного життя, що надає провідного значення діяльності держави, пов’язаній із забезпеченням вільного обміну інформацією, інтеграцією у світове інформаційне суспільство, забезпеченням інформаційної безпеки тощо. Така синкретизація класифікації функцій держави знижує актуальність і значущість їх розподілу на внутрішні й зовнішні, що особливо помітно в

умовах інтеграційних і глобалізаційних процесів у світовому співтоваристві, які розмивають грань між внутрішньою та зовнішньою сторонами економічної, політичної, соціальної й екологічної діяльності держави, і підтверджується дослідженнями останніх років [204, с. 20].

Поряд з інформаційною функцією держави згадують і про інформаційно-виховну функцію, інформаційно-комунікативну функцію держави тощо. Так, існує точка зору, що сучасному етапу розвитку суспільства більше відповідає остання зі згаданих функцій. Адже комунікація − це обмін інформацією, що має на увазі суб'єкт-об'єктні відносини й обов'язкове застосування принципу зворотного зв'язку. А при переході на так звану сервісну державу, що надає громадянам і організаціям послуги швидко та якісно, необхідно налагодити взаємодію державних структур з громадянами та організаціями, ту саму комунікацію, тобто взаємний обмін інформацією, що сьогодні має нерівноправний, далеко не партнерський і зовсім нерівний характер, як того потребують принципи розвитку демократичного суспільства [411, с.40].

На наше переконання, очевидно, що серед вчених-правознавців немає єдиної точки зору на те, що як явище виникла, існує й розвивається нова функція держави – інформаційна і, відповідно, щодо конструювання терміну «інформаційна функція держави».

Ж. Павленко у широкому розумінні інформаційну функцію трактує як загальносоціальну головну функцію держави, в якій можна виділити дві похідні функції: функцію інформаційного забезпечення діяльності держави в цілому, її органів, установ, посадових осіб та інформаційно-комунікативну функцію, тобто функцію інформаційного обслуговування громадян – діяльності державних і суспільних органів, організацій, установ, посадових осіб щодо задоволення потреб і законних інтересів громадян в отриманні необхідних зведень, повідомлень, знань, що стосуються політичних, економічних, соціально-культурних і соціально-побутових сторін життєдіяльності держави, особистості, суспільства.

У свою чергу, інформаційно-комунікативна функція, головне призначення якої – забезпечувати реалізацію конституційного права громадян на доступ до інформації, розпадається на низку самостійних елементів, головним з яких є інформування населення, що полягає в регулярному й цілеспрямованому наданні громадянам у встановленому законом порядку різних відомостей, повідомлень, знань, які об'єктивно, повно і вчасно характеризують роботу цих органів, а також прийняті ними рішення [440, с. 202–211].

Оскільки специфіка інформації як ресурсу впливає на розосереджнність елементів інформаційної функції й поєднання з іншими напрямами державної діяльності, то у вузькому розумінні інформаційна функція – це похідна кожної головної функції держави – захисту прав і свобод людини, економічної, соціальної, політичної, тому що здійснення будь-якої державної функції немислимо без інформаційного компонента.

Т. Костецька до основних ознак інформаційної функції Української держави, характерних функціям держави, включає такі:

– функція набуває рис стійкого, постійного напряму та виду діяльності Української держави, яка має власну періодизацію свого існування;

– у функції виявляється сутність і соціальне призначення держави, що пов'язуються із завданнями, які виникають перед державою на відповідному етапі її розвитку;

– завданнями, які є першоосновою інформаційної функції, на сучасному етапі розбудови нашої держави є: створення правових, організаційних засад, науково-технічних, економічних, фінансових та інших умов для реалізації інформаційних прав людини і громадянина, інформаційних потреб суспільства; формування системи національних інформаційних ресурсів, забезпечення національної інформаційної безпеки і в перспективі – побудова інформаційного суспільства;

– функція є реальною, оскільки завдання, напрями діяльності держави ґрунтується на конституційно-правових засадах;

– функція має комплексний характер, здійснюється в певних формах і конкретними методами. Зокрема, втілюється у функціях, компетенції відповідних державних органів [332, с. 113–119].

Здійснений аналіз дає змогу стверджувати, що інформаційна функція відзначається суттєвими ознаками основних функцій держави. Вона становить сформований у сучасних умовах основний напрям діяльності держави в інформаційній сфері, значення правового регулювання якого зумовлено об'єктивними процесами глобального та національного інформаційного розвитку. Вона безпосередньо виражає і предметно конкретизує сутність сучасної держави – досягнення демократії, розвиток громадянського інформаційного суспільства, глобальних інформаційно-комунікативних технологій.

На наше переконання, власне інформаційна функція демонструє приклад поєднання загальносоціальних, групових чи корпоративних, місцевих і приватних інтересів членів суспільства, а також національних та міжнародних потреб в інформаційній сфері. Тут виявляється і властива їй на сучасному етапі розвитку динаміка соціально-економічних, політичних і культурно-духовних, науково-технічних перетворень у житті інформаційного суспільства. Згадуючи поділ функцій держави на внутрішні та зовнішні, тенденції їх інтернаціоналізації, глобалізації та інтеграції, слід відзначити потенційну можливість додання внутрішнім функціям міжнародного значення, їх взаємодію із зовнішнім середовищем, взаємопов'язаність внутрішньої і зовнішньої політики держави.

Адже держави не існують ізольовано від інших, усі вони зобов'язані співпрацювати в межах світового співтовариства, брати участь у розв'язанні глобальних і регіональних проблем і конфліктів, у тому числі в інформаційній сфері. Отже, вони повинні погоджувати свої інтереси із загальними інтересами даного співтовариства.

Сучасні держави регламентують інформаційні процеси та інформаційні відносини як усередині країни, так і за її межами у відносинах з іншими

державами, міжнародними організаціями і наднаціональними утвореннями. Причому внутрішня реалізація інформаційної функції неможлива без планованої активної зовнішньої інформаційної взаємодії, оскільки інформаційну функцію доцільно вважати і внутрішньою, і зовнішньою. Такої думки дотримуються деякі сучасні українські правознавці [556, 189, 239].

Виходячи з класифікації функцій держави за тривалістю дії чи виконання на постійні та тимчасові, логічно стверджувати, що інформаційна функція є постійною, тому що вона існує практично на всіх етапах розвитку держави. Проте її значущість та інтенсивність реалізації на кожному етапі відрізняються. Зокрема, в умовах глобальних інформаційних процесів, активізації розвитку інформаційно-комунікативних технологій, поширення кіберзагроз національного і планетарного масштабів, забезпечення інформаційної функції держави набуває особливої значимості й інтенсивності.

Розгляд таких видів функцій держави як спеціальні (первинні) властиві тільки державі, й лише вона в особі відповідних органів держави забезпечує їх реалізацію, та неспеціальні функції держави – характеризують її діяльність як звичайного суб'єкта певних правових відносин, – цікавий при трактуванні держави як корпорації, що застосовує форми і методи діяльності, характерні для приватних компаній.

В інформаційній сфері можна виділити як первинні спеціальні, так і неспеціальні або вторинні функції держави. У першому випадку − це правове забезпечення реалізації інформаційної функції, встановлення основ відповідальності за правопорушення в інформаційній сфері, у другому випадку − забезпечення розвитку науково-технічного потенціалу і технологій виробництва, маркетинг і ринок продукції, управління інвестиціями, розвиток робочих місць і підготовки кадрів та ін. [440, с. 202–211].

Погоджуємося, що на сучасному етапі інформаційна функція відіграє ключову роль серед інших функцій держави, проте водночас вона взаємопов'язана з ними. Адже інші функції не можуть здійснюватись без попереднього інформування людини та громадянина про їх зміст, наприклад

до проведення референдуму чи виборів як політичної функції держави населення інформують про питання, яке буде винесено на розгляд або кандидатури осіб, які балотуються на виборні посади, тощо [205, с. 15–18].

Серебро М.В. вважає, що «незмінною сутністю держави є те, що саме вона є організаційно-інституціоналізованою формою певного порядку, що склався у суспільстві, і саме звідси розвивається в надскладну систему, якою є на теперішній час. Проте змістовно держави відрізняються одна від одної. Вбачається, що характеристика інтересу, який держава захищає за різних історичних періодів свого розвитку, є більш релевантною її змісту, ніж сутності, яка є статичною і має характеризувати державу усіх періодів, державу як явище. Держава за своєю сутністю є абсолютною цінністю, оскільки тільки вона інституціоналізує в собі складений у суспільстві порядок. Але якість та характеристики такого порядку можуть бути різними, тому необхідним є звернення до категорії змісту, яка покликана містити в собі динаміку розвитку конкретного типу держави, одним із яких і постає сучасна держава, основою порядку в якій є право» [561, с. 8].

Діяльності демократичної, соціальної і правової держави стосовно здійснення своїх функцій, як відомо, передує нормативно-правове закріплення, що визначає потенційний характер фактично усіх функцій держави. Регламентація функцій держави на конституційному рівні ще не гарантує їх ефективної реалізації, якщо не буде забезпечений відповідний інституційний механізм, тобто система спеціально уповноважених на їх виконання органів, відповідних посадових і службових осіб, установ та організацій. Окреслені питання також розглянемоі в наступних розділах роботи.

Таким чином, проаналізовані нами монографічні, дисертаційні дослідження, інші наукові праці засвідчують неоднозначний підхід авторів до функцій держави в інформаційній сфері. Зокрема, інформаційну функцію сучасної держави розглдають С. Глазунова, О. Яременко, О. Климентьєв, Ж. Павленко, Т. Костецька, М. Дзевелюк та ін.; інформаційно-комунікаційні

функції – Н. Карпчук, Л. Угрин, Є. Тихомирова, Ю. Збираник, І. Нікодимов, Г. Почепцов і т.д.; функцію забезпечення інформаційної безпеки як функцію сучасної держави – О. Тихомиров, Р. Калюжний, Т. Ткачук тощо.

Значна кількість учених виокремлюють державну інформаційну політику (І. Арістова, І. Сопілко), інформаційно-правову політику у сфері безпеки (О. Головко); державну політику у сфері забезпечення інформаційної безпеки України: (Т. Ткачук), політику інформаційної безпеки України (Б. Кормич), політику держави у сфері інформаційної безпеки людини (О. Золотар), державну політику інформаційної безпеки (І. Валюшко) і т. д. Це, безумовно, впливає на виокремлення відповідних функцій держави.

Зокрема, Т. Ткачук підкреслює, що забезпечення інформаційної безпеки України є визначальним напрямом державної політики, від якого залежатиме існування держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві. Основна мета державної політики у сфері забезпечення інформаційної безпеки України – це управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів [611, с. 30].

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.

У зв’язку з цим постає питання: чи доцільно виокремлювати згадані вище напрями державної політики у сфері забезпечення інформаційної безпеки України як самостійні функції або підфункції? Можливо, все ж таки функція забезпечення інформаційної безпеки становить передумову реалізації державної інформаційної політики України, захисту інформаційних прав і свобод людини та громадянина, захисту інформаційного суверенітету держави і загалом інформаційного простору?

Таких питань на цьому шляху виникає чимало, тому важливо здійснювати подальші дослідження з цієї тематики.

Зокрема, потребує уточнення позиція деяких дослідників щодо однопорядкового використання термінів «комунікативна функція держави», «інформаційно-комунікативна функція держави» та «інформаційна функція держави», «функція забезпечення інформаційної безпеки держави», а також з’ясування природи та змісту, їх співвідношення та визначення місця в системі існуючих функцій сучасної держави.

Якщо, наприклад, порівняти з фіскальною функцією держави, то забезпечують її здійснення фіскальні органи, що відзначаються відповідною системно-структурною організацією, формами і методами діяльності. У зв’язку з цим виникають питання, пов’язані із суб’єктами здійснення функцій сучасної держави в інформаційній сфері.

Видається, що в сучасних умовах роль функцій держави в інформаційній сфері лише посилюється, підкреслюється значення державних інституцій у процесі регулювання суспільних відносин, пов’язаних з інформацією, захистом інформаційних прав і свобод людини та громадянина, забезпечення інформаційної безпеки, запобігання і ліквідації загроз в інформаційному просторі. Ці функції реалізуються як на внутрішньодержавному, так і на міжнародному рівнях, тому потребують подальшого вивчення, удосконалення правових засад забезпечення, механізмів реалізації тощо.

Отже, у теорії держави і права закладено ґрунтовні концептуальні основи теорії функцій держави, а в науці конституційного права, адміністративного та інформаційного права, міжнародного права фактично найбільшою мірою розглядають ряд функцій держави в інформаційній сфері (розвитку інформаційного суспільства, захисту інформаційних прав людини і громадянина, забезпечення інформаційної безпеки тощо). Чимало ідей, сформульованих у працях учених за попередні десятиліття, плідно розвиваються і нині, збагачуючись новітніми ідеями і теоріями. Також поступово прослідковується зростаючий науковий інтерес до цієї проблематики в науці кримінального права і процесу, господарського права, цивільного права, фінансового права і т. д.

Отже, не тільки в межах різних спеціальностей юридичної науки підготовлено ґрунтовні дослідження, присвячені численним аспектам функцій держави в інформаційній сфері, включаючи функцію забезпечення інформаційної безпеки. Важливо, щоб такі наукові здобутки примножувалися, з відповідними результатами їх практичного втілення.

Висновки до розділу 1

У розділі з’ясовано фундаментальні проблеми, пов’язані з розвитком **інформаційного суспільства**, а також оцінено сучасний стан досліджень, що спрямовані на їх розв’язання, 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», висвітлено сучасні методологічні підходи до *вивчення функцій держави в сучасних умовах*, використані вченими у вітчизняній юридичній науці для їх пізнання.

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 такого 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 і захист національних інтересів (інституційний механізм).

Застосування системного підходу та критичний аналіз наукового доробку вчених, які займалися розробкою окремих аспектів інформаційного суспільства і зокрема інформаційної безпеки, дали змогу визначити проблематику, яка залишилися поза науковим фокусом. 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.

Наголошено, що серед складників методології дослідження зазначеної проблематики чільне місце посідають онтологія, гносеологія та аксіологія як вчення, що дозволили 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 уточнюється 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 в бік зумовленості їх суспільними потребами і належного закріплення й реалізації прав людини. Активізація розбудови громадянського та інформаційного суспільства зумовлює 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.
КОНЦЕПТУЛЬНІ ПІДХОДИ ДО РОЗУМІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРАВОВІ ЗАСАДИ ЇЇ РЕГУЛЮВАННЯ

Згідно зі ст. 17 Конституції України, забезпечення інформаційної безпеки визнано однією з найважливіших функцій держави, справою всього Українського народу. При цьому покладення обов'язків та відповідальності на народ теж змушує до створення певних умов з боку держави, включаючи її правотворчу, правозастосовну, правовиховну та інші види діяльності.

Хоча в Основному законі нашої держави не згадується інформаційне суспільство, інформаційна політика, форми і методи реалізації функції забезпечення інформаційної безпеки, однак загалом уже прийнято значну кількість нормативно-правових актів України у цій сфері, визначено об'єктно-суб'єктний склад механізму її регулювання та здійснення.

Інформаційна сфера та всі її складові, включаючи функцію забезпечення інформаційної безпеки, не є новими явищами політико-правової дійсності, вітчизняної і зарубіжної науки. При цьому, як демонструють сучасні реалії, тут досі існують прогалини правового регулювання, колізії, виникають протистояння і перешкоди.

Такі тенденції і закономірності характерні не лише для національного процесу реалізації свободи інформації, розвитку інформаційного суспільства, впровадження системи інформаційної безпеки в Україні, вони притаманні й багатьом іншим державам, поширені на всій міжнародній арені.

Така ситуація змушує науковців звернутись до вивчення проблематики забезпечення інформаційної безпеки як функції сучасних держав.

Такий напрям досліджень, на наш погляд, завжди буде актуальним, адже інформаційна сфера вкрай динамічна і вразлива. Фактично усі суб'єкти правовідносин користуються її можливостями, що покладає певні обов'язки, проте не всі складові цієї сфери врегульовані належним чином. Загалом у

віртуальному цифровому просторі – без жодних кордонів, вкрай складно гарантувати інформаційну безпеку особи, сім'ї, суспільства, держави, а відтак і міжнародну інформаційну безпеку в цілому.

1. Інформаційна безпека: поняття і правова природа. Інформаційна безпека держави та інформаційна війна

Поширеним є підхід щодо розкриття сутності інформаційної безпеки через більш широке поняття – національна безпека. Зокрема, він застосовується в енциклопедичній та довідковій літературі.

Так, у багатотомній юридичній енциклопедії *інформаційна безпека України* визначається як один із видів національної безпеки, важлива функція держави. Інформаційна безпека України передбачає: законодавче формування державної інформаційної політики; створення можливостей досягнення інформаційної достатності для ухвалення рішень суб'єктами права; гарантування свободи інформаційної діяльності та права доступу до інформації; всебічний розвиток інформаційної структури; підтримку розвитку національних інформаційних ресурсів; створення і впровадження безпечних інформаційних технологій; захист права власності держави на стратегічні об'єкти інформаційної інфраструктури України; охорону державної таємниці; створення загальної системи охорони інформації; захист національного інформаційного простору України; встановлення законодавством режиму доступу іноземних держав до національних інформаційних ресурсів; законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [680].

У контексті національної безпеки інформаційну безпеку розглядають М. Желіховський, В. Ліпкан, Є. Максименко, О. Степко, Л. Ткачук та інші вчені. Водночас дискусійним залишається питання самостійності інформаційної безпеки як елемента в системі національної безпеки.

Так, В. Ліпкан, Є. Максименко, М. Желіховський зазначають, що національна безпека являє собою цілісний екзистенціальний феномен, відтак не може бути репрезентована сукупністю корелятивно пов'язаних складових (економічна, інформаційна, політична безпека тощо). Національну безпеку слід аналізувати крізь призму її системних властивостей, отже, доцільно

стверджувати про національну безпеку в інформаційній сфері, екологічній сфері тощо. Адже з появою інших «складових», національна безпека як така не змінить своєї сутності. Водночас, коли йтиметься про прояви національної безпеки в різних сферах життєдіяльності, то поява чи то нових суспільних відносин чи сфер життєдіяльності жодним чином не вплине на зміст національної безпеки, лише змінить її [361].

На думку Б. Кормича, інформаційний аспект національної безпеки є її невід'ємним компонентом, і так само, як інформаційна безпека не може існувати поза межами загальної національної безпеки, національна безпека не буде всеохоплюючою в разі позбавлення своїх інформаційних векторів [324].

Н. Нижник, Г. Ситник, В. Білоус, аналізуючи загрози національній безпеці України в життєво важливих сферах діяльності, виокремлюють ряд основних функціональних складових (сфер) національної безпеки України: економічну, політичну, соціальну, воєнну, екологічну, епідемічну, технологічну та інформаційну безпеку. Відповідно, під інформаційною безпекою зазначені автори розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень на захист інформаційних ресурсів країни [410].

Дещо іншу позицію щодо співвідношення понять національної та інформаційної безпеки відстоюють вчені Ф. Медвідь, О. Младьонова, І. Проноза, О. Соснін, О. Степко, Л. Ткачук, М. Форос та інші. Зокрема, вони розглядають інформаційну безпеку як складову, підсистему чи елемент національної безпеки.

Наприклад, Ф. Медвідь зазначає, що інформаційна безпека України як важлива складова національної безпеки передбачає системну превентивну діяльність органів державної влади щодо надання гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому і спрямована на досягнення достатнього для розвитку державності та соціального прогресу рівня духовного та інтелектуального потенціалу країни [386].

Наступна позиція, що використовується при з'ясуванні змісту поняття «інформаційна безпека», засновується на визначенні характеру (статичного чи динамічного) цього суспільного явища.

Так, Д. Дубов, А. Корсунський та деякі інші вчені під інформаційною безпекою України розуміють стан захищеності її національних інтересів в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства й держави [217, с. 19–30].

В. Гасеський, В. Авраменко визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації [110, с. 17–18].

В. Богуш вказує, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави [145].

На переконання О. Сорокіна, інформаційна безпека розкривається як стан захищеності особистості, суспільства, держави від інформації, що носить шкідливий або протиправний характер, від інформації, що надає негативно впливає на свідомість особистості, перешкоджає сталому розвитку особистості, суспільства і держави. Інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючи також комп'ютери та інформаційно-телекомунікаційну інфраструктуру й інформацію, що в них знаходиться, який також забезпечує сталий розвиток особистості, суспільства й держави [580, 18-22].

Близькою за змістом видається позиція О. Дзьобаня і В. Пилипчука, які визначають інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства та держави в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, що забезпечує їх сталий розвиток.

В. Ярочкін визначає безпеку як стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек і загроз, який ґрунтується на діяльності людей, суспільства, держави, світового співтовариства з виявлення (вивчення), запобігання, послаблення, ліквідації та відбиття небезпек і загроз, здатних загубити їх, лишити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку [684, с. 7].

Інформаційна безпека – це стан захищеності систем оброблення і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення. Інформаційну безпеку, залежно від суб’єкта захисту інформації, прийнято поділяти на інформаційну безпеку держави, організації та особи [344].

Так, інформаційна безпека організації – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів щодо досягнення стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток. Часто здійснюється службами інформаційної безпеки.

Інформаційна безпека держави, як зазначає О. Князєв, характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо) інформаційних впливів, причому як до впровадження, так і до вилучення інформації [295].

Інформаційна безпека особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об’єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та

обмежувати свободу вибору, а також зазіхань на її майно та інтелектуальну власність.

Не можна не погодитися з В. Горлинським, який переконує, що реалії інформаційної діяльності людини з позиції феномена безпеки як об'єкта аксіологічної рефлексії свідчать про необхідність вироблення нової аксіологічної парадигми, яка відповідає новій організації публічного управління на підставі використання інформаційних технологій [187, с. 1–2].

Якщо ж розглядати інформаційну безпеку в динаміці, то її можна визначити як процес, певну діяльність, забезпечення нормального стану інформаційної сфери чи застосування заходів протидії інформаційній агресії та методів захисту інформаційного простору.

Наприклад, О. Логінов стверджує, що не слід обмежуватись поняттям «стан» при визначенні категорії «інформаційна безпека», і стверджує, що вона є процесом. Зокрема, на його думку, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності органів виконавчої влади [364, с. 153–161].

На думку А. Шумки, П. Черника, інформаційна безпека являє собою діяльність органів державного управління. Звідси витікає важливий висновок, що слід діяти активно, здійснюючи вплив на джерела інформаційної небезпеки [677, с. 10 –16].

Л. Харченко, В. Ліпкан, О. Логінов визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками, державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [634].

Л. Наливайко пропонує розуміти інформаційну безпеку як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця

безпека має включати ефективну протидію сукупності інформаційних загроз [400, с. 60–65].

О. Литвиненко, розкриваючи поняття «інформаційна безпека», трактує її як єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [357, с. 18].

Слід звернути увагу на ще один підхід до визначення поняття «інформаційна безпека», згідно з яким воно розглядається крізь призму суспільних відносин. У науковій літературі такий підхід визнається неординарним та інноваційним, але, на наш погляд, він дає змогу розкрити правову природу інформаційної безпеки, детально вивчити її структуру.

Зазначений підхід у своїх дослідженнях використовує В. Гуровський, який пропонує розуміти національну інформаційну безпеку України як суспільні відносини, пов’язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [198].

О. Литвиненко також визначає інформаційну безпеку як одну із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [356, с. 47-49].

П. Ткачук, Р. Гула, О. Сивак, О. Щурко та інші дослідники відзначають, що зміст поняття «інформаційна безпека» визначається через політико-інструментальний, технологічний та комплексний підходи. По-перше, політико-інструментальний підхід розкриває сутність інформаційної безпеки держави через стан її захищеності, при якій спеціальні інформаційні операції,

акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдають істотної шкоди національним інтересам і забезпечують прогресивний розвиток усіх сфер життя суспільства [262, с.160].

За визначенням Б. Кормича, це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, суспільства та держави [324, с. 92].

По-друге, технологічний підхід наголошує на захищеності насамперед інформаційної системи від випадкового або навмисного втручання, що завдає збитку власникам або користувачам інформації.

По-третє, комплексний підхід визначає інформаційну безпеку як стан захищеності інформаційного простору, його формування і розвиток в інтересах громадянина, організацій і держави в цілому, захист від неправомірного зовнішнього і внутрішнього втручання, стан інформаційної інфраструктури, в якому інформацію використовують у мирних цілях лише за призначенням, і вона нездатна негативно впливати на інформаційну чи інші системи як самої держави, так і інших країн [262, с. 160].

В одній із останніх публікацій з даної тематики, автором якої є Т. Ткачук, виявлено три концептуальні підходи до трактування інформаційної безпеки, а саме:

1) статичний (безпека як стан захищеності інформаційного середовища/ інформації, система гарантій тощо);

2) діяльнісний (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси і цінності);

3) комплексний (безпека як стан і процес).

Водночас згаданий дослідник обґрунтував авторську позицію, що найбільш прийнятним, зважаючи на сучасну практику забезпечення інформаційної безпеки держави, є останній. За такого підходу вбачається за

доцільне інформаційну безпеку держави розглядати як перманентний процес діяльності компетентних органів, спрямований на запобігання і протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Цей підхід ґрунтується на принципі, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища [610].

Правове регулювання інформаційної безпеки в Україні здійснюється на підставі Конституції України, Закону України «Про національну безпеку України» № 2469-VIII від 21.06.2018 р., Закону України «Про Концепцію Національної програми інформатизації» № 75/98-ВР від 04.02.1998 р., Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» № 537-V від 09.01.2007 р., Рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України», яке затверджене Указом Президента України № 47/2017 від 25.02.2017 р. тощо.

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 розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [244].

У Законі України «Про національну безпеку України» № 2469-VIII від 21.06.2018 р. 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 р. інформаційна безпека називається невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки, але саме поняття не деталізується.

Перехід держави до інформаційного суспільства потребує переосмислення в окремих випадках і розроблення нових механізмів регулювання відносин, що виникають між громадянами, їх об'єднаннями та державою. Усі суб'єкти інформаційних відносин повинні усвідомлювати і виконувати свою роль у цьому процесі, але саме держава покликана активно впливати на ці трансформаційні процеси, залучати до співпраці політиків, науковців, практиків, міжнародних експертів і громадськість.

Інформаційна безпека держави та інформаційна війна.

Події, які відбуваються в Україні в останні декілька років демонструють появу нових викликів і загроз у цій сфері. Зокрема, особливої уваги заслуговують різні форми впливу, протиборства тощо. З розвитком та впровадженням сучасних інформаційних технологій практично в усі сфери нашого життя, зростає рівень загроз несанкціонованого доступу в процес роботи систем та витоку важливої інформації. Технічний прогрес суттєво впливає на вирішення військових, торговельних, економічних конфліктів, внаслідок чого силові методи іноді поступаються інформаційним.

Тому очевидно, що змінилось традиційне чи класичне розуміння механізму забезпечення безпеки держави та суспільства, оскільки раніше, наприклад, не були поширені інформаційні атаки та інформаційні війни і фактично без участі держави, групи держав, а іноді й узгоджених дій світової спільноти неможливо убезпечитись від них.

Слід зазначити, що практично в усіх збройних конфліктах за останні десятиліття ефективно використовувалися методи та засоби інформаційної боротьби, які можуть призвести до таких трагічних наслідків як: зміна суспільного ладу та політичного устрою; розпад держави; втрата армії; занепад економічної системи в країні; втрата національної ідеї та духовних цінностей; загибель людей тощо [553, с. 18–23].

Проблематику *інформаційних впливів та протиборств, інформаційних воєн* неодноразово порушували і вивчали вітчизняні та зарубіжні дослідники. Тут варто назвати таких учених: Дж. Арквілли, Р. Гула, Г. Почепцов, Н. Камінська, Г. Карпенко, Я. Короход, І. Костюк, Д. Кюль, М. Лібікі, С. Любарський, Р. Моландер, Дж. Най, В. Остроухов, С. Расторгуєв, О. Саприкін, Г. Сасин, О. Сивак, П. Ткачук, П. Шевчук, О. Цуканова, В. Хорошко, Ю. Хохлачова, О. Щурко та ін. Разом з тим, неоднозначне розуміння згаданих категорій, іноді їх ототожнення, змушують і надалі привернути увагу, особливо стосовно з'ясування їх суті, а також правових основ запобігання їм і протидії.

Інформаційні війни як явище існували тією чи іншою мірою з давніх часів. Історичний розвиток людства свідчить про те, що поняття «інформаційна війна» завжди супроводжувало та визначало разом зі зброєю хід, характер і результат воєн, битв, операцій.

Видатний китайський воєнний теоретик Сун-Цзи у VI–V ст. до н.е. вперше запропонував використовувати інформаційні заходи як альтернативу бойовим діям. Він сформулював дев'ять заповідей, дотримання яких забезпечувало такий потужний вплив на духовний світ армії противника, що вона просто «розкладалася» ще до початку битви. Сун-Цзи зазначав, що «у війні, як правило, найкраща політика зводиться до захоплення держави цілісною... Здобути сотню перемог у боях – це не вершина мистецтва. Підкорити суперника без бою – ось вінець мистецтва» [590, с. 40].

Основні ідеї Сунь-Цзи активно розвивали й інші китайські мислителі. Зокрема, Чжуге Лян (III ст. н.е.). вважав, що «у воєнних діях атака на психіку – головне завдання. Психологічна війна – це головне, бій – це другорядна справа». Не абсолютизував збройне насильство і відомий прусський воєнний теоретик К. Клаузевіц, автор класичного визначення поняття «війна»: «Доведеться хоч-не-хоч визнавати і такі війни, які полягають лише в погрозі супротивнику» [382, с. 231]. Вперше термін «інформаційна війна» використав у 1985 р. в Китаї Шень Вейгуаном.

Здійснення інформаційних впливів з використанням інформаційної зброї (приховування інформації; подача її частково, в певному ракурсі; перебільшення наслідків) було зафіксовано літописцями на теренах України ще за Київської Русі. Так, загальновідомим є факт поїздки княгині Ольги до Константинополя, проте ні візантійські, ні руські джерела не висвітлюють причини та мети подолання такого довгого шляху. Войовничий князь Святослав заздалегідь повідомляв противника про свій похід, проте залишалися таємницею напрям та сили, котрі планувалося задіяти. Це давало можливість навести паніку у стані військ та швидко розгромити противника [195].

В інформаційному просторі України тривалий час спостерігається боротьба за управління ресурсами, вплив і контроль на території нашої держави. Події з кінця 2013 – початку 2014 рр. стали драматичними для України. Внаслідок дестабілізації внутрішньої політичної ситуації, анексії Криму та «гібридної війни» на сході України змінилася геополітична ситуація як у Європі, так і фактично в усьому світі.

Це, на нашу думку, потребує з'ясування природи і сутності таких споріднених категорій як інформаційна війна, інформаційний вплив, експансія, гібридна війна, електронна війна, хакерська війна, мережева війна, кібервійна, консцієнтальна війна, психологічна війна, інформаційне протиборство тощо.

Так, одним із перших у відкритому друці, хто написав про феномен інформаційних воєн, був М. Маклюєн у 1960 роках. Уже тоді було відомо, що «холодна війна» ведеться за допомогою інформаційних технологій, так як в усі часи війни велися за допомогою передових технологій. Дослідник відмітив, що якщо «гарячі» війни минулого використовували зброю, знищуючи ворогів одного за іншим, то інформаційна зброя за допомогою телебачення та кіно, навпаки, занурює все населення у певний світ уяви: «земна куля тепер – не більше, ніж село» [375, с. 5].

Інформаційна війна є тотальним явищем, де неможливо визначити його початок і кінець. Зокрема, на думку С. Расторгуєва, інформаційна війна – це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті та приховані цілеспрямовані інформаційні впливи систем (держав) одна на одну, з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи за допомогою таких засобів, використання яких дає змогу досягати задуманих цілей [530, с. 455 –456].

Можна погодитися з думкою О. Саприкіна, що інформаційна експансія є технологією набагато місткішою, ніж «інформаційна війна» або «інформаційна атака». Ці терміни можна вважати складовими інформаційної експансії. Інформаційна експансія – система, що склалася в засобах інформації розвинених держав, і методи, використані для пропагандистського забезпечення певних геополітичних цілей [552, с. 40–43].

У листопаді 1991 року аналізуючи досвід досягнення інформаційної переваги після операції «Буря у пустелі», генерал Гленн Отіс, колишній командувач Командування сухопутних військ США з навчання та доктрин, опублікував працю, в який стверджував, що «природа війни повністю змінилася. Та сторона, яка виграє інформаційну війну, – переможе…інформація є ключем до сучасної війни – у стратегічному, оперативному, тактичному і технічному планах». Офіційно визначеним термін «інформаційна війна» як комплексне спільне застосування сил і засобів інформаційної боротьби та збройної боротьби (при домінуванні засобів інформаційної боротьби) вперше застосували у керівних документах США, зокрема в директиві МО США Т 3600.1 від 12 грудня 1992 року під назвою «Інформаційна війна» [3].

У сучасному науковому дискурсі проблемі вивчення надскладного соціально-політичного явища «інформаційна війна» надається достатньо уваги. Різноманітність підходів до визначення основного змісту, відсутність єдиної системи класифікації призвели до унеможливлення створення уніфікованої

дефініції понять «інформаційна війна» та «інформаційно-політичний простір», відсутність методологічного осмислення співвідношення цих понять та ін.

Наприклад, А. Манойло зміст поняття «інформаційна війна розглядає на різних рівнях пізнання як соціальне явище; як поле політичних конфліктів; як особливу форму політичного конфлікту; як інструмент інформаційної політики [381]. А. Фісун до цього додає ще й форму психологічного впливу [624, с. 534–538].

Найбільш важливими, як відзначають В. Хорошко та Ю. Хохлачова, є електронна та психологічна війни. Електронна війна об'єктом свого впливу має засоби електронних комунікацій – радіозв'язку, телевізійних і комп'ютерних мереж. Психологічна війна здійснюється шляхом пропаганди, «промивання мозку» та іншими методами інформаційного оброблення населення. Далі згадані автори виділяють інформаційну війну, безліч визначень якої пов'язано складністю і багатогранністю такого явища, труднощами побудови аналогій з традиційними війнами. Якщо спробувати трансформувати визначення в поняття «інформаційна війна», то навряд чи вийде щось конструктивне. Це пов'язано з рядом особливостей інформаційної війни [635, 256].

Загалом залежно від основних аспектів дослідження об'єкта, які вирізняють науковці, та від гіпотез щодо сутності явища, виділяється вісім основних підходів до поняття «інформаційна війна».

Так, за *соціально-комунікативним підходом* трактують поняття інформаційна війна як сукупність окремих інформаційних заходів, інформаційних способів і засобів корпоративної конкуренції, що є продуктом еволюційного розвитку способів і засобів комунікації між людьми, суспільствами, державами та світом загалом. У межах цього підходу український дослідник Г. Почепцов визначає «інформаційну війну» як всеосяжну, цілісну стратегію, яка надає значущості та цінності інформації в процесах командування, управління і виконання наказів збройними силами й

реалізації національної політики [462]. Особливостями соціально-комунікативного підходу:

– відображення сутності досліджуваного явища лише як закономірного розвитку людського суспільства в рамках біологічної еволюції з домінуванням принципів природного відбору, боротьби за існування й виживання найбільш пристосованих як визначальних факторів громадського життя;

– визначення природи соціального конфлікту як вічного та непереборного;

– трактування інформаційної агресії як нової трансформованої форми природної агресії людини.

Маніпулятивно-психологічний підхід визначає суть інформаційної війни як системи способів і засобів психологічного впливу на індивідуальну та масову свідомість з метою спрямування її у вигідному для суб'єкта впливу напрямі. Формами інформаційної війни є використання психотропної зброї, побудова віртуального світу, підміна реальності та ін. Представники цього підходу вважають, що інформаційно-психологічна війна – це вплив на суперника через засоби масового психологічного впливу для зміни світогляду чи ініціювання процесу самознищення, добровільної здачі території, ресурсів і т.п. [394].

Тобто специфічними особливостями цього підходу є:

– розкриття психологічного впливу феномена;

– комплексне розкриття психологічного аспекту і маніпулятивної природи інформаційної війни;

– ігнорування оборонного (захисного) характеру інформаційної війни;

– нівелювання технічного аспекту, матеріальних засобів інформаційного протиборства;

– недостатнє прогнозування наслідків впливу економічної складової.

Військово-прикладний підхід зараховує інформаційну агресію до сфери військового протиборства й розглядає її у комплексі спільного застосування сил і засобів інформаційної та збройної боротьби. При цьому представники військово-прикладного підходу не вважають інформаційну війну окремим методом ведення війни. На їх думку, існує множина форм інформаційної війни, кожна з яких претендує на різні концепції, зокрема: командно-контрольні, розвідувальні війни; радіоелектронна боротьба; психологічні операції; хакерська війна, програмні атаки на інформаційні системи; інформаційно-економічна війна; кібервійни [60]. Кібервійну розглядають як процес розвитку та поширення інформаційних технологій. У військовій сфері – як комплексне використання високоточної зброї, технологій «Стелс», бойових і розвідувальних засобів з урахуванням футуристичних розробок у галузі роботизації й автоматизації [294, с. 78–84]. Характерні особливості цього підходу:

– системність, що дає можливість охопити політичний, економічний, психологічний та інший аспекти;

– «агресивний характер», зорієнтований на швидке досягнення бажаного тактичного результату з одночасною втратою стратегічної перспективи;

– ігнорування прогнозування наслідків для іншої сторони конфлікту;

– нівелювання соціального аспекту при домінуванні політичної складової конфлікту.

Державно-інструментальний підхід називає інформаційну війну інструментом зовнішньої та внутрішньої політики, «можливістю для збирання, оброблення та поширення безперервного потоку інформації…у відповідь на дії противника» [106, с. 43]. Особливістю цього підходу є абсолютизація ролі політичних інститутів і організації держави у веденні інформаційної війни й нівелювання впливу соціальних, економічних і психологічних чинників.

Геополітичний підхід. Дослідники вважають інформаційну війну явищем латентним мирного періоду міждержавного протиборства, що дозволяє вирішувати зовнішньополітичні завдання несиловими методами. Інформаційна війна стосується сфери геополітичного протиборства, її трактують як особливий вид відносин між державами, при якому для вирішення існуючих протиріч використовують методи, засоби й технології впливу на інформаційну сферу функціонування цих держав. Під інформаційною війною дослідники цього напряму розуміють дії, які спрямовані на завдання противнику конкретного, відчутного збитку в окремих галузях його діяльності [382, с.481].

З-поміж характеристик цього підходу виокремимо такі:

– охоплення геополітичних суб'єктів інформаційно-політичного простору;

– трактування інформаційної війни як певного природного закону;

– ігнорування значимості особистості як окремого об'єкта для впливу;

– недостатнє вивчення причин інформаційної війни.

Віртуально-кібернетичний підхід. Інформаційна війна розглядається як сукупність технічних, програмних та інших засобів, які використовують у віртуальному просторі, з метою ураження інформаційних систем противника (комп'ютерні віруси та ін.). Кібервійна – елемент інформаційної війни, що здійснюється з використанням засобів всесвітньої мережі у формі кібератак. Сутність інформаційної війни полягає в застосуванні прихованих цілеспрямованих інформаційних впливів інформаційних систем одна на одну з метою одержання певного прибутку в матеріальній сфері [530, с. 51].

Наголошено на тому, що інформаційно-блогова або мережева війна – це внутрішньо-середовищна особливість Інтернету, яка виявляється у формах жорсткої дискусії, цілковитого свавілля із взаємними образами, атаками на ресурси противника, зламами особистої інформації та ресурсів. Блоги стають потужним інструментом формування громадської думки [230, с. 48].

«Інформаційна війна, на думку американських теоретиків Дж. Аркуїла та Д. Ронфельдта, може бути частиною широкого та всеохоплюючого поняття ворожих дій – мережевої війни або кібервійни» [6].

Властивостями віртуально-кібернетичного підходу є:

– розкриття суті інформаційної війни крізь площину математичного виміру;

– виокремлення тенденцій сучасного інформаційного простору та розвитку інформаційних технологій (особливо в контексті інформаційно-блогових процесів);

– ігнорування психологічного аспекту явища;

– невизначеність ролі держави в цьому процесі;

– домінування теоретичного, а не практичного значення, відсутність рекомендацій та прийомів, які дали б змогу виявити інформаційну агресію і захиститися від неї.

Комплексний підхід. Український дослідник А. Фісун констатує, що жоден із зазначених підходів не розкриває сутності інформаційної війни комплексно ні як політичного конфлікту, ні як соціального явища, ні як соціокультурного феномена: «Інформаційна війна – це комплексний відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони чи взаємний вплив сторін одна на одну, який містить систему методів і засобів впливу на людей, їхню психіку та поведінку, на інформаційні ресурси та інформаційні системи, з метою досягнення інформаційної переваги (в забезпеченні національної стратегії), що обумовлює прийняття сприятливих для ініціатора впливу рішень або знищення інформаційної інфраструктури противника, з одночасним зміцненням і захистом власної інформації та інформаційних систем» [624, с. 534–538].

На нашу думку, до комплексного підходу слід зарахувати й дефініцію В. Ліпкана, Ю. Максименко, В. Желіховського: «Інформаційна війна – це

1) дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що ґрунтуються на інформації та

інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації та інформаційних системах;

2) нефізична атака на інформацію, інформаційні процеси та інформаційну інфраструктуру;

3) найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї)» [361, с. 270].

В ідеологіях маргінальних політичних формувань екстремістського та окультистського напрямів став популярним так званий *конспірологічний підхід.* Найбільш послідовним апологетом цього напрямку можна вважати О. Дугіна. Інформаційну війну він розглядає як форму тотального впливу глобальних політичних, економічних, терористичних, сектантських мережевих структур (хасидсько-парамасонська група, Захід на чолі з США, країни «золотого мільярда») з метою контролювання політичної, соціальної, економічної ситуації та інтенсифікації трансформаційних тенденцій духовності світового суспільства через спрямування інформаційних процесів в інтересах США, які одночасно створюють систему захисту власного мережевого коду, який ці процеси дешифрує та структурує.

Сегментами глобальної мережі у цьому підході є:

– пряме проамериканське лобі експертів, політологів, аналітиків, технологів, які контролюють владу та претендують на роль інтелектуальної еліти суспільства;

– представники великого бізнесу та політичної еліти, які орієнтовані на фінансово-економічну діяльність за кордоном;

– ЗМІ та ЗМК, які виконують функцію масованого інформаційного впливу за допомогою потоків візуальної та смислової інформації.

Тобто «інформаційну війну ведуть ідейні кілери — найманці з числа політиків, духівництва, інтелектуалів, які зраджують інтереси народу,

проституюючи совість і розум». Характерною рисою «мережевої війни», за О. Дугіним, є тотальний інформаційний вплив «мережевої п'ятої колони» «агентів впливу» – рушійної сили світового заколоту з метою десуверенізації країни [219]. Особливості цього підходу:

– дослідження мережевого характеру сучасного світового бізнесу, політичних проектів, терористичних формувань і сектантських організацій;

– розкриття сутності діяльності «агентів впливу»;

– надмірна абсолютизація поняття «мережі», ігнорування психологічних особливостей людини як самостійного індивіда;

– містично-конспірологічний погляд на роль світових глобальних структур, демонізація західного світу, захоплення ідеєю «світового єврейського заколоту», окультизм і расовий фактор.

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 [609, 368, с. 31–39].

Отже, на нашу думку, *інформаційна війна* – це суспільно-політичне явище, яке у 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 в *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 війнам, негативному 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, у яких опинилось українське суспільство останніми роками [667, с. 29 –35].

Таким чином, що 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 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.

2. Співвідношення інформаційної безпеки з деякими іншими видами безпеки

Одним з важливих завдань, як видається, є вивчення співвідношення, спільного і відмінного в деяких схожих категоріях, пов'язаних з інформаційною безпекою. Маються на увазі насамперед категорії економічна безпека, кібербезпека, екологічна безпека та ін. Отже, спробуємо з'ясувати це, виходячи з існуючих наукових джерел і нормативно-правової бази.

Економічна безпека та інформаційна безпека.

Економічаї безпека закріплена в Конституції України. Зокрема, ч. 1 ст.17 Конституції України встановлено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [316]. Однак зміст цього поняття та структура економічної безпеки держави як системи в Основному законі України не розкриваються. У відповідних науково-практичних коментарях ця правова категорія також не аналізується.

Разом з тим визначення терміна «економічна безпека» міститься у декількох підзаконних нормативно-правових актах. Так, у Методичних рекомендаціях щодо розрахунку рівня економічної безпеки України, затверджених Наказом Міністерства економічного розвитку та торгівлі 29.10.2013 р. за № 1277, економічна безпека визначається як стан національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз, забезпечувати високу конкурентоспроможність у світовому економічному середовищі і характеризує здатність національної економіки до сталого та збалансованого зростання [479].

У Методиці розрахунку рівня економічної безпеки України, яка діяла до методичних рекомендацій від 2013 р., під економічною безпекою розуміється стан національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз і здатний задовольняти потреби особи, сім'ї, суспільства та держави [479].

Наведені дефініції свідчать про певний розвиток поняття «економічна безпека», який відображає зміну пріоритетів держави у цій сфері. На наш погляд, закладення в основу цього поняття критерію здатності задовольняти потреби особи, сім'ї, суспільства та держави більш відповідає тим викликам та проблемам, які нині існують у національній економіці.

Засадниче значення для тлумачення економічної безпеки держави має формула однойменної спеціальності, закріпленої у Паспорті спеціальності 21.04.01 – економічна безпека держави (економічні науки), що затверджений Президією ВАК України 15.12.2004 р. за протоколом № 11-10/11т. Зокрема, відповідно до розділу 1 вказаного Паспорта спеціальності, економічна безпека держави – це галузь науки, яка досліджує національні економічні інтереси та загрози економічній безпеці України, здатність держави до захисту національних економічних інтересів від зовнішніх та внутрішніх загроз, а також здатності національної економіки зберігати та поновлювати процес суспільного відтворення і достатній оборонний потенціал у кризових ситуаціях [446]. Таке визначення побудоване на переліку об'єктів дослідження цієї галузі науки, які виступають об'єктами та напрямами системи економічної безпеки держави.

Варто також зазначити, що категорія «економічна безпека» вживається в Господарському кодексі України, але не деталізується. У цілому ж положеннями Господарського кодексу України доведено, що економічна безпека є основою економічної діяльності суб'єктів господарювання, які функціонують відповідно до вимог господарського законодавства. Основні норми господарського законодавства створюють достатньо міцну правову основу забезпечення економічної безпеки на мікрорівні (рівні суб'єктів господарювання) [143, с. 88–93].

Для розкриття сутності економічної безпеки потрібно звернутись і до міжнародно-правових джерел, оскільки цей термін увійшов у вітчизняний науковий обіг з міжнародної практики. Так, на 40-й сесії ООН 1985 р. було прийнято резолюцію «Міжнародна економічна безпека», де визначено, що

економічна безпека – це такий стан, за якого народ може самостійно, без тиску ззовні і будь-якого втручання визначати шляхи й форми свого економічного розвитку.

Питання економічної безпеки перебувають на постійному моніторингу в ООН, зокрема аналізуються міжнародні аспекти забезпечення економічної безпеки як основи для розвитку відносин між розвинутими країнами та країнами, що розвиваються. У цьому контексті слід згадати перші документи з цих питань: доповідь Генерального секретаря ООН «Концепція міжнародної економічної безпеки» 1987 р. та резолюцію Генеральної Асамблеї ООН «Міжнародна економічна безпека» 1987 р. У цих документах аналізуються національні та міжнародні джерела загроз економічній безпеці країн, що розвиваються, а також визначаються ключові проблеми світової економіки. Економічна безпека розглядається як стан економіки держави, який забезпечує здатність протистояти несприятливому зовнішньоекономічному впливу.

Наведені вище нормативні визначення економічної безпеки держави стали основою для відповідних теоретико-правових досліджень. Наприклад, автори монографії «Економічна безпека України: сутність і напрямки забезпечення» В. Шлемко та І. Бенько зазначають, що економічна безпека в найбільш загальному вигляді являє собою такий стан національної економіки, який дає змогу зберігати стійкість до внутрішніх і зовнішніх загроз і здатен задовольнити потреби особи, сім'ї, суспільства, держави [675].

Як бачимо, автори монографії повністю погоджуються з нормативним визначенням економічної безпеки, що міститься в Методиці розрахунку рівня економічної безпеки України від 2007 р.

Схожу позицію займає Г. Пухтаєвич, стверджуючи, що економічна безпека є таким станом національної економіки, який дає, забезпечує можливість захищати інтереси на національному рівні, відповідний рівень стійкості до зовнішніх та внутрішніх загроз, здатність розвивати та захищати життєво важливі інтереси громадян, суспільства, країни [527].

У юридичній енциклопедії економічна безпека характеризується як стан національної економіки з погляду забезпечення її розвитку та матеріальних інтересів людей. Такий стан досягається системою організаційно-правових, технологічних та інших заходів економічного змісту [680].

В. Предборський пропонує визначати сутність економічної безпеки як стан економіки й інститутів влади, за якого забезпечуються гарантований захист національних інтересів, соціальна спрямованість політики, достатній оборонний потенціал навіть за несприятливих умов розвитку внутрішніх та зовнішніх процесів [467].

Наведені позиції авторів свідчать про розгляд економічної безпеки у статиці, відповідно, її зміст розкривається через категорії «стан національної економіки» та «стан інститутів влади».

Серед науковців поширений динамічний підхід до визначення поняття «економічна безпека держави». Так, С. Лекарь зазначає, що, характеризуючи безпеку в економічному аспекті, її слід розуміти як можливість застосування ресурсів необхідних для нормального та стабільного функціонування господарської одиниці, а також для її економічного зростання [351, с. 399–402].

У статті Ю. Самойленко, М. Григорчук досліджуються певні аспекти юридичної природи економічної безпеки з позицій макрорівня (рівня держави). На думку авторів, економічна безпека держави є комплексом ефективних методів та форм захисту (з одного боку) і протидії (з іншого боку) різноманітним економічним проявам недружнього характеру, які загрожують встановленому законом порядку реалізації всіма суб’єктами фінансово-господарських відносин, визначених законодавчо прав на розвиток та об’єктивне самовідтворення, збільшенню добробуту на національному рівні, повноцінному забезпеченню потреб населення країни [551].

У Концепції економічної безпеки України вона розглядається як «спроможність національної економіки отримувати свій вільний, незалежний

розвиток і утримувати стабільність громадянського суспільства та його інститутів, а також достатній оборонний потенціал країни за всіляких несприятливих умов і варіантів розвитку подій, здатність Української держави до захисту національних економічних інтересів від зовнішніх і внутрішніх загроз [172, с. 56].

Досить часто у наукових працях застосовують системно-структурний підхід до розуміння економічної безпеки, який дає змогу розглядати її як логічно побудовану систему, елементи якої взаємопов'язані та взаємодіючі.

Так, В. Савін вважає, що економічна безпека являє собою систему захисту важливих інтересів країни [544].

Н. Попадинець наголошує, що економічна безпека – це сукупність умов, які забезпечують незалежність національної економіки, її стабільність і стійкість, здатність до постійного відновлення і самовдосконалення, здатність економіки забезпечувати ефективне задоволення ендогенних та екзогенних суспільних потреб [458, с. 20–23].

У правовому аспекті економічну безпеку держави можна розглядати як правовідносини, що виникають при забезпеченні органами публічної влади стану захищеності національної економічної системи.

Схожий підхід при дослідженні економічної безпеки держави використовують і вчені-економісти. Наприклад, І. Мішина пропонує розглядати економічну безпеку як систему економічних відносин і горизонтальних і вертикальних, між державою, регіонами, фірмами та окремими індивідами з приводу досягнення такого рівня економічного розвитку, при якому забезпечується ефективне задоволення потреб і гарантований захист інтересів усіх суб'єктів економіки, навіть при несприятливих умовах розвитку внутрішніх та зовнішніх процесів [625].

Економічна безпека пов'язана з іншою складовою національної безпеки – інформаційною. Вивчення доктринальної основи останньої категорії, на нашу думку, засвідчує різні підходи до розуміння природи і сутності інформаційної безпеки насамперед у юридичній науці та інших

галузях вітчизняної науки. Слід підкреслити термінологічну невизначеність, неоднозначність на авторське бачення цієї категорії.

В узагальненому вигляді інформаційну безпеку, як уже зазначалося визначено доцільність її розгляду крізь призму правовідносин, що виникають при забезпеченні стану захищеності інформаційного простору. Обґрунтованим є комплексне трактування сутності та гарантій забезпечення інформаційної безпеки держави як напряму державної політики у сфері національної безпеки та оборони, невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки. Це підтверджується аналізом положень Конституції України, Законів України «Про національну безпеку України», «Про Концепцію Національної програми інформатизації», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про оборону України» тощо, однозначно інформаційна безпека визнається одним із напрямів державної політики у сфері національної безпеки і оборони [662].

І хоча економічна безпека та інформаційна безпека різняться за об'єктом (економічна система, інформаційний простір тощо) та засобами забезпечення, проте мають і низку спільних рис. Так, йдеться про такі характерні риси або властивості:

1) є складовими національної безпеки;

2) їх забезпечення є найважливішою функцією держави;

3) їх регулювання здійснюється на відповідній правовій основі;

4) мають однакові рівні забезпечення (міжнародний, національний та локальний);

5) схожими фактично є їх суб'єкти – держави (відповідні органи і посадові особи), міжнародні організації, фізичні та юридичні особи і т.д.);

6) їх першочерговими цілями виступають запобігання та усунення загроз, захист суверенітету держави у визначених сферах.

На підставі вищевикладеного можна зробити висновок про те, що економічна безпека та інформаційна безпека є конституційними категоріями,

хоча зміст їх в Основному законі України не розкривається. Аналіз наукових досліджень свідчить про застосування різних підходів до з'ясування сутності економічної безпеки держави. При цьому найпоширенішими серед авторів є статичний, динамічний, системно-структурний та комплексний підходи. Єдине нормативне визначення економічної безпеки, що міститься в Наказі Міністерства економічного розвитку та торгівлі від 2013 р., засноване саме на статичному підході. У юридичній площині економічну безпеку держави можна розглядати як правовідносини, що виникають при забезпеченні органами публічної влади стану захищеності національної економічної системи.

Кібербезпека та інформаційна безпека.

Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [151, 23, 24, 570, 263, 150, с. 104–114].

Деякі експерти, включаючи і Д. Франсело, вважають, що останнім часом термін cybersecurity все частіше використовується, але при цьому багато керівників служб безпеки і просто експерти з інформаційної безпеки досі плутаються в тому, коли і як використовувати цей термін [30].

Тому потребує вивчення термін «кібернетична безпека», що наводиться в деяких національних стратегічних документах. У стратегії Франції, присвяченій питанням кібербезпеки, дано таке визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, оброблюються або передаються, і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними [46, с. 23].

Відповідно до цього визначення кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності

даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об'єктів, на які можуть діяти якісь загрози з кіберпростору, послуг інформаційних систем це визначення терміна дозволяє у розширеному вигляді включати включати якісь загрози функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Погоджуємося, що це положення має важливе методологічне значення в розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки.

У німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків. Вона повинна ґрунтуватися на комплексному підході, що є досить прагматичним, адже дає змогу розробити практичні кроки щодо забезпечення кібербезпеки, проте не надає достатніх методологічних підстав для проектування та оцінювання систем, що забезпечують цю безпеку. Про це побічно свідчить зміст десяти стратегічних напрямів у стратегії забезпечення кібербезпеки, оголошених федеральним урядом Німеччини [20, с.15].

Варті уваги наукові позиції українських дослідників щодо розуміння і змісту поняття «кібернетична безпека», її співвідношення з поняттям «інформаційна безпека». Зокрема, на основі законодавчих і доктринальних визначень зроблено висновки, що кібербезпека – це окремий випадок інформаційної безпеки, поява якого зумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж. У такому випадку О. Баранов подає таке визначення: кібербезпека – це інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж. Це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і

порушення цілісності, конфіденційності та доступності інформації [128, с. 54–62].

Надане згаданим автором визначення кібербезпеки засноване на діалектичному зв'язку категорій загального та одиничного у сфері інформаційної безпеки. Кібербезпека розглядається як одиничне стосовно інформаційної безпеки, яка виступає загальне. Запропонований підхід дає змогу розглядати проблеми кібербезпеки з позицій відносно напрацьованої теоретичної та практичної бази інформаційної безпеки та створювати несуперечливі моделі правового регулювання в цих сферах.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» 2017 р. визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Так, у цьому законі *кібербезпека* трактується як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [496].

У свою чергу, метою Стратегії кібербезпеки України (2016 р.) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [508].

Згадана Стратегія ґрунтується на положеннях Конвенції про кіберзлочинність, ратифікованої в 2005 р. законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020р. Стратегії національної безпеки України, затвердженої Указом Президента України 26 травня 2015 року за № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України».

Основу національної системи кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку визначені Стратегією завдання. Наприклад, на Міністерство оборони України, Генеральний штаб Збройних сил України відповідно до їхньої компетенції покладено здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури [508].

Визначені на законодавчому рівні пріоритети та напрями забезпечення кібербезпеки України включають, насамперед, розвиток безпечного, стабільного і надійного кіберпростору, що має полягати у:

– виробленні й оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

– розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які

відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри в кіберпросторі, які проводяться під егідою ОБСЄ, тощо.

На підставі ст. 14 Закону України «Про основні засади забезпечення кібербезпеки України» 2017 року регламентовано засади міжнародного співробітництва у сфері кібербезпеки за такими напрямами:

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами та спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб'єктів сектора безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог Законів України «Про порядок направлення підрозділів Збройних сил України до інших держав», «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України».

3. Відповідно до законодавства України у сфері зовнішніх відносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним

органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору [496].

Для реалізації таких напрямів співробітництва України у сфері кібербезпеки, на нашу думку, важливим є й вивчення відповідного зарубіжного досвіду, діяльності міжнародних організацій у згаданій сфері, прийнятих ними актів та ефективності їх реалізації.

На відміну від інших різновидів безпеки, зокрема екологічної чи економічної, сфера кібербезпеки останніми роками стала об'єктом міжнародно-правового регулювання та інших форм співпраці [212, 273, с. 25–32]. Але на цих питаннях ми зупинились в інщих розділах нашої роботи.

Кожна держава, включаючи Україну, покликана створити ефективну національну систему кібербезпеки; посилювати спроможності суб'єктів сектора безпеки та оборони для забезпечення ефективної боротьби з кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблювати міжнародне співробітництво у цій сфері. Слід підкреслити важливість і необхідність такого напряму діяльності, як забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка перебуває під юрисдикцією України й порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки та оборони України (критична інформаційна інфраструктура) тощо.

Конкретні зусилля мають бути спрямовані на забезпечення дієвих інструментів функціонування національної системи кібербезпеки, зміцнення інформаційної безпеки на національному, наднаціональному і міжнародному універсальному рівнях, враховуючи глобальний вимір порушеної проблематики. Неодноразово відзначалось на вищому владному рівні України, що найбільш пріоритетним напрямом нині є реформування власної інформаційної безпеки за рахунок створення дієвої системи кібербезпеки,

розбудова якої потребує розв'язання багатьох завдань як соціального і техногенного, так і, особливо, організаційного характеру.

Найбільш актуальні серед цих завдань: чітке визначення функцій суб'єктів забезпечення кібернетичної безпеки та розподіл повноважень між ними; забезпечення належної координації діяльності як загальних суб'єктів забезпечення кібернетичної безпеки, так і відповідних спеціальних суб'єктів; розроблення й упровадження найсучасніших підходів, форм і методів забезпечення кібернетичної безпеки, а також залучення до такого виду діяльності висококваліфікованих фахівців.

Екологічна безпека та інформаційна безпека. Забезпечення екологічної безпеки і підтримання екологічної рівноваги на території України, подолання наслідків Чорнобильської катастрофи, збереження генофонду Українського народу є обов'язком держави (ст. 16 Конституції України) [316].

Ці конституційні положення знайшли деталізацію і конкретизацію на рівні численної кількості законів та підзаконних нормативно-правових актів України. Так, згідно із Законом України «Про охорону навколишнього природного середовища» *екологічна безпека* є такий стан навколишнього природного середовища, при якому забезпечується запобігання погіршенню екологічної обстановки та виникнення небезпеки для здоров'я людей. Екологічна безпека гарантується громадянам України здійсненням широкого комплексу взаємопов'язаних політичних, економічних, технічних, організаційних, державно-правових та інших заходів. Діяльність фізичних та юридичних осіб, що завдає шкоди навколишньому природному середовищу, може бути припинена за рішенням суду (стаття 50) [497].

Екологічна безпека перебуває під контролем держави і регулюється нормативно-правовими актами, серед яких: Закон України «Про охорону навколишнього природного середовища», Закон України «Про пестициди і агрохімікати», Закон України «Про відходи», Закон України «Про захист рослин», Закон України «Про забезпечення санітарного та епідемічного благополуччя населення», Постанова Верховної Ради України «Про основні

напрями державної політики України в галузі охорони навколишнього природного середовища, використання природних ресурсів і забезпечення екологічної безпеки», Концепція екологічної безпеки України, Указ Президента України «Про державну стратегію України по охороні навколишнього середовища і забезпечення стійкого розвитку», Санітарні правила зберігання, транспортування і застосування мінеральних добрив у сільському господарстві № 1049-73, Інструкція з екологічного обґрунтування господарської та іншої діяльності тощо.

Згідно з п.4. ст. 3 Закону України «Про національну безпеку» 2018 р., державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо [489].

Питання екологічної безпеки фактично не нове в сучасній науці. Проте вітчизняні вчені не приділяли йому належної уваги в радянські часи або й ще раніше, на відміну від зарубіжний дослідників. Тому, можна стверджувати, що правовий інститут екологічної безпеки розвивається з часу проголошення незалежності зі становленням самостійної галузі – екологічного права України. Водночас, значний масив законодавчих актів, який регулює питання екологічної безпеки, демонструє комплексність і міжгалузевий характер цього поняття.

На переконання багатьох учених, розріняють такі види екологічної безпеки:

За територіальним поділом: загальносвітова екологічна; внутрішньодержавна; регіональна; місцева; екологічна безпека окремих об’єктів.

За видами екологічно небезпечної діяльності фізичних та юридичних осіб: технічна; хімічна; токсична; біологічна; генетична, радіаційна; транспортних засобів тощо.

За місцем шкідливих впливів на людину та навколишнє природне середовище: внутрішня екологічна безпека (запобігання, обмеження або

компенсація негативного впливу на працівників підприємств, установ, організацій, робота яких пов'язана з джерелом підвищеної небезпеки); зовнішня екологічна безпека (запобігання, обмеження або компенсація негативного впливу на громадян, що проживають на територіях, на яких розміщенні об'єкти підвищеної небезпеки). Види, обсяги, джерела і порядок надання компенсації, а також визначення територій, на які поширюються такі заходи, встановлює Кабінет Міністрів України за погодженням з місцевими органами державної влади і самоуправління на основі науково-економічного обґрунтування [117, 221, 275].

За структурою екологічна безпека охоплює: по-перше, об'єкти екологічної безпеки; по-друге, екологічні загрози; по-третє, систему захисту об'єктів екологічної безпеки від екологічних загроз.

Так, об'єктами національної екологічної безпеки є:

– людина і громадянин – їхні конституційні права і свободи;

– суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне й навколишнє природне середовище, природні ресурси;

– держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

З-поміж найбільш загальних і беззаперечних об'єктів екологічної безпеки, на наш погляд, є життя і здоров'я людей, безпечне навколишнє природне середовище та його компоненти (природні умови).

Слід зупинитись на суб'єктах забезпечення національної екологічної безпеки. Так, на основі вивчення положень Конституції України і в цілому чинного національного законодавства України можна визначити з-поміж них наступних: Президент України;Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; Прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні сили України, Служба безпеки

України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування.

Законом України «Про охорону навколишнього природного середовища» закріплюються екологічні вимоги щодо окремих видів діяльності: інвестиційної, господарської та діяльності у процесі розміщення і розвитку населених пунктів (містобудівної) (ст. ст. 51, 59); вимоги екологічної безпеки: щодо транспортних засобів (ст. 56); щодо проведення наукових досліджень впровадження відкриттів, винаходів, застосування нової техніки, імпортного устаткування, технологій і систем (ст. 57); щодо військових, оборонних об'єктів та військової діяльності (ст. 58); вимоги щодо охорони довкілля від неконтрольованого та шкідливого біологічного впливу (ст. 53); від акустичного, електромагнітного, іонізуючого та іншого шкідливого впливу фізичних факторів та радіоактивного забруднення (ст. 54); від забруднення виробничими, побутовими, іншими відходами (ст. 55); у процесі застосування засобів захисту рослин, мінеральних добрив, токсичних, хімічних речовин та інших препаратів (ст. 52) [497].

По суті, діяльність держави в особі її компетентних органів щодо управління якістю довкілля, забезпечення екологічної безпеки і підтримання екологічної рівноваги на території країни, подолання наслідків аварій і збереження генофонду народу становить екологічну функцію держави. На сьогодні вона визнана однією з основних функцій Української держави, так само як і функції забезпечення інформаційної та економічної безпеки.

Реалізація екологічної функції держави обумовлена конституційними та іншими законодавчими нормами, шляхом проведення відповідної державної політики на тому чи іншому етапі розвитку держави. Її принципові засади в Україні визначені Основними напрямами державної політики України в галузі охорони довкілля, використання природних ресурсів та забезпечення екологічної безпеки.

Підкреслимо, якщо функція забезпечення інформаційної безпеки спрямована на запобігання і протидію інформаційним загрозам, то екологічна

функція держави спрямована на усунення екологічних загроз. Так, останніми визнаються будь-які наявні чи потенційні негативні впливи довкілля на об'єкти екологічної безпеки, а також екологічно небезпечної діяльності людини на довкілля.

Закріплення у ст. 50 Конституції України права кожного на безпечне для життя і здоров'я довкілля та на відшкодування шкоди, заподіяної порушенням цього права [317], підняло його на найвищий рівень у системі основних суб'єктивних екологічних прав людини і громадянина. У конституційно-правовій та еколого-правовій літературі це право отримало назву «право на екологічну безпеку».

Юридичному опосередкуванню суб'єктивного права людини і громадянина на екологічну безпеку сприяють і наукові підходи, які викристалізувалися в науковій спеціальній літературі:

1) обгрунтування доцільності реалізації права на сприятливе навколишнє природне середовище як різновиду суб'єктивного права людини і громадянина, яке перебуває під захистом держави і гарантується наданням їм можливості звертатися за допомогою і захистом до компетентних державних органів;

2) виділення права людини і громадянина на здорове навколишнє природне середовище, яке закріплене в законі й здійснюється в межах загальних правовідносин. Способом реалізації цього права є факт проживання особи в незабруднених умовах і споживання безпечних для її здоров'я природних благ;

3) формування у системі екологічних прав суб'єктивного права людини і громадянина на безпечне для життя і здоров'я навколишнє природне середовище, точніше, права на екологічну безпеку, тобто забезпеченої системою права і законодавства юридичної можливості особи реалізовувати у передбачених законодавством формах надані їй повноваження у сфері екологічної безпеки з метою задоволення природних потреб у відповідній

екологічній обстановці, що виключає негативний вплив загроз техногенного або природного характеру на здоров'я та життя людини [221, 275].

Видається, що найширокою правовою категорією є «право людини і громадянина на екологічну безпеку». Це право тісно пов'язане з правами на життя, на охорону здоров'я, на інформацію, а також іншими, зумовлені тим, що людина, її честь, гідність, недоторканність та безпека визнаються в нашій державі найвищою соціальною цінністю (ст. 3 Конституції України) [317].

На наш погляд, право людини і громадянина на екологічну безпеку є інтегрованою категорією, яка грунтується на загальнолюдському природному праві на безпеку, що отримало юридичне оформлення на конституційному рівні та деталізоване у чинному законодавстві.

Можна констатувати, що неодноразово в науковій юридичній літературі зустрічається позиція, згідно з якою обґрунтовується доцільність виокремлення концепту «екологічна держава». Так, К. Машненков відзначає, що його доцільно розглядати в диференційованому вигляді. У найвищому своєму прояві екологічна держава ґрунтується на біоцентризмі, а не на антропоцентризмі, коли держава бере на себе відповідальність за сприятливі умови для існування не лише людей, а й усіх елементів екосистеми держави, збільшуючи її біорізноманіття і сприяючи її розвитку в цілому. Він пропонує критерії визначення міри екологічності чи контрекологічності держави на сучасному етапі державотворення [385].

Водночас розвиток інформаційно-комунікативних технологій, на нашу думку, потребує звернення уваги на засоби і способи охорони навколишнього природного середовища від акустичного, електромагнітного, іонізуючого та іншого шкідливого впливу фізичних факторів та радіоактивного забруднення. Місцеві ради, підприємства, установи, організації та громадяни при здійсненні своєї діяльності зобов'язані вживати необхідних заходів щодо запобігання та недопущення перевищення встановлених рівнів акустичного, електромагнітного, іонізуючого та іншого шкідливого фізичного впливу на навколишнє природне середовище і здоров'я людини в населених пунктах,

рекреаційних і заповідних зонах, а також у місцях масового скупчення і розмноження диких тварин.

Інший факт, що може сприяти негативним наслідкам, у тому числі для навколишнього середовища, це інформаційні конфлікти, включаючи інформаційні війни, кібератаки та інші форми інформаційного протиборства. Важливим є, безумовно, запобігання їм, а також своєчасна ефективна протидія.

Таким чином, як бачимо, значну увагу і законодавцем, і науковцями приділено вивченню питань екологічної безпеки, екологічних прав людини і громадянина, екологічної функції держави тощо. Разом з тим потребують ґрунтовного вивчення співвідношення екологічної безпеки та інформаційної безпеки, зокрема в контексті реалізації функцій держави, співвідношення екологічної держави і конституційної держави, а також інших пов’язаних категорій.

3. Принципи забезпечення державою інформаційної безпеки

З огляду на проаналізовані у попередніх розділах нашого дослідження природу і сутність інформаційного суспільства та інформаційної безпеки, а також функції держав, спрямовані на їх забезпечення, 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 і багатогранною, оскільки включає чимало складових, починаючи від створення умов регулювання й завершуючи реалізацією, охороною та 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.

Філософський підхід до розуміння поняття принципу розглядає його як першопочаток, те, що лежить в основі певної сукупності фактів, теорії, науки [623]. У юридичній енциклопедії запропоновано визначення поняття принцип (від франц. principe, від лат. principium – начало, основа) як основні засади, вихідні ідеї, що характеризуються універсальністю, загальною значущістю, вищою імперативністю і відображають суттєві положення теорії, вчення, науки, системи внутрішнього і міжнародного права [680].

Новий енциклопедичний словник дає таке розуміння: принцип (від лат. principium – начало, основа): 1) вихідне положення якої-небудь теорії, вчення, науки, світогляду, політичної організації; 2) основа побудови або дії якого-небудь приладу, машини тощо [413].

У «Словнику іншомовних слів» принцип визначено як центральне пояснення, особливість, покладена в основу створення або здійснення чого-небудь [569, с. 762].

За словником з конфліктології принцип (від лат. Princeps – «перший, головний») – основне вихідне положення будь-якої теорії, вчення, науки, світогляду, політичної організації [320, с. 374].

До поняття принципів звертає у своїх працях переважна більшість конституціоналістів, оскільки принципи є основоположними ідеями, що мають високий рівень сконцентрованості правових позицій і лежать в основі формування правових норм задля регулювання правових відносин.

У першу чергу, принципи – це ідеї. Елемент узагальнення, піднесений над конкретикою, що властивий ідеї, досить чітко простежується і в принципах права. Потім принципи перетворюються на норми, втілюються в них. Принципи концентрують результат розвитку права, в них втілюється нерозривний зв'язок минулого, сучасного та майбутнього [241, с. 22–28].

А. Колодій у своєму докторському дисертаційному дослідженні визначає принципи права як відправні ідеї його буття, які виражають найважливіші закономірності і підвалини даного типу держави і права, є однопорядковими з сутністю права і станоалять його головні риси, відрізняються універсальністю, вищою імперативністю і загально значимістю [298, с. 19].

Т. Фулей розглядає таке поняття, як загальнолюдські принципи права, під якими розуміються зафіксовані в позитивному праві його універсальні нормативні засади, які напрацьовані людством як глобальною макроцивілізаційною системою, об'єктивно зумовлені потребами і рівнем розвитку людської цивілізації та втілюють її найкращі здобутки у правовій сфері, визначають сутність і спрямованість правового регулювання і придатні до застосування у будь-якій системі права [627, с. 16].

Наразі прийнято значну кількість нормативно-правових актів України, ґрунтовне вивчення яких дає змогу проаналізувати принципи регулювання та забезпечення інформаційної безпеки.

Зокрема, у ст. 3 Закону України «Про національну безпеку України» 2018 р. закріплено, що державна політика у сферах національної безпеки і

оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України [489].

Виходячи з мети нашого дослідження, змушені акцентувати увагу насамперед на основоположних засадах, певних концептуальних ідеях, що становлять основу регулювання і забезпечення інформаційної безпеки на нинішньому етапі. Не дивлячись на те, що чітко на законодавчому рівні відповідні принципи не регламентовані, ґрунтовне вивчення національного законодавства дає змогу підкреслити таке.

По-перше, у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» 2007 р. є розділ II «Законодавче забезпечення розвитку інформаційного суспільства» та розділ III «Національна політика розвитку інформаційного суспільства в Україні», де зазначено, що при створенні інформаційного законодавства слід керуватися

– загальними принципами Конституції України,

– а також базуватися на принципах свободи створення, отримання, використання та поширення інформації; об’єктивності, достовірності, повноти і точності інформації; гармонізації інтересів людини, суспільства та держави в інформаційній діяльності; обов’язковості публікації інформації, яка має важливе суспільне значення; обмеження доступу до інформації виключно на підставі закону; мінімізації негативного інформаційного впливу та негативних наслідків функціонування ІКТ; недопущення незаконного поширення, використання і порушення цілісності інформації; гармонізації інформаційного законодавства та всієї системи вітчизняного законодавства.

Розділ IV «Організаційно-правові основи розвитку інформаційного суспільства в Україні» згаданого закону передбачає, що організаційно-правові основи розвитку інформаційного суспільства в Україні включають: інституційне, організаційне та ресурсне забезпечення; відповідні об'єднання громадян; механізми інтеграції України у світовий інформаційний простір та механізми реалізації Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки [244].

Як бачимо, на рівні Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» 2007 р. розмежовано загальні принципи Конституції України, спеціальні принципи створення інформаційного законодавства, а також організаційно-правові основи розвитку інформаційного суспільства в Україні.

По-друге, у Стратегії розвитку інформаційного суспільства в Україні, затвердженій Розпорядженням Кабінету Міністрів України 15 травня 2013 р. № за 386-р, для розвитку інформаційного суспільства передбачено застосовувати принципи:

– рівноправного партнерства державних органів, громадян і бізнесу;

– прозорості та відкритості діяльності державних органів;

– гарантованості права на інформацію, вільного отримання та поширення інформації, крім обмежень, установлених законом;

– свободи вираження поглядів і переконань;

– правомірності одержання, використання, поширення, зберігання та захисту інформації;

– інформаційної безпеки;

– постійного навчання;

– підконтрольності та підзвітності державних органів громадськості;

– сприяння пріоритетному розвитку інформаційно-комунікаційних технологій;

– чіткого розмежування повноважень і скоординованої взаємодії державних органів;

– гарантованості повного ресурсного забезпечення національних програм та проектів розвитку інформаційного суспільства [517].

Як бачимо; на рівні згаданої Стратегії розвитку інформаційного суспільства в Україні виокремлено принцип інформаційної безпеки. Такий прийом законодавчої техніки сприяє розкриттю відповідно додаткового значення досліджуваного нами явища.

По-третє, Закон України «Про основні засади забезпечення кібербезпеки України» закріпив положення, за яким застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень здійснюються з додержанням принципів:

1) мінімально необхідного регулювання;

2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між установленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

6) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є: відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу; таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури. Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань Закону [495].

По-четверте, Законом України «Про національну безпеку України» встановлено такі основні принципи, що визначають порядок формування державної політики у сферах національної безпеки і оборони:

1) верховенство права, підзвітність, законність, прозорість та дотримання засад демократичного цивільного контролю за функціонуванням сектора безпеки і оборони та застосуванням сили;

2) дотримання норм міжнародного права, участь в інтересах України у міжнародних зусиллях з підтримання миру і безпеки, міждержавних системах та механізмах міжнародної колективної безпеки;

3) розвиток сектора безпеки і оборони як основного інструменту реалізації державної політики у сферах національної безпеки і оборони, принципи державної політики у сферах національної безпеки і оборони [489].

Можна побачити в науковій літературі й інші дещо дискусійні підходи до визначення основних принципів інформаційної безпеки, поряд з принципами забезпечення національної безпеки, кібербезпеки, державної політики у цих сферах, розвитку інформаційного суспільства тощо.

Наприклад, розкриваючи принципи забезпечення безпеки (відкритих систем), йдеться про таке:

1) забезпечення інформаційної безпеки виконується відповідно до політики управління інформаційними ризиками;

2) архітектура системи управління інформаційними ризиками забезпечує оптимальний (раціональний) баланс витрат на управління інформаційними ризиками і загального збитку від інформаційних ризиків;

3) система управління інформаційними ризиками є централізованою і реалізує єдину політику управління;

4) безпека інформації досягається за рахунок комплексного використання нормативних, економічних та організаційних заходів, технічних, програмних і криптографічних засобів;

5) система управління повинна бути багаторівневою й однаково захищеною в усіх ланках;

6) повинна бути забезпечена безперервність функціонування на всіх життєвих циклах системи;

7) повинно бути забезпечено розмежування та обмеження доступу персоналу до інформації;

8) система повинна бути здатна до розвитку та адаптації до зміни умов функціонування;

9) наявність системи безперервного моніторингу за виконанням усім персоналом установлених правил роботи в інформаційній системі;

10) моніторинг та аудит ефективності системи і своєчасна її модернізація [259].

Не дивлячись на важливі акценти, сформульовані вище, не завжди можна погодитися повністю з такими основними принципами забезпечення інформаційної безпеки; це, швидше, принципи протидії загрозам безпеки та побудови систем управління інформаційними ризиками, інформаційної безпеки у вузькому розумінні.

На нашу думку, система принципів забезпечення інформаційної безпеки має формуватись і розвиватися на основі ширшого підходу,

включаючи співвідношення національних та наднаціональних інтересів у інформаційному просторі, об'єктивні умови чи основи існування інформаційного суспільства (організаційні, економічні; технологічні; правові та ін.).

Тому можна переважно погодитися з наступними підходами до визначення принципів інформаційної безпеки. Так, Б. Кормич пропонує для визначення принципів забезпечення інформаційної безпеки два комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу, а саме:

– комплекс питань, пов'язаних з інформаційною безпекою людини і суспільства, яка, в першу чергу, вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення;

– комплекс питань, пов'язаних з інформаційною безпекою держави, які, навпаки, пов'язані із застосуванням обмежень, заборон, жорсткою регламентацією певних типів відносин в інформаційній сфері і невід'ємним елементом яких є сила державного примусу [324, с. 117].

Ю. Уфімцев, В. Буянов, Е. Єрофеєв важливими принципами визначають: законність заходів із виявлення і запобігання правопорушенням в інформаційній сфері; безперервність реалізації і вдосконалення засобів і методів контролю й захисту інформаційних систем; економічна доцільність, тобто зіставлення можливих збитків і витрат на забезпечення безпеки інформації; комплексність використання всього арсеналу засобів захисту на всіх етапах інформаційного процесу [621, с. 53].

А. Стрельцов принципи діяльності із забезпечення інформаційної безпеки розділяє на:

– загальні (гуманізм, соціальну справедливість, об'єктивність, конкретність, ефективність, опора на підтримку і довіру народу, поєднання гласності і професійної таємниці, законність і конституційність);

– особливі (насамперед, принцип глобальності та ін.) [586, с. 129-168]. Логунов та О. Олійник при визначенні принципів забезпечення

інформаційної безпеки виходять з основних принципів міжнародного права, які володіють вищою імперативною юридичною силою. Але виникає питання: чи всі з перелічених таких принципів стосуються сфери інформаційної безпеки?

Загалом поділяємо підхід, відповідно до якого принципи забезпечення інформаційної безпеки включають:

– пріоритет прав, свобод і законних інтересів людини і громадянина;

– верховенство права, рівність усіх суб'єктів правовідносин перед законом;

– відповідальність держави перед людиною за свою діяльність;

– комплексний підхід до вирішення завдань забезпечення інформаційної безпеки;

– єдність і взаємозв'язок напрямів забезпечення інформаційної безпеки;

– розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки;

– участь у міжнародних і регіональних системах інформаційної безпеки;

– оперативність, своєчасність, превентивність і адекватність заходів щодо запобігання і захисту від зовнішніх інформаційних загроз та нейтралізації джерел внутрішніх інформаційних загроз [366].

Разом з тим, пропонуємо додати низку інших принципів:

– принцип пріоритету договірних (мирних) засобів у вирішенні інформаційних конфліктів;

– взаємодії державних і недержавних систем інформаційної безпеки;

– громадського контролю за діяльністю органів державної влади, що входять до системи забезпечення інформаційної безпеки України;

– презумпції нетаємності інформації, враховуючи її різновиди конфіденційного, публічного та іншого змісту;

– неперервного захисту, мобільності та динамічності системи інформаційної безпеки, різноманітності захисних засобів і способів;

– адекватності заходів захисту національних інтересів України в інформаційній сфері реальним та потенційним загрозам;

– економічної ефективності;

– створення єдиного цілісного механізму забезпечення національної інформаційної безпеки [669, с. 50–56].

Таким чином, наведені принципи забезпечення інформаційної безпеки є основоположними і вихідними засадами створення, функціонування і розвитку системи інформаційної безпеки у контексті цілісної системи національної безпеки. При цьому не запечеречується можливість їх включення також і до системи міжнародної колективної безпеки. Підкреслимо, що використання інформації, інформаційно-комунікаційних технологій як засобів досягнення мети, що виходить за рамки національної безпеки, потребує застосування дієвих механізмів протидії та встановлення відповідальності за заподіяні збитки в інформаційній сфері. Ми переконані, що потребують подальшого вивчення концептуальні науково обґрунтовані взаємоузгоджені принципи, прийоми і засоби, спрямовані на досягнення функціональної рівноваги та забезпечення реально діючої системи інформаційної безпеки.

4. Особливості правового регулювання забезпечення інформаційної безпеки як однієї з найважливіших функцій держави

Міжнародно-правове регулювання інформаційної безпеки та інформаційної сфери. Держави на міжнародному рівні, за участю інших суб'єктів міжнародно-правових відносин, створюють якісно нові норми і принципи права, завданням яких є врегулювання відносин в інформаційній сфері. Водночас суспільні відносини іноді випереджають чи виходять за межі такого регулювання, є приклади зловживання чи неналежного регулювання інформаційних відносин як на національному, так і транснаціональному рівнях.

Слід відзначити, що існуюча система правового регулювання інформаційної сфери є, швидше, трискладовою, аніж двоскладовою. Так, окрім традиційних систем національного та міжнародного права, де первинними та основними суб'єктами виступають суверенні держави, з'являється транснаціональне право, що визнає нормотворчу функцію також за недержавними приватними акторами [34].

Науково обґрунтованим та очевидним є виокремлення та існування міжнародного інформаційного права. Низка дисертаційних досліджень саме присвячена цьому феномену безпосередньо або в контексті становлення глобального інформаційного суспільства, міжнародного правопорядку, інформаційної безпеки, кіберпростору, захисту прав людини онлайн, захисту персональних даних, доступу до публічної інформації тощо.

Водночас можна зустріти виокремлення «міжнародного права в інформаційній сфері», міжнародного регіонального (панєвропейського) права в інформаційній сфері, поряд з «міжнародним інформаційним правом» з галузевим статусом.

Погоджуємося, що останнє певним чином відображає історично сформоване «запізнювання» міжнародно-правового регулювання порівняно з внутрішньодержавним правом. Відсутність єдиних підходів спричинюється також неоднорідністю структури міжнародного інформаційного права,

фрагментарністю правового регулювання та браком уніфікованої термінології. Існує значний обсяг міжнародно-правових актів на універсальному та регіональному рівнях, присвячених однорідним інформаційним відносинам, що дає змогу стверджувати про наявність ознак розгалуженого угрупування норм міжнародного інформаційного права [441].

Беззаперечний є внесок вітчизняного дослідника А. Пазюка, який фактично є засновником нового напряму наукових досліджень у науці міжнародного права. Його учні розвивають і розширюють запропоновані ідеї і концепції стосовно інформаційного простору, кіберправа, техно-соціальної природи Інтернету, захисту персональних даних і т. д. Він запропонував класифікацію, за якою виділяються такі напрями міжнародно-правового регулювання в інформаційній сфері:

а) міжнародно-правове регулювання змісту поширюваної інформації (інформаційний контент);

б) міжнародно-правове регулювання інформаційної і комунікаційної діяльності;

в) міжнародно-правове регулювання використання обмежених інформаційних ресурсів;

г) міжнародно-правове співробітництво з питань інформаційної безпеки;

д) міжнародно-правове регулювання використання інформаційно-комунікаційних технологій в інтересах людства, запобігання та подолання наслідків стихійних явищ тощо [442, с. 19].

На нашу думку, цей перелік може бути розширений, зокрема за суб’єктним критерієм чи за просторовою ознакою. Це пояснюється динамічним еволюційним, а іноді й фактично революційним шляхом розвитку інформаційної сфери, тобто багатовекторної та різновимірної системи об’єктів інформаційної інфраструктури. Глобальна мережа Інтернет не обмежує їх територіальними кордонами держав. Тобто це власне ті об’єкти, які поширюються як у межах юрисдикції держав, так і поза її межами.

Міжнародне право протягом тривалого часу розвивалося, виходячи з принципу технологічної нейтральності. Склалась усталена практика, заснована іноді на загальних формулюваннях, нечітких правилах поведінки. Це спричиняло стан правової невизначеності, відсутності дієвих гарантій прав та свобод в інформаційному просторі, розвитку інформаційного суспільства, кіберпростору, інформаційної безпеки. Іншими словами, певний період часу не було договірної основи міжнародно-правового регулювання. Водночас спостерігалось формування звичаєвого кіберправа тощо.

Євроінтеграційні та глобалізаційні процеси зумовили необхідність перегляду зафіксованих жорстких меж між національною та міжнародною сферами регулювання, тим самим змінюючи наше уявлення про належність тієї чи іншої групи міжнародних відносин до відповідної сфери регулювання [52, с. 425-455]. Тому не заперечують дослідники більш гнучкого підходу до нормативно-правового регулювання, який передбачає відхід від ідеї, згідно з якою право повинне походити з єдиного владного джерела, яким є суверен [65, с. 70–80].

О. Кирилюк підкреслює іншу тенденцію, яка стосується порушеної нами проблематики, що передбачає характеристику процесу глобалізації регуляторного механізму як націоналізацію міжнародного права в тому розумінні, що виробляються єдині для всіх суб’єктів стандарти, дотримання та виконання яких презюмується вже в силу їх прийняття і не потребує подальшої національно-правової імплементації. Оскільки у глобальному інформаційному суспільстві немає кордонів як таких, то не повинно бути й будь-яких обмежень для нормативно-правового регулювання за жодних причин. Тенденція до збереження розмежування між національним та міжнародним правом дуже швидко втрачатиме свою актуальність у контексті питань розвитку глобального інформаційного суспільства. Пріоритетними формами регулювання повинні стати універсальні стандарти та саморегулювання [287].

Однією з головних перешкод, що не дозволяла міжнародному праву стати універсальним регулятором інформаційного суспільства було

сприйняття кіберпростору не як єдиного утворення, а, навпаки, як сукупності розрізнених національних сегментів, де функціонують національні закони держав. У результаті такої правової фрагментації ми отримали конфлікт юрисдикцій, контролюючих функцій держав, надмірну зарегульованість одних об'єктів поряд з правовими прогалинами стосовно інших сфер, об'єктів інформаційної сфери. Поява Інтернету змусила усі галузі міжнародного права пристосовуватися до нових реалій технологічно орієнтованого світу. Кіберпростір є новим середовищем, в якому немає наднаціонального суверена, ефективні, універсальні міжнародні договори та спеціалізована судова система [9].

Проте суб'єкти міжнародно-правових відносин не демонструють зацікавленості в розробленні і прийнятті універсальних міжнародних стандартів регулювання Інтернету. Тому переважно основними регуляторами відносин у глобальній мережі є регіональні міжнародно-правові норми, норми «м'якого» права. Внаслідок цього отримуємо дискримінаційне становище деяких учасників відносин в Інтернеті, домінування сили над правом, зміну існуючих регулюючих, охоронних чи інших правил, які доводять свою неефективність, не убезпечують інформаційний простір від атак, внутрішніх протиріч тощо .

Не дивлячись на це, не можна стверджувати, що взагалі відсутній міжнародний договірний процес стосовно питань інформаційної безпеки, механізму її забезпечення.

На наше переконання, базовими міжнародно-правовими актами у сфері інформаційної безпеки є :

– Резолюція ГА ООН «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» від 04.12.1998 року, в якій вперше зазначалося про загрози міжнародній інформаційній безпеці у цивільному та воєнному аспектах;

– Резолюція ГА ООН «Створення глобальної культури кібербезпеки та оцінювання національних зусиль щодо захисту найважливіших інформаційних інфраструктур»;

– Окінавська Хартія глобального інформаційного суспільства (розвиток та ефективне функціонування електронної ідентифікації, електронного підпису, криптографії та інших засобів забезпечення безпеки та достовірності операцій);

– Стратегія в галузі ІКТ;

– Боротьба зі злочинним використанням інформаційних технологій та ін.

Важливе правозастосовне значення мають принципи, що стосуються міжнародної інформаційної безпеки, які були проголошені в доповіді Генерального секретаря ООН (A/58/373) 17.09.2003 р. У цій доповіді розкривається зміст низки понять: інформаційна безпека, інформаційний ресурс, інформаційний простір, інформаційна війна, інформаційна зброя, загроза інформаційній безпеці, міжнародний інформаційний тероризм, міжнародна інформаційна злочинність. Означені принципи міжнародної інформаційної безпеки стали підставою для проведення подальших міжнародних переговорів під егідою ООН та інших міжнародних організацій щодо проблем міжнародної інформаційної безпеки.

У доповіді розкривається п’ять основних принципів міжнародної інформаційної безпеки, які визначають права, обов’язки та відповідальність суб’єктів міжнародних відносин в інформаційному просторі. Вони окреслюють конкретні завдання, вирішення яких було б направлене на зменшення загроз у сфері міжнародної інформаційної безпеки, а також визначають роль ООН у контексті загальних зусиль у цій сфері. ООН покликана сприяти міжнародному співробітництву, метою якого є зменшення загроз у сфері міжнародної інформаційної безпеки і формування міжнародно-правової основи для запобігання виникненню інформаційних війн; створення системи міжнародного моніторингу для відстеження загроз в інформаційній

сфері; створення механізму вирішення конфліктних ситуацій у сфері інформаційної безпеки; створення механізму контролю виконання умов режиму міжнародної інформаційної безпеки.

Згідно із зазначеними принципами, діяльність кожної держави та інших суб'єктів міжнародного права в міжнародному інформаційному просторі повинна сприяти загальному соціальному та економічному розвитку і здійснюватися таким чином, щоб бути сумісною із завданнями підтримки світової стабільності й безпеки, суверенними правами інших держав, інтересами безпеки, принципами мирного врегулювання суперечок і конфліктів, незастосування сили, невтручання у внутрішні справи, поваги до прав і свобод людини. Ще один важливий принцип полягає в тому, що держави та інші суб'єкти міжнародного права повинні нести міжнародну відповідальність за діяльність в інформаційному просторі [214].

Одним з перших і найважливіших міжнародних актів щодо регулювання ІКТ, інформаційної сфери є *Окінавська Хартія глобального інформаційного суспільства,* яку підписали 22 липня 2000 року країни з G8. Цим документом проголошується необхідність подолання міжнародного розриву в галузі інформації та знань, закріплюються основні принципи та напрями формування й розвитку інформаційного суспільства, визначаються пріоритетні завдання держав щодо просування економічної та соціальної трансформації, яка стимулюється ІТ. У цьому контексті встановлені пріоритетні завдання держав щодо використання можливостей цифрових технологій, подолання електронно-цифрового розриву, сприяння загальній участі в глобальному інформаційному суспільстві та подальшого розвитку ІТ на підставі багатосторонньої співпраці.

Реалізація окреслених завдань передбачена діяльностістю урядів щодо зміцнення відповідної політики і нормативної бази, що стимулюють конкуренцію і новаторство, забезпечення економічної та фінансової стабільності, які сприяють співпраці з оптимізації глобальних мереж, боротьбі зі зловживаннями, які підривають цілісність мережі, скорочення розриву в

цифрових технологіях, інвестування в людей і забезпечення глобального доступу та участі в цьому процесі [425, с. 51–56, 72].

Крім того, важливе значення у механізмі забезпечення інформаційної безпеки, в першу чергу особи, займають:

– Загальна декларація прав людини від 10.12.1948 р.;

– Міжнародний пакт про громадянські і політичні права від 10.12.1966 р.;

– Європейська Конвенція про захист прав людини та основоположних свобод від 04.11.1950 р.;

– Конвенція ООН «Про доступ до інформації, участі громадськості в процесі вироблення рішень та доступі до правосуддя в питаннях, коли йдеться про захист довкілля» від 25.06.1998 р. тощо.

– Регламент ЄС щодо захисту персональних даних (GDPR) від 27.04.2016 р. та ін.

У зазначених документах закріплені міжнародні принципи та стандарти, які гарантують право на свободу інформації, свободу вираження поглядів, захист персональних даних, забезпечення інформаційної безпеки тощо.

Так, у *Загальній декларації прав людини* 1948 р. закріплено, що кожна людина має право на свободу пошуку, одержання і поширення інформації та ідей будь-якими засобами і незалежно від державних кордонів (ст. 19) [238]. Ця міжнародна універсальна норма закріплює право на доступ до інформації в цілому.

Міжнародний пакт про громадянські і політичні права (ст. 19) деталізує положення Загальної декларації прав людини і закріплює право кожної людини на свободу пошуку, одержання і поширення будь-яко\ інформації, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір. Користування передбаченими свободами накладає особливі обов’язки й відповідальність, а отже, пов’язане з певними обмеженнями, які однак, мають

установлюватися законом і бути необхідними: а) для поваги прав і репутації інших осіб; б) для охорони державної безпеки, громадського порядку, здоров'я чи моральності населення [392].

Конвенцією ООН «Про доступ до інформації, участі громадськості в процесі вироблення рішень та доступі до правосуддя з питань, що стосуються довкілля» 1998 р. закріплено з-поміж іншого надання такого різновиду публічної інформації як екологічна. «Державні органи у відповідь на запит про надання екологічної інформації надаватимуть громадськості таку інформацію у рамках національного законодавства», включаючи копії фактичних документів, які містять або охоплюють таку інформацію [301].

Як уже зазначалося, в інформаційній сфері закономірною тенденцією міжнародно-правового регулювання стало прийняття актів рекомендаційного характеру. Для прикладу наведемо *Довільську декларацію «Незмінна відданість свободі та демократії»* 2011 р. (закріплено свободу, повагу приватності та інтелектуальної власності, багатостороннє управління, кібербезпеку та захист від злочинності, що повинні лягти в основу розвитку Інтернету).

Інший важливий документ – *Комюніке ОЕСР щодо принципів розробки Інтернет-політики від 2011 року* закріплює основні принципи, які сприятимуть збереженню відкритості Інтернету поряд із захистом приватності, безпеки, прав дітей онлайн, відновленням довіри до Інтернету. Відкритий та доступний Інтернет визнається передумовою дотримання свободи вираження поглядів та законного обміну інформацією, знаннями і поглядами [17].

Згодом на основі положень *комюніке 2015 року саміту в Анталії G-20* держави взяли зобов'язання щодо скорочення цифрового розриву та визнали особливу відповідальність щодо забезпечення безпеки і стабільності у кіберпросторі.

Резолюція «Демократія у цифрову еру і загроза приватності та індивідуальним свободам» 2015 р. закріпила звернення до парламентів країн-

учасниць долучитися до розроблення та імплементації загальної стратегії розвитку Інтернету на користь людства. Йдеться про відмову від правових обмежень щодо свободи вираження поглядів та не перешкоджати вільному руху інформації, а також дотримання принципу мережевої нейтральності.

У свою чергу, *Декларація Монтре «Про захист персональних даних у глобальному світі: універсальне право, що поважає багатоманітність» 2005 р.* звертається до ООН щодо розроблення юридично обов'язкового документа, який чітко закріпив би право на захист персональних даних та приватності, а також відповідні контрольні механізми.

Спільна рекомендація BOIB 2001 р. щодо положень про захист знаків та інших прав промислової власності на позначення в Інтернеті до певної міри гармонізує спроби тлумачення чинного матеріального права, не стосується при цьому питань юрисдикції та застосованого права.

Серед регіональних міжнародних норм, які закріплюють права людини в інформаційній сфері, право на інформаційну безпеку, можна виділити:

– *Конвенцію Ради Європи «Про захист прав людини та основоположних свобод» 1950 р.* У її ст. 10 закріплено право кожного одержувати і передавати інформацію без втручання органів державної влади і незалежно від кордонів. Здійснення передбачених конвенцією свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для охорони порядку або запобігання злочинам, для охорони здоров'я або моралі, для захисту репутації або прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і неупередженості суду і є необхідними в демократичному суспільстві [303]

– *Конвенцію Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» 1981 р.* Держави – члени Ради Європи, які підписали Конвенцію, підтверджуючи свою відданість

свободі інформації незалежно від кордонів домовилися про забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав та основоположних свобод, зокрема її права на недоторканість приватного життя, у зв'язку з автоматизованим обробленням персональних даних, що її стосуються [302]

– *Декларацію Комітету Міністрів Ради Європи «Про свободу вираження поглядів та інформації» 1982 р.* Держави–члени Ради Європи оголошують про те, що в сфері інформації та ЗМІ вони намагаються досягти такої мети: проведення відкритої інформаційної політики в публічному секторі, що включає також доступ до інформації задля сприяння розумінню кожною людиною політичних, соціальних, економічних і культурних проблем та заохочення вільного обговорення цих проблем [200]

– *Рекомендації Комітету Міністрів Ради Європи*: «Про доступ до інформації, яка знаходиться в розпорядженні державних органів» 1981 р.; «Про передачу третім особам персональних даних, які знаходяться в розпорядженні державних органів» 1991 р.; «Про європейську політику доступу до архівів» 2000 р.; «Про доступ до офіційних документів» 2002 р. тощо.

Цікавий підхід вітчизняних дослідників стосовно класифікації нормативно-правових актів з питань розвитку глобального інформаційного суспільства за предметною сферою дії, покликаний полегшити їх використання у правозастосовній діяльності.

Так, першу групу становлять акти, спрямовані на регулювання глобального інформаційного суспільства як самостійного феномена (Окінавська хартія глобального інформаційного суспільства, Конвенція Ради Європи про інформаційне та правове співробітництво щодо «послуг інформаційного суспільства», Ініціатива «Електронна Європа – інформаційне суспільство для всіх» і т. д.).

Другу групу формують міжнародно-правові акти з питань інформаційного простору і кіберпростору, інформаційної безпеки й

кібербезпеки (Рекомендація ЮНЕСКО про розвиток і використання багатомовності та загальний доступ до кіберпростору, Хартія про збереження цифрового надбання, Концепція інформаційного простору та Угода про співпрацю у сфері інформації СНД, Комюніке Великої двадцятки за результатами саміту в Анталії, Декларація Монтре «Про захист персональних даних у глобальному світі: універсальне право, що поважає багатоманітність», Уфімська декларація країн-членів БРІКС, Довільська декларація «Групи восьми» «Незмінна відданість свободі та демократії» тощо).

Міжнародно-правові акти третьої групи сфокусовані на питаннях управління та функціонування Інтернету (Рекомендація РЄ щодо вільного, транскордонного потоку інформації в Інтернеті, Стратегія РЄ з управління Інтернетом, План дій ЄС щодо зміцнення безпечного використання Інтернету шляхом боротьби з незаконним та шкідливим контентом у глобальних мережах, «Цифровий порядок денний для Європи», Комюніке ОЕСР щодо принципів розроблення Інтернет-політики). Класифікуючою ознакою наступної категорії є заборона сексуальної експлуатації дітей та дитячої порнографії (Конвенція ООН з прав дитини та Факультативний протокол до неї від 2000 р., Лансаротська конвенція, Директива ЄС про боротьбу із сексуальним насиллям та експлуатацією дітей, а також дитячою порнографією).

Окрему групу становлять також міжнародно-правові акти щодо використання ІКТ у цілях розвитку людства (Конвенція Тампере, Санкт-Петербурзька декларація держав–членів АТЕС «Забезпечення довіри та безпеки у використанні ІКТ для сприяння економічному росту та процвітанню»). Самостійний предмет міжнародно-правового регулювання становлять також питання інтелектуальної власності (Спільна рекомендація ВОІВ щодо положень про захист знаків та інших прав промислової власності на позначення в Інтернет).

Важлива роль у розробленні та прийнятті міжнародно-правових актів щодо інформаційної сфери, на наше переконання, відводиться тематичним і спеціальним доповідям, моніторинговим звітам тощо.

На рівні наднаціонального регулювання інформаційної сфери в кінці 1990-х років XX ст. саморегулювання було визнане ефективним засобом протидії незаконному та шкідливому контенту онлайн. У цілому доцільно виокремити такі здобутки: *План дій* ЄС *щодо зміцнення безпечного використання Інтернету шляхом боротьби з незаконним та шкідливим контентом у глобальних мережах* 1999 р.; ініціатива 1999 р. *«Електронна Європа – інформаційне суспільство для всіх»*; ініціатива і 2010 «Європейське інформаційне суспільство для росту та зайнятості (2005–2010)»; *«Цифровий порядок денний для Європи»* 2010 р., яким визначено напрямки розвитку ЄС на період до 2020 р., і т. д.

У рамках ЄС урегульовано значні питання інформаційних обмінів, насамперед їх економічних аспектів. У межах же Ради Європи ці питання розглядаються крізь призму політичних аспектів, прав людини, розвитку і зміцнення демократії. Якщо держави–члени Ради Європи ухвалюють документи загального характеру, то правотворчий процес ЄС зосереджений на розробленні і прийнятті програм, ініціатив з питань кібербезпеки, інформаційного суспільства і т. д.

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 із взаємопов’язаних інфраструктурних елементів на внутрішньодержавних і наднаціональному рівнях [668, с. 51−59, 672, с. 106−114]. Сама інформаційна сфера відзначається транскордонним характером тощо.

Функціональний аспект міжнародно-правового регулювання інформаційної сфери загалом, інформаційної безпеки зокрема, зумовлений

здійсненням регулятивного впливу, спрямованого на впорядкування міжнародних інформаційних відносин, свободи інформації, а саме можливості збирати, обмінюватись, поширювати і використовувати інформацію; інтегративної чи координуючої функції, 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 і прийняття міжнародно-правових стандартів забезпечення інформаційної безпеки, створення дієвих інструментів їх реалізації.

Національне законодавство України з питань забезпечення інформаційної безпеки

Слід відзначити той факт, що питання інформаційної безпеки в масиві нормативно-правових актів України спочатку не розглядалось, згодом отримало опосередковане правове регулювання, і фактично лише останніми роками відзначається тенденція чіткого правового регулювання забезпечення інформаційної безпеки України.

З огляду на великий обсяг нормативно-правових актів у сфері інформаційної безпеки, їх певну несистемність та наявність випадків неузгодженості між ними, нормативну основу забезпечення інформаційної безпеки доцільно розглядати через критерії класифікації.

У науковій та навчальвій літературі вчені по-різному підходять до визначення критеріїв класифікації нормативно-правових актів у сфері інформаційної безпеки.

Так, одні вчені пропонували розглядати нормативну базу у сфері інформаційної безпеки з урахуванням існуючої ієрархії нормативних актів. Відповідно, на найвищому рівні розглядаються такі нормативно-правові акти:

– Конституція України, норми якої закріплюють концептуальні положення національної безпеки України в усіх сферах її існування,

– Концепція (основи державної політики) національної безпеки України;

– Доктрина інформаційної безпеки України,

– Закон України «Про основи національної безпеки України» (втратив чинність 2018 р.).

Ці документи врахували основні положення міжнародних договорів, ратифікованих Україною, які стосуються її національної безпеки [235].

На наш погляд, віднесення до найвищого рівня закону, а також доктрин і концепцій, які за своєю природою є підзаконними нормативно-правовими актами, не відповідає вже усталеному поділу нормативно-правових актів за їх юридичною силою, в якому найвищий щабель займає Конституція України.

На другому рівні автори розглядають закони конститутивного напряму, де визначаються важливі положення щодо забезпечення національної безпеки в інформаційній сфері («Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про інформацію», «Про державну таємницю», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про радіочастотний ресурс», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист суспільної моралі»).

До третього рівня автори відносять закони України інституційного рівня, де закріплені основні форми діяльності державних органів у процесі забезпечення національної безпеки в інформаційній та інших сферах життєдіяльності особи, суспільства та держави (зокрема Закони «Про оборону України», «Про Збройні сили України», «Про Службу безпеки України» тощо).

Нам видається, що віднесення законів, які є актами однакової юридичної сили, до другого і третього рівнів, є не коректним, оскільки ієрархія нормативно-правових актів передбачає підпорядкованість нижчестоящих вищестоящим, тобто чим вище рівень таких актів в ієрархії, тим вища їхня юридична сила. Отже, розгляд законів на третьому рівні невиправдано

зменшує їхню юридичну силу порівняно із законами, які автори розмістили на другий рівень.

Прикметно, що автори вищевказаної класифікації, на четвертому рівні розглядають джерела міжнародного права, а акти органів місцевого самоврядування не відносять до жодного рівня запропонованої ними системи.

У науковій літературі трапляється думка про те, що вимоги інформаційної безпеки повинні органічно включатися в усі рівні законодавства, в тому числі і в конституційне законодавство, основні загальні закони, закони щодо організації системи публічної влади, спеціальні закони, відомчі правові акти тощо. У зв'язку з цим, автори наводять таку структуру правових актів, орієнтованих на забезпечення інформаційної безпеки держави.

Перший блок – конституційне законодавство. Норми, що стосуються питань інформатизації, інформаційної безпеки тощо, входять у нього як складові елементи.

Другий блок – загальні закони, кодекси (про власність, про надра, про землю, про права громадян, про громадянство, про податки, про антимонопольну діяльність тощо), які включають норми з питань інформаційної безпеки.

Третій блок – закони про організацію управління, що стосуються окремих структур господарства, економіки, системи державних органів та про їх статус. Вони включають окремі норми щодо забезпечення інформаційної безпеки. Поряд із загальними питаннями інформаційного забезпечення та інформаційної безпеки конкретного органу, ці норми повинні встановлювати його обов'язки стосовно формування, актуалізації інформаційної безпеки, що представляє загальнодержавний інтерес.

Четвертий блок – спеціальні закони, які регламентують конкретні сфери відносин, галузі господарства, відповідні процеси. До них входить і Закон України «Про інформацію» та інші. Саме склад і зміст цього блоку законів і створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки.

П’ятий блок – підзаконні нормативні акти із забезпечення інформаційної безпеки [684,с. 36–37, 141, 668, с. 51−59].

Як відомо, переважно національне законодавство України класифікують за критерієм юридичної сили. З огляду на це, законодавство України з питань забезпечення інформаційної безпеки можна поділити на:

1. *Конституцію України та рішення Конституційного Суду України.* Так, поняття інформаційної безпеки має конституційну природу, оскільки закріплено у ч. 1 ст. 17 Основного Закону України норму, яка встановлює, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [316]. Водночас зміст функції держави щодо забезпечення інформаційної безпеки у Конституції України не розкривається.

Більш ґрунтовно Конституція України регулює інформаційну безпеку особи. Зокрема, ст. 31 Конституції України гарантує кожному таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з’ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо [316].

Конституційне право на недоторканість особистого та сімейного життя, закріплене у ст. 32 Конституції України, містить комплекс правомочностей особи щодо забезпечення особистої інформаційної безпеки. У структурі цього права можна виділити такі складові:

– заборона збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди;

– механізм законного втручання в особисте та сімейне життя особи у випадку відсутності її згоди на це, за умови наявності відповідних підстав у законі та обумовленістю інтересами національної безпеки, економічного добробуту та прав людини;

– право у судовому порядку спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації;

– право на відшкодування матеріальних і моральних збитків, завданих збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

– право громадян ознайомлюватися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, окрім відомостей, які становлять захищену законом таємницю.

Слід зазначити, що цю конституційну норму неодноразово аналізував Конституційний Суд України. Наприклад, у Рішенні Конституційного Суду № 2-рп/2012 від 20.01.2012 р. у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України, Суд дійшов висновку про те, що інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною. Збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя. Таке втручання допускається виняткове у випадках, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини [535].

У Рішенні Великої палати Конституційного Суду у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) окремих

положень абзацу першого пункту 40 розділу VI «Прикінцеві та перехідні положення» Бюджетного кодексу України від 11 жовтня 2018 року № 7-р/2018, наголошується, що втручання у конституційне право особи на приватне і сімейне життя вважатиметься законним у разі наявності підстави в національному законі, а також за умови, що такий закон відповідатиме принципу верховенства права, закріпленому в частині першій статті 8 Конституції України [534].

Засадниче значення для забезпечення інформаційної безпеки в Україні має конституційне право особи на інформацію та право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, які гарантуються ст. 34 Основного Закону.

Зокрема, ця конституційна норма встановлює, що кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [316].

2. Закони України у сфері інформаційної безпеки:

– *загальні* (Закон України «Про національну безпеку України», Закон України «Про інформацію», Закону України «Про Національну програму інформатизації», Закон України «Про доступ до публічної інформації», Закон України «Про друковані засоби масової інформації (пресу) в Україні», Закон України «Про телебачення та радіомовлення», Закон України «Про електронні довірчі послуги», Закон Украйни «Про електронну комерцію», Закон України «Про електронні документи та електронний документообіг» та інші);

– *спеціальні* Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист інформації в

інформаційно-телекомунікаційних системах», Закон України «Про захист персональних даних» тощо.

3. Підзаконні нормативно-правові акти, що стосуються різних аспектів охорони та захисту інформаційного простору України, зокрема: Доктрина інформаційної безпеки України, затверджена указом Президента України від 25.02. 2017 р. №47/2017; Указ Президента України «Про Стратегію сталого розвитку «Україна-2020» від 12.01.2015 р. № 5/2015; Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 р. № 373; Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15.05.2013 р. № 386-р; Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» від 08.10.1997 р. № 1126 (в редакції від 2011 р.); Постанова Кабінету Міністрів України «Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку» від 14.05. 2015 р. № 303; Розпорядження Кабінету Міністрів України Про схвалення Стратегії інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя від 27.12.2018 р. № 1100-р.

Нормативно-правові акти у сфері інформаційної безпеки можна класифікувати відповідно до напряму правового регулювання інформаційного простору.Згідно з цим критерієм можна виділити:

1. Нормативно-правові акти, які встановлюють основні положення щодо забезпечення інформаційної безпеки в Україні.

2. Нормативно-правові акти, які визначають концептуальні засади інформаційної безпеки.

3. Нормативно-правові акти, які регулюють доступ до інформації та її захист.

4. Нормативно-правові акти, що визначають порядок охорони державної таємниці.

5. Нормативно-правові акти у сфері захисту персональних даних.

6. Нормативно-правові акти з інформаційної безпеки телекомунікаційних систем.

7. Закони про електронний документообіг та електронний цифровий підпис.

8. Закони у сфері захисту кіберпростору.

9. Нормативно-правові акти, які визначають технічні аспекти захисту інформації в Україні.

10. Нормативно-правові акти у сфері захисту державної інформаційної інфраструктури, електронного урядування.

Здійснений нами аналіз стану правового регулювання забезпечення інформаційної безпеки на рівні національного законодавства України відзначається певною непослідовністю і подекуди несистемністю. Водночас 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 і регіонального рівнів у сфері інформаційної безпеки, імплементації існуючих міжнародно-правових стандартів у законодавство і практику його реалізації. На наш погляд, доцільна також активізація міжнародної правотворчої діяльності України у цій сфері, що посилить тим самим вплив нашої держави як суб’єкта міжнародного права, сприятиме удосконаленню правового регулювання забезпечення інформаційної безпеки.

Висновки до розділу 2

Розділ присвячений дослідженню поняття і правововової природи інформаційної безпеки, аналізу принципів забезпечення державою інформаційної безпеки, а також вивченню співвідношення інформаційної безпеки держави та інформаційної війни.

Зокрема 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 в 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 усіх пріоритетних сфер життєдіяльності, у тому числі, 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 війнам, негативному інформаційно-психологічному 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 останніми роками.

Таким чином, слід підкреслити, що 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 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.

З огляду на проаналізовані у 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 і багатогранною, оскільки включає чимало складових, починаючи від створення умов і регулювання й завершуючи реалізацією, охороною і захистом, відновленням або сприяння 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 із взаємопов'язаних інфраструктурних елементів на внутрішньодержавних і наднаціональному рівнях. Сама інформаційна сфера відзначається транскордонним характером тощо.

Визначено функціональний аспект міжнародно-правового регулювання інформаційної сфери загалом, інформаційної безпеки зокрема, який зумовлений здійсненням регулятивного впливу, спрямованого на впорядкування міжнародних інформаційних відносин, свободи інформації, а саме можливості збирати, обмінюватись, поширювати і використовувати інформацію; інтегративної чи координуючої функції, 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 і прийняття міжнародно-правових стандартів забезпечення інформаційної безпеки, створення дієвих інструментів їх реалізації.

На основі здійсненого аналізу стану правового регулювання забезпечення інформаційної безпеки на рівні національного законодавства України дійшли висновку, що воно відзначається певною непослідовністю і подекуди несистемністю. Водночас 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 їхній діяльності, виокремленні перспективних напрямів удосконалення в сучасних умовах.

Разом з тим, національне законодавство України потребує подальшого узгодження з існуючими міжнародно-правовими актами універсального і регіонального рівнів у сфері інформаційної безпеки, імплементації існуючих міжнародно-правових стандартів у законодавство і практику його реалізації. На наш погляд, доцільним є також активізація міжнародної правотворчої діяльності України у цій сфері, що посилить вплив нашої держави як суб'єкта міжнародного права, сприятиме удосконаленню правового регулювання забезпечення інформаційної безпеки.

РОЗДІЛ 3.
ЗАРУБІЖНИЙ ДОСВІД РЕАЛІЗАЦІЇ ФУНКЦІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ ДЕРЖАВ

Наразі основоположні визначальні категорії інформації, інформаційного суспільства, нформаційної політики, інформаційної безпеки, інформаційних прав людини та громадян потребують глибинного та адекватного осмислення, розкриття їх соціально-правової природи. Вивчення доктринальних і нормативних джерел дає змогу прослідкувати їх генезу, співвідношення інформаційної безпеки з деякими іншими видами безпеки, однопорядковими чи суміжними категоріями. Аналіз підходів до вивчення функцій держави у сучасних умовах демонструє їх багатогранну і різновекторну спрямованість, специфіку інформаційної функції держави та інформаційної функції органів держави, функції забезпечення інформаційної

Важливо привернути увагу до правових засад регулювання функції забезпечення інформаційної безпеки держави на національному і міжнародному рівнях. Також повноцінне її вивчення змушує виокремити поняття і складові механізму забезпечення інформаційної безпеки держави, зокрема нормативно-правовий та інституційний його виміри, загрози інформаційній безпеці Української держави та шляхи їх подолання.

Зарубіжний досвід реалізації функції забезпечення інформаційної безпеки держав, насамперед у європейській та американській моделях, демонструють найбільш успішні практики. Азійська модель забезпечення інформаційної безпеки, порівнянно з моделями інших сучасних держав, найбільш своєрідна та нестандартна.

1. Європейська модель забезпечення інформаційної безпеки сучасних держав

Моделі інформаційної безпеки європейських країн засновуються на відповідному законодавстві ***Європейського Союзу*** та національному законодавстві держав-учасниць. Головні акти ЄС у сфері захисту інформаційного простору: 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 року про захист фізичних осіб стосовно обробки 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.

Закон ЄС «Про ENISA та сертифікацію» прийнятий Європейським парламентом 12 березня 2019 року, а потім Радою Європейського Союзу 7 червня 2019 року, знаменує собою крок уперед для європейської стратегічної автономії. Він переслідує подвійну мету: прийняття постійного мандата ENISA – Європейського агентства з кібербезпеки та визначення Європейської основи сертифікації у сфері кібербезпеки, що має важливе значення для підвищення безпеки *Європейського єдиного цифрового простору*. Зазначений закон фокусується на двох ключових елементах:

1. *Агентство Європейського Союзу з кібербезпеки («ENISA»).*

Закон ЄС «Про ENISA та сертифікацію», спрямований на посилення ролі ENISA як центру консультацій та експертизи ЄС з питань кібербезпеки. До кола завдань ENISA входять:

Розроблення й реалізація політики та законодавства ЄС: ENISA відповідатиме за розроблення й реалізацію політики та законодавства ЄС у

сфері кібербезпеки. З цією метою ENISA буде, зокрема, публікувати думки та керівні принципи, розроблювала кращі практики з різних тем і допомагати державам-членам і установам, органам, офісам і агентствам ЄС в розробленні та просуванні політики кібербезпеки.

Нарощування потенціалу: ENISA допомагатиме державам–членам в запобіганні, виявленні та поліпшенні реагування на кіберзагрози й інциденти, а також в розробленні національних стратегій. ENISA також буде підтримуватиме обмін інформацією всередині й між секторами.

Оперативна співпраця на рівні ЄС: ENISA буде підтримувати співпрацю на рівні ЄС, сприяючи обміну ноу-хау і передовим досвідом, надаючи поради й рекомендації, а також організовуючи навчання з кібербезпеки на рівні ЄС. Крім того, ENISA допоможе розробити спільні заходи реагування на рівні ЄС та держав-членів у разі великих транскордонних інцидентів.

Підтримка і просування європейської системи сертифікації кібербезпеки: ENISA підтримуватиме та просуватиме європейську систему сертифікації кібербезпеки шляхом регулярного моніторингу розробок, надання рекомендацій щодо відповідних технічних специфікацій для використання при розробленні європейських схем сертифікації кібербезпеки, підготовки кандидатів на європейські схеми сертифікації кібербезпеки та оцінювання прийнятих Європейських схем сертифікації кібербезпеки. ENISA також публікуватиме керівні принципи та розроблятиме передові практики щодо вимог до кібербезпеки продуктів, послуг і процесів інформаційних технологій у співпраці з національними органами із сертифікації кібербезпеки та галуззю.

Знання та інформація, підвищення обізнаності й освіта, а також дослідження та інновації: ENISA зокрема, аналізуватиме нові технології, надаватиме тематичні оцінки очікуваного впливу технологічних інновацій на кібербезпеку, а також оцінюватиме кіберзагрози та інциденти для виявлення нових тенденцій і допомоги у запобіганні інцидентам. Ґрунтуючись на своїх

висновках, ENISA готуватиме звіти з метою надання рекомендацій для громадян, організацій і підприємств з кібербезпеки.

Міжнародне співробітництво: ENISA сприятиме міжнародному співробітництву з питань, пов'язаних з кібербезпекою, працюючи з третіми країнами та міжнародними організаціями або в рамках відповідних міжнародних структур співробітництва.

2. *Європейська система сертифікації кібербезпеки.*

Закон ЄС «Про ENISA та сертифікацію» також вводить європейські рамки сертифікації кібербезпеки як засіб створення європейських схем сертифікації кібербезпеки для продуктів, послуг і процесів інформаційно-комунікаційних технологій (ІКТ). Закон про кібербезпеку надає Комісії право приймати європейські схеми сертифікації кібербезпеки.

Європейська комісія опублікує «Профспілкову робочу програму», в якій будуть визначені стратегічні пріоритети європейських схем сертифікації кібербезпеки, щоб допомогти промисловості, національним органам і органам по стандартизації підготуватися до таких режимів сертифікації [81].

ENISA перевірятиме будь-які прийняті європейські схеми сертифікації кібербезпеки не рідше одного разу на п'ять років. Вона також підтримуватиме спеціальний веб-сайт, на якому публікуватиметься інформація про європейські схеми сертифікації кібербезпеки, європейські сертифікати кібербезпеки та заяви про відповідність стандартам ЄС.

Європейські схеми сертифікації кібербезпеки контролюватимуться національним наглядовим органом (або органами), призначеним окремими державами-членами. Наявні національні системи сертифікації будуть замінені новими загальноєвропейськими структурами.

Директива NIS спрямована на створення сильної та надійної Європи, яка ґрунтується на національних можливостях держав–членів у сфері кібербезпеки, створенні ефективних і дієвих механізмів захисту найважливіших економічних і соціальних інтересів нації, щоб колективно протистояти ризикам кібератак. Вона визначає правила безпеки в таких

критично важливих сферах: енергетиці, охороні здоров'я, транспорті, банківській діяльності та інфраструктурі, фінансовому ринку, цифровій інфраструктурі, а також вимоги безпеки у сферах онлайн-послуг (пошукових систем, хмарних технологій, торгових майданчиків тощо).

Директива NIS покладає на держави–членіи такі обов'язки:

1. Прийняття внутрішньодержавних стратегій NIS, які визначать стратегічні цілі у сфері кібербезпеки;

2. Формування національного органу, на який будуть покладені обов'язки щодо реалізації та контролю за дотриманням директиви;

3. Створення Computer Security Incident Response Teams, відповідальної за інциденти та загрози, які виникають у сферах, визначених директивою [207].

Європейська директива NIS стосується чотирьох основних питань: управління, співпраця, кібербезпека OSE (операторів загальних послуг), кібербезпека FSN (постачальників цифрових послуг).

Регламент (ЄС) 2016/679 Європейського парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб стосовно оброблення персональних даних та про вільне переміщення таких даних і скасування Директиви 95/46 / ЄС (*Загальні положення про захист даних, GDPR*) покликаний підсилити та уніфікувати захист персональних даних усіх осіб в ЄС. Регламент також направлено на експорт даних з ЄС.

GDPR спрямований насамперед на те, щоб дати громадянам контроль над власними персональними даними, і на спрощення нормативної бази для міжнародних економічних відносин шляхом уніфікації регулювання в рамках ЄС.

Ключові принципи GDPR:

– законність, справедливість і прозорість – повинні бути легальні підстави в рамках GDPR для збирання й використання даних, недопущення порушення будь-яких законів, відкритість, чесність від початку і до кінця про використання персональних даних;

– обмеження метою – оброблення має зводитися до того, що було заявлено суб'єкту даних. Усі конкретні завдання повинні бути закріплені в політиці приватності та чітко виконуватися;

– мінімізація даних – використання адекватної кількості даних для виконання поставлених цілей, обмежених тільки необхідною кількістю;

– точність – персональні дані мають бути точними й не повинні вводити в оману; виправлення неправильних даних;

– обмеження зберігання даних – не зберігати дані довше ніж потрібно, періодично проводити аудит даних і видаляти невикористовувані;

– цілісність і конфіденційність/безпека – зберігати дані в безпечному місці та приділяти достатню увагу збереженню даних;

– підзвітність – відповідальність за оброблення персональних даних та виконання всіх інших принципів GDPR, включаючи записи про конфіденційність; захист, використання, перевірки даних; призначення посадової особи щодо захисту даних (англ. DPO, data protection officer) [80].

Важливим моментом є те, що GDPR застосовується і до того, хто оброблює дані, і до того, хто збирає дані. Той, хто збирає дані, визначає мету і значення оброблення персональних даних, а процесор (обробник) відповідальний за безпосереднє оброблення даних, але обидва несуть відповідальність за дотримання норм GDPR.

Регламент GDPR замінив директиву Data Protection Directive від 1995 року. Постанову було прийнято 27 квітня 2016 року, набула чинності 25 травня 2018 року після дворічного перехідного періоду і, на відміну від директиви, вона не вимагає від урядів країн–учасниць ЄС ніяких змін у локальних законодавствах і, таким чином, є безпосередньо обов'язковою до виконання. Це стосується не тільки країн–учасниць ЄС, й будь-якої юридичної особи, яка оброблює персональні дані осіб ЄС.

За невиконання закону накладається штраф до 20 000 000 євро або до 4% від річного світового обороту компанії за попередній фінансовий рік, залежно від того, що більше.

У Регламенті також розширено поняття про персональні дані, введено поняття «транскордонна передача даних», «псевдонімізація», встановлено «право на забуття», визначено роль посадової особи щодо захисту даних (англ. DPO, data protection officer).

Розглянемо детальніше моделі інформаційної безпеки Франції та Німеччини.

Правовою основою ***забезпечення інформаційної безпеки Франції*** виступає Конституція, національне та європейське законодавство. Слід зазначити, що питання інформаційної безпеки держави та людини, у Конституції Французької Республіки не врегульовані, міститься лише бланкетна норма щодо встановлення законами правил користування громадянськими правами та публічними свободами, серед яких право на інформацію, плюралізм та свобода ЗМІ тощо.

Система інформаційної безпеки Франції є складовою національної безпеки, і основні її принципи закладені у Білих книгах оборони та національної безпеки.

Перша Біла книга з національної оборони, була опублікована у 1972 році. У ній викладено принципи оборонної політики Франції та основи стратегії ядерного стримування. Опублікована у 1994 році друга Біла книга була присвячена закінченню «холодної війни» і перенаправленню збройних сил на військові операції за межами національної території, що привело до професіоналізації збройних сил.

Процес глобалізації та боротьба з тероризмом зумовили розроблення нової концепції стратегії національної безпеки, яка об’єднує, не заважаючи їм, оборонну політику, політику внутрішньої безпеки, зовнішню політику та економічну політику. Ця концепція була закріплена у третій Білій книзі оборони та національної безпеки від 2008 року.

Такий новий підхід до формування стратегії національної безпеки Франції, що характеризується розширенням стратегічного мислення через інші причини, окрім оборонних, був зумовлений глобалізацією, яка глибоко

трансформує саму основу міжнародної системи, що стає більш нестабільною і непередбачуваною, ніж під час «холодної війни», і породжує нові загрози абсолютно різної природи. З 2009 року цю концепцію було включено до Оборонного кодексу Франції.

Особливістю Білої книги оборони та національної безпеки від 2008 року також є те, що в ній названо загрози, пов'язані з використанням інформаційних систем та засобів інформаційного впливу. Так, характеризуючи загрозу масштабних атак на інформаційні системи, зазначається, що останні пронизують основні системоутворювальні ланки економічної та суспільної життєдіяльності. Зокрема, залежність від інформаційних систем інженерних комунікацій, транспортної інфраструктури, продовольчого забезпечення і навіть управління обороною робить сучасне суспільство та його безпеку вразливими до випадкових пошкоджень та цілеспрямованих атак, які здійснюються через обчислювальні мережі. Загроза шпіонажу та стратегічного впливу обґрунтовується поширенням застосування у міждержавних відносинах засобів «м'якої сили», маніпулювання свідомістю через ЗМІ та Інтернет, посяганнями на науковий, економічний, оборонний потенціал Франції та її території, небезпекою культурної експансії [235].

Четверта Біла книга опублікована в 2013 році під головуванням Франсуа Олланда. П'ятий документ під трохи іншою назвою Стратегічного оборонного огляду та національної безпеки 2017 року (Оборонний огляд) опубліковано в кінці 2017 року під головуванням Еммануїла Макрона.

В Оборонному огляді значна увага приділяється інформаційним загрозам та заходам протидії ним. Так, зазначається, що у кіберпросторі деякі напади, зумовлені їх масштабами та серйозністю, можуть бути віднесені до категорії збройної агресії. Труднощі з розподілом акцій і поєднання прямих дій з методами впливу і пропаганди уможливлюють безліч сценаріїв інструменталізації з метою дестабілізації або підтримки простіших операцій. Облік кіберзагроз та їх еволюції тим складніший, що він не може

обмежуватися периметром оборони через заплутування питань і участі державних і приватних суб'єктів. У зв'язку з цим, наголошується, що армії повинні повністю планувати та проводити операції в цифровому просторі аж до тактичного рівня в ланцюжку планування і проведення кінетичних операцій. Операції в цифровому просторі розширюють діапазон традиційних ефектів, доступних політичній владі, і використовують зростаюче оцифрування опонентів Франції як державних, так і недержавних. Ця здатність потребує посилених і досить гнучких людських ресурсів, а також постійного розроблення конкретних технічних рішень [85].

Крім того, для забезпечення інформаційної безпеки в Оборонному огляді допускається проведення бойових дій у кіберпросторі, що означає оборонну або наступальну боротьбу по всьому цифровому середовищу проти державних або недержавних супротивників.

Стратегії національної безпеки, викладені у Білих книгах, покладаються в основу Законів про військове планування. Сьогодні чинним є Закон Франції «Про військове планування на період з 2019 до 2025 року та інші положення, що стосуються оборони» № 2018-607 від 13.07.2018 р.

Для Франції серйозною загрозою її інформаційному простору залишається так званий «кіберджихадизм», який полягає у застосуванні інтернет-технологій та послуг, особливо соціальних мереж в просуванні джихадизм – насильства. Він здійснюється шляхом злому урядових сайтів, корпоративних сайтів або організацій, пропаганди та вербування. Заходами протидії ньому виступають блокування сайтів та акаунтів, створення контрпропагандистських сайтів тощо.

Система забезпечення інформаційної безпеки Франції складається з таких спеціальних суб'єктів: Національне агентство безпеки інформаційних систем (Agence nationale de la securite des systemes d'information, ANSSI), Служба аудіовізуальних матеріалів (Service audiovisuel), Міжвідомче управління з цифрових технологій (La direction interministérielle du numérique, DINUM), Вища рада аудіовізуальних засобів (Le Conseil supérieur de

l’audiovisuel, CSA), Національна Комісія по захисту даних та свобод (Nationale Informatique et Libertés, CNIL) та деякі інші.

Національне агентство безпеки інформаційних систем (*Agence nationale de la securite des systemes d’information, ANSSI*) – французька служба з національною компетенцією, створена декретом в липні 2009 року, підпорядковується Генеральному секретаріату оборони та національної безпеки (Secretariat general de la defense et de la securite nationale, SGDSN), який відповідає за надання Прем’єр-міністру допомоги у виконанні його обов’язків у галузі оборони та національної безпеки, зокрема інформаційної. ANSSI замінило Центральне управління інформаційної безпеки, що було створене декретом у липні 2001 року. Його бюджет становить 80 мільйонів євро, а штат складається з 600 агентів.

ANSSI відповідає за просування технологій, систем і національного досвіду з метою сприяння впровадженню цифрової економіки. Водночас, основні зусилля фахівців ANSSI спрямовані на реалізацію заходів, викладених у національній стратегії безпеки та оборони. Основними цілями агентства є: підвищення ефективності управління та координації діяльності органів державної влади, суб’єктів критичної інфраструктури, суспільства в умовах інформатизації; забезпечення промислової безпеки; організація захисту національної інформаційно-телекомунікаційної інфраструктури в умовах військової загрози, в тому числі кібервійни; підтримка технічних засобів, необхідних для виконання покладених на агентство завдань, в актуальному стані. До його повноважень належать:

– формування державної політики у сфері оборони та безпеки інформаційних систем;

– розроблення організаційно-правових і технічних заходів захисту державних інформаційних систем та контроль за їх виконанням;

– моніторинг, виявлення, оповіщення і реагування на кібератаки, спрямовані на державні інформаційно-телекомунікаційні системи;

– виявлення і реагування на вірусні атаки, реалізація адаптаційних механізмів захисту від них;

– запобігання загрозам через сприяння розробленню програмного забезпечення та засобів обчислювальної техніки, яким можна довіряти;

– консультативна функція і підтримка суб'єктам критичної інфраструктури;

– систематичне інформування громадськості про загрози, зокрема через урядовий веб-портал з питань ІБ;

– розроблення і придбання основних продуктів, призначених для захисту найбільш чутливих ділянок міжвідомчої державної мережі;

– реалізація засобів контролю управління і зв'язку з питань оборони та національної безпеки;

– сертифікація комплексних систем захисту інформації [421].

Прикметно, що ANSSI є спадкоємцем цілого ряду організацій, спочатку створених з військової точки зору, які відповідали за забезпечення безпеки конфіденційної інформації держави, а саме: Технічний відділ шифрування (створений в Алжирі, 1943 р.); Центральна технічна служба шифрування (в Парижі, 1951 р.); Центральна служба безпеки телекомунікацій (1977 р.); Національна служба безпеки інформаційних систем (1986 р.); Центральне управління комп'ютерної безпеки (2001 р.).

У реалізації інформаційної політики Франції бере участь і Служба аудіовізуальних матеріалів (*Service audiovisuel*), яка діє при канцелярії Президента. Служба проектує аудіовізуальні технічні платформи Президента Республіки, організовує його виступи та забезпечує їх трансляцію по всій території країни та за кордоном.

Крім того, ця Служба веде фотографічний блок щодо діяльності Президента та життя Єлисейського палацу, керує банком фотографій та взаємодіє зі ЗМІ та громадськістю. Важливою функцією цієї Служби є аудіовізуальний моніторинг ЗМІ та формування відповідного архіву

матеріалів. В цілому її діяльність спрямована на формування іміджу Президента.

З огляду на активну інформатизацію діяльності органів державної влади, у складі Генерального секретаріату уряду (*le Secretariat general du gouvemement, SGG*), що підпорядковується Прем'єр-міністру, на початку 2011 року (Декрет № 2022-193 від 21.02.2011) було створено Міжвідомчий директорат з питань інформаційних систем та зв'язку (*Direction interministerielle des systemes d'information et de communication, DISIC*)**.** Він відповідав за функціонування інформаційно-телекомунікаційних систем, призначених для обміну інформацією між різними відомствами та з громадянами. Основними завданнями підрозділу були: проектування інформаційно-телекомунікаційної інфраструктури уряду з урахуванням потреб діяльності та оптимізації ресурсів, організація закупівлі обладнання, програмного забезпечення та інформаційних послуг, розподіл електронно-обчислювальної техніки між міністерствами, впровадження нових інформаційних систем, забезпечення стратегічного планування розвитку інформаційної інфраструктури.

Метою створення DISIC був моніторинг тенденцій у галузі інформаційних технологій, оптимальне використання інформаційних ресурсів завдяки спільним банкам даних, запобігання ризикам безпеки інформації, пов'язаних із впровадженням масштабних проектів, підвищення обслуговування користувачів інформаційних систем [421].

25 жовтня 2019 року директорат DISIC було реорганізовано у Міжвідомче управління з цифрових технологій (*La direction interministérielle du numérique, DINUM)*. Ця установа відповідає за цифрову трансформацію держави в інтересах громадян і агентів в усіх її аспектах: модернізація державної інформаційної системи, якість цифрових державних послуг, створення інноваційних послуг для громадян. DINUM є службою прем'єр-міністра, яка підпорядковується міністру дій і державних рахунків і перебуває в розпорядженні міністра економіки і фінансів і державного секретаря з питань

цифрових технологій. Головне завдання міжвідомчого управління полягає у забезпеченні цифрового перетворення міністерств, консультуванні уряду і розвитку послуг та загальних ресурсів, зокрема міжвідомчої мережі державних FranceConnect, data.gouv.fr або api.gouv.fr.

За підтримки міністерств DINUM реалізує пілотну програму TECH.GOUV по прискоренню цифрової трансформації державної служби .

Вища рада аудіовізуальних засобів (*Le Conseil supérieur de l'audiovisuel, CSA*) – французький державний орган з регулювання аудіовізуальних засобів. Це регулювання діє на благо свободи вираження думок в інтересах громадськості та професіоналів. Її діяльність засновується на таких засадах:

– повага і захист прав і свобод людини;

– економічне і технологічне регулювання ринку;

– соціальна відповідальність.

CSA є незалежним державним органом, створеним на підставі закону «Про внесення змін до закону Леотара від 30 вересня 1986 року» від 17 січня 1989 року. Це означає, що він діє від імені держави, яка делегувала йому свою компетенцію в галузі регулювання аудіовізуального сектора. Він підзвітний уряду, але не підпорядковується йому. CSA є юридичною особою, вона складається з колегії та адміністрації, що діє на всій території Франції [61].

Крім забезпечення свободи аудіовізуальних комунікацій, Вища рада з аудіовізуальних засобів розширила свою загальну місію і адаптувалася до темпів технологічних, економічних і соціальних змін. Не зводячи її до ролі аудіовізуального інспектора, закон покладає на неї функції, які охоплюють як захист свободи спілкування, повагу до людей і громадськості, технічне та економічне регулювання сектора, а також дії, пов'язані з громадськими інтересами та соціальною єдністю.

Наприклад, CSA видає дозволи на використання радіочастот для мовлення телевізійних або радіоканалів. Це гарантує, що поширювані програми відповідають нормам, які стосуються захисту неповнолітніх,

оброблення інформації, організації виборчих кампаній, представництва суспільства.

Вища рада аудіовізуальних засобів виконує такі *функції*.

Управління частотою, що передбачає розподіл частот, гарантію прийому для населення і оптимальні умови використання для операторів, планування і реорганізацію частот, міжнародну координацію.

Моніторинг програм, зокрема включає перевірку дотримання законів, правил і зобов'язань, прийнятих операторами. Для місцевого телебачення і більшої частини місцевого радіо моніторинг здійснюється за допомогою територіальних аудіовізуальних комітетів, розташованих у регіонах. Моніторинг програм проводиться щодня, щоб забезпечити дотримання зобов'язань мереж і радіостанцій, які сприяють реалізації основних цілей, що становлять загальний інтерес, серед яких: програмна етика; захист неповнолітніх; соціальна згуртованість і боротьба з дискримінацією; плюралізм вираження думок і чесність інформації; поширення європейських і франкомовних кінематографічних та аудіовізуальних творів; доступність програм; захист та ілюстрація французької мови.

Рекомендаційна функція реалізується через розроблення CSA рекомендацій, які надають засобам масової інформації загальні орієнтири, в тому числі про те, як поводитися з найбільш чутливими темами. Вона також працює над цими питаннями узгоджено із засобами масової інформації, наприклад, за допомогою хартій, які розробляються спільно, або за допомогою колективної мобілізації.

Економічне регулювання, що проводиться CSA, здійснюється як з точки зору доступу до ринків аудіовізуальних медіа-послуг, так і з точки зору відносин між гравцями на цих ринках.

Призначувальна функція полягає у призначенні президентів національних медіа компаній та членів ради директорів цих компаній.

Моніторинг концентрації засобів масової інформації передбачає аналіз економічних ризиків, пов'язаних з розподілом нових частот, за

допомогою консультацій з громадськістю та попередніх оцінок впливу. Закон передбачив чіткий режим, щоб уникнути надмірної концентрації засобів масової інформації: таким чином, одна особа не може контролювати понад сім компаній, що мають дозвіл на роботу у сфері національних телевізійних послуг. Що стосується радіо, то одна людина не може мати дозвіл на послуги, які в сукупності надаються понад 150 мільйонам людей. Крім того, обмежена сукупна діяльність в області друкованих засобів масової інформації, поширення і видання телевізійних і радіомовних послуг.

Арбітраж як функція CSA виконується шляхом надання посередництва при вирішенні труднощів, що виникають між суб'єктами аудіовізуального сектора, зокрема за допомогою погоджувальних запитів, якими займається CSA. Вона також може вирішувати спори між операторами та дистриб'юторами. *Експертна функція* охоплює діяльність по дослідженню та наданню висновків з питань, що належать до компетенції CSA, за запитами Уряду та інших державних органів.

Наглядовий орган із захисту особистих даних у Франції – це Національна Комісія по захисту даних та свобод (фр. *Nationale Informatique et Libertés, CNIL*), яка відповідає за забезпечення належного застосування GDPR у Франції. Вона також відповідає за підтримку державних і приватних організацій, що беруть участь у процесі їх дотримання [61]. Комісія CNIL створена в 1978 році згідно із законом Informatique et Libertés. CNIL є незалежним адміністративним органом, яка складається з 18 членів і апарату, що включає 199 контрактних агентів штату. Склад Комісії:

– 4 парламентарії (2 депутати, 2 сенатори);

– 2 члени Економічної, Соціальної та Екологічної Ради;

– 6 представників вищих судів (2 державних радники, 2 радники Касаційного суду, 2 радники Рахункової палати);

– 5 кваліфікованих осіб, що призначаються головою Національних зборів (1 особа), головою сенату (1 особа) в Раді міністрів (3 особи). Термін

повноважень уповноважених становить 5 років або, для парламентаріїв, термін, що дорівнює їх виборній посаді;

– Президент CADA (Комісія з доступу до адміністративних документів).

Члени CNIL збираються на пленарних засіданнях один раз на тиждень за порядком денним, розробленим за ініціативою його Президента. Важлива частина цих засідань присвячена розгляду законопроектів та указів, що надсилаються урядом, та аналізу наслідків технологічних інновацій для конфіденційності.

Важливою складовою інформаційної безпеки є регулювання цифрового простору. Зокрема у Франції усвідомлення мережі Інтернет як джерела ризиків та загроз національній безпеці держави відбувалося поступово і було зумовлено зростанням залежності від інформаційно-технологічних процесів та все ширшим використанням цифрових технологій у найважливіших сферах французького суспільства і держави.

Так, у Білій книзі з оборони та національної безпеки від 2008 року саме кібератаки та національні інфраструктури були визнані найбільш імовірними основними загрозами на найближчі п’ятнадцять років. У зв’язку з цим було встановлено обов’язок держави розвивати потенціал для запобігання та реагування на кібератаки та зробити це одним з пріоритетів своєї організації національної безпеки. Зокрема, було наголошено на необхідності раннього виявлення кібератак для організації протидії чим. Що стосується запобігання, то пропонувалося ширше використання продуктів і мереж з високим рівнем безпеки, а також створення пулу спеціалістів для обслуговування урядових департаментів та операторів, що мають життєво важливе значення.

Відповідно до пропозицій цієї Білої книги від 2008 року було створено Національне агентство безпеки інформаційних систем (ANSSI). Для розроблення національної стратегії цифрової безпеки цим органом було утворено Стратегічний комітет з кібербезпеки.

Згодом зі створенням цього органу в 2011 році у Франції було опубліковано першу національну кіберстратегію: «Оборона і безпека інформаційних систем: стратегія Франції». Ця стратегія містить чотири основні цілі: забезпечення світового лідерства в питаннях кібероборони, охорона апарату прийняття рішень у Франції за допомогою захисту суверенної інформації, підвищення рівня кібербезпеки критично важливих елементів інфраструктури, а також забезпечення безпеки в кіберпросторі [63].

У Білій книзі від 2013 року було констатовано збільшення кількості та складності атак на інформаційні системи численних французьких підприємств і підприємств державного сектора, що стало ключовим чинником для посилення державного контролю за операторами, що мають життєво важливе значення (поняття, яке визначається законом як: «оператор, відсутність якого може серйозно загрожувати економічному або військовому потенціалу, безпеці або стійкості нації»).

Керівні принципи, встановлені в Білій книзі від 2013 року, були закладені у Закон Франції про військове планування від 18.12.2013 р., яким, серед іншого, передбачався обов'язок операторів, що мають життєво важливе значення, дотримуватися стандартів безпеки, визначених ANSSI при взаємодії з операторами; мати надійні механізми виявлення кіберзагроз, керованих ANSSI, або купувати надійних постачальників послуг; повідомляти про серйозні інциденти в ANSSI [45, 46].

Крім того, ANSSI, у співпраці з промисловими колами, також виступило з додатковими пропозиціями для операторів інфраструктури з метою надати сприяння власникам, операторам і наглядовим державним структурам у сфері застосування норм безпеки. Водночас ANSSI спільно з групою партнерів запустило ініціативу по акредитації організацій – «Знак відповідності у сфері кібербезпеки» (Cyber-security label) – для компаній, що працюють в IT і секторах забезпечення онлайн-безпеки. Мета цього процесу акредитації – забезпечити високі стандарти рішень французьких виробників у цій галузі як для внутрішнього ринку, так і для експорту в треті країни [62].

У 2015 році Франція прийняла Національну стратегію цифрової безпеки. Розроблена для підтримки цифрового переходу французького суспільства, вона відповідає новим викликам, що виникають в результаті еволюції цифрового використання і пов'язаних з ним загроз. У ній визначено п'ять напрямів діяльності:

– гарантувати національний суверенітет;

– забезпечувати рішучу відповідь проти актів кіберзлочинності;

– інформувати громадськість;

– зробити цифрову безпеку конкурентною перевагою для французьких компаній;

– зміцнити голос Франції на міжнародному рівні.

У цілому стратегія кібербезпеки Франції містить п'ять ключових цілей на шляху створення «цифрової республіки», з одночасним забезпеченням безпеки та гнучкості інформаційно-комунікаційних систем. Ці п'ять стратегічних пріоритетів включають: 1) захист основоположних інтересів Франції в кіберпросторі – таких як державні інформаційні системи та критично важливі елементи інфраструктури; 2) забезпечення взаємної довіри, приватності та захисту персональних даних у мережі за допомогою розроблення продуктів для кібербезпеки, а також надання юридичної та технічної допомоги в цій галузі; 3) підвищення обізнаності в питаннях кібербезпеки та зростання потенціалу в цій галузі в національному масштабі; 4) створення сприятливої атмосфери для розвитку підприємницької діяльності, інвестицій в інформаційно-комунікаційні технології та інноваційного бізнесу; 5) розроблення «дорожньої карти» для досягнення європейської стратегічної цифрової автономії [22, 31].

Цю стратегію згодом розширено за допомогою Міжнародної стратегії Франції щодо цифрових технологій, яка була представлена міністром Європи та закордонних справ у грудні 2017 року. Цей текст узагальнює всі стратегічні орієнтації, які Франція просуває у цифровому світі навколо трьох стовпів: управління, економіка, безпека.

Інтернет-простір як сцена регулярних агресивних дій, що мають потенційно драматичні наслідки, розглядається і в Стратегічному огляді оборони та національної безпеки 2017 року (далі – Оборонний огляд).

Зокрема, констатується що нові умови конфронтації (кіберпростір, екзо-атмосферний простір) та засоби дій в інформаційному полі (Інтернет, соціальні мережі, цифрова пропаганда) дають змогу діяти дистанційно, звільняючись від кордонів «усередині» і «зовні» держав, а також від традиційних поділів між мирними, кризовими й воєнним часом.

Такі засоби стають все більш привабливими, оскільки вони нині погано регулюються законодавством, до того ж існує мало інструментів контролю. Замість того щоб переслідувати фізичні активи, вони націлені на цілі, що безпосередньо закладені в основу суспільства (наприклад, критичні інфраструктури та ресурси), а також на його нематеріальні аспекти (моральний дух і політична згуртованість). Звичайні пропагандистські інструменти, розгорнуті за допомогою офіційних ЗМІ й таємних засобів впливу, тепер поєднуються з тролями соціальних мереж і групами хакерів. Проведені з різним ступенем обережності, зусилля щодо дезінформації, посилені Інтернетом, можуть призвести до м’яких форм підривної діяльності, спрямованої на загострення напруженості в суспільстві, проти якого вона спрямована, а також на здійснення впливу і сприяння політичному паралічу [85].

В Оборонному огляді в контексті нових можливостей для злочину з потенціалом розвитку розглядаються анонімайзери (мережа TOR) та створення електронних валют (особливо Bitcoin).

Крім того, наголошується на геополітичному значенні та впливі сервісних компаній, що працюють в Інтернеті, зокрема Google, Facebook і Baidu. Їх великі бази користувачів дають їм можливість збирати й контролювати величезні обсяги даних, а також надавати основні послуги. Володіння, збирання й оброблення цих даних є важливою перевагою як з економічної, так і зі стратегічної точок зору (інформація, прогнозування

тощо). Ці платформи стали критично важливими для боротьби з тероризмом, кібербезпеки, захисту персональних даних і, в деяких випадках, виявлення кібератак, атрибуції та відповідного реагування.

Для посилення захисту інтернет-простору Франція виступає за його міжнародно-правове регулювання, однак це питання залишається дискусійним, оскільки низка держав заперечує проти цього та поки невідомі механізми забезпечення такого регулювання.

У лютому 2018 року Генеральний секретар оборони та національної безпеки Франції представив Огляд стратегії кіберзахисту. У ньому визначається доктрина цифрового кризового управління. Цей огляд роз'яснює цілі національної стратегії кіберзахисту та підтверджує актуальність французької моделі й основну відповідальність держави у цій галузі.

Реалізацію зазначених вище програмних документів у сфері цифрової безпеки Франції здійснює система органів державної влади, головними з яких є ANSSI, Міністерство оборони та Міністерство внутрішніх справ.

Як уже зазначалося, ANSSI є національним органом, який відповідає за захист інформаційних систем і мереж як у державному, так і приватному секторах [25]. Він є провідним гравцем, що забезпечує кібербезпеку для Франції, а також забезпечує діяльність Групи реагування на надзвичайні ситуації у кіберпросторі (CERT), яка також надає рекомендації та поради в щодо захисту і стійкості громадських мереж і найважливіших елементів інфраструктури, проводить аудит інформаційної безпеки секретної урядової інфраструктури, а також навчає урядових спеціалістів. CERT виступає державним центром моніторингу, оповіщення та реагування на комп'ютерні атаки та на своєму сайті регулярно публікує й оновлює інформацію з питань кібербезпеки, рекомендації та приклади з практики для державних органів, підприємств і рядових громадян.

ANSSI також є материнською організацією для Оперативного центру безпеки інформаційних систем (*Centre Opérationnel de la Sécurité des Systemes d'Information, COSS*I), який є державною організацією, що несе особисту

відповідальність за визначення і запобігання кібератак проти державних інформаційних систем.

Міністерство збройних сил має подвійну місію захисту мереж, які лежать в основі його дій та інтеграції цифрової боротьби в ядро військових операцій. З метою консолідації дій Міністерства у цій сфері на початку 2017 року було засновано командування з питань кібернетичного захисту (COMCYBER), під командуванням начальника штабу збройних сил.

Завдання Міністерства внутрішніх справ полягає в боротьбі зі всіма формами кіберзлочинності, націленими як на національні інститути та інтереси, економічних суб'єктів та державні органи, так і на окремих осіб. З цією метою воно мобілізує спеціалізовані центральні служби та територіальні мережі Національної поліції, Національної жандармерії та внутрішньої безпеки. Вони відповідають за розслідування, спрямоване на виявлення і відправлення до суду осіб, які вчинили кібератаки. Крім того, діяльність міністерства сприяє попередженню та підвищенню обізнаності громадськості.

На європейському рівні Франція захищає амбітне бачення і концепцію «цифрової стратегічної автономії ЄС», яка гарантує колективний потенціал, ініціативи та дії країн-членів. Ця концепція охоплює такі сфери:

Технологічна. Промислова політика ЄС підтримує передові науково-дослідні та дослідно-конструкторські можливості в цілях сприяння впровадженню цифрових технологій і послуг щодо безпеки, надійність яких повинна бути оцінена. Інтеграція безпеки в усі цифрові компоненти також дасть конкурентну перевагу європейським пропозиціям.

Сфера регулювання. Зовнішня політика ЄС повинна визначати правила, що враховують вимоги конкурентоспроможності й потенціал цифрових технологій, зберігаючи при цьому захист громадян, підприємств, держав-членів відповідно до спільних цінностей (право на недоторканність приватного життя та захист персональних даних, захист критичної інфраструктури).

Сфера можливостей. ЄС відіграє ключову роль у заохоченні та підтримці розвитку потенціалу в галузі кіберзахисту державних і приватних структур в державах-членах, а також самих європейських інститутів, спираючись на європейські ноу-хау. Він також може надавати підтримку щодо підготовки та навчання, що створює синергію і запобігає дублюванню потенціалу [18].

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 здійснюються такими державними органами, як ANSSI, CERT, COSSI, Міністерство оборони, COMCYBER та Міністерство внутрішніх справ. Кібербезпека розглядається Францією як національний пріоритет, який в даний час стосується кожного з її громадян [660, с. 188−191].

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 актах.

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 й кіно. Цензура не здійснюється [40].

У 2009 році Конституцію ФРН було доповнено статтею 91c, яка заклала основу для співпраці федерального уряду і урядів земель у сфері інформаційних технологій. Це положення є широким з урахуванням постійного прогресу інформаційних технологій і його зростаючого значення для державного управління. Воно включає в себе фактичні і юридичні аспекти такої співпраці. Закріплено 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 IT) від 25.07.2015 р. Закон відводить Федеральному відомству з безпеки в сфері інформаційних технологій (нім. BSI) центральну роль в захисті критично важливих інфраструктур у Німеччині. При цьому під критичними інфраструктурами розуміються об'єкти, установки або їх частини, які належать до секторів енергетики, інформаційних технологій і телекомунікацій, транспорту й 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.

27 березня 2019 року Федеральне міністерство внутрішніх справ також опублікувало проект закону про безпеку інформаційних технологій, в якому міститься цілісний підхід до безпеки цієї сфери. Крім іншого, передбачається запровадження зручного для споживача ярлика IT-безпеки для комерційних продуктів, а також посилення компетенції BSI та розширення переліку правопорушень у сфері кібербезпеки та пов'язаних з ними слідчих дій. Законопроект також збільшує кількість адресатів звітності та зобов'язань. У цілому закон, як очікується, створить певні економічні складнощі для компаній і органів державної влади [51].

Головним суб'єктом системи забезпечення інформаційної безпеки німецької держави виступає *Федеральне відомство з безпеки в сфері інформаційних технологій (BSI*). Це цивільний орган влади у структурі Федерального міністерства внутрішніх справ Німеччини, який відповідає за питання безпеки IT. BSI як національний орган з кібербезпеки розроблює інформаційну безпеку у цифровому просторі шляхом запобігання, виявлення та реакції для держави, економіки та суспільства.

Повноваження та засади діяльності BSI визначаються Законом про Федеральне відомство з інформаційної безпеки (нім. Act BSI) від 1991 р. Метою BSI є профілактичне посилення інформаційної та кібербезпеки з метою полегшення і просування безпечного використання інформаційних та комунікаційних технологій у державі, бізнесі та суспільстві. Наприклад, BSI розроблює орієнтовані на практику мінімальні стандарти та рекомендації для цільової групи для дій у сфері IT і безпеки Інтернету, щоб допомогти користувачам уникнути ризиків.

BSI також відповідає за захист федеральних IT-систем. Це означає захист від кібератак та інших технічних загроз проти IT-систем і мереж федеральної адміністрації. BSI один раз на рік звітує перед Комітетом внутрішніх справ Бундестагу Німеччини.

Завдання BSI включають у себе:

– захист федеральних мереж, виявлення і захист від атак на державні мережі;

– тестування, сертифікація та акредитація IT-продуктів і послуг;

– запобігання шкідливим програмам або вразливості в IT-продукти та послуги;

– консалтинг у сфері інформаційної безпеки для федеральної адміністрації та інших цільових груп;

– інформування та підвищення інформованості громадян про IT та безпеки Інтернету (цифровий захист споживачів);

– інформування та сенсибілізація економіки на тему IT та інтернет-безпеки;

– розроблення єдиних і обов’язкових стандартів інформаційної безпеки;

– Розробка криптосистем для федеральних IT [11].

Організаційна структура BSI характеризується логічністю побудови, чіткістю повноважень відділів, прямою відповідальністю їх керівників та відповідністю сучасним умовам та завданням, які стоять перед цим відомством.

15 квітня 2019 року було запроваджено нову організаційну структуру BSI, яка враховує нові вимоги та зростання персоналу BSI. За допомогою завдань у сфері цифрового захисту споживачів або сертифікації і стандартизації, а також розроблення безпечного оцифровування у сфері енергопереходу, охорони здоров’я або нового стандарту мобільного зв’язку 5G, BSI виконує важливу наскрізну функцію в якості головного центру компетенції для кібербезпеки. За новою організаційною структурою BSI розділений на вісім відділів, сім з яких є відділами з повноваженнями у сфері IT і один відділ для адміністративних завдань [73].

Особливістю структури є новий відділ технічних компетенцій. Підрозділи цього відділу охоплюватимуть такі теми, як штучний інтелект, безпека промислових систем управління, хмарні обчислення, безпечні інфраструктури 5G, радіаційна безпека або аналіз апаратних і програмних продуктів. Крім того, в структуру входить управлінський персонал, розділений на три секції.

Схематично структуру BSI можна зобразити так:

1. Відділ телекомунікаційних компетенцій: Керівник.

Спецвідділ ТК 1 – IT системи.

Спецвідділ ТК 2 – IT-інфраструктури.

2. Відділ КМ – Крипто-технології та IT-менеджмент: Керівник.

Спецвідділ КМ 1 – Утвердження і забезпечення систем безпеки VS і IT.

Спецвідділ КМ 2 – Специфікація, розроблення й тестування крипто, VS та IT систем безпеки.

Спецвідділ КМ 3 – Управління IT.

3. Відділ ОК – Оперативна кібербезпека: Керівник.

Спецвідділ ОК 1 – Виявлення

Спецвідділ ОК 2 – Реакція

4. Відділ СС – Стандартизація та сертифікація: Керівник.

Спецвідділ СС 1 – Стандартизація, принципи сертифікації, нагляд.

Спецвідділ СС 2 – Процедура сертифікації.

5. Відділ ОП – Кібербезпека в оцифруванні та для електронних ідентифікаторів: Керівник.

Спецвідділ ОП 1 – кібербезпека для електронних ідентифікаторів.

Спецвідділ ОП 2 – кібербезпека в оцифруванні.

6. Відділ BL – Консалтинг для федеральних, регіональних і місцевих органів влади: Керівник.

Спецвідділ К 1 – Рекомендації з інформаційної безпеки.

Спецвідділ К 2 – Управління клієнтами та право.

Спецвідділ К 3 – Інформаційна безпека консолідованих федеральних комп'ютерних центрів і мереж.

7. Відділ КЕС – Кібербезпека для економіки та суспільства: Керівник.

Спецвідділ КЕС 1 – Критичні інфраструктури.

Спецвідділ КЕС 2 – Економіка і суспільство.

8. Відділ А – Адміністративні завдання: Керівник.

Організація.

Підбір та розвиток персоналу.

Засоби особистої гігієни.

Домашнє господарство.

Внутрішній сервіс.

Закупівлі та забезпечення.

Охорона об’єктів та безпека.

BSI є центральним органом по сертифікації безпеки IT-систем в Німеччині (безпека комп’ютерів і даних, захист даних). Тестування і сертифікація можливі відповідно до стандартів Керівництва по базовому захисту IT, Зеленої книги, ITSEC і Загальних критеріїв.

BSI є національним органом у сфері криптографії, який розроблює рекомендації та технічні керівництва для криптографічних процедур і бере участь у розробленні міжнародних криптографічних стандартів.

У середині 2017 року BSI заснував центр компетенцій для об’єднання діяльності BSI у сфері штучного інтелекту і машинного навчання [12].

Щоб просувати альтернативи пропрієтарним продуктам (на які зберігаються як немайнові, так і майнові авторські права), BSI стає все більшим прихильником використання та розвитку вільного програмного забезпечення.

Відповідно до Закону про BSI, орган, який є центральним звітним органом з інформаційної безпеки, зберігає всі дані журналу, які створюються під час онлайн-спілкування між громадянами та адміністративними органами федерального уряду.

BSI контролює діяльність *Національного центру кіберзахисту (далі – Cyber-AZ*), який був запущений 1 квітня 2011 року. Cyber-AZ є міжвідомчим органом німецької влади на федеральному рівні, метою якого є запобігання електронним атакам на IT-інфраструктуру у ФРН та її економіку. Центр кіберзахисту (Cyber-AZ) є основним елементом Стратегії кібербезпеки 2011 року, прийнятої Федеральним урядом. Він має на меті оптимізувати оперативне співробітництво та координувати заходи захисту та оборони. Це робиться на основі цілісного підходу, який поєднує різні загрози в кіберпросторі: кібер-шпигунство, кібертероризм та кіберзлочинність. Мета: швидкий обмін інформацією, швидкі оцінки та отримані в результаті рекомендації щодо дій. Так само, як ситуація із загрозою змінилася з 2011 року, змінився і Cyber-AZ.

Він розвинувся від простого інформаційного центру до центральної платформи співпраці органів безпеки ІТ.

У контексті забезпечення інформаційної безпеки людини важливе місце посідає Закон ФРН «Про Інтернет» від 1997 р., який визначив відповідальність за поширення недозволених матеріалів (насилля, агресія, порнографія, злочинність, образа людської гідності), сформулював правила конфіденційності персональних даних, електронного підпису та відповідальності провайдерів за зміст інформаційних продуктів, які поширюються через їхні мережі. У рамках угоди про діяльність радіостанції «Німецька хвиля» зацікавленим країнам надаються супутникові послуги для поширення національних програм через засоби комунікації ФРН. Федеральний уряд також надає фінансову підтримку та інформаційні продукти для виготовлення, ліцензування й поширення таких програм в інших регіонах світу [543, с. 97–114].

На військовому рівні забезпечення інформаційної безпеки Німеччини здійснюється Федеральними збройними силами Німеччини (Бундесвером), зокрема відділом інформаційних та комп’ютерних мережевих операцій командування стратегічної розвідки.

Командування стратегічної розвідки також здійснює управління супутниковою розвідувальною системою SAR-Lupe, яка була запущена в грудні 2008 року. За допомогою п’яти супутників система SAR-Lupe, яка вважається однією з найдосконаліших систем у своєму роді, може передавати зображення з роздільною здатністю менше одного метра незалежно від денного світла і погоди. Таким чином, можна пояснити майже будь-яку точку на землі. Система збирає та оцінює інформацію про військово-політичну ситуацію в окремих країнах і альянсах потенційного або фактичного противника і його збройних сил.

Суттєве значення для забезпечення інформаційної безпеки має й супутникова система зв’язку Бундесверу SATCOMBw, яка розпочала свою роботу з жовтня 2009 року. Вона включає роботу двох супутників, які

покривають східну і західну півкулі планети й організують нові та безпечні канали зв’язку.

Отже, система забезпечення інформаційної безпеки Франції та Німеччини ґрунтується на усвідомленні ризиків і загроз, які зумовлюються швидким розвитком інформаційних та комунікаційних технологій. Тому політика цих країни у вказаній сфері є послідовною, засновується на компетентних оцінках та стратегіях, спрямована на професійну підготовку кадрів та розвиток технологій. Так, одним з головних суб’єктів системи забезпечення інформаційної безпеки Франції виступає Національне агентство безпеки інформаційних систем (ANSSI), а у Німеччині – Федеральне відомство з безпеки у сфері інформаційних технологій (нім. BSI) та відділ інформаційних та комп’ютерних мережевих операцій командування стратегічної розвідки Бундесверу. Основними тенденціями в роботі цих суб’єктів є збільшення бюджету, розширення штату, технологічне лідерство та міжнародне співробітництво [660, с. 188−191].

2. Американська модель забезпечення інформаційної безпеки сучасних держав

Загалом ***державна політика США у сфері інформаційної безпеки*** пройшла значний еволюційний шлях. Так, на думку О. Бусол, він складається з чотирьох етапів:

– виникнення (1939–1947 рр.);

– становлення (1947–1982 рр.);

– активний розвиток (1983–2001 рр.);

– докорінне вдосконалення (2001 р. – дотепер) [152].

З приходом у 1981 р. до влади президента США Р. Рейгана та його адміністрації управління інформаційними ресурсами, відповідно із «Законом про свободу інформації», напрям інформаційної безпеки був визначений як пріоритетний в урядовій політиці.

Ще 1992 р. у США прийнято програми *«Національна інформаційна політика» та «Глобальна інформаційна політика» (GII).* GII базувалася на п’яти ключових принципах: залучення приватних інвестицій, сприяння конкуренції, введення гнучких механізмів регулювання, які мають забезпечити пристосовування до швидких технологічних змін та ринкової конкуренції; надання відкритого доступу до існуючих мереж усім провайдерам і користувачам; забезпечення загальнодоступних інформаційних послуг, створення «електронного уряду».

Військово-політичне керівництво США з початку 90-х років приділяло значну увагу розвитку інформаційних технологій, високо оцінюючи їх потенційні можливості для досягнення військової переваги. Саме про це стверджується у директиві МО США TS 1992 р. «Інформаційна війна». Так, було зазначено на необхідності всебічного обліку інформаційних ресурсів при організації планування і функціонування систем управління в інтересах підвищення ефективності дії своїх військ в умовах протидії супротивника. Складовими концепта «інформаційна війна» стало: оперативна безпека, введення супротивника в оману, психологічні операції, електронна війна і

вогневе знищення, які проводяться в комплексі з глибокою і всебічною розвідкою як для дезорганізації системи управління противника, так і для захисту власної системи управління в ході бойових дій. При цьому інформація, що циркулює в системі управління, розглядається як високопріоритетний об'єкт впливу і захисту, зниження або підвищення достовірності. Для Пентагону, який використовує кількасот різних інформаційних систем і мереж, питання інформаційної безпеки фактично прирівнюється до питань військової безпеки [650].

Інформаційні військові дії проводяться для досягнення інформаційної переваги в інтересах національної військової стратегії і здійснюються шляхом впливу на інформацію та інформаційні системи противника при одночасному захисті власної інформації і своїх інформаційних систем [127, с. 70 –76].

За 1997–2001 роки на законодавчому рівні у сфері інформаційної безпеки США було зроблено чимало: пом'якшено експортні обмеження на криптографічні продукти, сформовано інфраструктуру з відкритими ключами, розроблено ряд стандартів про електронний цифровий підпис – FIPS 186-2 (2000 р.). Тим самим зосереджено увагу на одному з важливих додатків – аутентифікації, що проводиться за аналогічною з криптографічними засобами методикою. На базі цих актів у США сформовано загальнонаціональну інфраструктуру електронної аутентифікації.

Окрім цього, в законодавстві США прийнято директиви, спрямовані на захист інтересів АНБ, ФБР, ЦРУ, Міністерства оборони. У доповіді 2001 р. президент США Д. Буш у штаб-квартирі ЦРУ зазначив про основні загрози національній безпеці США, з-поміж яких тероризм, інформаційна війна, розповсюдження зброї масового ураження та засобів її доставки.

Збирання розвідувальних даних із комп'ютерних систем противника дає можливість отримувати щодо нього дані стратегічного й оперативного характеру та виявляти уразливі місця в його інформаційних системах. Тож у США розроблено та реалізуються програми, спрямовані на розширення можливостей розвідки з добування й оброблення інформації щодо загроз

національній інформаційній інфраструктурі з боку інших держав. Крім традиційних методів агентурної роботи, ЦРУ приділяє велику увагу аналізу відкритих джерел і добуванню інформації із закритих (конфіденційних) баз даних програмним шляхом. У США на офіційному рівні визнають, що контроль над секретними комунікаціями противника при одночасному захисті своїх власних надає їм унікальні можливості для збереження лідируючих позицій у світі.

У 2009 р. конгресмени США О. Сноу та Д. Рокфеллер підготували та ініціювали проект закону США «Акт про кібербезпеку» *(The Cybersecuri ty Actof 2009)* [94], в якому закріплено повноваження Президента США відключати доступ до мережі Інтернет на всій території США у надзвичайних випадках загроз національній безпеці. У цьому ж році американський політик О. Джілібрен ініціював законодавчий проект «Акт глобальної відповіді на кібервиклики» *(Fosteringa Global Responseto Cyber Attac ks Act)*, в якому містяться положення щодо взаємодії уряду США з урядом будь-якої іншої держави в питаннях організації протидії злочинам у кіберпросторі.

Крім того, у 2009 р. у США оприлюднено «Огляд кібербезпекової політики» *(CyberSecurityReview)*, в якому визначено, що Білий дім має сформувати нову структуру системи національної кібербезпеки. До ключових завдань керівництва США у цій сфері віднесено: забезпечення центральної ролі Білого дому у формуванні кібербезпекової політики з метою демонстрування як суспільству США, так і міжнародним партнерам серйозність намірів американського керівництва; перегляд законодавства та політики; посилення федерального законодавства та відповідальності; просування інформаційних проектів державного, регіонального та локального рівня у сфері кібербезпеки.

У «Зауваженнях щодо забезпечення безпеки національний кіберінфраструктурі» (2009 р.) [82] Б. Обама зробив висновок про те, що «...кіберзагрози є одними з найсерйозніших викликів економічній та національній безпеці, з яким зіткнулася нація». З огляду на це, Б. Обама

оголосив цифрову інфраструктуру США стратегічною національною цінністю, а захист цієї інфраструктури – національним пріоритетом. Окреслено ним також і основні напрями, спрямовані на вирішення зазначених вище проблем: розроблення ефективної стратегії забезпечення безпеки інформаційних і комунікаційних мереж; розроблення систем запобігання та реагування на кібератаки; посилення партнерства між державою та приватним сектором; збільшення інвестицій в іноваційні технології, а також наголошено на початку масштабної національної кампанії щодо посилення готовності суспільства до протидії кіберзагрозам.

У 2010 р. з метою реалізації захисту держави та уряду від кібератак та хакерів президент США затвердив «Ініціативу зі всеосяжної національної кібербезпеки» Ради національної безпеки США, яка містить дванадцять загальних положень. Ця ініціатива є складовою частиною розділу Військової доктрини США, що стосується кібернетичної оборони. Документом передбачено створення єдиної федеральної мережі, пов'язаної захищеними каналами зв'язку, який у свою чергу, має здійснюватися через контрольовані точки доступу. Крім того, ініціатива передбачає об'єднання всіх наявних у США центрів оперативного реагування на кіберзлочини з метою підвищення ефективності їх діяльності та проведення більш глибокого аналізу щодо хакерських атак. Також з метою протидії іноземним кібершпигунам документом передбачено створення підрозділів кіберконтррозвідки в державних органах США, зокрема для захисту секретних внутрішніх мереж Міністерства оборони США від терористичних атак.

Передбачено також створення системи управління ризиками для прогнозування наслідків зламу систем, викрадення або пошкодження інформації та мінімізації збитків від таких протиправних втручань. АНБ спільно з партнерами приватного сектора розробили план спільних заходів протидії загрозам у неурядових комп'ютерних мережах. Таким чином держава бере участь у захисті ключових приватних інфраструктурних мереж (телекомунікації, електромережі, мережі банківських розрахунків, інтернет-

провайдери). Запроваджено роботу програми «Ейнштейн» (англ. *EINSTEIN Program* або *Einstein*) – система виявлення втручань, яка захищає мережеві шлюзи вищих державних органів і відомств США від несанкціонованого доступу. Програмне забезпечення було розроблено ІТ-командою екстреної готовності США (US-CERT), яка є оперативним підрозділом Національного управління кібербезпеки міністерства внутрішньої безпеки США.

Законодавство США складається з федеральних законів та законів штатів, створюючи правову основу для формування єдиної державної політики в галузі захисту інформації для забезпечення інтересів національної безпеки. Йдеться, зокрема, про такі закони: «Про свободу інформації» 1967 р., «Про висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю» 1974 р., «Про право на фінансову таємницю» 1978 р., «Про доступ до інформації про діяльність ЦРУ» 1984 р., «Про комп'ютерне шахрайство та зловживання» 1986 р., «Про безпеку комп'ютерних систем» 1987 р., «Про інформаційну безпеку», «Про реформу управління інформаційними технологіями» 1996 р., «Про удосконалення інформаційної безпеки» 1997 р., «Про управління інформаційною безпекою» 2002 р. і 2014 р., «Про обмін інформацією про кіберзагрози» від 2015 р., «Про Агентство з питань кібербезпеки та безпеки інфраструктури» 2018 р. та інші.

Загалом система нормативного регулювання інформаційної безпеки США, насамперед федеральне законодавство, у цій сфері включає чотири основні напрями:

- інформаційна безпека держави;
- захист даних фінансових установ;
- безпека інформації організацій охорони здоров'я;
- діяльність правоохоронних органів по збиранню інформації.

Відповідно, основними законами у вказаних напрямах є: Федеральний закон «Про управління інформаційною безпекою» від 2014 (FISMA), Федеральний закон Грема-Ліча-Блілі від 1999 р., Федеральний закон «Про мобільність та підзвітність медичного страхування» від 1996 р., «Акт

патріота» від 2001 р., Федеральний закон «Про обмін інформацією про кіберзагрози» від 2015 р.

Федеральний закон «Про управління інформаційною безпекою» (FISMA). На сьогодні діє його друга редакція від 2014 р., але науковий інтерес становить і його перша редакція від 2002 р.

Федеральний закон «Про управління інформаційною безпекою» 2002 р. стосувався посилення інформаційної безпеки федерального уряду, в тому числі за допомогою вимоги про розроблення обов'язкових стандартів управління ризиками інформаційної безпеки. Цей Акт визнав важливість інформаційної безпеки для інтересів США в галузі економіки та національної безпеки. Закон вимагав, щоб кожне федеральне агентство розроблювало, документувало й реалізовувало загальноагентську програму забезпечення інформаційної безпеки для інформації та інформаційних систем, які підтримують операції й активи агентства, в тому числі надані або керовані іншим агентством, підрядником або іншим джерелом.

FISMA привернув увагу федерального уряду до кібербезпеки та прямо підкреслила політику, засновану на оцінюванні ризику, для забезпечення рентабельної безпеки. Згідно з цим законом посадові особи агентств, директори з інформаційних технологій та генеральні інспектори зобов'язувалися проводити щорічні перевірки програми агентств з інформаційної безпеки й повідомляти про результати в Офіс управління та бюджету (Office of Management and Budget, далі – OMB), який використовував ці дані для надання допомоги у виконанні обов'язків по нагляду та для підготовки щорічного звіту Конгресу про дотримання агентством цього закону.

Наприклад, у 2008 фінансовому році федеральні агентства витратили 6,2 мільярда доларів, щоб забезпечити державні інвестиції в інформаційні технології, які становлять приблизно 68 мільярдів доларів, або близько 9,2 відсотка від загального портфеля інформаційних технологій [84].

Мета цього закону полягала у покладенні обов’язків на федеральні відомства, Національний інститут стандартів і технологій (NIST) та OMB для посилення систем інформаційної безпеки. Зокрема, FISMA вимагав від керівника кожного агентства впроваджувати політику та процедури для економічно обґрунтованого зниження ризику безпеки інформаційних технологій до прийнятного рівня.

NIST відповідає за розроблення стандартів, вказівок та пов’язаних з ними методів забезпечення належної інформаційної безпеки для всіх операцій та активів агентства, за винятком національних систем безпеки. NIST тісно співпрацює з федеральними відомствами, щоб поліпшити їхнє розуміння та впровадження FISMA для захисту їх інформації та інформаційних систем і публікує стандарти та рекомендації, які забезпечують основу для сильних програм інформаційної безпеки в агенціях. NIST виконує свої статутні обов’язки через відділ комп’ютерної безпеки Лабораторії інформаційних технологій [71]. NIST розроблює стандарти, метрики, тести та програми валідації для просування, вимірювання та підтвердження безпеки в інформаційних системах та послугах.

Відповідно до цього закону інформаційна безпека визначається як:

– захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, поширення, модифікації або знищення;

– забезпечення цілісності інформації від неправомірної зміни або знищення, включаючи гарантії її справжності;

– забезпечення конфіденційності, що означає підтримання встановлених обмежень доступу і поширення інформації, включаючи закритість даних про приватне життя і про власність;

– доступність, яка означає швидкий і надійний доступ до інформації [96].

Федеральний закон «Про модернізацію інформаційної безпеки» від 2014 р. (далі – *FISMA* 2014) був реакцією на зростаючу кількість кібератак на федеральний уряд. Він змінив Федеральний закон «Про управління

інформаційною безпекою» від 2002 р., зокрема було запроваджено модернізовані федеральні методи забезпечення безпеки для розв'язання виникаючих проблем безпеки. Ці зміни призводять до зменшення загального обсягу звітності, підсилюють використання безперервного моніторингу в системах, підвищують концентрацію уваги на агенціях щодо дотримання вимог та на звітності, що більш орієнтована на питання, спричинені інцидентами безпеки.

FISMA 2014, поряд із Законом «Про скорочення обсягу паперової роботи» від 1995 р. і Законом «Про реформу управління інформаційними технологіями» від 1996 р. (Закон Клінгера–Коена), прямо підкреслює політику, що ґрунтується на оцінці ризику для економічно вигідної безпеки.

На підтримку і посилення цього законодавства OMB за допомогою циркуляра А-130 «Управління федеральною інформацією як стратегічним ресурсом» вимагає від виконавчих органів федерального уряду:

– складання плану безпеки;

– перевірки наявності призначених посадових осіб, що відповідають за безпеку;

– періодичного перегляду засобів контролю безпеки у своїх системах;

– авторизації системи оброблення даних до початку операцій, а потім періодично.

Зазначені управлінські обов'язки передбачають, що відповідальні посадові особи агентства розуміють ризики й інші чинники, які можуть негативно вплинути на їх місію.

Крім того, ці посадові особи повинні розуміти поточний стан своїх програм безпеки та заходів безпеки, запланованих або чинних, для захисту їх інформації та систем, щоб робити обґрунтовані судження та інвестиції, які належним чином знижують ризик до прийнятного рівня. Кінцева мета полягає в проведенні повсякденних операцій агентства і виконанні заявлених завдань агентства з адекватною безпекою або безпекою, що сумірна ризику,

включаючи величину збитку, викликаного несанкціонованим доступом, використанням, розкриттям, з боєм, модифікацією або знищенням інформації.

Публікації FISMA розробляються NIST відповідно до його статутних обов'язків та Закону FISMA 2014 року. NIST відповідає за розроблення стандартів і керівництв по інформаційній безпеці, включаючи мінімальні вимоги для федеральних систем. Однак такі стандарти та керівні принципи не повинні застосовуватися до систем національної безпеки без згоди відповідних федеральних посадових осіб, які здійснюють політичне керівництво такими системами. Публікації FISMA відповідають вимогам Циркуляра А-130 OMB.

В якості ключового елемента Проекту впровадження FISMA, NIST також розробив інтегровану структуру управління ризиками, яка ефективно об'єднує всі пов'язані з FISMA стандарти безпеки та керівництво для сприяння розробленню комплексних і збалансованих програм захисту інформації агентствами.

Законодавчий акт FISMA 2014 визначає роль Департаменту внутрішньої безпеки (DHS) в управлінні реалізацією політики захисту інформації цивільних відомств федерального виконавчого органу, наглядом за дотриманням відомствами цієї політики та наданням допомоги OMB у розробленні цієї політики. Цей закон надає повноваження Департаменту розроблювати та контролювати виконання обов'язкових директив для інших відомств, в координації та відповідно до політики та практики OMB. Він також:

– уповноважує DHS надавати оперативну та технічну допомогу іншим цивільним установам федерального виконавчого органу на прохання відомства;

– розміщує федеральний центр інцидентів інформаційної безпеки (функція, яку виконує US-CERT) в межах DHS за законом;

– авторизує розгортання технології DHS до мереж інших агентств (на вимогу цих агентств);

– доручає OMB переглядати політику щодо сповіщення осіб, які постраждали від порушень даних федеральних агентств;

– вимагає від агентств повідомляти Конгрес про великі інциденти інформаційної безпеки, а також про порушення даних, коли вони відбуваються та щорічно [87].

Закон FISMA 2014 також сприяв внесенню OMB поправок в Циркуляр А-130 для усунення неефективної та високовитратної звітності та відображення змін в законодавстві та технологічних досягненнях. Зокрема, щодо безпеки та конфіденційності оновлений Циркуляр А-130 підкреслює їх роль у життєвому циклі федеральної інформації і являє собою перехід від розгляду вимог безпеки та конфіденційності в якості заходів щодо забезпечення відповідності до найважливіших елементів комплексної, стратегічної та безперервної програми, заснованої на оцінюванні ризику, у федеральних агентствах.

Федеральний закон Грема-Ліча-Блілі від 1999 р. встановлює правило фінансової конфіденційності, правило про гарантії та обов'язок захисту інформації від її розкриття під штучним приводом (Pretexting protection), правило фінансової конфіденційності, яке регулює збирання і розкриття особистої фінансової інформації клієнтів фінансовими установами [38]. Це також відноситься до компаній, незалежно від того, чи є вони фінансовими установами, які отримують таку інформацію.

Правило про гарантії вимагає від усіх фінансових установ розроблювати, впроваджувати та підтримувати запобіжні заходи для захисту інформації клієнтів. Правило про гарантії застосовується не тільки до фінансових установ, які збирають інформацію від своїх власних клієнтів, але також і до фінансових установ, таких як агентства з кредитної звітності, оцінювачі та іпотечні брокери, які отримують інформацію про клієнтів від інших фінансових установ.

Pretexting (іноді його називають «соціальною інженерією») виникає, коли хтось намагається отримати доступ до особистої непублічної інформації

без відповідних повноважень на це. Це може спричинити запит приватної інформації під час видання себе за власника облікового запису, телефону, адреси, електронної пошти або навіть «фішингу» (тобто використання фальшивого веб-сайту чи електронної пошти для збирання даних). Зазначений закон зобов'язує організації, на які він поширюється, вживати заходів щодо запобігання розкриттю інформації під штучними приводами. Законом передбачено максимальне покарання за незаконні дії з особистою інформацією фінансового характеру – до десяти років позбавлення волі.

Федеральний закон «Про мобільність та підзвітність медичного страхування» від 1996 р. був прийнятий в основному для оновлення потоку інформації про охорону здоров'я. Визначає, як особиста інформація, що зберігається в галузях охорони здоров'я та медичного страхування, повинна бути захищена від шахрайства та крадіжки, а також усуває обмеження на страхове покриття медичного обслуговування. За розголошення особистих даних або їх несанкціоноване використання законом передбачено покарання до п'яти років позбавлення волі.

«Акт патріота» 2001 року, прийнятий відразу після подій 11 вересня, передбачає розширення повноважень федеральних служб при здійсненні збиранні особистої інформації та даних громадян [102]. Закон санкціонує прослуховування/здійснення перехоплення інформації, що проходить через провідні, телефонні або електронні засоби зв'язку для збирання доказів про комп'ютерне шахрайство або незаконне використання; криміналізує діяльність, пов'язану з кібертероризмом; передбачає створення регіональних комп'ютерних судових лабораторій для підвищення кібербезпеки.

Закон «Про обмін інформацією про кіберзагрози» від 2015 р. є федеральним законом США, розробленим для поліпшення кібербезпеки в Сполучених Штатах за допомогою більш широкого обміну інформацією про загрози кібербезпеки та для інших цілей. Закон дозволяє обмін інформацією про інтернет-трафік між урядом США і технологічними та виробничими компаніями.

Основні положення закону дозволяють компаніям ділитися особистою інформацією з урядом, особливо у випадках загроз кібербезпеці. Не вимагаючи такого обміну інформацією, цей акт створює систему, що дозволяє федеральним агентствам отримувати інформацію про погрози від приватних компаній.

Що стосується конфіденційності, то в законі містяться положення, які забороняють обмін особистими даними, які не мають відношення до кібербезпеки. Будь-яка особиста інформація, яка не видаляється під час процедури обміну, може використовуватися різними способами. Ці загальні індикатори кіберзагроз можна використовувати для судового переслідування за кіберзлочини, але вони також можуть використовуватися як докази злочинів, пов'язаних із застосуванням фізичної сили [2].

Окрему увагу слід звернути на правове регулювання доступу до офіційних документів уряду США, яке передбачено в Законі США «Про свободу інформації» (Freedom of Information Act), який було прийнято в 1966 р. Згідно із положеннями цього закону, уряд США зобов'язаний оприлюднювати правила, кінцеві рішення щодо спірних питання, політичні заяви та інші правові джерела. Така законодавча позиція є гарантією від створення «таємного (закритого) законодавства». Дія Закону США «Про свободу інформації» поширюється на всі міністерства та відомства, незалежні комісії та інші комітети, управління та відділи, які входять до складу виконавчої гілки влади. Відповідно до цього закону, будь-який з подібних закладів зобов'язаний оприлюднювати інформацію, що міститься в кожному обліковому документі. При цьому важливою особливістю закону є закріплене в ньому право приватних осіб, які намагаються отримати певний документ, не надавати пояснення, для чого він їм потрібен.

Разом з цим цей закон регулює межі права громадськості на доступ до урядової інформації, коли воно поступається місцем іншим цінностям. Зокрема, головним винятком у зазначеному законі є зустрічне право органів виконавчої влади засекретити відповідним указом чи іншим чином документи,

щоб зберегти в таємниці зміст матеріалів, які стосуються оборони держави або її зовнішньої політики, в інтересах забезпечення національної безпеки США [421].

Зазначений закон протягом своєї історії зазнав багато змін, найбільш значними з яких є Федеральні Закони: «Про конфіденційність» від 1974 р., «Про свободу електронної інформації» від 1996 р., «Про визначення розвідувальної інформації» від 2002 р., «Про відкритий уряд» від 2007 р., «Про реформу Уолл-стрит» від 2010 р. та «Про покращення FOIA» від 2016 р.

Уряди штатів поліпшують кібербезпеку шляхом підвищення інформованості громадськості про фірми зі слабкою безпекою. У 2003 р. в Каліфорнії було прийнято Закон про повідомлення про порушення безпеки, згідно з яким будь-яка компанія, яка зберігає особисту інформацію громадян Каліфорнії та має порушення безпеки, повинна розкривати подробиці події. Особиста інформація включає ім'я, номер соціального страхування, номер посвідчення водія, номер кредитної картки або фінансову інформацію. Кілька інших штатів наслідували приклад Каліфорнії й прийняли аналогічні правила повідомлення про порушення безпеки. Вказані правила передбачають покарання для фірми за збої в кібербезпеці, надаючи їм свободу вибору способів захисту своїх систем. Крім того, таке регулювання стимулює компанії добровільно інвестувати в кібербезпеку, щоб уникнути потенційної втрати репутації та економічних втрат, які можуть виникнути в разі успішної кібератаки.

Політика США у сфері захисту інформаційного простору та ведення інформаційних війн здійснюється шляхом розроблення та реалізації національних стратегій, державних військових програм та доктрин. Далі проведемо аналіз ключових з них.

Національна стратегія кібербезпеки США. Сполучені Штати Америки одні з перших усвідомили стратегічну важливість забезпечення безпеки кіберпростору. Розвиток інформаційної сфери, збільшення її ролі у житті суспільства і держави та пов'язане з цим збільшенням загроз в економіці, яка

все більше залежала від інформаційно-комунікаційних технологій, а також терористичні акти 2001 р. стали причиною прийняття Національної стратегії захисту кіберпростору 2003 р. Відповідно до цієї стратегії, відповідальність за забезпечення безпеки кіберпростору була розподілена між агентствами та федеральними міністерствами, а координаційним органом став створений роком раніше Департамент внутрішньої безпеки США (DHS). Водночас розпочали роботу понад 50 пунктів Мережі запобігання та інформування про кіберзагрози.

У 2009 р. було представлено «Огляд політики в кіберпросторі», в якому на підставі аналізу сформованої системи кібербезпеки пропонувався план щодо її удосконалення для більш адекватного забезпечення кіберзахисту США. Цей огляд базувався на документі «Всеосяжна національна ініціатива кібербезпеки» 2008 р. Ключовими змінами в системі захисту кіберпростору були створення посади координатора державної політики у сфері кібербезпеки, відповідального за міжвідомчу взаємодію, загальний розвиток стратегії й політики та зменшення ролі держави в питаннях захисту критичних інфраструктур. Віднині приватні компанії повинні були самі забезпечувати свою безпеку у кіберпросторі, а держава залишала за собою функцію загального керівництва та стандартизації.

Розвиток міжнародної співпраці з питань кіберзахисту зумовив прийняття «Міжнародної стратегії США щодо кіберпростору. Процвітання, безпека і відкритість мережевого світу» (International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World) від 2011 р. [48].

Ця стратегія за своєю сутністю була першим політико-стратегічним документом, в якому закріплювався комплексний підхід регулювання по широкому спектру питань у сфері кіберпростору, а сам кіберпростір визначався як самостійна предметна сфера регулювання, яка потребує міжнародного співробітництва. Метою цієї стратегії було створення єдиної платформи міжнародної взаємодії з питань кіберпростору на основі американських підходів до кібербезпеки. Для реалізації політики США у сфері

кіберпростору було створено посаду старшого координатора з питань кіберпростору в Державному департаменті США.

Важливим напрямом Міжнародної стратегії США щодо кіберпростору було нарощування потенціалу, яке передбачало надання допомоги країнам, що розвиваються шляхом забезпечення їх необхідними, знаннями, ресурсами та фахівцями, у тому числі для розроблення національних стратегій кібербезпеки.

Прикладом співпраці США з іншими країнами у сфері кіберзахисту може слугувати підписання у 2013 р. «Спільної заяви президентів Російської Федерації та Сполучених Штатів Америки про нову сферу співпраці в зміцненні довіри», де було прописано співпрацю і в галузі захисту критично важливих інформаційних систем, і механізми зниження рівня небезпеки в кіберпросторі.

На сьогодні виконання цих домовленостей зупинено через агресію РФ проти України.

Нова Адміністрація США у вересні 2018 року представила своє бачення на політику захисту кіберпростору у Національній стратегії кібербезпеки США (далі – Кіберстратегія США). Цей документ засновується на розпорядженні Президента США № 13800 «Про посилення кібербезпеки Федеральних мереж і критичної інфраструктури» (Executive Order, «Strengthening of Federal Networks and Critical Infrastructure») [76] та стратегії Національної безпеки США від 2017 р. (National Security Strategy of the United States of America) [69]. Структурно Кіберстратегія США складається з таких розділів: «Розділ I: Захист американського народу, Америки та американського способу життя»; «Розділ II: Забезпечення процвітання Америки»; «Розділ III: Збереження миру методом примусу»; «Розділ IV: Посилення американського впливу». У кожному розділі встановлені напрями, визначено мету та відповідні пріоритетні дії.

Названі розділи Кіберстратегії США корелюються із завданнями Адміністрації Президента США у сфері кіберзахисту, а саме:

– забезпечувати безпеку Америки шляхом захисту мереж, систем, програмних функцій і даних;

– забезпечувати процвітання Америки шляхом побудови безпечної, успішної цифрової економіки та стимулювання розвитку інновацій на національному рівні;

– забезпечувати мир і безпеку шляхом збільшення можливостей Сполучених Штатів Америки спільно з їх союзниками та партнерами по стримуванню, за необхідності – і щодо покарання осіб і держав, що використовують цифрові інструменти в зловмисних цілях;

– розширювати американський вплив за кордоном з метою більш широкого впровадження основних принципів відкритого, функціонально сумісного, надійного і безпечного Інтернету [68].

Будь-яка стратегія розроблюється на підставі оцінювання ризиків, загроз, тенденцій, потенціалу тощо, тобто аналізу ситуації. У Кіберстратегії США аналіз поточної ситуації представлений у таких напрямах:

1. Констатація збільшення впливу кіберпростору на всі сфери суспільного життя сучасного світу в цілому та на політичне, соціальне, економічне, державне життя Америці зокрема.

2. Підтримка та просування американського бачення відкритого, функціонально сумісного, надійного і безпечного Інтернету.

3. Визнання фактів використання супротивниками та конкурентами переваг вільного Інтернету для нанесення шкоди економічним, військовим та політичним інтересам США, їх партнерів та союзників.

Прикметно, що РФ, Іран та Північна Корея прямо обвинувачуються в проведенні низки хакерських атак проти американських та транснаціональних компаній та їх партнерів. Китаю інкримінується використання кіберпростору для здійснення економічного шпигунства і крадіжки об’єктів інтелектуальної власності, вартість яких вимірюється трильйонами доларів.

Крім того, зазначається про загрози від недержавних структур, у тому числі терористичних і злочинних угруповань, які використовують

кіберпростір для отримання прибутку, вербування нових учасників, популяризації своїх ідей і нападу на Сполучені Штати, їх союзників і партнерів.

Доцільно детальніше розглянути основні елементи Кіберстратегії США, цілі, а також змістовні підрозділи, що визначають пріоритетні дії.

Розділ І. Захист американського народу, Америки та американського способу життя формулює ключову мету: управляти ризиками кібербезпеки для підвищення захисту та стійкості інформації громадян США і інформаційних систем. Цей основоположний елемент охоплює три підрозділи.

Підрозділ перший – забезпечення безпеки Федеральних мереж та інформації передбачає пріоритетні дії: подальшу централізацію управління і нагляду за Федеральною громадянською безпекою; узгодження управління ризиками та діяльністю у сфері інформаційних технологій; удосконалення управління ризиками Федеральної системи логістичних ланцюжків; посилення кібербезпеки Федеральних підрядників; забезпечення провідних позицій Уряду по найкращих інноваційних практиках.

Новим напрямом державної політики у сфері кіберзахисту є розвиток системи управління ризиками в ланцюжках поставок федерального рівня, яка охоплює, в тому числі, визначення чітких повноважень щодо виключення (в окремих випадках) з процесу постачань і закупівель тих постачальників продуктів і послуг, які вважаються ризикованими. Ці дії будуть поєднуватися із зусиллями по управлінню ризиками в ланцюгах поставок, пов’язаних з інфраструктурою країни [68]. Як видається, ступінь ризику використання продукції того чи іншого постачальника повинен визначатися в кожному окремому випадку.

Як приклад забезпечення безпеки кіберпростору у цьому напрямі можна навести інформаційну кампанію проти китайського виробника апаратного забезпечення Supermicro. У недавніх повідомленнях ЗМІ, з посиланням на розслідування, проведене виданням Bloomberg Businessweek, говорилося про впровадження зі схвалення уряду Китаю апаратних закладок в

серверні плати, що використовуються багатьма американськими компаніями, в тому числі Amazon і Apple [93]. Як повідомляється, чіпи-закладки було вставлено під час виробничого процесу на заводах Supermicro оперативними агентами з підрозділу Народно-визвольної армії Китаю.

Підрозділ другий – захист критичної інфраструктури, охоплює такі пріоритетні дії: удосконалення розподілу функцій і сфер відповідальності; визначення пріоритетів дій залежно від характеру ідентифікованих національних ризиків; залучення провайдерів інформаційно-комунікаційних технологій як посередників кібербезпеки; захист американської демократії; створення сприятливих умов для інвестицій у кібербезпеку; визначення пріоритетів національних досліджень і сприяння розвитку інвестицій; поліпшення транспортної, морської та космічної кібербезпеки.

Варто звернути увагу на те, що безперешкодний доступ і свобода дій у космосі США вважає життєво важливими елементами забезпечення своєї безпеки та економічного процвітання. Космічні активи й допоміжна інфраструктура мають вирішальне значення для навігації, розвідки, спостереження, супутникового зв'язку і моніторингу погоди. У зв'язку з цим планується активізація зусиль щодо захисту теперішніх і майбутніх космічних активів і підтримка інфраструктури від кіберзагроз через взаємодію з промисловістю і міжнародними партнерами [68]. У США вже створюються космічні війська, а головними супротивниками у цій сфері визнаються Китай та РФ.

Підрозділ третій – боротьба з кіберзлочинністю і поліпшення звітності про інциденти включає такі пріоритетні дії: заходи щодо поліпшення звітності та реагування на інциденти; підвищення ефективності електронного нагляду, а також удосконалення законодавства про комп'ютерні злочини; зниження загроз від транснаціональних злочинних організацій у кіберпросторі; спрощення затримання злочинців, які перебувають за кордоном; зміцнення потенціалу правоохоронних органів країн-партнерів у боротьбі з кіберзлочинністю.

Удосконалення законодавства про комп'ютерні злочини передбачає розширення можливостей правоохоронних органів по законному збиранню необхідних доказів злочинної діяльності та проведення подальших оперативно-слідчих та судово-процесуальних дій. Збирання необхідної інформації може відбуватися і за межами США. Якщо раніше для здійснення подібної діяльності використовували так звані угоди про взаємну правову допомогу, які реалізуються, в тому числі, в рамках Будапештської конвенції з протидії кіберзлочинності, то прийнятий «CLOUD Act» S2383 дає правоохоронним органам значні повноваження щодо отримання інформації, що зберігається на тих серверах американських компаній, які знаходяться за межами США. Таким чином, укладення угод і відповідне повідомлення держав про проведення слідчих заходів на їх території більше не потрібно.

Діяльність щодо зниження загроз від транснаціональних злочинних організацій у кіберпросторі передбачається здійснювати шляхом наділення федеральних міністерств і відомств необхідними юридичними повноваженнями та ресурсами по боротьбі з міжнародною кіберзлочинністю, в тому числі щодо виявлення та ліквідації бот-мереж, чорних ринків та іншої інфраструктури, що використовується для здійснення кіберзлочинів, а також боротьбі з економічним шпигунством. Для ефективного стримування, знешкодження та запобігання кіберзагрозам правоохоронні органи будуть тісно взаємодіяти з приватними компаніями з метою протидії викликам, які породжують технологічні бар'єри, такі як технології анонімності та шифрування, з метою отримання доказів з обмеженим часом дії для цілей відповідного судового процесу. Діяльність правоохоронних органів по боротьбі з кіберзлочинністю є силовим ресурсом нації, яка, крім усього іншого, виконує функцію стримувального фактора [68].

Розділ II: Сприяння американському процвітанню визначає ключову мету: збереження впливу США в технологічній екосистемі, а також розвиток кіберпростору в якості відкритого двигуна економічного зростання, інновацій та ефективності. Цей розділ складається з трьох підрозділів.

Підрозділ перший – сприяння розвитку життєздатної та стійкої цифрової економіки, спрямований на такі пріоритетні дії як: стимулювання гнучкої та захищеної технологічної торгівлі; визначення пріоритету інновацій; інвестування в інфраструктуру наступного покоління; сприяння вільному транскордонного потоку даних; підтримки лідерства США в передових технологіях; сприяння повному життєвому циклу кібербезпеки.

Сприяння розвитку і захист американських винаходів та інновацій має вирішальне значення для забезпечення стратегічної переваги США в кіберпросторі. Уряд має намір сприяти створенню інновацій, заохочуючи установи та програми, які є рушійною силою конкурентоспроможності держави. Уряд налаштований цілеспрямовано протидіяти неправомірним злиттям і поглинанням, а також боротися з крадіжкою інтелектуальної власності. Однією з цілей є забезпечення лідерства Сполучених Штатів у сфері нових технологій і сприяння виявленню та забезпечення підтримки цих технологій з боку уряду, включаючи штучний інтелект, квантову інформатику й телекомунікаційну інфраструктуру наступного покоління.

Підтримка лідерства США в передових технологіях також передбачає просування американських інновацій у сфері кібербезпеки в усьому світі такими способами: 1) використання торгових операцій; 2) підвищення рівня обізнаності про інноваційні інструменти та послуги у сфері кібербезпеки американського походження і виробництва; 3) викриття та протидію репресивним режимам, які використовують такі інструменти та послуги з метою порушення прав людини; 4) усунення бар’єрів у створенні єдиного глобального ринку кібербезпеки [68].

Підрозділ другий – заохочення і забезпечення інноваційності США передбачає такі пріоритетні дії оновлення механізмів огляду іноземних інвестицій і діяльності в США; підтримка сильної та збалансованої системи захисту інтелектуальної власності; захист конфіденційності та цілісності американських ідей.

Підрозділ третій – створення висококласного кадрового штату співробітників кібербезпеки, що передбачає такі пріоритетні дії: створення і підтримка кадрового резерву; розширення можливості для перепідготовки та освіти для американських службовців і робітників; збільшення кадрового персоналу кібербезпеки федерального рівня; використання виконавчих органів для виявлення та заохочення талановитих кадрів.

Розділ III: Збереження миру за допомогою сили, де основна мета: виявлення, протидія, припинення, ослаблення інтенсивності, а також стримування дій у кіберпросторі, які дестабілізують і суперечать національним інтересам США, зі збереженням переваги США в кіберпросторі та за допомогою кіберпростору. Цей основний елемент охоплює два підрозділи.

Підрозділ перший – підвищення кіберстабільності за допомогою норм відповідальної поведінки держав у якості пріоритетних дій передбачає заохочення загальної прихильності до норм, що діють у кіберпросторі.

Підрозділ другий – виявлення і стримування неприйнятної поведінки в кіберпросторі, спрямований на необхідність таких пріоритетних дій: керівництво заявленими цілями, а також взаємодія з розвідувальними органами; введення відповідних заходів впливу за негативні наслідки в кіберпросторі; створення кіберстримуючих ініціатив; протидія шкідливому кібервпливу та інформаційних операцій.

Розділ IV: Посилення американського впливу. Як ключову мету він формулює: збереження довгострокової відкритості, функціональної сумісності, безпеки та надійності Інтернету, який підтримується і посилюється інтересами США. Цей розділ включає два підрозділи.

Підрозділ перший – сприяння відкритому, функціонально сумісному надійному і безпечному Інтернету в якості пріоритетних дій визначає: захист і сприяння свободі Інтернету; співробітництво з країнами-однодумцями, промисловістю, академічним і цивільним суспільством; сприяння багатосторонній моделі управління використання Інтернету; сприяння

багатосторонній функціональній спільній надійній комунікаційній інфраструктурі та підключення до Інтернету; підтримка ринків щодо інноваційності США по всьому світу.

Принцип свободи Інтернету є основою американської Кіберстратегії. США декларують свій намір просувати цей принцип в якості міжнародного стандарту. Водночас будь-які спроби інших держав обмежити цю свободу, навіть під приводом боротьби з тероризмом та забезпечення безпеки, визнаються політичними загрозами та ознаками авторитаризму.

Інтернет розглядається як сфера реалізації свободи слова, права на мирні зібрання та приватне життя. Відповідно, принцип свободи Інтернету є гарантією цих прав та складовою національної безпеки.

При цьому свобода слова в Інтернеті також розглядається в контексті вільного поширення інформації в режимі он-лайн, що сприяє розвитку міжнародної торгівлі та комерції, розробленню та впровадженню інновацій , а також зміцнює як національну, так і міжнародну безпеку. Свобода слова в он-лайн просторі також розглядається як важливий аспект зовнішньої політики США, зокрема боротьби з кіберзлочинністю і тероризмом.

У зв’язку з цим Сполучені Штати наголошують про допомогу іншим країнам у просуванні свободи слова в Інтернеті за допомогою таких майданчиків, як Коаліція за свободу в Інтернеті (Freedom Online Coalition), членом-засновником якої є США.

У цьому напрямі США планує впровадження на міжнародному рівні багатосторонньої моделі управління Інтернетом. Суть її полягає в прозорості та рівній участі держави, приватного сектора, громадянського суспільства, наукових кіл і технічного співтовариства в управлінні Інтернетом.

Підрозділ другий – створення міжнародного кіберпотенціалу, що пов’язується з пріоритетними діями, спрямованими на поліпшення кібермобілізуючих заходів.

Так, передбачається активізація зусиль з автоматизованого обміну інформацією про кіберзагрози, що має практичну цінність, сприятиме

зміцненню координації у сфері кібербезпеки та обмінів аналітичною і технічною інформацією. Крім того, Сполучені Штати мають намір знизити збитки та вплив транснаціональної кіберзлочинності та терористичної діяльності налагодженням співпраці та зміцненням можливостей органів безпеки та правоохоронних органів, їх партнерів для нарощування необхідного кіберпотенціалу [68].

Отже, Кіберстратегія США від 2018 р. орієнтована на збереження лідерства, посилення впливу і просування інтересів США на міжнародній арені. Безпека кіберпростору США виступає складовою їх національної безпеки, що підтверджується кореляцією напрямів однойменних стратегій. Забезпечення захисту он-лайн простору у Сполучених Штатах здійснюється на засадах свободи Інтернету. У цьому аспекті пріоритетним визнається розроблення та запровадження багатосторонньої моделі управління Інтернетом. Одночасно визнається необхідність запобігати використанню свободи в Інтернеті для створення політичних загроз. Розвиток та стійкість цифрової економіки розглядається як основа американського процвітання. У цьому векторі першочерговими кроками визнаються: розроблення інновацій та інвестування в інфраструктуру останнього покоління із залученням приватного сектора та громадянського суспільства; розвиток міжнародного співробітництва; створення кадрового резерву, що передбачає навчання, розвиток, удосконалення потенціалу спеціалістів у сфері кіберзахисту. Важливо, що саме висококваліфіковані кадри у сфері забезпечення кібербезпеки визнаються стратегічною перевагою для національної безпеки США, тому пошук молодих талантів та спеціалістів здійснює уряд по всьому світу в межах різноманітних державних програм.

Стратегії та програми захисту кіберпростору США розробляються і на військовому рівні. Діяльність у цій сфері бере свій початок з прийняття концепції «Революції у військовій справі» (Revolution in Military Affairs) від 1991 р., яка передбачала використанням ІКТ для забезпечення управління, контролю і розвідки, ведення інформаційних війн, а також застосування різних

видів нелетальної зброї [66]. Зазначена стратегія стала основою для модернізації збройних сил Сполучених Штатів та розроблення програми ведення інформаційних війн.

Так, 21 грудня 1991 р. було представлено директиву Міністерства оборони США TS 3600.1 «Інформаційна війна» (Information Warfare), що містила положення щодо інформаційного протиборства збройними силами.

При цьому, інформаційна війна трактувалася як інформаційна перевага над противником, для досягнення якої передбачалося втручання, пошкодження або руйнування його інформаційних систем при захисті власних систем і мереж [47].

Ведення інформаційних війн США здійснюється шляхом проведення *інформаційних операцій (далі – ІО)*. Міністерство оборони США визначає ІО як комплекс заходів впливу на інформацію та інформаційні системи противника при здійсненні захисту власної інформації та інформаційних систем [53, 54]. ІО може бути спрямована як на автоматизовані механізми вироблення рішень, так і на осіб, що приймають рішення. Методи ІО – це вплив, порушення, пошкодження або захоплення інформації при забезпеченні безпеки власних ресурсів. Забезпечувальними заходами ІО є збирання інформації за допомогою проведення культурного і психологічного аналізу населення територій, проведення операцій; розвідувальна підтримка; зв’язок із громадськістю; спільні операції тощо. Рівні проведення: національний та міжнародний. Час проведення ІО: проводиться в період кризи, конфлікту та в мирні часи.

У мирний час ІО забезпечують військово-політичні цілі держави за допомогою впливу на погляди та механізми прийняття рішень противника. У період кризи ІО можуть бути використані як гнучкий стримувальний механізм демонстрації намірів, інформування про національні інтереси з метою впливу на механізми прийняття рішень противника. Під час конфлікту ІО можуть застосовуватися для досягнення як фізичних, так і психологічних результатів з метою забезпечення військових завдань. У постконфліктний період ІО

продовжують забезпечувати національні військово-політичні цілі та впливати на бачення ситуації противника [42].

ІО поділяються на такі види:

– електронна боротьба (Electronic Warfare);

– мережеві комп'ютерні операції (Network Computer Operations);

– військові операції інформаційної підтримки (Military Information Support Operations – MISO);

– дезінформація противника (Military Deception);

– безпека операцій (Operations Security).

На міжнародному рівні ІО проводяться на підставі об'єднаних доктрин. Зокрема, у 2006 р. було прийнято «Об'єднану доктрину інформаційних операцій», в якій наголошувалося про необхідність усунення можливої невідповідності в концепціях і доктринах ведення ІО союзників і партнерів по коаліції; інтеграції союзників і партнерів по коаліції в процес планування ІО; вироблення механізмів своєчасного виявлення уразливостей багатонаціональних сил і прийняття необхідних заходів щодо їх усунення [53, 54].

У 2012 р. було оновлено «Об'єднану доктрину інформаційних операцій», згідно з якою ІО тепер націлені на інтегроване використання інформаційного потенціалу під час військових операцій з метою впливу, порушення, спотворення процесу прийняття рішень супротивником при забезпеченні безпеки власних ресурсів. Під інформаційним потенціалом розуміються інструменти, техніки або види діяльності, що задіють дані, інформацію або знання для створення ефектів і необхідних оперативних умов у трьох вимірах інформаційного середовища: фізичному (системи контролю та управління, відповідна інфраструктура, особи, які приймають рішення), інформаційному (то, де і як інформація збирається, оброблюється, зберігається, передається і захищається) і когнітивному (свідомість тих, хто передає, отримує або відповідає на інформацію або діє відповідно до неї) [53, 54].

Доктрини ІО деталізувалися у військових програмах та стратегіях. Наприклад, у 2006 р. було прийнято першу «Національну військову стратегію

ведення операцій у кіберпросторі», яка визначала сфери відповідальності Міністерства оборони в кіберпросторі, а також механізми взаємодії з іншими відповідальними міністерствами та агентствами.

Система органів забезпечення інформаційної безпеки США доволі складна та складається з великої кількості суб'єктів різного підпорядкування та рівня повноважень. У зв'язку з цим розглянемо основні елементи моделі інформаційної безпеки США.

16 листопада 2018 року президент Дональд Трамп підписав закон «Про Агентство з питань кібербезпеки та безпеки інфраструктури» *(The Cybersecurity and Infrastructure Security Agency, CISA).*

Цей акт забезпечує реорганізацію та ребрендинг ініціативи Національного захисту та управління програмами (National Protection and Programs Directorate, NPPD) всередині міністерства національної безпеки. CISA стало самостійним федеральним агентством, яке займається цивільними та федеральними програми кібербезпеки. Зазначене агентство включає Національний центр кібербезпеки та інтеграції комунікацій (NCCIC).

До створення CISA, NCCIC переробив свою організаційну структуру у 2017 році, інтегруючи подібні функції, які раніше виконувались незалежно від американської команди з питань готовності до надзвичайних ситуацій (US-CERT) та Кібергрупи реагування на надзвичайні ситуації промислових систем управління (ICS-CERT). NCCIC виступає центром інформації та експертизи. Він забезпечує глобальний обмін інформацією про кібер- та комунікаційні послуги, ділиться даними зі спільнотою кібербезпеки.

CISA є національним радником з питань ризиків, який працює з партнерами для захисту від сьогоднішніх загроз і співпрацює для створення більш безпечної та стійкої інфраструктури для майбутнього.

Це Агентство надає зацікавленим сторонам широкі знання та практики в галузі кібербезпеки та безпеки інфраструктури, ділиться цими знаннями для забезпечення кращого управління ризиками та застосовує їх на практиці для захисту основних ресурсів нації.

Основні напрями діяльності CISA:

– захист федеральної мережі;
– комплексний кіберзахист;
– стійкість інфраструктури та польові операції;
– аварійний зв’язок.

У сфері захисту критично важливої інфраструктури CISA здійснює обмін інформацією, навчання та вправи, оцінює ризик та вразливість, синтезує та аналізує дані, проводить оперативне планування та координацію, операції спостереження та реагує на випадки та відновлення.

Департамент внутрішньої безпеки (DHS): здійснює операційне керівництво Федеральною кібербезпекою і має повноваження координувати зусилля з питань кібербезпеки уряду, випускати обов’язкові оперативні директиви, в яких детально розглядаються дії, які відомства повинні вжити для поліпшення своєї кібербезпеки. DHS також забезпечує оперативну та технічну допомогу агентствам, у тому числі через функціонування Федерального центру інцидентів інформаційної безпеки. Цей Департамент забезпечує загальну безпеку агентств через Національну систему захисту кібербезпеки та програму постійної діагностики та пом’якшення наслідків та надає допомогу у реагуванні на інциденти через Національний центр інтеграції в кібербезпеку та комунікації (NCCIC). DHS також сприяє обміну інформацією у федеральному уряді та приватному секторі.

Агентство національної безпеки/Центральна служба безпеки (NSA/ CSS, NSA) очолює уряд США у сфері криптології, яка охоплює як продукти та послуги розвідки сигналів (SIGINT), так і забезпечення інформаційної безпеки, а також дозволяє здійснювати операції в комп’ютерних мережах (CNO), щоб отримати перевагу в прийнятті рішень для нації та союзників за будь-яких обставин.

NSA виступає світовим лідером у сфері радіоелектронного перехоплення. Метою агентства є забезпечення національної безпеки США за допомогою технічних засобів.

Основні завдання агентства:

– радіоперехоплення;
– електронна розвідка;
– захист урядової інформації;
– забезпечення криптографічної безпеки.

Агентство національної безпеки США має завод з виробництва інтегральних мікросхем для своїх обчислювальних систем. Виходячи з відкритої інформації, на ньому також виготовляються мікросхеми, які за своїми характеристиками, функціями та зовнішнім виглядом практично не відрізняються від компонентів, використовуваних в електронних системах потенційного супротивника. Вони призначені для таємної установки в системах оброблення даних і управління інших держав, де виконують роль електронних закладок і можуть передавати зняту інформацію по радіоканалах або, реагуючи на зовнішній сигнал, паралізувати комп'ютери стратегічних систем. NSA контролює два вузлових центри мережі Інтернет у штатах Меріленд і Каліфорнія, а також проводить сканування значної кількості вузлів підключення користувачів цієї мережі в інших регіонах США і за кордоном. На думку експертів, такі операції здійснюються з відома компаній Sprint, Ameritech Bell Communications і Pacific Bell, які володіють комерційними системами телекомунікацій [260].

У структурі NSA діє Центральна служба безпеки (*CSS*), яка забезпечує своєчасну і точну криптологічну підтримку, знання і допомогу військовій криптологічній спільноті. Вона сприяє повному партнерству між NSA і криптологічними елементами Збройних сил і групами з високопоставленими військовими та цивільними лідерами для вирішення критичних військових питань на підтримку цілей національної та тактичної розвідки. CSS координує і розроблює політику і керівництво для розвідувальних служб і місій з кібербезпеки NSA для забезпечення військової інтеграції.

У Міністерстві Оборони США створені сили швидкого реагування в засобах масової інформації. Їх завдання свого часу сформулював колишній

директор ЦРУ У. Студеманн. Він заявив, що сили реагування повинні використовувати всі можливі пропагандистські прийоми та засоби для цільового інформаційно-психологічного впливу на населення тих країн і регіонів, де збройні сили США планують або здійснюють бойові операції.

Агентство оборонних інформаційних систем (*Defense Information Systems Agency, DISA*) Міністерства оборони США виконує безліч функцій, пов'язаних з підтримкою військових інформаційних систем, і, зокрема, функції, пов'язані із забезпеченням їх надійності та безпеки. Директору DISA підпорядковується Об'єднаний центр забезпечення роботи комп'ютерних мереж (Joint Task Force for Computer Network Operations, JTF-CNO1) Міністерства оборони США, який був створений в 1998 році як єдиний центр координації дій по захисту Оборонної інформаційної інфраструктури.

Основні завдання JTF-CNO:

– виявлення вторгнень в інформаційні системи підрозділів Міністерства оборони та інших відомств;

– аналіз виявлених вторгнень у контексті поточної військової обстановки з урахуванням наявної розвідувальної інформації;

– оцінювання впливу вторгнень на функціонування інформаційних мереж і військові операції;

– підготовка плану дій по відновленню роботи комп'ютерних мереж;

– координація необхідних дій з різними підрозділами Міністерства оборони та іншими відомствами;

– самостійне здійснення конкретних заходів щодо забезпечення безпеки інформаційних систем.

До складу сил, що відповідають за інформаційну безпеку армії США, також входять:

– Перше командування інформаційними операціями американської армії (U.S. Army's 1st Information Operations Command (LAND) (1ST IOC [L]),

раніше відоме як Підрозділ по наземним військовим інформаційним операціям (Land Information Warfare Activity, LIWA);

– Морське командування оборонними операціями в кіберпросторі (Navy Cyber Defense Operations Command);

– Армійський центр реагування на загрози інформаційної безпеки (*ACERT*) [16].

Розвідувальна спільнота: Найважливішим компонентом кібербезпеки є отримання та аналіз інформації про загрози та шкідливих суб'єктів, діяльність яких спрямована або на конкретні суб'єкти господарювання, або на більш широкі федеральні підприємства. Під керівництвом Управління директора національної розвідки Спільнота розвідки надає необхідну інформацію Федеральному уряду та охоплює роботу 17 органів, включаючи Агентство національної безпеки та Центральне розвідувальне управління.

Офіс із питань управління та бюджету (OMB): OMB уповноважений здійснювати нагляд за практикою безпеки та конфіденційністю інформації федеральних відомств, а також за розроблення та впровадження відповідних політик та рекомендацій. Федеральний головний офіцер з питань інформаційної безпеки очолює відділ з питань кібер- і національної безпеки OMB, який виконує функції спеціальної команди в Управлінні електронного уряду (Управління Федерального головного директора з питань інформації (OFCIO)), що працює під керівництвом Федерального агентства з метою визначення пріоритетів інформаційної безпеки. Підрозділ з питань кібер- і національної безпеки OMB співпрацює з партнерами в уряді для розроблення політики в галузі кібербезпеки, проведення на основі фактичних даних аналізу виконання програм кібербезпеки агентства та координації відповіді на кібер-інциденти. Управління інформації та регуляторних справ несе відповідальність за надання допомоги федеральним агентствам з питань конфіденційності, розроблення федеральної політики конфіденційності та нагляду за виконанням федеральними агентствами політики конфіденційності.

Комітет національної системи безпеки проводить обговорення питань політики, встановлює національну політику, напрями, операційні процедури та керівні вказівки для інформаційних систем, що експлуатуються урядом США, його підрядниками або агентами, які містять секретну інформацію, включають розвідувальну діяльність, криптографічну діяльність, пов'язану з національною безпекою, передбачають командування і контроль над збройними силами, використання обладнання, яке є невід'ємною частиною зброї або систем озброєнь або має вирішальне значення для безпосереднього виконання військових або розвідувальних завдань.

Комітет складається з членів з правом голосу з 21 департаменту та агентства виконавчої влади уряду США. Крім того, існує 14 офіційних спостерігачів від комітетів, що представляють додаткові організації за межами виконавчої влади. Комітет здійснює роботу щодо захисту систем національної безпеки шляхом розроблення операційних політик, процедур, керівних принципів, директив, інструкцій і стандартів. Очолює комітет директор з інформаційних технологій (CIO) Міністерства оборони [16].

Федеральні агентства: Закон FISMA вимагає, щоб керівники федеральних агентств відповідали за безпеку федеральних інформації та інформаційних систем у своїх відповідних відомствах. Кожен керівник агентства може делегувати це повноваження своєму головному керівникові інформації (CIO) та/або Старшому службовцю по інформаційній безпеці Агентства – роль, яку зазвичай виконує головний керівник інформаційної безпеки (CISO). Агентства несуть відповідальність за призначення необхідних людей, процеси та технології для захисту федеральних даних.

Рада національної безпеки (NSC): NSC – це виконавчий офіс Президента, відповідальний за координацію політичних ініціатив зі старшими радниками Президента, посадовими особами кабінету та радниками військової та розвідувальної спільноти. Управління кібербезпеки NSC виконує цю роль у питаннях кібербезпеки, консультуючи Президента щодо національної безпеки та зовнішньої політики. NSC та OMB координують і співпрацюють з

федеральними відомствами для реалізації пріоритетів кібербезпеки Адміністрації.

Адміністрація загальних служб (GSA) надає управлінську та адміністративну підтримку всьому федеральному уряду. Сюди входять нещодавно створені Центри передового досвіду, які надають експертні поради, консультації, розробку та підтримку впровадження рішень у сферах: хмарного прийняття; оптимізації IT-інфраструктури; клієнтського досвіду; аналітики надання послуг; контактних центрів. GSA також приймає Федеральну програму управління ризиками та авторизацією (FedRAMP), яка сприяє використанню безпечних хмарних сервісів уряду.

Федеральне бюро розслідувань (ФБР) – це складова частина Міністерства юстиції, відповідальна за провідні федеральні розслідування вторгнень у кібербезпеку та напади, здійснені проти державних та приватних інтересів злочинцями, закордонними противниками та терористами. Можливості та ресурси ФБР для вирішення проблем, пов'язаних з кібербезпекою, включають Кібервідділ, Команди дій з кіберзахисту, що розгортаються у глобальному масштабі, та партнерства з федеральними, державними та місцевими правоохоронними органами та організаціями кібербезпеки.

Отже, усвідомлення Сполученими Штатами масштабності впливу цифрових технологій на всі процеси в 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 в 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 проведенням інформаційних операцій. Такі

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

3. Азійська модель забезпечення інформаційної безпеки сучасних держав

Розглянемо азійську модель забезпечення інформаційної безпеки сучасних конституційних держав 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 кіберпростору та інформаційної безпеки.

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.

У Конституції КНР від 04.12.1982 р. (у редакції 2018 р.) немає поняття «інформаційна безпека» та «інформація», але декларується свобода слова та право на таємницю листування. Зокрема, відповідно до ст. 40 Конституції КНР від 04.12.1982 р. свобода і таємниця листування громадян КНР захищається законом. Жодна організація або приватна особа не може, на яких би то не було підставах вчиняти замах на таємницю листування громадян, за винятком випадків, коли в інтересах державної безпеки чи кримінального розслідування органам громадської безпеки або прокуратури дозволяється переглядати кореспонденцію при дотриманні передбачених законом процедур [309].

Головним актом у сфері інформаційної безпеки КНР є Закон про кібербезпеку Китайської Народної Республіки, який був прийнятий Постійним комітетом Всекитайських зборів народних представників 07.11.2016 р. і набрав чинності 01.06.2017 р. (Закон про кібербезпеку КНР).

Цей закон знаходиться на вершині пірамідального законодавства про кібербезпеку. Він є еволюцію існуючих раніше правил і норм з кібербезпеки з різних рівнів і сфер, асимілюючи їх для створення структурованого закону на макрорівні. Закон також пропонує основні норми з певних питань, які не є

невідкладними, але мають довгострокове значення. Ці норми будуть слугувати юридичною основою при виникненні нових питань [64].

Закон про кібербезпеку КНР закріплює:

– вимоги безпеки інтернет-провайдерів, продуктів і послуг.

– правила захисту персональної інформації;

– принцип суверенітету кіберпростору;

– правила транснаціональної передачі даних в критично важливій інформаційній інфраструктурі;

– систему безпеки для ключової інформаційної інфраструктури.

Сфера дії цього закону поширюється на операторів мереж і підприємства в «критичних секторах». У Китаї до підприємств, що працюють у критичних секторах, відносять вітчизняні мережеві підприємства, які займаються телекомунікаціями, транспортом, енергією, водними ресурсами, надають інформаційні, фінансові, громадські послуги та забезпечують електронні урядові сервіси. Тобто це підприємства критично важливої інформаційної інфраструктури, яка в разі її руйнування, втрати функції або витоку даних може серйозно поставити під загрозу національну безпеку, національний добробут, засоби до існування людей або громадські інтереси. У зв'язку з цим до операторів такої інфраструктури висуваються суворіші вимоги щодо безпеки, закупівлі мережевих продуктів і послуг, зберігання даних і передачі даних. При цьому якщо їм необхідно передати дані за кордон, вони повинні спочатку пройти оцінку безпеки урядом Китаю.

Закон про кібербезпеку КНР визначає «мережевих операторів» як власників мереж, менеджерів і постачальників мережевих послуг. Будь-які підприємства або установи, які надають послуги та здійснюють ділову діяльність через мережі, також можуть бути визнані операторами мереж. Це означає, що закон може бути застосовано до всіх підприємств в Китаї, які керують своєю власною електронною поштою або іншими мережами передачі даних.

Законом передбачається, що мережеві оператори, серед іншого, повинні: уточнити обов'язки у сфері кібербезпеки у своїй організації,

прийняти технічні заходи для забезпечення безпеки роботи мережі і запобігання витоків і крадіжки даних; і повідомляти про будь-які інциденти кібербезпеки як користувачам мережі, так і відповідному відділу по реалізації політики безпеки для цього сектора [101].

Згідно зі ст. 9 Закону про кібербезпеку КНР, оператори мереж повинні дотримуватися соціальних норм і комерційної етики, бути чесними, заслуговувати на довіру і виконувати зобов'язання щодо захисту мережевої безпеки, приймати нагляд з боку уряду і громадськості та нести соціальну відповідальність [21]. Водночас статею 41 цього закону встановлюється обов'язок мережевих операторів збирати і зберігати особисту інформацію відповідно до закону, адміністративних регламентів та їх угоди з користувачами.

Таким чином, усі підприємства, які збирають і генерують персональні дані китайських громадян, згідно із законом, зобов'язані зберігати ці дані в межах Китайської Народної Республіки. Такі законодавчі вимоги ускладнили роботу в КНР іноземних компаній. На практиці склалося декілька варіантів виконання вимог закону про кібербезпеку КНР в частині зберігання даних.

Одні міжнародні компанії вирішили найняти місцевих постачальників серверів даних для зберігання своїх даних про громадян Китаю відповідно до правил. Послуги центрів оброблення даних у Китаї швидко зростають. Huawei, Tencent і Alibaba розширюють й інвестують у центри оброблення даних як локально, так і за кордоном, кидаючи виклик таким компаніям, як Microsoft, Google та Amazon, які не мають такої домашньої переваги. Інші міжнародні компанії побудували свої власні дата-центри в Китаї або орендують центри для даних, в яких розміщують свої сервери та обладнання (колокейшн).

Наприклад, компанія Apple передала свої китайські операції з iCloud південно-китайської компанії «Guizhou-Cloud Big Data». Незабаром після цього вони оголосили, що інвестують у будівництво двох нових центрів оброблення даних у Китаї, яке повинно початися в 2020 році, щоб зберігати свої китайські дані iCloud відповідно до Закону про кібербезпеку КНР.

Крім того, зазначений закон передбачає вибіркові перевірки, сертифікацію та обов'язок співпраці з китайськими органами безпеки. Тобто на запит правоохоронних органів компанії зобов'язані надати вхідний код, шифрування або іншу важливу інформацію, що збільшує ризик втрати цієї інформації, передачі місцевим конкуренти, або вона може бути використана самою владою КНР.

Закон про кібербезпеку КНР також містить положення про юридичну відповідальність за його невиконання. Зокрема, за порушення правил локалізації даних на території Китаю на компанію може бути накладений штраф, призупинена діяльність або відкликана ліцензія чи дозвіл на ведення бізнесу.

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 запущений у 2003 році. Його 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. д.

Проект «Золотий щит» передбачає обмеження доступу до низки іноземних сайтів, веб-сторінки фільтруються по кодовим словам, пов'язаним з національною безпекою та чорним списком сайтів. Сайти, які розміщені в 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, що дозволяє віднести російську модель забезпечення інформаційної безпеки до азійської моделі. Для підтвердження такої тези слід вказати на такі події.

На форумі з кібербезпеки, у квітні 2016 р., високопоставлені китайські чиновники та їхні російські колеги зібралися в Москві. Серед делегатів були Лу Вей – глава державної канцелярії Китаю у справах інтернет-інформації, Фан Бінсін – так званий батько Великого китайського фаєрволу та Ігор Щеголєв, помічник президента Володимира Путіна з питань Інтернету та колишній міністр зв'язку. Основний договір про форум Ігор Щеголєв і Фан Бінсін уклали на зустрічі в грудні 2015 року в Пекіні. У 2016 р. секретар Ради безпеки РФ двічі зустрічався з членами політбюро Китаю з інформаційної безпеки, а в червні В. Путін відправився в Пекін, щоб підписати спільне комюніке про кіберпростір [336].

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

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

Так, відповідно до ст. 24 Конституції РФ, збирання, зберігання, використання та поширення інформації про приватне життя особи без її згоди не допускаються. Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані забезпечити кожному можливість ознайомитися з документами і матеріалами, що безпосередньо зачіпають його права і свободи, якщо інше не передбачено законом [310].

Стаття 29 Конституції РФ гарантує свободу вираження поглядів, право на вільний доступ до інформації, свободу масової інформації та забороняє цензуру.

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

У контексті реалізації права на інформацію вказаний 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.

Так, Законом про інформацію забороняється розповсюдження повідомлень і матеріалів іноземного ЗМІ, що виконує функції іноземного агента і визначеного відповідно до Закону РФ від 27.12.1991 року № 2124-1 «Про засоби масової інформації», і (або) заснованого ним російської юридичної особи без вказівки на те, що ці повідомлення і матеріали створені і

(або) поширені такими особами. Форма, вимоги до розміщення і порядок розміщення такої вказівки встановлюються уповноваженим центральним органом виконавчої влади [422].

Для організаторів поширення інформації в мережі «Інтернет» встановлено низку додаткових обов'язків щодо зберігання інформації на території РФ, за невиконання яких передбачено адміністративну 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» і 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 [422]. Зазначені норми були внесені у Закон про інформацію 06.07.2016 р. «пакетом Ярової» та анонсувалися як заходи протидії тероризму та забезпечення громадської безпеки, але на практиці викликали дискусію щодо обмеження права на свободу вираження поглядів, права на інформацію й 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.

Так, навесні 2018 року, після відмови соціальної мережі «Телеграм» надати ключі шифрування органам державної безпеки, Роскомнагляд вирішив заблокувати інтернет-адреси, через які обслуговувалася соціальна мережа. Проблема полягала в тому, що виконати вимоги влади було технічно неможливо, а інтернет-адреси часто збігалися з тими, які обслуговували і інші інтернет-сервіси. В результаті дій Роскомнагляду було заблоковано близько 20 мільйонів інтернет-адрес, включаючи ті, що обслуговували такі популярні сервіси, як Amazon, Google та ін. [654, с. 73-83].

У контексті зростання залежності організаторів поширення інформації від органів державної влади РФ, серед іншого і в політичному аспекті, варто зазначити про ситуацію щодо співпраці російської мережі «ВКонтакте» з російським спецслужбами.

Зокрема, внаслідок запиту польського користувача російської мережі «ВКонтакте» про власні персональні дані, на який соціальна мережа була змушена відповісти, враховуючи, що в іншому випадку була б піддана великому штрафу через прийнятий Регламент про захист даних, з’ясувалися колосальні обсяги інформації, якою вона володіє. Крім того, хід багатьох недавніх судових справ свідчить про те, що «ВКонтакте», а також ряд інших великих компаній передають інформацію в правоохоронні органи, нехтуючи судовою процедурою [50].

Закон про інформацію в частині регулювання використання інформаційних систем визначає основні поняття у цій сфері, закріплює види інформаційних систем (федеральна, регіональна, муніципальна та інша), встановлює порядок застосування інформаційних технологій з метою ідентифікації громадян РФ, запроваджує національну систему доменних імен та низку реєстрів інформації, регламентує обмеження доступу до різних видів інформації.

У контексті посилення державного контролю за використанням ІТ слід згадати новий Федеральний Закон «Про внесення змін до статті 4 Закону РФ «Про захист прав споживачів» від 02.12.2019 р. № 425-ФЗ. Згідно з цим законом, при продажу окремих видів технічно складних товарів з попередньо встановленими програмами для електронних обчислювальних машин споживачеві забезпечується можливість використовувати окремі види технічно складних товарів з попередньо встановленими російськими програмами для електронних обчислювальних машин. Перелік окремих видів зазначених технічно складних товарів, порядок складання і ведення переліку російських програм для електронних обчислювальних машин, які повинні бути введені, і порядок їх попередньої установки визначає Уряд РФ [417].

Прикметно, що Асоціація торгових компаній і товаровиробників електропобутової та комп'ютерної техніки (РАТЕК), в яку входять у тому числі Apple, Dell, IBM, HP, Google, Samsung, Intel, «М-Відео», надсилала листа В. Путіну з проханням відхилити цей закон. У ньому йшлося про те, що вступ закону в силу негативно відіб'ється на розвитку галузі, а також призведе до монополізації у сфері розроблення російського програмного забезпечення [140].

В аспекті захисту інформації зазначений закон встановлює, що державне регулювання відносин у сфері захисту інформації здійснюється шляхом встановлення вимог про захист інформації, а також відповідальності за порушення законодавства РФ про інформацію, інформаційні технології і захист інформації. Володілець інформації, оператор інформаційної системи у випадках, встановлених законодавством РФ, зобов'язані забезпечити:

1) запобігання несанкціонованому доступу до інформації та (або) передачі її особам, які не мають права на доступ до інформації;

2) своєчасне виявлення фактів несанкціонованого доступу до інформації;

3) запобігання можливості несприятливим наслідкам порушення порядку доступу до інформації;

4) недопущення впливу на технічні засоби оброблення інформації, в результаті чого порушується їхнє функціонування;

5) можливість негайного відновлення інформації, модифікованої чи знищеної через несанкціонований доступ до неї;

6) постійний контроль за забезпеченням рівня захищеності інформації;

7) знаходження на території РФ баз даних інформації, з використанням яких здійснюються збирання, запис, систематизація, накопичення, зберігання, уточнення (оновлення, зміна), витяг персональних даних громадян РФ [422].

Крім розглянутих вище змін до Закону про інформацію, які були внесені «законом Ярової», цей закон зазнав ще таких важливих поправок:

– Федеральний закон № 139-ФЗ від 28.07.2012 року – доповнення «про захист дітей», яким запроваджено «Єдиний реєстр заборонених сайтів»;

– Федеральний закон № 187-ФЗ від 02.07.2013 року – закон, що передбачає можливість блокування сайтів, які містять неліцензійний контент, на вимогу правовласника;

– Федеральний закон № 398-ФЗ від 28.12.2013 року – положення, пов’язані з блокуванням екстремістських сайтів;

– Федеральний закон № 97-ФЗ від 05.05.2014 року – «закон про блогерів», який зобов’язує власників популярних сайтів і блогів реєструватися в Роскомнагляді;

– Федеральний закон № 90-ФЗ від 01.05.2019 року – закон про «суверенний Інтернет», метою якого є збільшення стійкості Рунета.

Слід зазначити, що у законодавстві РФ та наукових дослідженнях інформаційна безпека розглядається як складова національної безпеки держави. Зокрема, у *Концепції національної безпеки РФ* (на сьогодні цей документ уже втратив чинність), яка була прийнята, серед іншого, і внаслідок посилення засобів інформаційного ураження, до сфер, національні інтереси в яких становлять предмет національної безпеки, належать: економічна, соціальна, внутрішньополітична, інформаційна, міжнародна, військова, оборонна та екологічна.

Національні інтереси Росії в інформаційній сфері полягають у дотриманні конституційних прав і свобод громадян щодо отримання інформації і користування нею, в розвитку сучасних телекомунікаційних технологій, у захисті державних інформаційних ресурсів від несанкціонованого доступу. У Концепції національної безпеки РФ зазначалося також про посилення загроз національній безпеці РФ в інформаційній сфері. Зазначалося, що серйозну небезпеку являють собою прагнення ряду країн до домінування у світовому інформаційному просторі, витіснення Росії із зовнішнього і внутрішнього інформаційного ринку; розробка низкою держав концепції інформаційних війн, що передбачає створення засобів небезпечного впливу на інформаційні сфери інших країн світу; порушення нормального функціонування інформаційних та телекомунікаційних систем, а також збереження інформаційних ресурсів, отримання несанкціонованого доступу до них [424].

З огляду на визначені національні інтереси та загрози в інформаційному просторі РФ, у Концепції національної безпеки РФ були сформульовані такі головні завдання у сфері забезпечення інформаційної безпеки: захист та удосконалення інформаційної інфраструктури держави; створення умов для реалізації конституційних прав і свобод громадян у сфері інформаційної діяльності; інтеграції російської держави у світовий інформаційний простір; протидія розв'язуванню інформаційних війн.

Зміцнення інформаційної безпеки названо в Концепції національної безпеки РФ серед найважливіших довгострокових завдань. Роль інформаційної безпеки та її місце в системі національної безпеки країни визначаються також тим, що державна інформаційна політика тісно взаємодіє з державною політикою забезпечення національної безпеки країни через систему інформаційної безпеки, де остання виступає важливою сполучною ланкою всіх основних компонентів державної політики в єдине ціле [380].

Проаналізована Концепція національної безпеки РФ була замінена *Стратегією національної безпеки РФ від 2009 р.,* на сьогодні діє її друга редакція від 2015 р. (*Стратегія*). У цьому базовому документі стратегічного

планування аналізується стан національної безпеки з урахуванням розвитку інформаційних технологій та появою нових інформаційних інструментів.

Так, у Стратегії наголошується на чиненні інформаційного тиску на РФ з боку США та їх союзників при реалізації політики стримування Росії. При цьому, на думку розробників Стратегії, здійснюються маніпуляції із суспільною свідомістю, з'являються нові види протиправної діяльності, пов'язаної з використанням ІКТ.

У зв'язку з цим, зазначається про необхідність удосконалення системи виявлення та аналізу загроз в інформаційній сфері, протидії їм; вживання заходів для підвищення захищеності громадян і суспільства від деструктивного інформаційного впливу з боку екстремістських і терористичних організацій, іноземних спеціальних служб і пропагандистських структур; забезпечення розвитку інформаційної інфраструктури, доступності інформації з різних питань соціально-політичного, економічного і духовного життя суспільства, рівного доступу до державних послуг на всій території держави, в тому числі з використанням інформаційних і комунікаційних технологій; впровадження сучасних ІКТ; розвитку загального гуманітарного та інформаційно-телекомунікаційного середовища на територіях держав–учасниць Співдружності Незалежних Держав і в суміжних регіонах; сприяння формуванню системи міжнародної інформаційної безпеки та інше [419].

Варто звернути увагу на те, що ідеологічні та стратегічні аспекти, «дорожні карти» реалізації російської моделі інформаційної безпеки відображені у *Доктрині інформаційної безпеки РФ* (*Доктрина*) та державних програмах. Доктрина була затверджена Указом Президента РФ 5 грудня 2016 р. за № 646. Вона являє собою систему офіційних поглядів на забезпечення національної безпеки Російської Федерації в інформаційній сфері [423]. У ній розкривається поняття інформаційної сфери, національних інтересів та загроз у цій сфері тощо. Структура Доктрини включає п'ять розділів: I «Загальні положення»; II «Національні інтереси в інформаційній сфері»; III «Основні інформаційні загрози і стан інформаційної безпеки»; IV «Стратегічні

цілі і основні напрямки забезпечення інформаційної безпеки», V «Організаційні основи забезпечення інформаційної безпеки».

Зокрема, 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 і безпека держави [423].

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 поділені 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 інформаційній безпеці РФ можна поділити 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 і 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, які впливають на стан інформаційної безпеки, є нарощування низкою зарубіжних країн можливостей інформаційно-технічного впливу на інформаційну інфраструктуру в 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 і 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 [423]. 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 та права конфіденційності в Інтернеті. Такий підхід діаметрально протилежний підходу, що застосовується ЄС для боротьби з недостовірними новинами («фейками»).

Так, з метою протидії російським «фальшивим новинам» у структурі ЄС була створена спеціальна робоча група «з протидії російській дезінформації» (EU vs Disinformation campaign). Не обмежуючи доступу

європейських користувачів до інформації з російських джерел, на спеціальному сайті публікуються спростування фактів, які розміщуються в російському інформаційному просторі, особливо іноземними мовами. Такий підхід відповідає практиці «мережевого нейтралітету» [29].

У Доктрині наводиться оцінка стану інформаційної безпеки у різних сферах: оборони, науки, технологій, освіти, економічної галузі, державної та громадської безпеки, стратегічної стабільності та партнерства.

Інформаційна безпека в аспекті обороноздатності РФ характеризується збільшенням кількості та масштабів воєнно-політичних акцій з боку іноземних держав та організацій, посиленням розвідувальної діяльності іноземних держав та посиленням загроз для критично важливої інфраструктури держави.

Стан інформаційної безпеки РФ у галузі науки, технологій та освіти, відповідно до Доктрини, характеризується недостатньою ефективністю наукових досліджень, спрямованих на створення перспективних інформаційних технологій, низьким рівнем впровадження вітчизняних розробок і недостатнім кадровим забезпеченням у сфері інформаційної безпеки, а також низькою поінформованістю громадян в питаннях забезпечення особистої інформаційної безпеки. При цьому заходи щодо забезпечення безпеки інформаційної інфраструктури, включаючи її цілісність, доступність і стійке функціонування, з використанням вітчизняних інформаційних технологій і вітчизняної продукції часто не мають комплексної основи [423].

Незадовільна оцінка надана стану інформаційної безпеки в економічній площині держави через зростання кіберзлочинності, недостатню поширеність інформаційних технологій у виробництві та сфері послуг, залежність російського виробництва від іноземних ІТ (програмне забезпечення, компонентна база, засоби зв’язку та ін.).

У контексті інформаційної безпеки РФ стосовно стратегічної стабільності і рівноправного стратегічного партнерства, у Доктрині зазначається про прагнення окремих держав використовувати технологічну перевагу для

домінування в інформаційному просторі. Існуючий нині розподіл між країнами ресурсів, необхідних для забезпечення безпечного і сталого функціонування мережі «Інтернет», не дає змогу реалізувати спільне справедливе, засноване на принципах довіри управління ними. Відсутність міжнародно-правових норм, що регулюють міждержавні відносини в інформаційному просторі, а також механізмів і процедур їх застосування, які враховують специфіку інформаційних технологій, ускладнює формування системи міжнародної інформаційної безпеки, спрямованої на досягнення стратегічної стабільності і рівноправного стратегічного партнерства.

У Доктрині, на підставі викладеного аналізу стану інформаційної безпеки, сформульовано кроки для поліпшення її забезпечення в кожній з наведених вище сфер. У цілому такі забезпечувальні заходи можна звести до таких напрямів: *протидія та запобігання* (використання ІТ з протиправною метою у політичній, економічній, соціальній та інших сферах); *підвищення захисту та безпеки* (суверенітету, інформації, критично важливої інфраструктури, інформаційних об'єктів, громадян та територій, єдиної мережі електрозв'язку РФ, функціонування зразків військового озброєння тощо); *розвиток* (інновацій, науки та освіти, вітчизняної конкурентоспроможності, кадрового потенціалу, культури особистої інформаційної безпеки, національної системи управління російським сегментом Інтернету тощо).

В умовах збройної агресії РФ проти України, велике значення в якій має і інформаційна війна, практичний інтерес становлять стратегічні цілі РФ у сфері забезпечення інформаційної безпеки держави.

Так, відповідно до військової політики Російської Федерації основними напрямами забезпечення інформаційної безпеки в сфері оборони країни є:

а) стратегічне стримування та запобігання військовим конфліктам, які можуть виникнути в результаті застосування інформаційних технологій;

б) вдосконалення системи забезпечення інформаційної безпеки Збройних Сил РФ, інших військ, військових формувань і органів, що включає в себе сили та засоби інформаційного протиборства;

в) прогнозування, виявлення та оцінювання інформаційних загроз, включаючи загрози Збройним Силам РФ в інформаційній сфері;

г) сприяння забезпеченню захисту інтересів союзників РФ в інформаційній сфері;

д) нейтралізація інформаційно-психологічного впливу, в тому числі спрямованого на підрив історичних основ і патріотичних традицій, пов'язаних із захистом вітчизни [418].

Реалізація політики РФ у сфері інформаційної безпеки здійснюється і через розробку і виконання відповідних державних програм. Так, окремий розділ Державної програми РФ «Інформаційне суспільство (2011-2020 роки)», затвердженої розпорядженням Уряду РФ №1815-р від 20 жовтня 2010 року, присвячений забезпеченню інформаційної безпеки.

Основні завдання підпрограми «Безпека в інформаційному суспільстві»:

– забезпечення контролю і нагляду, дозвільної та реєстраційної діяльності у сфері зв'язку, інформаційних технологій і масових комунікацій;

– забезпечення безпеки функціонування інформаційних і телекомунікаційних систем;

– розвиток технологій захисту інформації, що забезпечують недоторканність приватного життя, особистої і сімейної таємниці, безпеку інформації обмеженого доступу;

– протидія поширенню ідеології тероризму, екстремізму, пропаганди насильства [447].

Організаційна складова інформаційної безпеки РФ характеризується розмежуванням повноважень між усіма гілками влади та визначенням компетенції федеральних органів влади й органів державної влади суб'єктів

федерації. Склад системи забезпечення інформаційної влади визначає Президент РФ.

Систему забезпечення інформаційної безпеки РФ утворюють такі суб'єкти: Рада Федерації та Державна Дума Федеральних Зборів РФ (в першу чергу Комітет Державної думи з безпеки), Рада Безпеки РФ, Уряд РФ (Міністерство цифрового розвитку, зв'язку і масових комунікацій РФ, Міністерство внутрішніх справ), Центральний банк РФ, Військово-промислова комісія РФ, органи судової влади, федеральні органи виконавчої влади (зокрема, Федеральна служба по нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій, Федеральна служба безпеки, Служба зовнішньої розвідки) та міжвідомчі органи, виконавчі органи суб'єктів федерації, органи місцевого самоврядування, компетенція яких включає вирішення завдань щодо забезпечення інформаційної безпеки.

У той самий час учасниками системи забезпечення інформаційної безпеки РФ є: власники об'єктів критичної інформаційної інфраструктури і організації, які експлуатують такі об'єкти, засоби масової інформації і масових комунікацій, організації грошово-кредитної, валютної, банківської та інших сфер фінансового ринку, оператори зв'язку, оператори інформаційних систем, організації, що здійснюють діяльність по створенню і експлуатації інформаційних систем і мереж зв'язку, по розробленню, виробництву та експлуатації засобів забезпечення інформаційної безпеки, з надання послуг у сфері забезпечення інформаційної безпеки, організації, що здійснюють освітню діяльність у цій галузі, громадські об'єднання, інші організації та громадяни, які, відповідно до законодавства, беруть участь у вирішенні завдань щодо забезпечення інформаційної безпеки [423].

Діяльність органів із забезпечення інформаційної безпеки РФ здійснюються за такими принципами: принцип законності правовідносин у сфері інформаційної безпеки, рівності учасників таких правовідносин; принцип вільного доступу до інформації; принцип пропорційності між інтересами громадян в інформаційній сфері та обмеженнями з боку держави

при забезпеченні національної безпеки; принцип продуктивної співпраці між державою, громадськими організаціями, бізнесом та громадянами при вирішенні завдань у сфері інформаційної безпеки; принцип достатності сил та засобів забезпечення інформаційної безпеки та принцип виконання міжнародних норм та договорів.

У Доктрині також визначено завдання державних органів у рамках діяльності щодо забезпечення інформаційної безпеки. Серед яких:

а) забезпечення захисту прав і законних інтересів громадян і організацій в інформаційній сфері;

б) оцінювання стану інформаційної безпеки, прогнозування і виявлення інформаційних загроз, визначення пріоритетних напрямів їх запобігання і ліквідації наслідків їх прояву;

в) планування, здійснення і оцінка ефективності комплексу заходів щодо забезпечення інформаційної безпеки;

г) організація діяльності та координація взаємодії сил забезпечення інформаційної безпеки, вдосконалення їх правового, організаційного, оперативно-розшукового, розвідувального, контррозвідувального, науково-технічного, інформаційно-аналітичного, кадрового та економічного забезпечення;

д) вироблення і реалізація заходів державної підтримки організацій, що здійснюють діяльність з розроблення, виробництва і експлуатації засобів забезпечення інформаційної безпеки, з надання послуг у сфері забезпечення інформаційної безпеки, а також організацій, що здійснюють освітню діяльність у цій галузі [423].

Розглянемо детальніше правовий статус спеціальних суб’єктів реалізації функції забезпечення інформаційної безпеки в РФ.

Так, Міністерство цифрового розвитку, зв’язку і масових комунікацій РФ створено 15 травня 2018 р. указом Президента РФ №215 на базі Міністерства зв’язку і масових комунікацій (Мінкомзв’язку).

Основні напрями його діяльності: інформаційна держава, що передбачає інформатизацію державних органів на федеральному та регіональному рівнях, координацію та моніторинг у цій сфері, цифрове перетворення галузі освіти, охорони здоров'я, виборів. Електронний уряд включає електронні державні послуги та відповідну інфраструктуру. Діяльність у сфері медіа спрямована на безпеку та контроль Інтернету, цифрову обізнаність, розвиток телебачення нового покоління. Реформування телекомунікацій: державне регулювання телекомунікацій, якості зв'язку, супутникового зв'язку тощо. Цифрова економіка, що охоплює федеральну програму інформаційної безпеки. IT-сфера, в цьому векторі планується розвиток кадрового потенціалу, створення сприятливих умов для розвитку IT, побудова технопарків у сфері високих технологій. Міжнародна співпраця. Оброблення персональних даних.

Вказане міністерство бере участь у реалізації федеральної програми «Інформаційна безпека». Відповідно до паспорта цієї програми, викликами і загрозами для реалізації цілей розвитку цифрової економіки у сфері інформаційної безпеки є зростання масштабів комп'ютерної злочинності, в тому числі міжнародної, відставання РФ у розробленні і використанні вітчизняного програмного забезпечення, недостатній рівень кадрового забезпечення у сфері інформаційної безпеки.

Ключові показники, які планується досягти до 2024 року:

– 100 експортноорієнтованих компаній-розробників отримають підтримку;

– 90% мережевого трафіку російського сегмента мережі «Інтернет» будуть маршрутизуватися на території Росії;

– 97% населення використовуватимуть засоби захисту інформації;

– менш як 10% становитиме вартісна частка закуповуваного або орендованого органами державної влади іноземного програмного забезпечення [447].

Крім того, планується побудувати ефективну систему захисту прав особи, бізнесу та держави в інформаційному середовищі, забезпечити стабільний захист інформаційної інфраструктури та конкурентоспроможність вітчизняних технологій та розробок у сфері ІТ.

Федеральна служба нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій (далі – Роскомнагляд) є федеральним органом виконавчої влади, що здійснює функції по контролю і нагляду у сфері засобів масової інформації, в тому числі електронних, і масових комунікацій, інформаційних технологій і зв'язку, функції по контролю і нагляду за відповідністю оброблення персональних даних вимогам законодавства РФ у сфері персональних даних, а також функції з організації діяльності радіочастотної служби.

Роскомнагляд є уповноваженим федеральним органом виконавчої влади щодо захисту прав суб'єктів персональних даних [420].

Зазначена служба знаходиться у підпорядкуванні Мінкомзв'язку, а свою діяльність здійснює як безпосередньо, так і через свої територіальні органи у взаємодії з іншими органами виконавчої влади, місцевого самоврядування та громадськими організаціями.

Роскомнагляд здійснює функції регулювання, контролю та нагляду в усіх сферах інформаційного середовища РФ, а саме: сфері ІТ, зв'язку та масових комунікацій. Для виконання цих функцій він наділений дуже широкими повноваженнями.

У сфері ІТ Роскомнагляд реалізує контрольно-наглядові функції за діяльністю організаторів поширення інформації в Інтернеті в частині зберігання інформації про користувачів Інтернету та рух голосової інформації, тексту та зображень, а також інших електронних повідомлень в Інтернеті. Ліцензує діяльність з виготовлення екземплярів аудіовізуальних творів, програм для електронних обчислювальних машин, баз даних і фонограм на будь-яких видах носіїв. Проводить акредитаційну та експертну діяльність у цій галузі.

У сфері зв’язку Роскомнагляд здійснює державний контроль та нагляд:

– за дотриманням вимог до побудови мереж електрозв’язку та поштового зв’язку, вимог до проектування, будівництва, реконструкції та експлуатації мереж і споруд зв’язку;

– за дотриманням операторами зв’язку і власниками мереж зв’язку спеціального призначення вимог до пропуску трафіку та його маршрутизації;

– за дотриманням порядку розподілу ресурсу нумерації єдиної мережі електрозв’язку РФ;

– за відповідністю використання операторами зв’язку та власниками мереж зв’язку спеціального призначення виділеного їм ресурсу нумерації встановленому порядку використання ресурсу нумерації єдиної мережі електрозв’язку РФ;

– за виконанням організаціями федерального поштового зв’язку та операторами зв’язку вимог закону в частині фіксування, зберігання та подання інформації про операції, що підлягають обов’язковому контролю, а також за організацією та здійсненням ними внутрішнього контролю;

– за виконанням правил використання радіоелектронних засобів або високочастотних пристроїв та правил приєднання мереж електрозв’язку до мережі зв’язку загального користування, в тому числі умов приєднання [420].

У сфері масових комунікацій Роскомнагляд здійснює контрольну і наглядову діяльність у сфері ЗМІ, телерадіомовлення та електронних комунікацій. Проводить реєстрацію ЗМІ, ліцензування діяльності з теле- та радіомовлення, видає дозволи на поширення продукції зарубіжних періодичних друкованих видань на території РФ. Здійснює контроль за одержанням редакцією ЗМІ, мовником або видавцем грошових коштів з іноземних джерел. Організує та забезпечує роботу Федеральної конкурсної комісії з телерадіомовлення та Експертної ради з масових комунікацій. Визначає правила проведення експертизи інформаційної продукції та проводить акредитацію експертів. Забезпечує виконання «Про захист дітей від

інформації, що завдає шкоди їх здоров'ю та розвитку» від 29 грудня 2010 р. № 436-ФЗ.

Окремо звернемо увагу на повноваження Роскомнагляду щодо контролю за діяльністю інтеренет-мережі. Зокрема, він створює, формує та веде єдину автоматизовану інформаційну систему «Єдиний реєстр доменних імен, покажчиків сторінок сайтів в мережі «Інтернет» і мережевих адрес, що дозволяють ідентифікувати сайти в мережі «Інтернет», що містять інформацію, поширення якої в РФ заборонено». Водночас він вживає заходів щодо обмеження доступу до інформаційних ресурсів в інформаційно-телекомунікаційних мережах, в тому числі в Інтернеті. Для цього Роскомнагляд визначає порядок взаємодії оператора єдиного реєстру з провайдером хостингу і порядок отримання доступу до інформації, яка міститься в єдиному реєстрі, оператором зв'язку, що надає послуги з надання доступу до Інтернету [420].

Крім того, Роскомнагляд забезпечує роботу Універсального сервісу перевірки обмеження доступу до сайтів і (або) сторінок сайтів в Інтернеті та веде Реєстри: забороненої інформації, порушників авторських прав, організаторів поширення інформації, агрегаторів новин, інформації, що містить заклики до масових безладів, здійснення екстремістської діяльності, участі в несанкціонованих масових (публічних) заходах, недостовірну суспільно значущу інформацію, поширювану під виглядом достовірних повідомлень.

Окремим напрямом діяльності Роскомнагляду є захист прав суб'єктів персональних даних. У цьому аспекті його компетенція поширюється на ведення Порталу персональних даних, Реєстру операторів персональних даних, створення Консультативної ради тощо.

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.

Висновки до розділу 3

У розділі досліджено моделі забезпечення інформаційної безпеки сучасних держав. У глобальному аспекті порівняння систем правового забезпеченні інформаційної безпеки в Україні, у європейських та азійських країнах, країнах Північної Америки визначено і доведено пріоритетні, реальні та неприйнятні моделі для подальшого вдосконалення системи інформаційної та кібербезпеки Української держави.

З'ясовано моделі інформаційної безпеки європейських країн, що засновуються на відповідному законодавстві Європейського Союзу та національному законодавстві держав-учасниць. Головні акти ЄС у сфері захисту інформаційного простору: 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 року про захист фізичних осіб стосовно обробки 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 щодо 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 здійснюються такими державними органами, 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 актах.

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 передачі інформації за допомогою радіо і кіно. Цензура не здійснюється.

У 2009 році Конституція ФРН було доповнено статею 91c, яка заклала основу для співпраці федерального уряду і урядів земель у сфері інформаційних технологій. Це положення є широким з урахуванням постійного прогресу інформаційних технологій і його зростаючого значення для державного управління. Воно включає в себе фактичні і 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 IT) від 25.07.2015. Закон відводить Федеральному відомству з безпеки у сфері інформаційних технологій (нім. – BSI) центральну роль у захисті критично важливих інфраструктур в Німеччині. При цьому під критичними інфраструктурами розуміються 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.

Наголошено на тому що в Сполучених штатах Америки по-іншому врегульовано проблему забезпечення інформаційної безпеки, аніж у європейських країнах. Так, усвідомлення Сполученими Штатами масштабності впливу цифрових технологій на всі процеси в 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 в 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 можуть бути: електронна боротьба, мережеві комп'ютерні операції, військові операції інформаційної підтримки, дезінформація противника, безпека операцій.

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 азіатської моделі зумовлено наявністю тенденцій до запозичення РФ китайського досвіду регулювання інформаційної безпеки і 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 в першу чергу 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 запущений 2003 році. Його 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 із 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.д.

Проект «Золотий щит» передбачає обмеження доступу до низки іноземних сайтів, веб-сторінки фільтруються по кодовим словам, пов'язаним з

національною безпекою та чорним списком сайтів. Сайти, які розміщені в 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, що дозволяє віднести російську модель забезпечення інформаційної безпеки 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 актах та міжнародних документах.

Контент-аналіз Конституції РФ свідчить про відсутність у її тексті поняття «інформаційна безпека», лише використовується термін «державна безпека». Конституційні положення про право на інформацію та заборону ц

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

и У контексті реалізації права на інформацію названий закон визначає основні поняття у цій сфері, закріплює статус інформації як об’єкта м 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.

ь

з

а

Для організаторів поширення інформації в мережі «Інтернет» встановлено низку додаткових обов'язків щодо зберігання інформації на території РФ, за невиконання яких передбачено адміністративну 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» та 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 та 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 IT-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 і 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 поділені 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 із концепції Доктрини, загрози інформаційній безпеці РФ можна поділити 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 і 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 і порушення територіальної цілісності інших держав. У 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 та права конфіденційності в Інтернеті. Такий підхід діаметрально протилежний підходу, що застосовується 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

Нині актуальним є комплексне дослідження проблеми забезпечення інформаційної безпеки як функції сучасних держав, що ґрунтується на теоретичних основах, конституційних та інших правових засадах регулювання і реалізації цієї функції в Україні та інших державах, задля визначення певних особливостей, стану забезпечення такого регулювання, його удосконалення та реалізації в сучасних умовах.

При цьому потрібно закцентувати увагу на певних проблемах, пов'язаних із функцією забезпечення інформаційної безпеки держав. Сформульовано висновки і пропозиції стосовно удосконалення її правового регулювання та реалізації в умовах реформ в Україні, а також у процесі євроінтеграції, інтервенції та глобалізації. Від успішних результатів у сфері інформбезпеки значною мірою залежать роль і місце нашої держави в світовому порядку денному, усталеному глобальному інформаційному просторі, залежить рівень захисту національних інформаційних інтересів, нашого інформаційного суверенітету, прав та інтересів людини і громадянина.

1. Механізми забезпечення інформаційної безпеки держави: теоретичний і законодавчий виміри

У контексті нашого дослідження важливо з'ясувати зміст правової категорії «механізм забезпечення інформаційної безпеки» та визначити підхід українського законодавця до розуміння цієї категорії. Це дасть змогу комплексно та ґрунтовно розглянути структуру механізму забезпечення інформаційної безпеки держави, виявити причини недостатньої дієвості цього механізму в цілому та окремих його елементів зокрема.

Багатокомпонентність цього поняття викликає необхідність розпочати аналіз з його ключового компоненту – «забезпечення інформаційної безпеки». Саме різноманітність наукових поглядів на сутність забезпечення інформаційної безпеки зумовлює множинність підходів до визначення її механізму.

Так, у Словнику української мови забезпечення тлумачиться як:

– створення надійних умов для здійснення чого-небудь; гарантування чогось;

– захист, охорона кого-, що-небудь від небезпеки [572].

Якщо проаналізувати юридичні та економічні терміни, які містять лексему «забезпечення», то можна навести такі її трактування:

– комплекс заходів та засобів, створення умов для належного функціонування чогось та/або нормального перебігу процесу;

– діяльність щодо створення засобів та застосування сукупності заходів та засобів.

У науковій літературі, як правило, за основу береться широке розуміння поняття «забезпечення», яке поєднує всі вище наведені його тлумачення, але з акцентуванням на його діяльнісному аспекті.

Зокрема, А. Стрельцов підкреслює, що забезпечення є сукупністю діяльності із забезпечення, засобів забезпечення та суб'єктів забезпечення. Діяльність із забезпечення полягає в наданні допомоги суб'єктам у досягненні поставлених цілей. Засоби забезпечення утворюють сукупність матеріальних,

духовних, фінансових, правових, організаційних і технічних засобів, необхідних для діяльності із забезпечення. Суб'єктами забезпечення є індивіди, організації та органи держави, що здійснюють діяльність із забезпечення [586, с.44].

В. Предборський дійшов висновку, що діяльність із забезпечення безпеки виникає як соціальний феномен щодо подолання протиріч між об'єктивною реальністю – небезпекою і потребами особи, соціальних груп, суспільства і держави на засадах попередження, локалізації та обмеження. Небезпека як така є об'єктом управлінської діяльності по усуненню, запобіганню, локалізації загроз безпеці. До предмета цієї діяльності автор відносить конкретні загрози небезпеки (військові, політичні, економічні та ін.), а також конкретні матеріальні носії цих загроз (природні та соціально-економічні явища) [467, с. 13].

Досить цікавою видається запропонована В. Предборським концепція двовимірності діяльності із забезпечення безпеки. Зокрема, вчений вказує, що діяльність із забезпечення безпеки має горизонтальний та вертикальний виміри, які складаються із взаємопов'язаних і взаємообумовлених рівнів. Так, до горизонтального виміру цієї діяльності пропонується відносити діяльність із забезпечення безпеки особи, підприємства, регіону, держави, суспільства, міжнародної спільноти. До вертикального виміру належать забезпечення політичної, військової, економічної, інформаційної, наукової, технічної безпеки тощо [467, с. 14].

Слід наголосити, що наведені висновки вчений зробив у межах дослідження економічної безпеки України, але, на наш погляд, вони цілком можуть бути використані і при вивчені інформаційної безпеки, оскільки стосуються загальних ознак, які є спільними для обох складових національної безпеки України (як інформаційної, так і економічної).

У монографічному дослідженні «Правові засади інформаційної безпеки України» (Харків, 2018 р.) її автори наводять визначення понятійно-категоріального апарату у сфері державної безпеки, які були запропоновані

Службою безпеки України внаслідок досліджень сектора безпеки України, що здійснювалися у 2005–2007 рр. Зокрема, забезпечення державної безпеки визначається як спеціальний вид діяльності у сфері національної безпеки, яка здійснюється системою державних органів та військових формувань з використанням комплексу правових, організаційних, режимних, контррозвідувальних, оперативно-розшукових, службово-бойових та військових заходів, спрямованих на захист об'єктів державної безпеки [141, с. 56]. Варто зазначити, що запропоноване визначення засновується на поширеному в науці підході до розуміння «забезпечення» як діяльності з реалізації заходів, проте воно не знайшло свого відображення в українському законодавстві.

О. Тихомиров, досліджуючи систему забезпечення інформаційної безпеки держави, пропонує використовувати методологічний підхід, за яким можна розглядати її забезпечення як своєрідну діяльність, одним з основних, але не єдиним суб'єктом якої є держава. При цьому зміст державного забезпечення інформаційної безпеки автор інтерпретує як систему державних гарантій в інформаційній сфері, прямо чи опосередковано визначених фундаментальними нормативно-правовими актами, що регламентують інформаційну сферу суспільних відносин [602, с. 72].

В. Ліпкан, Ю. Максименко, В. Желіховський використовують діяльнісний підхід до розуміння забезпечення інформаційної безпеки держави та вказують на те, що забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек [361, с.161].

Водночас дефініцію забезпечення інформаційної безпеки ці автори формулюють як систему теоретико-методологічних, нормативно-правових, інформаційно-аналітичних, управлінських, розвідувальних, контррозвідувальних, оперативно-розшукових, кадрових, науково-технічних, ресурсних та інших заходів, спрямованих на забезпечення свідомого

цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, за якого державними, міжнародними та недержавними інституціями створюються необхідні й достатні умови для реалізації і прогресивного розвитку інформаційних інтересів, ефективне функціонування самої системи забезпечення інформаційної безпеки [361, с. 267].

А. Нашинець-Наумова забезпечення інформаційної безпеки визначає як діяльність, спрямовану на захист інформаційних інтересів особи, суспільства, держави, її адміністративно-територіальних утворень з метою гарантування інформаційної незалежності України та захисту її інформаційної системи від внутрішніх і зовнішніх загроз [403,с. 50].

Т. Ткачук у рамках дослідження правового забезпечення інформаційної безпеки в умовах євроінтеграції України вказує на те, що забезпечення інформаційної безпеки України є складним комплексним поняттям, що охоплює велике коло процесів і явищ, пов'язаних із протидією загрозам безпеці національних інтересів в інформаційній сфері. Зміст цього поняття автор розкриває крізь призму сукупності діяльності щодо недопущення шкоди властивостям об'єкта безпеки, зумовленої інформацією та інформаційною інфраструктурою, а також засобів і суб'єктів цієї діяльності. При цьому мету забезпечення інформаційної безпеки держави він визначає як досягнення стану захищеності суспільних відносин від прояву зовнішніх і внутрішніх загроз, пов'язаних з інформацією та інформаційною інфраструктурою у процесі захисту національний цінностей, реалізації національних інтересів, досягнення національних цілей [611, с. 104].

У наведеному визначенні автор закріплює перелік структурних елементів (об'єкт, суб'єкт, загрози, засоби, мета та ін.), які в багатьох дослідженнях належать до механізму або системи забезпечення інформаційної безпеки. Такий підхід розгляду структури саме забезпечення інформаційної безпеки, а не її системи чи механізму, порівняно з іншими наявними у науковій літературі підходами, видається дещо вузьким.

Т. Перун обґрунтовує думку про те, що забезпечення інформаційної безпеки являє собою складний соціально-правовий механізм, під яким слід розуміти формування та проведення державної політики щодо створення та підтримки необхідного рівня захищеності об'єктів безпеки за допомогою здійснення заходів нормативно-правового, організаційного, управлінського і іншого характеру, заходів, адекватних загрозам життєво важливим інтересам особи, суспільства та держави у інформаційній сфері [449, с. 52].

На увагу заслуговує і точка зору російського вченого В. Ярочкіна, який забезпечення безпеки інформації характеризує як безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення і розвитку системи захисту, безперервному контролі її стану, виявленні її вузьких і слабких місць і протиправних дій [684].

Що стосується сфери українського законодавства, то поняття забезпечення інформаційної безпеки активно використовується, але його зміст не деталізується.

У Доктрині інформаційної безпеки РФ категорія забезпечення інформаційної безпеки визначається 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 [423].

У наукових дослідженнях різних напрямів національної безпеки, серед яких і інформаційний, широко використовується системно-структурний підхід, який дає змогу розглядати забезпечення безпеки на різних рівнях її системи або механізму забезпечення. Така поширеність цього підходу у юридичних працях, напевно, зумовлена вже усталеним вченням про механізм правового регулювання, механізм державного управління, механізм реалізації права тощо. Крім того, український законодавець також досить часто використовує цю категорію, зокрема розділ 6 Доктрини інформаційної

безпеки України присвячений саме механізму реалізації Доктрини. Також у цьому документі вживаються поняття механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави шкідливої інформації, механізму реалізації зобов'язань, механізмів регулювання роботи, механізму взаємодії держави та інститутів громадянського суспільства, механізму електронного урядування, механізму захисту. Однак жодне з наведених понять безпосередньо у Доктрині не розкривається.

Отже, розглянемо теоретичні засади категорії «механізм забезпечення інформаційної безпеки». Етимологія слова «механізм» грецька, означає «зброя, машина» і має такі основні значення:

– пристрій для передачі й перетворення рухів, у якому рух одного або декількох елементів викликає певні рухи решти;

– внутрішній пристрій, внутрішня будова машини, устаткування;

– сукупність станів і процесів, із яких складається будь-яке фізичне, хімічне, фізіологічне, економічне, психологічне явище;

– система, пристрій, спосіб, що визначають порядок певного виду діяльності [223, с. 355–372].

Термін «механізм» у юриспруденції означає внутрішній устрій системи, сукупність процесів і станів, з яких складається будь-яке явище. Механізм можна також визначити як сукупність взаємопов'язаних елементів, що становлять певну систему, яка перебуває в стані руху [397]. Наведене визначення можна екстраполювати на сферу забезпечення інформаційної безпеки держави, механізм якого приводить у дію визначену законодавством функцію держави із забезпечення інформаційної безпеки.

У контексті дослідження інформаційної безпеки вчені пропонують різні концепції механізму її забезпечення. Наприклад, В. Ліпкан, Ю. Максименко, В. Желіховський під державно-правовим механізмом інформаційної безпеки розуміють систему взаємопов'язаних і взаємоузгоджених державно-правових інституцій, завданнями яких є створення умов для успішної реалізації інформаційної політики [361, с. 137].

О. Зозуля характеризує механізми забезпечення інформаційної безпеки як сукупність державних інститутів і структур громадянського суспільства, а також практичних заходів, важелів, стимулів, способів дій із визначення та організації (залучення) необхідних матеріальних, духовних, людських ресурсів, інтеграції різних сфер суспільства з метою досягнення завдань забезпечення інформаційної безпеки України [249, с. 45].

Особливістю цього авторського погляду є також те, що розгляд забезпечення інформаційної безпеки здійснюється крізь призму множинності її механізмів, тоді як переважна більшість дослідників у цій сфері виділяє загальний механізм чи систему забезпечення інформаційної безпеки.

Б. Кормич розглядає державно-правовий механізм інформаційної безпеки систему органів державної влади загальної і спеціальної компетенції, задіяних у процесі формування та реалізації політики інформаційної безпеки, внутрішні й зовнішні ролі та відносини якої регулюються системою правових норм і принципів [325, с. 132].

При цьому вчений наголошує, що ефективність захисту інформаційної безпеки держави в цілому забезпечується ефективністю кожної складової її державно-правового механізму, який складається з трьох взаємопов’язаних елементів. По-перше, це сукупність державних інституцій, задіяних у процесі формування і впровадження політики інформаційної безпеки, тобто інституціональний механізм інформаційної безпеки. По-друге, це сукупність ролей та відносин, яка включає правові відносини, що виникають при проведенні політики інформаційної безпеки та специфічні ролі. Форми і методи діяльності суб’єктів проведення цієї політики. По-третє, це ієрархічна сукупність правових норм та принципів, яка регулює зміст і процес проведення політики інфорбезпеки, тобто правовий механізм інформаційної безпеки [325, с. 132–133].

Науково доцільним видається підхід В. Приходько до визначення механізму забезпечення безпеки на підставі аналізу поняття механізму державного управління. Зокрема, автор визначає механізм державного

управління як систему, що призначена для практичного здійснення державного управління та досягнення поставлених цілей, яка має певну структуру, методи, важелі, інструменти впливу на об'єкт управління з відповідним правовим, нормативним та інформаційним забезпеченням. Враховуючи вищенаведене, вчений пропонує такий перелік механізмів управління: механізми-знаряддя (інструменти), механізми-системи (набір взаємопов'язаних елементів) та механізми-процеси (послідовність певних перетворень). Залежно від того, які саме проблеми і як вирішуються із застосуванням конкретного державного механізму управління, він може бути складним (комплексним) і включати в себе декілька самостійних механізмів [222, с. 61–62].

У цьому ракурсі цікавою є структура самого комплексного механізму державного управління, яка може складатися з таких видів механізмів:

– економічного (механізми державного управління банківською, грошово-валютною, інвестиційною, інноваційною, кредитною, податковою, страховою діяльністю тощо);

– мотиваційного (сукупність командно-адміністративних та соціально-економічних стимулів, що спонукають державних службовців до високоефективної роботи та організаційні структури, а також результати їх функціонування);

– політичного (механізми формування економічної, соціальної, фінансової, промислової політики тощо);

– правового (нормативно-правове забезпечення: закони і постанови Верховної Ради України, укази Президента України, постанови і розпорядження Кабінету Міністрів України, а також методичні рекомендації та інструкції тощо) [608, с. 188−193].

А. Нашинець-Наумова зазначає, що механізм забезпечення інформаційної безпеки є системою різних засобів (політичних, кадрових, оперативно-розшукових, інформаційних, правових), за допомогою яких

забезпечується захист інформаційних інтересів держави, суспільства, особи від внутрішніх і зовнішніх загроз [403, с. 53].

Близьким за змістом поняттю механізм забезпечення є поняття система забезпечення інформаційної безпеки, багато вчених розглядають забезпечення інформаційної безпеки крізь елементи її системи.

Термін «система» походить з грецької мови і означає складене з частин з'єднання; у філософському сенсі розуміють ціле, утворене шляхом об'єднання закономірно пов'язаних один з одним предметів, явищ тощо. Останні є її елементами, складовими частинами. При цьому якості системи як самостійного цілого ніколи не зводяться до якостей елементів, що утворюють систему Оскільки елементи об'єднуються в систему, підкоряючись об'єктивним закономірностям, між ними виникають стійкі зв'язки, що формують внутрішню форму, тобто структуру системи. Таким чином, будь-яка система складається з елементів і системоутворюючих зв'язків [656, с. 26–27].

Дослідники В. Ліпкан, Ю. Максименко, В. Желіховський під системою забезпечення інформаційної безпеки пропонують розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення. Вони виділяють три аспекти забезпечення інформаційної безпеки:

1) інформаційно-технічну безпеку – управління потенційними чи реальними загрозами з метою захисту комп'ютерних, телекомунікаційних технологій та інших технологій зв'язку;

2) інформаційно-психологічну безпеку – управління реальними чи потенційними загрозами, що можуть завдати шкоди психіці людини, суспільства;

3) інформаційну безпеку у сфері прав і свобод людини – управління реальними чи потенційними загрозами з метою забезпечення права на інформацію [361, с. 158–197].

На наш погляд, наведене визначення системи забезпечення інформаційної безпеки не є вдалим, оскільки формулювання визначення поняття через те саме поняття (система….– це система…) може свідчити про логічну помилку *idem per idem*.

А. Нашинець-Наумова зазначає, що система забезпечення інформаційної безпеки – це внутрішня структура, систематизована сукупність, єдність, взаємозв'язок і диференціація окремих її елементів (об'єкт, суб'єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз) [403, с. 29]. Вона вважає ключовими елементами такої системи – перелік рівнів інформаційної безпеки та перелік її загроз. Нам видається, що в запропонованому визначенні немає змістовного елемента, який пояснював би внутрішньою структурою чого саме є система забезпечення інформаційної безпеки.

Авторка також наголошує, що слід розрізняти поняття «система забезпечення інформаційної безпеки», «механізм забезпечення інформаційної безпеки», а систему забезпечення інформаційної безпеки розглядає як сукупність елементів, з яких така система складається (у вузькому розумінні), механізм та стратегію забезпечення (у широкому розумінні) .

На наш погляд, якраз система забезпечення інформаційної безпеки є ширшим поняттям, оскільки вона являє собою відокремлену від середовища та взаємодіючу з ним сукупність взаємопов'язаних елементів, тоді як механізм є внутрішнім устроєм такої системи та/або може бути її елементом. Принаймні такий погляд ліг в основу вчення про юридичний (правовий) механізм.

У своєму дослідженні А. Нашинець-Наумова одночасно приходить до висновку, що система забезпечення інформаційної безпеки у широкому розумінні також включає механізм та стратегію її забезпечення [403, с. 53]. Внаслідок цього нівелюється її попереднє обґрунтування співвідношення

системи та механізму забезпечення інформаційної безпеки й стає незрозумілим, який підхід (широкий чи вузький) до вказаних понять обрала сама авторка, а якщо пропонуються обидва, то яка характеристика цих понять відповідно до цих підходів.

Схожий з нашою позицією щодо співвідношення механізму та системи забезпечення інформаційної безпеки висновок Л. Євдоченка, який пропонує розглядати систему державного забезпечення інформаційної безпеки України як комплексний механізм реалізації національних інтересів в інформаційній сфері та захисту цих інтересів від зовнішніх і внутрішніх інформаційних загроз, зважаючи на негативні чинники адаптації системи державного забезпечення інформаційної безпеки до динаміки глобалізаційних процесів на основі узагальнення міжнародного досвіду [227, с. 20].

Г. Ситник, аналізуючи систему забезпечення національної безпеки висловлює співзвучну нашому погляду позицію. Так, вчений пропонує розуміти систему забезпечення національної безпеки як складову системи національної безпеки, а саме – сукупність взаємопов'язаних та взаємообумовлених механізмів (інституційних, організаційних, правових та інших) та суб'єктів забезпечення національної безпеки (посадові особи держави, органи державної влади та місцевого самоврядування, державні установи та заклади, сили та засоби сектора безпеки, інститути громадянського суспільства, окремі громадяни), які на основі чинного законодавства трансформують політику національної безпеки в цілеспрямовану скоординовану діяльність (заходи політичного, правового, організаційного, воєнного та іншого характеру) щодо реалізації національних інтересів (передусім щодо виявлення, прогнозування, запобігання та нейтралізації загроз безпеці особи (громадянина), суспільства та держави) [190, с. 355–356].

О. Зозуля під системою забезпечення інформаційної безпеки пропонує розуміти сукупність уже існуючих і спеціально створюваних органів, формальних і неформальних державних і громадських структур, соціальних

груп, суспільних об’єднань, окремих осіб, а також правових, політичних, економічних, інформаційних та інших зв’язків між ними, механізмів, інструментів та технологій щодо забезпечення життєво важливих інтересів в інформаційній сфері особи, суспільства і держави. Учений також зауважує, що структурним елементом системи забезпечення інформаційної безпеки є система державного управління інформаційною безпекою [249, с. 44].

Як бачимо, при формулюванні цієї дефініції використано комплексний підхід, який дає змогу об’єднати в систему забезпечення інформаційної безпеки інституційну систему, систему державного управління інформаційною безпекою, складові (політична, нормативна, економічна, технічна) механізму забезпечення інформаційної безпеки, механізм реалізації інтересів в інформаційній сфері.

Здійснений 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» свідчить про відсутність усталеного підходу до визначення вказаних категорій. За таких умов, з одного боку, існує широкий простір для відповідних теоретико-правових пошуків, які в цьому випадку часто призводять до збільшення дискусійних питань та протиставлення наукових позицій. Зокрема, у 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 і 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. Водночас під *системою забезпечення інформаційної безпеки* пропонується 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, в цьому напрямі досліджень серед авторів немає узгодженої позиції щодо змісту та співвідношення категорій «механізм» та «система». Так, в одних наукових працях 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 вказаної функції держави та ускладнюється її вдосконалення.

Таким чином, на підставі вищевикладеного 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, 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 здійснюються заходи із забезпечення безпеки. Їх можна поділити на соціальні (особа, суспільство, держава, їх інтереси, права та свідомість) та технічні (інформація, інформаційна інфраструктура, інформаційні технології тощо).

У контексті запропонованих нами теоретичних положень проаналізуємо законодавчий вимір механізму забезпечення інформаційної безпеки України. У Доктрині інформаційної безпеки України об'єкти прямо не визначаються, тому їх перелік можна встановити на підставі системного аналізу її положень. Так, її розробники оперують поняттями «життєво важливі інтереси в інформаційній сфері» та «актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері», саме їх розгляд дає можливість зробити висновок про об'єкти механізму забезпечення інформаційної безпеки [213].

Зокрема, крізь призму визначених законодавцем життєво важливих інтересів особи в інформаційній сфері варто виділити такі об'єкти в механізмі забезпечення інформаційної безпеки особи: право на інформацію, право на недоторканість приватного життя особи (конфіденційність) та свідомість і психіка (захищеність від деструктивних інформаційних впливів). Такий підхід українського законодавця до об'єктів механізму забезпечення інформаційної безпеки особи видається дуже вузьким, особливо з огляду на конституційну пріоритетність соціального вектора у діяльності держави (йдеться про статтю 3 Основного Закону України).

Наприклад, у Доктрині, що аналізується, відсутні засади системи «інформаційної гігієни» для особистості, також не враховується такий важливий сегмент інформаційної безпеки особи, як безпека особи в Інтернеті, що особливо актуально для дітей і неповнолітніх. У цій Доктрині взагалі не розглядаються в якості об'єктів інформаційного захисту культурна, наукова, мистецька та інші сфери розвитку особистості, а також духовні, моральні та культурні цінності особи.

Що стосується об'єктів забезпечення інформаційної безпеки на рівні суспільства і держави, то в Доктрині, що розглядається, міститься достатньо великий перелік життєво важливих інтересів суспільства і держави в інформаційній сфері. Так, відповідно до її ч. 2 ст. 3, національними інтересами суспільства і держави в інформаційній сфері є:

– захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

– захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

– всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірної та об'єктивної інформації;

– забезпечення вільного обігу інформації, крім випадків, передбачених законом;

– розвиток та захист національної інформаційної інфраструктури;

– збереження і примноження духовних, культурних і моральних цінностей Українського народу;

– забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

– вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

– зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

– розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;

– формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

– створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

– розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

– безпечне функціонування й розвиток національного інформаційного простору та його інтеграція в європейський і світовий інформаційний простір;

– розвиток системи стратегічних комунікацій України;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

– забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

– захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

– формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

– розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та в супутниковому мовленні за межами України [213].

Наведений перелік національних інтересів в інформаційній сфері містить певні суперечності та дублювання положень. Наприклад, абзаци «захист українського суспільства від агресивного впливу деструктивної пропаганди РФ» та «захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду…» несуть однакове змістовне навантаження. Зміст другого абзацу повністю охоплює перший. Положення про «розвиток технологічної інфраструктуру інформаційного суспільства» та положення про «розвиток ІКТ та інформаційних ресурсів» за своєю суттю є тотожними, а також охоплюють положення абзацу щодо розвитку інформаційної інфраструктури. Тобто у зазначених трьох абзацах через різні формулювання стверджується про розвиток ІКТ та інформаційної інфраструктури.

Абзац щодо «всебічного задоволення потреб у доступі до достовірної та об'єктивної інформації» є логічним наслідком положення про «забезпечення

вільного обігу інформації, крім випадків, передбачених законом». Таке застереження стосовно наявності випадків обмеження доступу до інформації включає й випадки, викладені в окремому положенні про «захист державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом», тобто знову декілька абзаців мають однаковий зміст.

Крім того, фактично однаковий сенс мають положення стосовно «формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів» та положення про «створення системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди». При цьому, на наш погляд, є некоректним використання поняття «правова система», коли мова йде про певний механізм або нормативну підставу. Правова система – це широке поняття, яке означає сукупність усіх юридичних засобів та явищ у державі.

Варто також звернути увагу на невдалий підхід розробників Доктрини інформаційної безпеки України до визначення національних інтересів в інформаційній сфері через лексеми «забезпечення розвитку», «формування системи», «розвиток…», «захист…» тощо, оскільки ці словосполучення означають напрями діяльності, плани на майбутнє, а не вже існуючий національний інтерес.

У законодавстві України наявне визначення національних інтересів, зокрема у Законі України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII під національними інтересами розуміються життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток [489].

Таким чином, при формуванні переліку національних інтересів в інформаційній сфері доцільніше виходити з таких категорій, як цінності та визначальні потреби особи, суспільства та держави. Відповідно, національні

інтереси, закріплені у Доктрині, що розглядається, більше стосуються напрямів реалізації інформаційної політики держави та форм забезпечення інформаційної безпеки, а не національних інтересів як таких.

Отже, на підставі аналізу положень Доктрини про національні інтереси в інформаційні сфері можна виділити такі об'єкти забезпечення інформаційної безпеки в Україні:

1. Соціальні:

– особа (її права та свободи в інформаційному середовищі); суспільство; українська діаспора; національні меншини; підприємства установи та організації; держава; державні органи;

– свідомість; психіка; імідж держави, духовні моральні, культурні цінності; етнокультурна ідентичність;

– медіа-середовище; мовне середовище; медіа-культура; національний інформаційний простір.

2. Технічні:

– ІКТ та інформаційна інфраструктура;

– інформація (її обіг, захист та доступ до неї);

– система стратегічних комунікацій.

З поняттям об'єктів забезпечення інформаційної безпеки тісно пов'язане поняття загроз в інформаційному просторі. Загроза інформаційній безпеці – явище, дії негативних чинників або процес, через які соціальні об'єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері, а також порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об'єктів інформаційної безпеки [582, с. 94].

Наступним елементом механізму забезпечення інформаційної безпеки є *суб'єкти* такого забезпечення, якими виступають особа, суспільство (його певні групи чи об'єднання) та держава (в цілому, окремі державні органи та органи місцевого самоврядування). У Доктрині інформаційної безпеки України суб'єкти прямо не визначаються, але аналіз розділу Доктрини щодо

механізму її реалізації дає змогу виділити такі суб'єкти забезпечення інформаційної безпеки держави: Рада національної безпеки і оборони України; Кабінет Міністрів України; Міністерство інформаційної політики України; Міністерство закордонних справ України; Міністерство оборони України; Міністерство культури України; Державне агентство України з питань кіно; Національна рада України з питань телебачення і радіомовлення; Державний комітет телебачення і радіомовлення України; Служба безпеки України; Розвідувальні органи України; Державна служба спеціального зв'язку та захисту інформації України; Національний інститут стратегічних досліджень.

З наведеного переліку випливає, що у Доктрині визначені суб'єкти забезпечення інформаційної безпеки – державні органи, а відповідні суб'єкти на рівні суспільства та особи не згадуються. Прикметно, що у Доктрині інформаційної безпеки РФ окремий пункт присвячений переліку суб'єктів, які складають організаційну основу системи забезпечення інформаційної безпеки, зокрема визначено 12 таких суб'єктів та 12 учасників системи у цій сфері.

На наш погляд, чим чіткіше встановлено коло суб'єктів забезпечення інформаційної безпеки, тим краще розуміння уповноваженими суб'єктами механізму такого забезпечення, і, як наслідок, підвищення його ефективності. Їх аналіз здійснюватимемо у наступних підрозділах.

2. Загрози інформаційній безпеці: проблеми визначення та подолання

Враховуючи відсутність єдиного загальноприйнятого підходу до розкриття розуміння понять «інформаційна безпека», «загрози інформаційній безпеці», а також їх активне поширення у суспільно-державному житті та на міжнародній арені з непередбачуваними переважно негативними наслідками, вважаємо доцільним привернути увагу наукової спільноти до цієї проблематики. Насамперед, потребують розмежування однорідні та споріднені поняття «загроза», «ризик», «небезпека», «виклик» тощо, а також «інформаційна загроза», інформаційний конфлікт», інформаційна війна», «інформаційне протистояння», «інформаційне протиборство», «інформаційний тероризм» та ін.

Звісно, першочергово слід звернутись до існуючих нормативно-правових актів у цій сфері. І протягом тривалого часу в полі зору законодавців перебували ці питання.

Ще Законом України «Про основи національної безпеки України» у ст. 7 (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018 р.) до загроз національним інтересам і національній безпеці в інформаційній сфері було віднесено такі:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп’ютерна злочинність та комп’ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [494].

У цьому законі немає трактування загроз інформаційній безпеці, але було визначено поняття «загрози національній безпеці» як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України (ст. 1). З огляду на врегулювання завдань забезпечення свободи слова та інформаційної безпеки, кібербезпеки та кіберзахисту, можна зробити висновок, що це однопорядкові і відмінні категорії, як і відповідні їм загрози.

У свою чергу, в Законі України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII закріплено визначення «загрози національній безпеці України» – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. Вони, згідно з п. 5. ст. 3, як і відповідні пріоритети державної політики у сферах національної безпеки і оборони, визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України [489].

Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII більше уваги приділяє питаню загроз у цій сфері. Зокрема, індикатори кіберзагроз визначаються як показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози. Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів. Тут розкриваються поняття кіберінцидентів та кібератак, кіберзлочинів (комп’ютерних злочинів), кібертероризму і кібершпигунства тощо [495].

У Доктрині інформаційної безпеки України», затвердженій Указом Президента України №47/2017 від 25 лютого 2017 р., перелічено актуальні

загрози національним інтересам та національній безпеці України в інформаційній сфері:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів;

– підживлення панічних настроїв, загострення і дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [213].

Як бачимо, автори Доктрини при виділенні загроз інформаційній безпеці держави використали той самий підхід, що й до визначення

національних інтересів в інформаційній сфері, тобто наявні повторення, неповнота переліку, термінологічна невизначеність, донесення однієї думки за рахунок різних формулювань тощо. Наприклад, декілька разів використовується поняття «спеціальні інформаційні операції», при цьому в національному законодавстві це поняття не розкривається і стає незрозумілим, чому загрозою визнаються лише спеціальні інформаційні операції. Крім того, при характеристиці першої загрози розробники Доктрини не вказали, від кого вона походить, напевно, мається на увазі РФ, однак при констатації наявності загрози, особливо у доктринальному документі, бажано чітко вказувати джерело її походження. Те саме стосується і формулювання загрози «поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій», не уточнюється, від кого походить ця загроза.

У цілому ж закріплені у Доктрині положення щодо спеціальних інформаційних операції описують одну й ту саму загрозу – перманентну інформаційну війну РФ проти України, що здійснюється різними засобами як в українському національному інформаційному просторі, так і в глобальному.

Що стосується термінологічної невизначеності, то розробники Доктрини інформаційної безпеки України дуже вільно оперують поняттями, зміст яких у законодавчих актах не розкривається. Зокрема, використовуються поняття «інформаційна експансія» та «інформаційне домінування» без урахування особливостей їх співвідношення, яке наявне в науковій літературі.

Так, інформаційна експансія – це діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою:

– поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;

– витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками;

– збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ;

– нарощування присутності власних ЗМІ в інформаційній сфері об’єкта проникнення і тому подібне [361].

При цьому за критеріями масштабності, інтенсивності та характеру засобів, інформаційна експансія займає найнижчий рівень інформаційного протиборства, тоді як до найвищого рівня відносять інформаційну війну.

Водночас, як випливає з наведеного визначення інформаційної експансії, саме інформаційне домінування є однією з її цілей, і, відповідно, наслідком такої експансії. Таким чином, інформаційне домінування є складовою інформаційної експансії, тому є неточним виділення інформаційної експансії та інформаційного домінування як окремих загроз.

Певні питання викликає і віднесення авторами Доктрини до загроз таких проблем, як недосконалі законодавство та інформаційна інфраструктура, неефективність державної інформаційної політики та недостатній рівень медіа-культури суспільства. Враховуючи те, що йдеться про загрози інформаційній безпеці держави, яка є складовою національної безпеки, то в умовах гібридної війни з РФ особи, відповідальні за виникнення вказаних загроз, вочевидь, мають нести і кримінальну відповідальність. Однак на практиці закріплення вказаних загроз у Доктрині інформаційної безпеки України не викликало належної реакції ані з боку громадянського суспільства, ані з боку державних органів.

На наш погляд, недоліки аналізу загроз інформаційної безпеки, що викладені у Доктрині, також зумовлені відсутністю відповідного переліку загроз у профільному законі. На сьогодні більш детальний перелік загроз в інформаційній сфері представлено у Стратегії національної безпеки України (Стратегія), яка була введена у дію Указом Президента № 287/2015 від 26.05.2015 р.

Відповідно до п. 3.6 Стратегії, загрозами інформаційній безпеці є: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Згідно з п. 3.7 Стратегії, загрозами кібербезпеці і безпеці інформаційних ресурсів виступають: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Пунктом 3.8 Стратегії визначені загрози безпеці критичної інфраструктури, а саме: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення [585].

Отже, п.п. 3.6, 3.7 та 3.8 Стратегії присвячені загрозам інформаційній безпеці, загрозам кібербезпеці і безпеці інформаційних ресурсів та загрозам безпеці критичної інфраструктури. На наш погляд, поділ загроз на вказані групи не є вдалим, оскільки не враховано структура механізму забезпечення інформаційної безпеки держави та місця елементів у ньому. Зокрема, загрози інформаційній безпеці є широким поняттям, яке включає загрози кібербезпеки, інформаційної інфраструктури тощо. Водночас складовою інформаційної інфраструктури є критично важлива інформаційна інфраструктура. Разом з тим аналіз загроз в інформаційній сфері, закріплений у Стратегії, більш ґрунтовний. На наш погляд, доцільно було б його врахувати при розробленні Доктрини інформаційної безпеки України. Адже, враховуючи принцип загального і спеціального нормативного акту, спеціальний науково обгрунтований документ повинен містити всебічний та повний аналіз стану інформаційної безпеки, в тому числі і в аспекті існуючих загроз.

Таким чином, на підставі вивчення положень Доктрини інформаційної безпеки України, закріплені у ній загрози інформаційної сфери можна класифікувати за джерелом походження на зовнішні та внутрішні.

Зовнішні загрози: проведення державою-агресором спеціальних інформаційних операцій проти України як на її території, так і поза її межами; інформаційна експансія та інформаційне домінування держави-агресора.

Внутрішні загрози включають: недостатню розвиненість національної інформаційної інфраструктури; неефективність державної інформаційної політики; недосконаліть законодавства; невизначеність стратегічного наративу; недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Наведена класифікація загроз чітко вказує на помилковий аналіз ситуації у сфері інформаційної безпеки держави, що був проведений авторами Доктрини інформаційної безпеки України. В умовах гібридної війни не зовсім правильно у профільному доктринальному документі зазначати лише про дві загрози, що походять з боку держави-агресора, та зазначати про шість внутрішніх загроз, які створюються самими органами державної влади і суспільством. Така оцінка ситуації знижує ефективність механізму забезпечення інформаційної безпеки.

Можна погодитися з В. Демиденком у тому, що важливим є покладення відповідних повноважень, а також відповідальності не лише на суб'єктів механізму забезпечення інформаційної безпеки, визначених Доктриною, а й на інші органи публічної влади центрального, регіонального і локального рівнів, зокрема, органи місцевого самоврядування у законодавстві України у цій сфері [201, с. 141–153]. На наш погляд, чим чіткіше встановлено коло суб'єктів забезпечення інформаційної безпеки, тим краще розуміння уповноваженими суб'єктами механізму такого забезпечення, і, як наслідок, підвищення його ефективності.

Отже, аналіз деяких нормативно-правових актів демонструє відсутність на законодавчому рівні поняття загроз інформаційній безпеці держав. Тому варто звернутися до доктринальних джерел, енциклопедичних та інших наукових видань. Найбільш широко загрози інформаційним ресурсам

розглядають як потенційно можливі випадки природного, технічного або антропогенного характеру, 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 вразливості 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 [457].

Загроза (англ. *threat*) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають «атакою». Загроза безпеці інформації (англ. *security threat*) – загрози викрадення, зміни або знищення інформації. Вони бувають випадковими або навмисними [599].

До загроз інформаційній безпеці системи управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій у роботі самого обладнання. Через їх численність 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 у 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 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 інформаційній системи органів влади); закономірні (загрози стійкого, повторюваного характеру, зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки: численні атаки хакерів на офіційні сайти ФБР, ЦРУ США) [457, 599, 266].

Цей перелік, звісно, можна продовжувати, але очевидний такий висновок. Поняття загрози розглядаються переважно абстрактно або спрощено, подекуди звужено, відірвано від контексту поняття «інформаційна безпека» і майже не пов'язано із 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.

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 і не створювати небезпеку посягання, але тією чи іншою мірою підривають ці фундаментальні цінності держави та суспільства [414].

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 і реальної системи моніторингу та управління загрозами, іншими ризиками для інформаційної безпеки держави.

З метою запобігання і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання сучасної держави, з огляду на відповідні функції і завдання, потягає 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, запобігання інформаційним конфліктам та оперативне їх подолання. Враховуючи активну глобалізацію інформаційно-комунікаційних мереж, важливо не тільки державам, а й міжнародним організаціям долучатися до співпраці у напрямі протидії різноманітним видам інформаційної агресії.

3. Проблеми і напрями удосконалення нормативно-правової складової механізму забезпечення інформаційної безпеки української держави

Функціонування механізму забезпечення інформаційної безпеки має відповідну правову основу, що складається з нормативно-правових актів різної юридичної сили та різних напрямів регулювання інформаційної сфери (захист інформації, персональні дані, технічний аспект інформаційної безпеки, кібербезпека тощо). Зазначена нормативна база є елементом механізму забезпечення інформаційної безпеки, його складовою, яка:

1. Визначає організаційну будову механізму забезпечення інформаційної безпеки.
2. Регулює діяльність суб'єктів забезпечення інформаційної безпеки в державі, встановлює їх права, обов'язки та форми відповідальності.
3. Установлює напрями забезпечення інформаційної безпеки, принципи та засоби такого забезпечення.
4. Закладає засади державної політики у сфері інформаційної безпеки.
5. Виступає ознакою законності функціонування механізму забезпечення інформаційної безпеки.
6. Скеровує подальший розвиток та вдосконалення механізму забезпечення інформаційної безпеки в цілому та ІКТ зокрема.

Значною мірою нормативно-правову основу забезпечення інформаційної безпеки нами проаналізували в попередніх розділах дослідження. Її ми розглянули на міжнародному рівні та рівні національного законодавства України.

Для систематизації актів у сфері забезпечення інформаційної безпеки деякі вчені використовують метод структурування, відповідно до якого виділяються такі рівні системи законодавства:

а) при вертикальному структуруванні – рівень міжнародно-правових актів і рівень нормативно-правових актів України. У рамках міжнародно-правових актів, у свою чергу, можна виділити окремий блок – правові акти

Європейського Союзу. Нормативно-правові акти України можна поділити, відповідно, на рівень: конституційного регулювання, законів України, указів Президента України, постанов і розпоряджень Кабінету Міністрів України;

б) при горизонтальному структуруванні поділ норм відбувається відповідно за галузями, тобто законодавство в галузі інформаційної безпеки включає в себе норми конституційного, кримінального, цивільного, адміністративного, трудового та інших галузей законодавства [229, с. 73–76].

Основними недоліками нормативно-правової складової механізму забезпечення інформаційної безпеки держави є такі.

Термінологічна невизначеність, яка полягає у відсутності базових дефініцій, насамперед у стратегічних та доктринальних нормативно-правових актах, що ускладнює розуміння державної політики у сфері забезпечення інформаційної безпеки і знижує ефективність реалізації механізму такого забезпечення. Наприклад, аналіз Доктрини інформаційної безпеки України, який був проведений у попередньому підрозділі цієї роботи, засвідчив ігнорування законодавцем необхідності розкриття вживаних ним нових і спірних понять («інформаційна експансія», «інформаційне домінування», «спеціальні інформаційні операції»).

Слід зазначити, що вивчення наукових праць з питань інформаційної безпеки дає змогу говорити про збіг поглядів учених щодо серйозності проблеми термінологічної невизначеності інформаційного законодавства України.

Так, Т. Ткачук у своєму дисертаційному дослідженні наголошує: «Термінологія, що застосовується у сфері забезпечення інформаційної безпеки, хибує на брак єдності, неоднозначні тлумачення, а то й узагалі відсутні визначення багатьох понять, у тому числі ключових. Усе це створює серйозні перешкоди як для правотворчої діяльності в інформаційній сфері, так і для правозастосовної, а також зайвий раз засвідчує відсутність системності у розв’язанні вказаних проблем». При цьому автор зазначає, що до теперішнього часу немає законодавчого визначення такого базового термін як

«інформаційна безпека» чи «безпека інформації», хоча самі ці термінологічні сполучення вживаються в деяких законах [611, с. 302].

Акцентовано увагу, що чинне законодавство України не містить відповідного розгорнутого тлумачення поняття «інформаційна безпека держави», проте нормативні акти, які торкаються питань інформаційної безпеки, закономірно розглядають її в контексті більш загального поняття національної безпеки. Такий підхід значно обмежує та звужує зміст категорії «інформаційна безпека держави», позаяк виключно інформаційне середовище слугує каналом реалізації загроз національній безпеці в усіх сферах діяльності держави. Інформаційну безпеку України визначено як стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їхніх суб'єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері. В основу даного підходу покладено принцип, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища. А для цього захищати національні інтереси й цінності, виходячи з виявлення загроз і намірів противника, замало. Даний підхід передбачає також протидію та активні контрзаходи у процесі забезпечення інформаційної безпеки України.

Ми погоджуємося з наявністю проблеми відсутності ключових понять у сфері забезпечення інформаційної безпеки, зокрема, як було нами встановлено в українському законодавстві немає визначення поняття «забезпечення інформаційної безпеки», «загроза в інформаційній сфері». Однак варто уточнити, що зміст терміна «інформаційна безпека» закріплено в чинному законі та в декількох інших нормативних документах.

Згідно зі ст. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537-V, 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 розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [244].

В Угоді про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав – учасниць СНД від 11.09.1998 р. інформаційна безпека визначається як стан захищеності інформаційного середовища суспільства, що забезпечує його (середовище) формування, використання і розвиток в інтересах громадян, організацій, держави (абз. 18 ст. 1) [471].

Крім того, у Законі України «Про телекомунікації» від 18.11.2003 р. № 1280-IV розкривається зміст поняття інформаційної безпеки телекомунікаційних мереж. Дефініція «безпека інформації» закріплена в Угоді про співробітництво і взаємодію між Адміністрацією Державної служби спеціального зв'язку та захисту інформації України і Службою інформації та безпеки Республіки Молдова від 23.12.2016 р.

Неузгодженість нормативно-правових актів між собою зумовлена частим неврахуванням положень чинного законодавства при розробленні нового. Зокрема, яскраво засвідчують цю проблему різні підходи до визначення загроз інформаційної сфери, що містяться у Стратегії національної безпеки України від 2015 р. та Доктрині інформаційної безпеки України.

Несистемність законодавства у сфері інформаційної безпеки означає велику кількість нормативно-правових актів різної юридичної сили, які фрагментарно врегульовують суспільні відносити у сфері інформаційної безпеки та її забезпечення.

Експерти також наголошують на несистемності вітчизняної правової політики в інформаційній сфері. Значна кількість законодавчих актів ухвалюється з метою вирішення певних тактичних завдань, задоволення

кланових інтересів, часто без урахування стратегічних орієнтирів та реальних українських умов. Показовим з цієї точки зору є спроби перегляду законодавства щодо дозволу рекламування алкоголю та тютюну [211].

Застарілість значної частини законодавства та відсутність динаміки законодавчої діяльності в цьому аспекті, прикладами невідповідності умовам часу є Закон України «Про друковані засоби масової інформації (пресу) в Україні» 1993 р., Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» від 08.10.1997 р. № 1126 (в редакції від 2011 р.) тощо. Повільна адаптація національного законодавства до європейських стандартів та світових тенденцій у сфері інформаційної безпеки в цілому підтверджується, серед іншого, і відсутністю в українському законодавстві юридичного механізму реалізації права на забуття в Інтернеті. На відміну від РФ, яка запровадила такий механізм доволі оперативно – через два роки після прийняття Судом ЄС Рішення Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014 р.).

Проте глибинною проблемою нормативно-правової складової механізму забезпечення інформаційної безпеки держави є *невиконання вимог законодавства* всіма суб'єктами механізму, передусім органами державної влади всіх рівнів. У цьому аспекті на увагу заслуговують висновки експертизи інформаційного законодавства України, проведеного представниками ОБСЄ, про те, що рівень правової культури громадян України змушує розглядати ситуацію із зовсім іншого боку, порівняно з країнами Європейського Союзу. Недостатньо ретельне та чітке дотримання законодавства складає найважливішу проблему правової політики держави, зокрема це стосується й інформаційної сфери. Показовим є намагання певних сил створити новітні зони недоторканості, сформувати потужні системи пільг та переваг, що діють поза законодавством. Забезпечення єдності та невідворотності дії Закону є провідним завданням держави [109, с. 5–7].

З огляду на означені недоліки нормативно-правової складової механізму забезпечення інформаційної безпеки держави, головним напрямом

її удосконалення видається систематизація нормативно-правових актів у цій сфері. Вона дасть можливість вирішити проблему термінологічної неузгодженості, усунути протиріччя між актами різної юридичної сили та забезпечить єдність нормативно-правового поля. Нині в наукових колах триває дискусія щодо форми такої систематизації: кодифікація чи інкорпорація.

Ідея кодифікації інформаційного законодавства на державному рівні обговорюється протягом останніх дев'ятнадцяти років, зокрема ще в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» наголошувалося на необхідності прийнятти Інформаційний кодекс України. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 06.02.2007 р. № 537-V також передбачає розроблення такого кодексу.

Отже, прихильники кодифікації акцентують увагу на закріпленні норми щодо прийняття Інформаційного кодексу в чинному законі та дискутують щодо його структури та змістовних аспектів. Так, можна виділити такі підходи до концепції Інформаційного кодексу України.

Перший підхід був запропонований і розроблявся Державним комітетом телебачення і радіомовлення України. Він ґрунтувався на тому, що в основу Інформаційного кодексу мали бути покладені «Концепція національної інформаційної політики», а також змінений відповідно до сучасних вимог суспільного розвитку Закон України «Про інформацію» [486]. Враховуючи стрімкий розвиток ІКТ, зміну політичних умов та суттєве збільшення нормативної бази, порівняно з часом, коли цей підхід пропонувався, а також те, що Закон про Концепцію національної інформаційної політики так і не було прийнято, зазначений підхід зараз видається вузьким та не актуальним.

Другий підхід запропонував сам законодавець у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 06.02.2007 р. № 537-V, зокрема в ньому закріплено перелік розділів, які мають бути враховані при розробленні Інформаційного кодексу, а саме – розділ про засади електронної торгівлі, правову охорону прав на зміст комп'ютерних програм, удосконалення захисту прав інтелектуальної власності, в тому числі авторського права при розміщенні та використанні творів у мережі Інтернет, про охорону баз даних, дистанційне навчання, телемедицину, надання органами державної влади та органами місцевого самоврядування юридичним та фізичним особам інформаційних послуг з використанням мережі Інтернет, комерційну таємницю тощо [244].

Третій підхід розробила група фахівців Інституту держави і права імені В.М. Корецького. На їхню думку, Інформаційний кодекс має складатися із чотирьох частин: 1) базова (загальна), яка містила б системо-утворювальні норми, що регулюють базові відносини у сфері інформації та інформатизації; 2) галузева частина, яка має регулювати інформаційні відносини в окремих сферах життя особи, держави, суспільства; 3) третя частина має містити видові норми і регулювати інформаційні відносини суб'єктів у сфері створення, пошуку, одержання, використання, зберігання та поширення окремих видів (категорій) інформаційної продукції або в окремих складових інформаційного процесу; 4) частина щодо спеціальних норм, яка регулює відносини стосовно створення і використання інформаційних технологій та телекомунікаційних систем [519].

Запропонована структура Інформаційного кодексу, на наш погляд, є дещо заплутаною й може викликати труднощі як на стадії його розроблення кодексу, так і в процесі застосування. Наприклад, не є зрозумілим співвідношення другої (галузевої) частини, третьої частини з видовими нормами та частини щодо спеціальних норм. По суті, всі три частини, не дивлячись на різні назви, містять спеціальні норми, оскільки стосуються окремих сфер суспільних відносин. При цьому положення другої частини

(галузевої), яка стосується регулювання інформаційних відносин в окремих сферах життя особи, суспільства і держави, змістовно охоплює і положення третьої частини стосовно регулювання відносин суб'єктів при реалізації права на інформацію. Адже особа, суспільство і держава є окремими суб'єктами права на інформацію, і реалізація цього права породжує виникнення інформаційних відносин у сферах життя цих суб'єктів.

На наш погляд, якщо говорити про кодифікацію інформаційного законодавства, то доцільно розробити Кодекс про інформацію та інформаційну безпеку України, обов'язковими розділами якого мають бути: загальні положення (в якому 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.

Четвертий підхід щодо кодифікації запропонованували Урядова комісія з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади у проекті «Концепції реформування законодавства України у сфері суспільних інформаційних відносин». Передбачалося здійснювати систематизацію інформаційного законодавства в три етапи:

1) інкорпорація законодавства – визначення ієрархічної системи та структури інформаційного законодавства на рівні правової доктрини;

2) виокремлення в системі законодавства галузі та закріплення її у Зводі законів України як розділу «Інформаційне законодавство»;

3) кодифікація – розроблення і прийняття Верховною Радою України такого нормативного акта як Кодекс України про інформацію.

Систематизація інформаційного законодавства, на думку розробників, мала проводитися методом агрегації – удосконалення окремих правових норм чи створення нових міжгалузевих правових інститутів не повинно було

порушувати цілісність та призначення інформаційного законодавства, а поліпшувати його дієвість у цілому [322].

На сьогодні інкорпорація інформаційного законодавства через розроблення Зводу законів України з розділом «Інформаційне законодавство» нам видається недоцільною з огляду на таке. По-перше, легальна інкорпорація не властива українській законодавчій традиції. По-друге, в умовах «турборежиму» роботи парламенту та несистемного збільшення законодавчого масиву постійне забезпечення актуальності такого Зводу законів видається просто неможливим. По-третє, в легальній інкорпорації шляхом видання відповідних Зводів законів просто відпала потреба, оскільки цей результат інкорпорації замінюється можливостями інкорпорації споживачем правової інформації із застосуванням здобутків інформатики: комп'ютерних інформаційно-аналітичних систем, у тому числі із застосуванням Інтернету. Тобто кожна зацікавлена особа самостійно може за заданими нею критеріями здійснити для своїх потреб інкорпорацію інформаційного законодавства. Саме з цієї причини у більшості країн відмовилися від легальної інкорпорації через видання Зводів законів [641, с. 47–49].

Важливо звернути увагу, що сьогодні деякі законодавці згадують ідею інкорпорації законодавства у сфері інформаційної безпеки та використовують цей термін для обґрунтування необхідності прийняття по суті нових законів. Так, йдеться про презентацію концепції «Закону про медіа» (проект № 2693), де його автори наголошували, що це спроба саме інкорпорації законодавства про медіа.

Водночас у пояснювальній записці до проекту цього закону його ж автори говорять про застарілість законодавства у сфері ЗМІ, пропонують запровадити нові форми регулювання та види медіа, внести зміни до 12 законів та ще 5 скасувати.

Таким чином, враховуючи те, що інкорпорація є формою систематизації законодавства, яка полягає в зовнішньому впорядкуванні вже

наявних нормативно-правових актів без зміни змісту норм права, а інкорпорація інформаційного законодавства покликана його упорядкувати за одним чи кількома критеріями без зміни змісту [519] то вказаний проект Закону про медіа № 2693 ніяк не підпадає під інкорпорацію законодавства. Він є проектом поточного закону, який спрямований на фрагментарне врегулювання сфери медіа.

Варто зазначити, що обґрунтування необхідності прийняття нових законів потребами систематизації відповідної сфери законодавства є дуже поширеним прийомом серед їх розробників, але в результаті прийняття законопроектів систематизації не відбувається. Такі закони, безумовно, оновлюють та розвивають відповідну галузь, можуть бути покладені в основу подальшої роботи з консолідації або кодифікації актів. У зв'язку з цим, багато дослідників інформаційної безпеки пропонують, у першу чергу, розробити спеціальні закони щодо регулювання окремих аспектів забезпечення інформаційної безпеки.

Так, О. Ярема зазначає, що для інституційного розвитку правового забезпечення інформаційної безпеки необхідно прийняти закон «Про інформаційну безпеку» [682, с. 244−252].

Т. Ткачук пропонує свій проект Закону «Про інформаційну безпеку» основу для інших нормативних актів у сфері забезпечення інформаційної безпеки, а також керівних документів державної політики в інформаційній сфері та процесу стратегічного планування забезпечення інформаційної безпеки України. Автор наголошує на тому, що нинітакий закон має чітко визначати сферу правового регулювання, засадничі принципи забезпечення інформаційної безпеки, основні загрози правам та інтересам людини, суспільства й держави, котрі цим законом охороняються, зміст і пріоритетні напрями державної політики у цій сфері та засоби її реалізації, перелік та компетенцію органів державної влади, що забезпечують різні складові інформаційної безпеки [611, с. 332−333].

У структурі цього проекту передбачається сім розділів, які присвячені загальним положенням, засадам функціонування державної системи забезпечення інформаційної безпеки, забезпеченню безпеки інформації з обмеженим доступом, захисту відкритої (загальнодоступної) інформації від протиправних маніпуляцій з нею, захисту від недостовірної та шкідливої інформації, негативного інформаційно-психологічного впливу, протидії інформаційному екстремізму, видам відповідальності за правопорушення у сфері інформаційної безпеки.

Особливу увагу слід приділити пропозиції Т. Ткачука закріпити в законі про інформаційну безпеку розділ щодо засад протидії інформаційному екстремізму. Так, автор пропонує визначити вичерпний перелік чітких критеріїв, за якими інформація визнається екстремістською (що загрожує конституційному ладу України), зокрема, умисел суб'єкта її розповсюдження, конкретні умови оприлюднення тощо. Підкреслюються важливість чіткого формулювання вказаних критеріїв, аби уникнути багатозначності їх тлумачення, що може призвести до фактичного запровадження цензури. Належність інформації до екстремістської має встановлюватися спеціальною експертизою, питання щодо організації та проведення якої теж мають бути врегульовані цим законом [611, с. 340].

Ми не можемо погодитися з такою пропозицію з огляду на такі аргументи. По-перше, сумніви викликає доцільність використання самого поняття «інформаційний екстремізм», оскільки воно не має теоретичного підґрунтя, хоча й використовується у соціологічних дослідженнях та ЗМІ. На наш погляд, є хибним виділяти вид екстремізму за критерієм способу здійснення екстремістських дій, оскільки його види визначаються на підставі характеру екстремістської ідеології (політичний, релігійний, націоналістичний, молодіжний, екологічний). Тобто здійснення екстремістської діяльності з використанням інформаційних ресурсів та засобів інформаційного впливу є проявом не «інформаційного екстремізму», а певного виду екстремізму (залежно від спрямованості і цілей екстремістської

діяльності) в інформаційній сфері. Наприклад, пропаганда національної переваги в соціальних мережах є проявом націоналістичного екстремізму, а не інформаційного.

По-друге, хоча в законодавстві України немає визначення екстремізму, у світі сформувалося загальне його розуміння, яке не може суттєво відрізнятися від офіційних визначень, що містяться в кримінальних законах держав.

Так, під екстремізмом слід розуміти прихильність в ідеології та політиці до крайніх поглядів і засобів у досягненні певних цілей. Він виступає проти існуючих громад, структур та інституцій, намагаючись підірвати їх стабільність, розхитати та ліквідувати їх заради своїх цілей (як правило, силовими засобами) [226, с. 191]. Таким чином, екстремістська діяльність завжди здійснюється у формі кримінально караного діяння. Варто зазначити, що розробник пропозиції, яку ми аналізуємо, екстремістською визнає таку інформацію, яка загрожує конституційному ладу України.

По-третє, посягання на конституційний лад України є діянням найвищого ступеня небезпеки і, відповідно, склад цього злочину визначається у Кримінальному кодексі України (КК України), зокрема у ст. 109 КК України «Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади». Так само, як і інші прояви екстремістської діяльності: ст. 110 КК України «Посягання на територіальну цілісність і недоторканність України», ст. 161 КК України «Порушення рівноправності громадян залежно від їх расової, національної належності або ставлення до релігії», ст. 178 «Пошкодження релігійних споруд чи культових будинків», інші злочини проти свободи віросповідання (ст. 179–181 КК України), ст. 260 КК України «Створення не передбачених законом воєнізованих або збройних формувань», ст. 257 «Бандитизм», ст. 258 «Терористичний акт», інші злочини, пов’язані з тероризмом (ст. 258-1–258-5), ст. 300 КК України «Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну

нетерпимість та дискримінацію» та низка інших злочинів, якщо вони вчинюються на ґрунті расової, національної чи релігійної ворожнечі або розбрату тощо, ст. 436 «Пропаганда війни», ст. 436-1 «Виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів» та інші. Крім того, вчинення злочину на ґрунті расової, національної, релігійної ворожнечі чи розбрату або на ґрунті статевої приналежності є обтяжуючою обставиною.

По-четверте, згідно зі ст. 3 КК України злочинність діяння, а також його караність та інші кримінально-правові наслідки визначаються тільки цим Кодексом. Закони України про кримінальну відповідальність, прийняті після набрання чинності цим Кодексом, включаються до нього після набрання ними чинності [337].

Таким чином, немає необхідності встановлювати в законі про інформаційну безпеку ознаки екстремістських діянь і тим більше відповідальність за них. У протилежному випадку, буде мати місце або дублювання законодавчих положень (у законі та КК України), або порушення вимог КК України.

По-п’яте, у питанні криміналізації екстремістської діяльності (закріплення в кодексі окремих складів злочинів) ми поділяємо думку В. Климчука про те, що чинна в Україні нормативно-правова база є достатньою для протидії екстремістській діяльності, а в разі введення в КК України відповідальності за екстремістські діяння такі норми утворюватимуть небажану конкуренцію з положеннями антитерористичного законодавства України та відповідними статтями КК України [293].

В аспекті криміналізації діянь, спрямованих на спричинення негативного інформаційного впливу на свідомість громадян України, увагу слід звернути на пропозиції Міністерства культури, молоді та спорту України щодо запровадження адміністративної відповідальності за розповсюдження дезінформації, порушення правил спростування, надання відповіді та вимог

прозорості та кримінальної відповідальності за системне та умисне масове розповсюдження дезінформації.

Так, законопроектом передбачається кримінальне покарання у вигляді штрафу та виправних робіт за систематичне умисне масове розповсюдження завідомо недостовірних повідомлень про факти, події або явища, що становить загрозу національній безпеці, громадській безпеці, територіальній цілісності, суверенітету, обороноздатності України, праву українського народу на самовизначення, життя та здоров'я громадян, стану довкілля в період відсутності повного контролю України за державним кордоном України [503, 504].

Таке формулювання складу злочину, на наш погляд, є невдалим та складним для кваліфікації. Зокрема, великі питання викликає суб'єктивна сторона цього складу злочину – як встановлювати умисел суб'єкта на масове поширення, які ознаки можуть його підтвердити? Не зрозуміло, як визначати «завідомість» недостовірних повідомлень, у яких випадках розповсюдження буде вважатися масовим.

Також проблеми на практиці викличе і необхідність у кожній справі визначати конкретну загрозу безпеці, територіальній цілісності, суверенітету, обороноздатності тощо та якимось чином установлювати причинно-наслідковий зв'язок між завідомо недостовірним повідомленням та такою загрозою. Враховуючи те, що законодавець у різних нормативно-правових актах застосовує різні підходи до визначення загроз, а також те, що неможливо передбачити всі можливі варіанти загроз у єдиному переліку, правильна кваліфікація цього складу є маловірогідною.

Кваліфікованим складом цього злочину є його вчинення з використанням комп'ютерних програм, призначених для автоматичного масового поширення інформації (ботів), або спеціально організованої системи (групи) облікових записів чи користувачів інформаційних послуг або засобів умисного фальшування (підробки) джерел інформації [503, 504]. У цьому випадку простіше буде довести масовість поширення (використання ботів,

груп облікових засобів), але описані вище труднощі з оціночними поняттями залишаються.

Розробники цих пропозицій також установлюють особливості призначення покарання за вказані склади злочинів, а саме – запровадження обов'язкового касаційного перегляду та обов'язкового звернення касаційного суду за попереднім висновком до ЄСПЛ. Така процедура анонсується як захист від зловживань і при цьому не уточнюється, від чиїх зловживань (слідчого, суду чи іншого суб'єкта кримінального процесу), тоді виникає питання, чи не буде це дискримінацією осіб, засуджених за вчинення інших злочинів, адже їх мправу вестимуть ті ж самі суб'єкти кримінального процесу, але без особливої процедури щодо захисту від зловживань?

Сам процесуальний запобіжник у вигляді обов'язкового звернення касаційного суду за попереднім висновком до ЄСПЛ викликає не менше питань. По-перше, ЄСПЛ надає консультативні висновки з принципових питань, які стосуються тлумачення або застосування прав і свобод, визначених Конвенцією або протоколами до неї, тобто при наданні висновку ЄСПЛ аналізує Конвенцію і не буде заглиблюватися в деталі кримінальної справи і тим більше проводити моніторинг дій слідчого чи суду на предмет наявності зловживань. По-друге, ЄСПЛ точно не буде надавати консультативні висновки з кожної справи. По-третє, такі висновки не є обов'язковими (ст. 5 Протоколу 16 до Конвенції). По-четверте, для отримання консультативного висновку касаційний суд повинен буде зробити відповідний запит до ЄСПЛ, обґрунтувати необхідність такого висновку, а ЄСПЛ вправі відмовити у задоволенні такого запиту. Враховуючи відсутність у Протоколі 16 до Конвенції критеріїв прийнятності таких запитів, можна спрогнозувати численні відмови.

У цілому залучення ЄСПЛ до кожної справи про притягнення до відповідальності за вказані вище злочини є невиправданим перекладанням на нього функцій національних судів. Тому ми вважаємо, що цей процесуальний запобіжник просто не працюватиме. При цьому видається не коректним

пропонувати законодавчий механізм, який передбачає обов'язкову участь ЄСПЛ, без попередніх консультацій з Європейським Судом та без його попередньої згоди щодо можливості впровадження такого механізму.

З іншого боку, у цій законодавчій пропозиції зазначається про обов'язкове звернення касаційного суду за попереднім висновком до ЄСПЛ, а не про обов'язкове отримання попереднього висновку ЄСПЛ. Тобто у випадку відмови ЄСПЛ у наданні такого висновку касаційний суд формально виконає свій обов'язок і продовжить розгляд справи. І тоді просто втрачається сенс такої процедури, оскільки жодного захисту від зловживань вона не забезпечить.

Отже, розглянуті пропозиції Міністерства культури, молоді та спорту України щодо доповнення КК України новими складами злочинів у сфері дезінформації, на нашу думку, є небезпечними (містять багато ризиків для зловживань, переслідувань, помсти та цензури) і не можуть бути прийняті парламентом.

У контексті вдосконалення механізмів протидії поширенню недостовірної інформації важливим є досвід ЄС щодо регулювання відносин інтернет-користувачів з компанією Google Ink. в аспекті захисту персональних даних. Так, у 2014 р. Велика Палата Суду ЄС прийняла Рішення за запитом Національного Суду Іспанії у справі Google Spain SL, Google Inc.v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Зазначене рішення стосувалося тлумачення Директиви ЄС 95/46/ЄС (Директива про захист персональних даних) щодо права на забуття в Інтернеті (англ. *right to be forgotten*) та стало підставою для розроблення відповідного механізму реалізації для громадян ЄС. Розглянемо деталі цієї справи. У 1998 році іспанська газета La Vanguardia опублікувала, на замовлення Міністерства праці та соціальних справ Іспанії, в своєму друкованому виданні два оголошення про примусовий продаж майна, задля погашення боргів із соціального забезпечення. Пізніше в Інтернеті була розміщено електрону версію цього випуску газети. Одне з оголошень стосувалося майна

громадянина Іспанії Маріо Костеха Гонсалеса, в якому прямо зазначалося його ім'я.

У листопаді 2009 року Маріо Костех Гонсалес зв'язався з газетою і поскаржився, що в пошуковій системі Google його ім'я прив'язане до посилань на зазначені оголошення. Він попросив видалити дані, що відносяться до нього, стверджуючи, що примусовий продаж мав місце багато років тому і ця інформація більше не актуальна. Газета відповіла, що видаляти його дані недоцільно, оскільки публікація була достовірною, законною і зроблена на замовлення іспанського Міністерства праці та соціальних справ.

У зв'язку з цим, Маріо Костех Гонсалес звернувся до Google Spain в лютому 2010 року з проханням видалити посилання на пов'язане з ним оголошення. Google Spain, вважаючи, що відповідальним органом у цій справі є Google Inc., офіс якого знаходиться в Каліфорнії (США), перенаправила запит йому.

Згодом Маріо Костех Гонсалес подав скаргу в Іспанське агентство із захисту даних (Agencia Española de Protección de Datos, AEPD) з вимогою, щоб газета видалила ці дані і щоб Google Spain або Google Inc. були зобов'язані видалити посилання на зазначені дані. Свою скаргу заявник обґрунтовував правом на захист приватного і сімейного життя (ст. 8 Конвенції про захист прав людини і основоположних свобод) і правом на захист персональних даних. 30 липня 2010 року директор AEPD відхилив скаргу на газету, але залишив у силі скаргу на Google Spain і Google Inc., закликавши їх видалити посилання, на які надійшли скарги, і зробити доступ до даних неможливим.

У свою чергу, Google Spain і Google Inc. подали окремі позови до Національного Суду Іспанії на рішення Іспанське агентство із захисту даних. Їх правова позиція засновувалася на таких твердженнях:

– Google Inc. не входить у сферу дії директиви ЄС 95/46/ЄС, і її дочірня компанія Google Spain не несе відповідальності за пошукову систему;

– у функції пошуку не було обробки персональних даних;

– навіть якби вони оброблялися, ні Google Inc., ні Google Spain не могли розглядатися як контролер даних;

– у будь-якому випадку суб'єкт даних (заявник) не мав права на видалення законно опублікованих матеріалів [37].

З огляду на необхідність тлумачення Директиви ЄС 95/46/ЄС, Національний Суд Іспанії звернувся до Суду ЄС за попереднім рішенням щодо таких питань:

– територіальна сфера дії Директиви;

– чи встановлює Директива так зване право бути забутим;

– правове становище постачальника послуг інтернет-пошуку відповідно до зазначеної Директиви, особливо з точки зору її матеріального охоплення і того, чи може пошукова система розглядатися контролер даних.

Суд ЄС ухвалив, що оператор пошукової системи в Інтернеті несе відповідальність за оброблення персональних даних, які він виконує, що з'являються на веб-сторінках, опублікованих третіми сторонами, він є контролером даних.

Що стосується територіального охоплення Директиви, Суд зазначив, що Google Spain є дочірньою компанією Google Inc. на території Іспанії і, отже, «установою» в значенні Директиви. Суд відхилив аргумент Google Inc. про те, що вона не здійснювала оброблення даних в Іспанії, ухваливши, що просування і продаж рекламного місця її дочірньою компанією Google Spain було достатнім для того, щоб становити оброблення за змістом Директиви. В іншому випадку був би можливим підрив ефективності Директиви й основних прав і свобод людини, які Директива прагне забезпечити. Таким чином, Суд дійшов висновку, що Google Inc. і Google Spain повинні розглядатися як єдина економічна одиниця [36].

Суд вказав, що фізичні особи за певних умов мають право звертатись із запитами до пошукових систем про видалення неточної, недоречної або застарілої інформації, яка містить персональні дані про них. Проте це правило не є універсальним, а право на забуття – абсолютним: рішення в аналогічних

справах будуть виноситися на основі конкретних обставин, щоб виключити їх протиріччя з фундаментальними правами людини (свободи слова та друку) – принцип *a case-by-case assessment*. У цьому рішенні розглядається право на недоторканність приватного життя та право на захист персональних даних у контексті законних інтересів громадськості щодо доступу до інформації.

Внаслідок вказаного Рішення Google опублікувала онлайн-форму, яку громадяни ЄС можуть використовувати для запиту щодо видалення посилань з результатів пошуку, якщо пов'язані дані «неадекватні, неактуальні або більше не актуальні, або є надмірними для цілей, щодо яких вони були оброблені» [36] 31 травня 2014 року, в перший день служби, Google отримала понадбільше 12 000 запитів від людей, які просили компанію видалити певні посилання про них з результатів пошуку [75].

Разом з тим, 19 червня 2015 року Google оголосила, що видалятиме посилання на nonconsensual порнографію («порнопомста») за запитом. Коментатори відзначили, що це не те ж саме, що реалізація «права бути забутим», оскільки в компанії вже є політика, що стосується конфіденційних особистих даних, таких як номери соціального страхування і номери кредитних карт. Однак група захисту прав споживачів Consumer Watchdog згодом закликала Google розширити право бути забутим для користувачів зі США, подавши скаргу до Федеральної торгової комісії [28].

Прикметно, що в даний час подібні вимоги про видалення згадок імені та інших персональних даних з пошукових систем відповідно до законодавства ЄС задовольняються компанією Google тільки на європейських піддоменах, таких як Google.co.uk або Google.fr, але не на Google.com. Згідно із заявою голови ради директорів Google, така політика пошукової системи залишиться незмінною до нового судового рішення або прийняття відповідного закону [83]. Таким чином, для реалізації права на забуття в Інтернеті особа має звернутися з відповідним запитом до оператора пошукової системи, а у випадку відмови – до національного органу, до повноважень якого входить розгляд питань щодо захисту персональних даних, або до суду. Проте

для вирішення такого питання в адміністративному порядку необхідна закріплена нормативно-правовим актом процедура, якої в українському законодавстві поки немає. Отже, громадяни України позбавлені права на видалення з пошукових систем посилань на небажану для них інформацію, що є суттєвим недоліком механізму забезпечення інформаційної безпеки особи.

У зв'язку з цим пропонуємо внести в законодавство України зміни і доповнення щодо закріплення порядку реалізації права на забуття в Інтернеті, ключовими положеннями якого має бути:

1. Закріплення права особи (суб'єкта даних) на негайне видалення контролером (оператором пошукової системи) небажаної для неї інформації, що містить її персональні дані та підпадає під визначені законом критерії.

2. Види інформації, які підлягають негайному видаленню, зокрема це неактуальна, неправдива, незаконно поширювана (оброблена) інформація, а також інформація, яка втратила значення для заявника внаслідок певних обставин або відпала потреба, для якої вона була опрацьована. Обов'язково потрібно чітко розкрити критерії кожного виду інформації та узгодити їх з переліком, наведеним у ст.17 GDPR. Передбачити окремі винятки (наприклад, щодо інформації про не зняту та непогашену судимість).

3. Форма запиту до контролера даних (дані заявника, відомості про сайт та інформацію, посилання на яку має бути припинено, зазначення підстав для такого припинення та згода на оброблення персональних даних заявника).

4. Строки та особливості розгляду контролером даних такого запиту.

5. Дії контролера даних за наслідками розгляду запиту (видалення посилань на інформацію, зазначену в запиті, повідомлення про це заявника чи направлення мотивованої відмови).

6. Оскарження відмови у судовому порядку (строки звернення до суду, підсудність спору, особливості доказування).

7. Оскарження відмови в адміністративному порядку, для чого слід визначити уповноважений орган, установити його компетенцію та порядок розгляду оскарження відмови контролера видалити посилання на інформацію.

8. Визначити взаємодію уповноваженого органу з оператором пошукової системи (контролером даних), органами державної влади та місцевого самоврядування й заявником.

9. Установити відповідальність оператора пошукової системи (контролером даних) за невиконання законних вимог уповноваженого органу, а також відповідальність інших суб'єктів у даному правовідношенні.

Що стосується уповноваженого органу з нагляду та контролю за реалізацією права на забуття в Інтернеті, то ним має бути національний орган із захисту персональних даних. На сьогодні контроль за дотриманням прав людини і громадянина та вимог законодавства у сфері захисту персональних даних здійснює Департамент у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини.

На наш погляд, аналіз визначених у законодавстві завдань та повноважень цього Департаменту свідчить про його юридичну та технічну неможливість оперативно й ефективно реагувати на випадки порушення оброблення персональних даних та поновлення порушених прав.

Як випливає із звіту діяльності цього Департаменту протягом 2018 р. ним було проведено 41 перевірку, з яких 31 планова, 6 позапланових, 4 моніторингових візити [319]. При цьому 33 перевірки були проведені у державних органах та органах місцевого самоврядування. Наведені статистичні дані свідчать про певну формальність контролю за дотриманням прав у сфері захисту персональних даних та повну відсутність участі цього Департаменту у вирішення ситуацій, в яких внаслідок використання персональних даних зачіпається честь, гідність чи ділова репутація особи (дифамація), здійснюється булінг в Інтернеті (особливо актуальна проблема для неповнолітніх, яка часто закінчується самогубством), поширюється незаконно здобута інформація тощо. Такі ситуації виникають щодня й потребують негайного вирішення. Зараз особа, яка зіткнулася з однією з наведених форм порушення права на персональні дані може звернутися до суду або, якщо наявні ознаки злочину, до правоохоронних органів. Однак, з

огляду на українські реалії судовий розгляд може тривати роками, а заява про відповідний злочин може взагалі не бути внесена до Єдиного реєстру досудового розслідування. За таких умов небажана або незаконно поширювана інформація тривалий час залишатиметься у відкритому доступі або взагалі не буде видалена.

У зв'язку з цим ми пропонуємо створити національний, колегіальний орган із широкими повноваженнями та технічними можливостями по захисту персональних даних за зразком Національної комісії з інформатизації та свободи Франції (CNIL). Обґрунтування зазначеної пропозиції більш детально викладено в наступному підрозділі.

4. Інституційна складова забезпечення інформаційної безпеки української держави та її удосконалення в сучасних умовах

Забезпечення інформаційної безпеки держави здійснюються уповноваженими суб’єктами, які в сукупності становлять інституційну складову його механізму. У науковій літературі інституціональний аспект забезпечення інформаційної безпеки розглядається по-різному: як система, механізм, суб’єктний рівень чи складова.

Наприклад, Б. Кормич розглядає інституціональний механізм інформаційної безпеки як ієрархічну сукупність органів різних гілок влади та різних рівнів, які в межах своєї компетенції вирішують конкретні завдання з формування та реалізації політики інформаційної безпеки. До складу цього механізму автор відносить такі державні органи та посади: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні сили України, Служба безпеки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України [325, с. 142].

Автор зазначає, що механізм інформаційної безпеки повинен включати цілу низку різних владних інститутів, які тим або іншим чином здійснюють узгоджену комплексну діяльність в інформаційній сфері. Разом з тим слід відмітити, що було б абсолютно помилковим зводити цей механізм виключно до системи державного управління [325].

На думку автора, інституціональний механізм представляє собою складну багаторівневу систему, яка, з одного боку, об'єднується особливою загальною функціональною спрямованістю, а з іншого, розділяється специфічними особливостями, пов'язаними з рівнем компетенції і характером відповідних цілей. Власне кажучи, інституціональним суб'єктам кожного з рівнів відповідає окрема специфічна функція - функція формування або

функція реалізації політики інформаційної безпеки. Функція формування державної політики інформаційної безпеки включає в себе діяльність компетентних органів держави щодо встановлення стратегічних цілей, завдань, основних принципів та напрямів державної діяльності в цій сфері, розробку концепцій та рішень загальнодержавного довгострокового значення. Функція реалізації політики інформаційної безпеки спрямована на досягнення тактичних та оперативних цілей, забезпечує вирішення конкретних завдань, застосування відповідних засобів, форм та методів державного впливу на суспільні відносини в цій сфері [325].

Таким чином, основні цілі, які переслідує держава, як суб'єкт політики інформаційної безпеки та головні принципи її проведення повинні ґрунтуватися на інтегрованій політичній волі народу як джерела державної влади. А процес інтеграції і реалізації відповідної політичної волі народу повинен розкриватися в інституціональній (організаційній) структурі певного владного механізму, на якій покладені відповідні функції.

Іншими словами, політика інформаційної безпеки реалізується сукупністю інститутів публічної влади та інститутів громадянського суспільства, до компетенції яких входить вирішення питань щодо створення безпечних умов функціонування і розвитку інформаційної сфери [325].

Водночас дослідник Н. Грабар визначає інституційний механізм забезпечення інформаційної безпеки як особливу структурну складову частину державного механізму, що забезпечує створення норм і правил, які регулюють взаємодію різних економічних суб’єктів в інформаційній сфері щодо запобігання загроз інформаційній безпеці. Інституційний механізм приводить у дію інститути (формальні і неформальні), структурує взаємодії суб’єктів, які здійснюють контроль над дотриманням установлених норм і правил [191, с. 171].

Учений О. Зозуля виділяє інституційну систему державного управління інформаційною безпекою, яка являє собою складну багаторівневу систему, що, з одного боку, об’єднується особливою загальною функціональною

спрямованістю, а з іншого – розділяється специфічними особливостями, пов’язаними з рівнем компетенції та характером відповідних цілей [250, с. 148].

Аналіз забезпечення інформаційної безпеки крізь призму його суб’єктів дає можливість сформулювати дефініції та класифікувати ці суб’єкти. Зокрема, деякі автори під суб’єктами системи забезпечення інформаційної безпеки України розуміють систему державних і недержавних інституцій, а також громадян України, об’єднаних спільною метою щодо захисту національних інтересів в інформаційній сфері. Отже, виходячи з такого визначення, коло суб’єктів забезпечення інформаційної безпеки України являє собою багаторівневу систему, що має спільну мету – забезпечення інформаційної безпеки України, але різні повноваження, можливості, засоби тощо. До цих суб’єктів можна віднести:

– державу, що здійснює свої функції через відповідні органи державної влади шляхом створення системи забезпечення інформаційної безпеки;

– громадян, суспільні або інші організації та об’єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства України [119, с. 41].

У контексті нашого дослідження доцільно виділити *інституційну складову механізму забезпечення інформаційної безпеки держави*, яка являє собою сукупність інститутів державної влади та місцевого самоврядування, інститутів громадянського суспільства та інших уповноважених суб’єктів, які, у встановленому законом порядку, забезпечують належне функціонування цього механізму.

У чинному законодавстві України перелік суб’єктів забезпечення інформаційної безпеки не закріплений, для його встановлення варто вдатися до системного аналізу перш за все доктринальних та стратегічних документів у сфері національної безпеки в цілому та інформаційної безпеки держави, зокрема.

Прикметно, що раніше законодавець ґрунтовніше підходив до визначення інституційної складової механізму забезпечення інформаційної безпеки. Так, у Концепції національної безпеки України (втратила чинність у 2003 р.) була закріплена мета, структура та поняття системи забезпечення національної безпеки, яка включала і коло суб'єктів інформаційної безпеки.

У зазначеній Концепції система забезпечення національної безпеки визначалась як організована державою сукупність суб'єктів державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства України. У ній закріплювалися такі основні суб'єкти системи забезпечення національної безпеки:

- Український народ;
- Верховна Рада України;
- Президент України;
- Рада національної безпеки і оборони України;
- Кабінет Міністрів України;
- Конституційний Суд України;
- суди загальної юрисдикції;
- Прокуратура України;
- Національний банк України;
- міністерства й інші центральні органи виконавчої влади;
- Воєнна організація держави [321].

На сьогодні, розглядаючи Доктрину інформаційної безпеки України, Стратегію Національної безпеки України, Закон України «Про національну безпеку та оборону» та Закон України «Про основні засади забезпечення кібербезпеки України», можна встановити коло суб'єктів, які становлять інституційну складову механізму забезпечення інформаційної безпеки України, а саме:

- Верховна Рада України;
- Президент України;

- Рада національної безпеки і оборони України;
- Національний інститут стратегічних досліджень;
- Кабінет Міністрів України;
- Міністерством культури, молоді та спорту України;
- Міністерство закордонних справ України;
- Міністерство оборони України;
- Міністерство внутрішніх справ України
- Державне агентство України з питань кіно;
- Державна служба спеціального зв'язку та захисту інформації України;
- Національна рада України з питань телебачення і радіомовлення;
- Державний комітет телебачення і радіомовлення України;
- Служба безпеки України;
- розвідувальні органи України.

Верховна Рада України як єдиний орган законодавчої влади в Україні визначає основи національної безпеки, основи організації Збройних сил України, затверджує загальну структуру, чисельність та функції правоохоронних органів та військових формувань, визначає засади внутрішньої та зовнішньої політики, формує відповідну законодавчу базу в цих напрямах, затверджує укази Президента України про введення надзвичайного і воєнного стану та про загальну чи часткову мобілізацію, здійснює парламентський контроль.

Окремими структурами парламенту, які здійснюють законопроектну роботу у сфері національної інформаційної безпеки, є профільні парламентські комітети. Йдеться, наприклад, про Комітет з питань гуманітарної та інформаційної політики, Комітет з питань есвободи слова; Комітет з питань цифрової трансформації, Комітет з питань транспорту та інфраструктури.

Інформаційне забезпечення діяльності парламенту здійснюється Прес-службою, Управлінням комп'ютеризованих систем та Інформаційним управлінням Апарату Верховної Ради України, яке висвітлює діяльність

законодавчого органу, проводить моніторинг, працює з публічною інформацією та інформаційними ресурсами, організовує відкриті заходи тощо.

Президент України забезпечує інформаційну безпеку держави через правотворчу, представницьку, організаційну, контрольну та кадрову функції, які випливають з повноваженяь щодо керівництва у сферах національної безпеки та оборони, формування Ради національної безпеки і оборони України, призначення вищого командування військових формувань, розроблення і прийняття нормативних документів у сфері інформаційної безпеки, координації у сфері кібербезпеки, призначення половини складу Національної ради України з питань телебачення та радіомовлення тощо.

Здійснення Президентом України повноважень, у тому числі і в сфері інформаційної безпеки, забезпечує Офіс Президента, який є постійно діючим допоміжним органом. У його структуру входять наступні профільні департаменти, відповідальні за інформаційну безпеку та інформаційну політику: Департамент інформаційної політики, Департамент інформаційних технологій, Департамент з питань національної безпеки та оборони, Департамент забезпечення доступу до публічної інформації. Ці департаменти здійснюють організаційне, консультативне, аналітичне супроводження діяльності Президента України по забезпеченню інформаційної безпеки держави. Окремо слід зазначити про Департамент забезпечення зв’язків із Верховною Радою України та Кабінетом Міністрів України, який здійснює комунікацію між Президентом України та зазначеними органами влади. В контексті інформаційної безпеки важливе значення має і діяльність Прес-секретаря Президента України, який підтримує позитивний імідж глави держави та висвітлює його діяльність у медіа.

Важливу роль у забезпеченні інформаційної безпеки держави відіграє Рада національної безпеки і оборони України, яка реалізує правотворчі, консультативні та контрольні функції у векторі інформаційної безпеки. Цей координаційний орган очолює Президент України і він же формує його персональний склад.

Так, Рада національної безпеки і оборони України подає на розгляд глави держави пропозиції з таких питань: визначення стратегічних національних інтересів України в інформаційній сфері, концептуальних підходів та напрямів збереження національної інформаційної безпеки; доцільність утворення, реорганізації та ліквідації органів виконавчої влади в інформаційній сфері; проект державного бюджету за статтями, що пов'язані з підтримкою на належному рівні національної інформаційної безпеки; заходи інформаційного та іншого змісту відповідно до масштабу потенційних та реальних загроз національним інтересам України [135, с. 150]. У структурі Ради національної безпеки і оборони України працює Національний координаційний центр кібербезпеки, який координує та контролює національну систему кібербезпеки, а також формулює пропозиції щодо змісту Стратегії кібербезпеки України.

Національний інститут стратегічних досліджень здійснює аналітично-прогностичне супроводження діяльності Президента України, у тому числі й у сфері інформаційної безпеки. Він є базовою науковою установою, що безпосередньо підпорядковується Президенту України, а його головним завданням є розроблення науково обґрунтованих рішень з питань інформаційної політики та безпеки держави.

Кабінет Міністрів України є вищим органом у системі органів державної виконавчої влади, підконтрольний і підзвітний Верховній Раді України в межах, передбачених Конституцією та законами України, забезпечує державний, у тому числі й інформаційний, суверенітет і економічну самостійність України, вживає заходів щодо забезпечення обороноздатності, інформаційної безпеки України, прав і свобод людини й громадянина в інформаційному просторі, громадського порядку і протидії кіберзлочинності, контролює ресурсне забезпечення національної системи кібербезпеки, організовує аудит інформаційної безпеки на об'єктах критичної інфраструктури, проводить державну інформаційну політику, координує

роботу міністерств, інших органів виконавчої влади у напрямі забезпечення інформаційної безпеки тощо.

Безпосереднє формування та реалізація державної політики у сфері інформаційного суверенітету та інформаційної безпеки здійснює Міністерство культури, молоді та спорту України. Після реорганізації 2019 року зазначене міністерство виконує функції попередніх Міністерства інформаційної політики, Міністерства культури та Міністерства молоді та спорту. Варто зазначити, що до організації міністерств у 2019 р. основним суб'єктом протидії інформаційній агресії з боку РФ виступало Міністерство інформаційної політики.

Зокрема, у Доктрині Інформаційної безпеки України були визначені такі функції Міністерства інформаційної політики:

– моніторинг засобів масової інформації та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення інформації, поширення якої заборонено в Україні;

– моніторинг загроз національним інтересам і національній безпеці в інформаційній сфері;

– сприяння Міністерству закордонних справ України щодо донесення офіційної позиції України до іноземних засобів масової інформації;

– формування поточних пріоритетів державної інформаційної політики, контролю їх реалізації;

– координація діяльності центральних та місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету України;

– урядові комунікації;

– кризові комунікації, зокрема під час проведення антитерористичної операції та в особливий період;

– вжиття заходів в інформаційній сфері, пов'язаних із запровадженням правових режимів надзвичайного чи воєнного стану;

– розроблення стратегічного наративу та його імплементації;

– вироблення і впровадження стратегії інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій;

– розроблення та впровадження єдиних стандартів підготовки фахівців у сфері урядових комунікацій для потреб державних органів [213].

Отже, основним напрямом діяльності цього міністерства було забезпечення інформаційного суверенітету держави, що передбачало розповсюдження суспільно важливої інформації в Україні та за її межами, підтримання належного функціонування державних інформаційних ресурсів, розвиток вітчизняного кіновиробництва, сприяння реалізації права на інформацію та свободу слова (захист прав журналістів, незалежність ЗМІ, захист прав споживачів інформації), підтримання позитивного іміджу України у світі, розвиток державних комунікацій. Останній включає заходи підтримки прес-служб державних органів, методичні рекомендації державним та комунальним ЗМІ, освітні програми та тренінги для державних службовців. Діяльність у вказаних напрямах супроводжувалася законодавчими ініціативами та експертними висновками.

Результатами роботи міністерства стали розробка та випуск Білої книги спеціальних інформаційних операцій проти України 2014–2018 рр., запуск Мультимедійної платформи іномовлення України та розробка інтернет-проекту «Інформаційні війська України», суть якого полягає в інформуванні підписників цього проекту про фейковість відповідної інформації, її спростування та поширення правдивих новин. У межах моніторингу ЗМІ та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення забороненої інформації формувався перелік інтернет-ресурсів, рекомендованих Експертною радою при вказаному міністерстві до блокування.

Зараз правонаступником Міністерства інформаційної політики є Міністерство культури, молоді та спорту України, яке є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику серед іншого та у сферах популяризації

України у світі, державного іномовлення, інформаційного суверенітету України та інформаційної безпеки, відновлення та збереження національної пам'яті. Відповідно до окреслених напрямів зазначене міністерство складає на підставі звернень Ради національної безпеки і оборони України, СБУ, Національної ради з питань телебачення і радіомовлення перелік осіб, що створюють загрозу національній безпеці, який оприлюднює на власному офіційному веб-сайті, та забезпечує його своєчасне оновлення; вживає дозвільні, обмежувальні та контрольні заходи щодо ввезення та розповсюдження видавничої продукції, що має походження або виготовлена та/або ввозиться з території держави-агресора, тимчасово окупованої території України; розроблює заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи; розроблює проекти законів та інших нормативно-правових актів з питань, що належать до його компетенції, та інше [473].

У контексті результатів роботи цього новоствореного міністерства слід розглянути його пропозиції щодо протидії дезінформації, які викликали великий суспільний резонанс та спротив з боку медіа спільноти.

Законопроект «Про протидію дезінформації» має й інституційний аспект, зокрема, пропонується запровадити інститут Уповноваженого з питань інформації, який призначає Кабінет Міністрів України з кандидатів, запропонованих Мін'юстом, Міністерством культури, молоді та спорту України та Уповноваженим Верховної Радою України з прав людини.

Ключовими повноваженнями Уповноваженого з питань інформації є:

– моніторинг інформаційного простору та реагування на заяви щодо поширення дезінформації;

– фіксація та перевірка інформації на предмет наявності ознак дезінформації;

– звернення до поширювачів інформації із заявами про відповідь або про спростування дезінформації;

– звернення до суду із позовами про спростування та надання права на відповідь щодо дезінформації;

– звернення до суду із заявами про обмеження доступу до інформації за відсутності вихідних даних розповсюджувача або відсутності реакції на його заяви;

– звернення до правоохоронних органів у випадку наявності ознак кримінального правопорушення [53, 54].

Вказані законодавчі пропозиції викликали стурбованість у експертів та представників медіа, які наголошують, що проблемним моментом законопроекту є створення спеціального механізму для державного втручання в інформаційну сферу – Уповноваженого з питань інформації, і наділення його надзвичайно широкими і монопольними повноваженнями у сфері інформації, без наявності достатніх запобіжних механізмів проти зловживань. Механізм, запропонований у законопроекті, не відповідає міжнародним зобов'язанням України, зокрема положенням статті 10 Конвенції з прав людини і основоположних свобод та судовій практиці ЄСПЛ, і являє собою надмірне втручання у свободу слова [247].

На наш погляд, пропозиція щодо запровадження інституту Уповноваженого з питань інформації суперечить чинному законодавству у наступних аспектах.

1. Згідно з чинним законодавством, «Уповноважений» не входить до системи центральних органів виконавчої влади, а міністерства позбавлені права надавати подання Кабміну щодо утворення нового органу влади.

2. У проекті немає чіткого механізму взаємодії поширювача інформації та Уповноваженого у випадку направлення останнім вимоги щодо розміщення відповіді на інформацію та вимоги про спростування та обмеження доступу до інформації. Не визначені випадки законної відмови поширювача інформації у задоволені запиту, строки розгляду запиту, порядок оскарження такого запиту.

3. Не визначено процедури віднесення інформації до дезінформації: не встановлено критеріїв, правил збирання доказів, не передбачено права

поширювача інформації представити свою позицію у процесі визнання відомостей дезінформацією. Уповноважений наділяється необмеженим правом визнавати відомості дезінформацією та ініціювати відповідну комунікацію (вимоги, звернення до суду, адміністративна відповідальність) з поширювачем інформації.

4. Наведені вище недоліки законопроекту (п. 2, 3) у сукупності із запровадженням суттєвих адміністративних штрафів (5, 20 мінімальних заробітних плат) за невиконання вимог Уповноваженого створює суттєві загрози для зловживань та втручання у діяльність ЗМІ та/або обмеження свободи вираження поглядів.

5. Неоднозначне трактування понять «масова інформація», «поширювач інформації» та вимога до поширювачів розміщувати власні ідентифікаційні дані несе ризики порушення принципу анонімності як гарантії свободи вираження поглядів.

Наступним суб'єктом, який має спеціальні повноваження у сфері забезпечення інформаційної безпеки, є Міністерство закордонних справ. Доктрина інформаційної безпеки України передбачає покладання на нього таких повноважень:

– формування та реалізацію стратегії публічної та культурної дипломатії України;

– координацію інформаційної діяльності державних органів у зовнішньополітичній сфері;

– забезпечення просування інтересів України за кордоном інформаційними засобами;

– забезпечення донесення позиції України до керівництва іноземних держав, парламентів та урядів, зовнішньополітичних відомств, представників бізнесу та експертних кіл, широкої громадськості, сприяння просуванню позитивного іміджу України;

– сприяння просуванню українських телеканалів у кабельні та супутникові мережі за кордоном;

– забезпечення налагодження взаємодії з міжнародними партнерами як на двосторонній, так і на багатосторонній основі з метою застосування міжнародного досвіду та найкращих практик у контексті протидії інформаційним загрозам [213].

Спеціальним суб'єктом забезпечення інформаційної безпеки виступає *Адміністрація Державної служби спеціального зв'язку та захисту інформації України* (*Держспецзв'язку*), яка створює належні умови функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону. Ця служба є центральним органом виконавчої влади, очолюється Головою, який призначається за поданням Прем'єр-міністра України.

Держспецзв'язку здійснює технічний та криптографічний захист інформації, організовує кіберзахист, забезпечує діяльність телекомунікаційних систем та радіочастотного ресурсу, підтримує безпечний поштовий зв'язок спеціального призначення, захищає державні інформаційні ресурси та інформацію, в тому числі і від технічних розвідок, вживає захисних заходів у сфері електронного документообігу, електронної ідентифікації та електронних довірчих послуг, у межах своєї компетенції забезпечує діяльність суб'єктів у сфері боротьби з тероризмом, організовує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Новим суб'єктом у системі центральних органів виконавчої влади є Міністерство цифрової трансформації України (Мінцифри), яке було створено у вересні 2019 р. Мінцифри є головним органом у системі центральних органів

виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії [500].

Аналіз цілей, завдань та повноважень Мінцифри викликає питання в телеологічному аспекті. Зокрема, чи існує організаційна та економічна доцільність створення такого міністерства? Адже функції Мінцифри дублюють функції діючих Держспецзв'язку, Міністерства інфраструктури України тощо. Наприклад, таке завдання Мінцифри, як розвиток інфраструктури широкосмугового доступу до Інтернету та телекомунікацій прямо стосується компетенції Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, а за логікою – і Міністерства інфраструктури України та Державного агентства інфраструктурних проектів України.

Завдання Мінцифри щодо розвитку цифрових навичок та цифрових прав громадян логічніше було віднести до відома Міністерства освіти України та/або Міністерства юстиції України (далі – Мін'юст). Тим більше, що в Україні вже не один рік Мін'юст реалізує загальнонаціональну програму «Я МАЮ ПРАВО!», в межах якої і можна було б здійснювати просвітницьку діяльність громадянам про їх «цифрові права». Проте Мінцифри виконує це завдання шляхом запуску онлайн-платформи, на якій містяться відеоролики (як зазначають у самому міністерстві – «освітні серіали») про базові цифрові навички, цифрові навички для вчителів та про безпеку дітей в Інтернеті. Прикметно, що ця онлайн-платформа розроблена приватними партнерами

(контент та технічна сторона знімального процесу, соціологічні опитування) за підтримки швейцарсько-української Програми EGAP, що реалізується Фондом Innovabridge та Фондом «Східна Європа», а фінансується Швейцарською агенцією з розвитку та співробітництва. Отже, ці відеоролики розроблені приватними компаніями та організаціями, і участь Мінцифри у цьому проекті зводиться до оголошення загальної інформації про цей проект та звітування про нього як про досягнення всього Уряду. За таких умов очевидно, що цей проект з тим самим успіхом, але з меншими бюджетними витратами міг бути реалізований і Міністерством освіти чи Мін'юстом. І розмістити ці освітні серіали також можна було на сайті цих міністерств. Тому створювати ціле міністерство для проведення таких просвітницьких заходів, як видається, не цілком прийнятно для країни зі складними економічною та військовою ситуацією.

Дискусійним здається підхід Кабміну до визначення таких напрямів діяльності Мінцифри, як цифровізація, цифровий розвиток, цифрові інновації, розвиток інформаційного суспільства, інформатизація. У цьому переліку наявні несумісні поняття (відбивають відношення цілого й частини) й тавтологія (логічна помилка *idem per idem*).

Так, відповідно до Закону України «Про Національну програму інформатизації» від 04.02.1998 р. № 74/98-ВР, інформатизація – це сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки [491].

Із цього поняття випливає, що інформатизація означає розвиток інформаційного суспільства та включає цифровий розвиток і цифрові інновації.

Водночас, згідно з Концепцією розвитку цифрової економіки та суспільства України на 2018–2020 роки цифровізація – це насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір [516]. Таким чином, цифровізація є частиною інформатизації, ці поняття співвідносяться як ціле та частина.

Що стосується діяльності Мінцифри у напрямах цифрової економіки, електронної комерції та бізнесу, у сфері розвитку ІТ-індустрії, то очевидно що вони входять до сфери Міністерства розвитку економіки, торгівлі та сільського господарства України. Цифрова економіка включає такі компоненти: ІТ-індустрія та електронний бізнес. Складовою електронного бізнесу виступає електронна комерція. Тобто визначення таких напрямів є множиною підпорядкованих та несумісних понять.

Завдання Мінцифри у сфері надання електронних та адміністративних послуг, у сферах електронних довірчих послуг та електронної ідентифікації повністю збігається із завданнями Держспецзв'язку.

Увагу слід звернути і на заходи Мінцифри стосовно створення та забезпечення функціонування: системи електронної взаємодії державних електронних інформаційних ресурсів; системи електронної взаємодії органів виконавчої влади; інтегрованої системи електронної ідентифікації; єдиного веб-порталу електронного урядування; єдиного державного веб-порталу відкритих даних; національного реєстру електронних інформаційних ресурсів; єдиного державного веб-порталу електронних послуг [500]. Шість із семи вказаних систем було створено до появи Мінцифри, а їх функціонування забезпечувалося Державним агентством з питань електронного урядування України (Агентство).

Наприклад, систему електронної взаємодії державних електронних інформаційних ресурсів було запроваджено в 2018 р. і координувалося Агентством. Систему електронної взаємодії органів виконавчої влади було створено у 2012 р., її впровадження здійснювалося Агентством. Рішення про

затвердження положення про інтегровану систему електронної ідентифікації було прийнято 19.06.2019 р., тобто до створення Мінцифри. Єдиний веб-портал електронного урядування та єдиний державний веб-портал відкритих даних розробили у 2015 р. Національний реєстр електронних інформаційних ресурсів було сформовано ще в 2004 р. Єдиний державний веб-портал електронних послуг був створений у грудні 2019 р., але на базі Єдиного державного порталу адміністративних послуг (діє з 2013 р.) та Реєстру адміністративних послуг (діє з 2013 р.).

Отже, стверджувати про заходи Мінцифри щодо створення вказаних систем не зовсім коректно, а необхідність покладання на Мінцифри повноважень із забезпечення функціонування цих систем залишається не цілком обґрунтованою.

Варто звернути увагу на те, що Агентство якраз і було перетворено у Мінцифру, але Положення про Агентство не скасовано, що породжує певну плутанину в організації органів державної виконавчої влади та свідчить про невисоку ефективність комунікації між державними органами.

Враховуючи вищенаведене, можна зробити висновок про доцільність використання бюджетних коштів, закладених на забезпечення організації та функціонування Мінцифри, на реальну цифровізацію (технічне оснащення медичних установ, військової сфери, криміналістичної діяльності тощо). На жаль, план роботи Мінцифри на 2020 р. лише підтверджує наш висновок про перспективи цього міністерства.

Зокрема, перелік заходів, пов’язаних з публічними послугами, зумовлений об’єднанням Єдиного державного порталу адміністративних послуг (діє з 2013 р.) та Реєстру адміністративних послуг (діє з 2013 р.) у новий Єдиний державний веб-портал електронних послуг. Приведення у відповідність назв адміністративних послуг до нової їх назви «електронні послуги» передбачає 12 заходів на 2020 р. Виникає питання: навіщо змінювати назви цих послуг і назву їх реєстру, щоб потім займатися проведенням аудиту

послуг, приведенням їх у відповідність з назвою реєстру, оптимізацією реєстру тощо?

Заходам Мінцифри щодо розвитку цифрових навичок та цифрових прав громадян присвячено 11 пунктів, усі з яких виконані або будуть виконані не Мінцифрою, а сторонніми організаціями за рахунок партнерів та/або бюджетних коштів. Наприклад, такий захід, як проведення першого всеукраїнського дослідження з цифрової грамотності українців (включно з окупованими територіями), за інформацією Мінцифри, проведено MLS Group за кошти європейських партнерів. Тобто це міністерство лише курує цей проект і оприлюднює інформацію по ньому, а не займається його розробленням, змістовним наповненням та впровадженням, тому логічно було б у плані роботи чесно вказати про координацію проекту цифрової освіти, а не викладати 11 пунктів діяльності, яку виконуватимуть сторонні спеціалісти.

Аналогічна ситуація з планами Мінцифри на 2020 щодо розвитку і підтримки ІТ галузі з 7 пунктів – 6 пов'язані з розробленням законодавчої бази. Однак дисонанс викликають останні 61 пункт плану роботи Мінцифри, присвячені юридичному, організаційному, фінансовому забезпеченню апарату міністерства. Дискусійною є доцільність внесення таких пунктів (відбір кандидатів на посади, нарахування заробітної плати, ведення діловодства тощо) до плану роботи, адже така діяльність не є метою міністерства, це звичайна поточна діяльність, яка забезпечує виконання визначених законом завдань цього органу.

Окремо слід звернути увагу в контексті інформаційної безпеки на мобільний застосунок «ДіЯ» з електронними документами (електронне водійське посвідчення та свідоцтво про реєстрацію) та даними про людину з реєстрів, який запровадив Уряд 30.01.2020 р.

Принцип його роботи полягає в ідентифікації особистості на основі QR-коду в застосунку. Після сканування відкривається офіційна сторінка державного реєстра, який підтверджує існування або відсутність документа. Застосунок ДіЯ міститиме також свідоцтво про реєстрацію транспортного засобу. Електронні права та техпаспорт формуватимуться автоматично на

основі даних із державного реєстру. Електронні права у смартфоні замінятимуть посвідчення особи лише під час внутрішніх пересувань країною. На наш погляд, користь від цього застосунку набагато менша ніж витрати на забезпечення його функціонування, захист персональних даних та запобігання можливим ризикам його використання у терористичних, корупційних, військових цілях. Виникає питання: які існують гарантії безпеки цих даних у смартфоні, якщо працівники МВС будуть протидіяти незаконному використанню цього мобільного додатка? Наприклад, якщо смартфон з цим застосунком викрадуть, чи зможуть використати його у злочинних цілях (наприклад, агенти спецслужби чи члени терористичної організації). Що робити, якщо буде зламана сама ця система чи буде втручання через систему МВС? В цілому ця ініціатива видається не зовсім доречною в умовах військових дій на окупованій території України, проведення спеціальних операцій ворогом та активізації терористичної діяльності у світі.

На підтвердження нашої позиції наведемо оцінку стану захисту кіберпростору України державними органами. Так, аналітик безпеки, програміст і очільник організації «Українські кібервійська» зазначає, що безпека сайтів в Україні на просто нулячому рівні і ніхто цим не займався всі роки незалежності. Порівняно з Росією, все набагато гірше. Президент України, Кабмін, Рада, спецслужби – у всіх сайти діряві [681].

Наступним суб’єктом забезпечення інформаційної безпеки є Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації є органом державного регулювання у сфері телекомунікацій, інформатизації користування радіочастотним ресурсом та надання послуг поштового зв’язку. Вона здійснює повноваження органу ліцензування, дозвільного органу, регуляторного органу та органу державного нагляду (контролю) [490].

Міністерство оборони України у напрямі забезпечення інформаційної безпеки держави має створювати умови для функціонування системи військово-цивільних зв’язків у місцях постійної дислокації та розгортання

підрозділів Збройних сил України, інших військових формувань, а також організовувати і забезпечувати:

– зв’язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в районі проведення антитерористичної операції в Донецькій та Луганській областях;

– протидію спеціальним інформаційним операціям, спрямованим проти Збройних сил України та інших військових формувань;

– супроводження інформаційними засобами виконання завдань оборони України;

– донесення достовірної інформації до військовослужбовців Збройних сил України, інших військових формувань, зокрема через засоби масової інформації Збройних сил України [213].

У сфері кіберзахисту Міністерство оборони України, Генеральний штаб Збройних сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану [495].

Функції активної протидії інформаційним загрозам та захисту інформаційного простору держави здійснює Служба безпеки України (далі – СБУ). Вона також виступає одним з головних суб’єктів національної системи кіберзахисту.

Зокрема, СБУ здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть

створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [495]. Крім того, СБУ виявляє загрози інформаційній безпеці держави шляхом постійного моніторингу мережі Інтернет і вітчизняних та іноземних ЗМІ. Вживає заходів щодо протидії спеціальним інформаційним операціям, які проводяться проти України.

Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі [495].

У цілому в системі центральних органів державної виконавчої влади функціонує чотири спеціальних суб'єкти та п'ять суб'єктів зі спеціальними повноваженнями у сфері забезпечення інформаційної безпеки держави. Водночас у жодного з цих органів немає спеціальних повноважень щодо забезпечення права особи на захист персональних даних та пов'язаних з ним прав (право на забуття в Інтернеті, право на недоторканість приватного життя, право на захист від кібербулінгу та інше).

У зв'язку з цим ми пропонуємо створити спеціальний, національний орган із захисту персональних даних – Національну комісію із захисту персональних даних. Вона виступала б центральним органом виконавчої влади, який формувався б на засадах колегіальності, був підпорядкований Кабміну та підзвітний Верховній Раді України.

Основними засадами формування та діяльності Національної комісії із захисту персональних даних мають стати:

– оптимізація системи органів виконавчої влади, яка передбачає раціональне використання людських та фінансових ресурсів (бюджетних коштів), чіткий розподіл повноважень, пряму відповідальність державного

органу за невиконання щорічного плану роботу, ефективну реалізацію повноважень, а не імітацію роботи шляхом розроблення численних пропозицій, презентацій, організації конференцій та інше;

– економічна доцільність створення державного органу означає, що такий орган має використовувати весь потенціал для ефективного вирішення питань, які перед ним порушуються, насамперед громадянами. Тобто діяльність державного органу повинна приводити до конкретних результатів у кожному випадку звернення громадян. Результатом звернення особи до державного органу має бути юридичний наслідок (розгляд звернення по суті, а не відписка; оперативне вжиття заходів для розв'язання спірної ситуації, а не затягування розгляду і перенаправлення звернень тощо);

– широкі повноваження державного органу, які необхідні для його якісної роботи у визначеній сфері;

– якісне технічне та кадрове забезпечення, що особливо актуально для державних органів у сфері інформаційної безпеки.

Отже, пропонуємо створити Національну комісію із захисту персональних даних на вищевказаних засадах, а її склад сформувати паритетно з представників:

– Держспецзв'язку;
– Служби безпеки України;
– Департаменту кіберполіції Національної поліції;
– Міністерства цифрової трансформації;
– Уповноваженого Верховної Ради України з прав людини;
– наукових установ;
– громадських організацій.

Діяльність цієї комісії має забезпечуватися апаратом, що складається зі штатних працівників. Ключовою структурною одиницею його має стати технічний відділ із сучасним обладнанням і компетентними IT спеціалістами. Основним завданням цього відділу має стати швидке реагування на

порушення прав осіб у кіберпросторі та збирання необхідної інформації для захисту прав у суді або початку кримінального провадження.

Наприклад, у випадку кібербулінгу, його жертва не має ані юридичної, ані технічної можливості встановити булера і припинити цькування, також відсутній законодавчо встановлений чіткий механізм реагування державних органів на такі ситуації. При створенні Національної комісії із захисту персональних даних саме вона могла б відповідати за захист прав осіб у кіберпросторі, а спеціалісти її апарату (технічного відділу) самостійно або у взаємодії з іншими органами (кіберполіцією, Держспецзв'язку тощо) повинні швидко встановлювати винного та вживати необхідних заходів щодо притягнення його до відповідальності та відновлення порушених прав жертви кібербулінга.

Створення Національної комісії із захисту персональних даних має супроводжуватися ліквідацією Департаменту у сфері захисту персональних даних та представника Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних, з передачею їх функцій новоствореній Національній комісії.

До повноважень Національної комісії із захисту персональних даних пропонується віднести:

1. Захист прав громадян у сфері персональних даних.

Передбачається, що будь-яка людина зможе зв'язатися з Національною комісією із захисту персональних даних, коли вона зазнає труднощів зі здійсненням своїх прав на захист даних. Комісія повинна забезпечити громадянам ефективний доступ до своїх даних, що отримуються в процесі оброблення, в тому числі у сфері:

– електронної репутації (запити на видалення даних в Інтернеті);

– комерції (запити на припинення реклами поштою);

– управління людськими ресурсами (механізми контролю, такі як відеоспостереження або геолокалізація транспортних засобів);

– діяльності фінансових установ, державних органів тощо.

Комісія повинна забезпечити громадянам захист їх прав у випадках кібербулінгу, зокрема на технічному та юридичному рівнях. У кожному випадку звернення особи з приводу її цькування в Інтернеті результатом роботи Комісії має бути: встановлення даних булера, необхідних для його притягнення до відповідальності та/або звернення до суду; припинення поширення негативної інформації щодо особи – жертви булінгу; роз'яснення заявнику юридичних аспектів відновлення порушених прав; вжиття інших необхідних заходів.

Доцільно передбачити створення на веб-сайті Комісії онлайн-сервісу, для розгляду скарг щодо: видалення особистих даних в Інтернеті, заперечення проти отримання реклами поштою і оновлення точності особистих даних.

2. Регулювання захисту даних.

Регулювання захисту даних може здійснюватися різними інструментами: нагляд за оброблення даних; офіційних висновків по законопроєктах, які вплинуть на захист даних; розроблення юридичних механізмів, що спрощують виконання попередніх формальностей; надання рекомендацій державним органам та зацікавленим особам; робота із запитами на консультації від контролерів даних.

3. Контроль та санкції.

Основною формою контролю мають бути інспекційні перевірки, які є методом нагляду за контролерами даних. Це дасть Комісії можливість перевіряти реалізацію профільного закону.

За наслідками перевірки Національна комісія із захисту персональних даних зможе:

- винести попередження, яке має бути оприлюднено;
- застосувати грошову санкцію (за прикладом європейських країн, наприклад у Франції, штраф за порушення персональних даних становить до 150 000 євро і до 300 000 євро за неодноразові порушення);
- прийняти постанову про припинення і відмову в обробленні даних;
- скласти адміністративний протокол.

У разі серйозних порушень основних прав і свобод керівник Національної Комісії повинен направити запит до компетентного органу для прийняття будь-яких необхідних заходів безпеки.

4. Інформування та освіта.

Основне завдання Національної комісії із захисту персональних даних – інформувати людей про їхні права, надані їм українським законодавством. Основною формою інформування передбачається зробити розгляд приватних запитів про надання консультацій або додаткової інформації. Також можливе проведення інформаційних кампаній, орієнтованих на широку публіку, за допомогою преси, власного веб-сайту, соціальних мереж і цільових семінарів.

Звісно, запропоновані пропозиції щодо перспектив удосконалення забезпечення інформаційної безпеки держави не є вичерпними. В умовах європейської та євроатлантичної інтеграції, розвитку глобального інформаційного простору, інформаційних та інших війн з'являються і з'являтимуться надалі нові виклики, що потребуватимуть посиленої уваги та активності представників органів публічної влади України усіх рівнів, наукової спільноти, міжнародних експертів і громадськості, їх взаємодії та узгоджених своєчасних ефективних рішень задля належної реалізації однієї з найважливіших функцій держави, справи всього Українського народу – забезпечення інформаційної безпеки.

Висновки до розділу 4

У розділі 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 та запропоновано шляхи їх вирішення, зокрема в Українській державі.

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 у цьому випадку часто призводять до збільшення дискусійних питань, та протиставленні наукових позицій. Зокрема, у 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.

Водночас, під системою забезпечення інформаційної безпеки ми 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 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 щодо реалізації державної функції щодо забезпечення інформаційної безпеки як на теоретичному, так і на законодавчому рівнях. У зв'язку з цим знижується загальна ефективність реалізації вказаної функції держави та ускладнюється її вдосконалення.

Таким чином, на підставі вищевикладеного 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, 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 здійснюються заходи із забезпечення безпеки. Їх можна поділити на соціальні (особа, суспільство, держава, їх інтереси, права та свідомість) та технічні (інформація, інформаційна інфраструктура, інформаційні технології тощо.

Проведено аналіз деяких нормативно-правових актів, який демонструє відсутність на законодавчому рівні поняття загроз інформаційній безпеці держав. Тому варто звернутися до доктринальних джерел, енциклопедичних та інших наукових видань. Найбільш широко загрози інформаційним ресурсам

розглядають як потенційно можливі випадки природного, технічного або антропогенного характеру, 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: загрози (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 залякувальний характер); 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 інформаційній 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. Поняття загрози розглядаються переважно абстрактно або спрощено, подекуди звужено, відірвано від контексту поняття «інформаційна безпека» і майже не пов'язано із 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.

Здійснено аналіз стану правового регулювання забезпечення інформаційної безпеки на рівні національного законодавства України. З’ясовано, що він відзначається певною непослідовністю і подекуди

несистемністю. 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. Названа функція, безумовно, пов'язана з реалізацією інших функцій Української держави, визначених органів публічної влади.

Разом з тим, національне законодавство України потребує подальшого узгодження з існуючими міжнародно-правовими актами універсального і регіонального рівня у сфері інформаційної безпеки, імплементації існуючих міжнародно-правових стандартів у законодавство і практику його реалізації. На наш погляд, доцільна також активізація міжнародної правотворчої діяльності України у даній сфері, що посилить вплив нашої держави як суб'єкта міжнародного права, сприятиме удосконаленню правового регулювання забезпечення інформаційної безпеки.

Проведений науковий аналіз Доктрини інформаційної безпеки України дає змогу установити її техніко-юридичні недоліки, а саме: змістовні повторення, загальні формулювання, дублювання положень інших нормативно-правових актів. Крім того, виявлено і 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 часи.

У зв'язку з ци, існує нагальна потреба у розробленні комплексного нормативного акту щодо проведення спеціальних інформаційних операцій. На наш погляд, нормативно-правовий акт про інформаційні операції слід

р

о 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 забезпечення законності його функціонування.

б Основним напрямом удосконалення нормативно-правової складової
иказаного механізму вважаємо систематизацію, за якою можна буде вирішити
проблему термінологічної неузгодженості, усунути протиріччя між актами
різної юридичної сили та забезпечити 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.

з З’ясовано вектор удосконалення конституційного та правового
регулювання проблемних питань, запропоновано реальні механізми для
реформування існуючих механізмів та інституцій, запропоновано конкретні
заходи для швидкого й ефективного нормотворення та усунення існуючих
проблем.

а 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.

н Безпосередньо детермінують посягання на інформаційну безпеку, так
само як і на державний суверенітет, територіальну цілісність держави України

ь

к

о

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 і не створювати небезпеку 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 «загроз» є нагальною і має бути спрямована на формування ефективної і реальної системи моніторингу та управління загрозами, іншими ризиками для інформаційної безпеки держави.

З метою запобігання і 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, запобігання інформаційним конфліктам та оперативне їх подолання. Враховуючи активну глобалізацію інформаційно-комунікаційних мереж, важливо не тільки державам, а й міжнародним організаціям долучатися до співпраці у напрямі протидії різноманітним видам інформаційної агресії.

ВИСНОВКИ

Активізація досліджень в інформаційній сфері в Україні останніми роками зумовлена різними чинниками. 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, кірбербезпеки, інформаційної війни та інформаційної оборони,

На наш погляд, це зумовлено багатьма обставинами, тенденціями й закономірностями. Зокрема, 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, крадіжки персональної інформації та її поширення, розпалювання конфліктів у соціальних мережах або інформаційної (гібридної) війни, що має прихований і тривалий характер.

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, [illegible] простору тощо.

глобального та національного інформаційного розвитку, безпосередньо виражає і предметно конкретизує сутність сучасної держави – досягнення демократії, розвиток громадянського інформаційного суспільства, глобальних інформаційно-комунікативних технологій.

Поряд з інформаційною функцією держави згадують і про 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 та зарубіжної науки. Насамперед відзначимо наукові здобутки на даному шляху О. Тихомирова, А. Пазюка, Т. Ткачука та багатьох інших авторів.

Постало чимало питань, насамперед стосовно доцільності виокремлення напряму державної політики у сфері забезпечення інформаційної безпеки України як самостійні функції або підфункції, можливо функція забезпечення інформаційної безпеки становить передумову реалізації державної інформаційної політики України, захисту інформаційних прав і свобод людини та громадянина, захисту інформаційного суверенітету держави і загалом інформаційного простору.

Всебічний аналіз базової досліджуваної категорії – «інформаційна безпека» – дає змогу 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).

Правове регулювання інформаційної безпеки в Україні, реалізації функції забезпечення інформаційної безпеки держави здійснюється на підставі 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 – це 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 у національному і 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.

Грунтовне 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.

Моделі інформаційної безпеки Франції та Німеччини є ефективними, відповідають сучасним викликам та загрозам, які стоять перед національною безпекою цих країн. Їх розвиненість 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 здійснюється насамперед, Федеральним відомством з безпеки в сфері інформаційних технологій (BSI), Національним центром кіберзахисту, відд,ілом інформаційних та комп'ютерних мережевих операцій командування стратегічної розвідки Бундесверу.

По-друге, 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 та інші. 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.

По-третє, 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.

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 вказаної 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 поділити на соціальні (особа, суспільство, держава, їх інтереси, права та свідомість) та технічні (інформація, інформаційна інфраструктура, інформаційні технології тощо).

Аналіз Доктрини інформаційної безпеки України дає можливість установити її техніко-юридичні недоліки, а саме: змістовні повторення, загальні формулювання, дублювання положень інших нормативно-правових актів. Крім того, виявлені і 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 в умовах гібридної агресії РФ вкрай важливе значення має чітка регламентація проведення інформаційних операцій у мирний та воєнний часи. У зв'язку з цим, існує потреба у 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 до забезпечення законності його функціонування. Основним напрямом удосконалення нормативно-правової складової такого механізму вважаємо систематизацію, завдяки якій можна вирішити проблему термінологічної неузгодженості, усунути протиріччя між актами різної юридичної сили та забезпечити єдність нормативно-правового поля.

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 у законодавство України зміни і доповнення щодо закріплення порядку реалізації права на забуття в Інтернеті.

Розгляд інституційної складової механізму забезпечення інформаційної безпеки держави дав можливість 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).

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. 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 та 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 розробку 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 у політичні процеси держави зумовлює необхідність установлення засад 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 ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism. By: Matusitz, Jonathan; Breen, Gerald-Mark. Journal of Human Behavior in the Social Environment, Feb. 2011, Vol. 21 Issue 2 P. 109–129. URL: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN.
2. Act S.754 «To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes». URL: https://www.congress.gov/bill/114th-congress/senate-bill/754.
3. Adams J. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. NewYork, 1998. 368 p.
4. Alberts D.S., Garstka J.J., Stein F.P. Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP Publ., 2nd Edition (Revised). Aug 1999, Second Print Feb. 2000. P. 284: http://www.dodccrp.org/files/Alberts_NCW.pdf
5. Arab Convention on Combating Information Technology Offences 21.12.2010. URL: http://cms.unov.org/DocumentRepositoryIndexer/ Get DocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd.
6. Arquilla J. Ronfeldt D. Cyber war is Coming! Comparative Strategy 2 (April-June 1993). URL: http:// www.rand.org/ pubs/reprints/RP223.html
7. Assuring a Trusted and Resilient Information and Communications Infrastructure. White House. URL: https://www.whitehouse.gov/assets/ documents/Cyberspace_Policy_Review_final.pdf;
8. Beling E. Die Lehre vom Verbrechen. Tbingen, 1906. 624 s.
9. Bellia P. Cyberlaw: Problems of Policy and Jurisprudence in the Information Age. West Group, 2007. 803 p.
10. Bobrovnyk S., Shevchenko A., Didych T. Forms of Modern Lawmaking in the System of a Theoretical and Applied Paradigm of Law Knowledge. International Journal of Recent Technology and Engineering (IJRTE). 2019. Vol. 8 Issue 4S.
11. BSI – Fragen und Antworten zu den Aufgaben und Themen des BSI. URL: www.bsi.bund.de.
12. BSI gewinnt mit Methoden der Künstlichen Intelligenz zwei Disziplinen der CHES 2018 Challenge. URL: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/KI-Sicherheitskonferenz_14112018.html.

13. Carter W.A., Carter W.A., Zheng D.E. The Evolution of Cybersecurity Requirements for the U.S. Financial Industry. 2015. July. URL: http://csis.org/files/publication/150717_Carter_CybersecurityRequirements_Web.pdf
14. Cebrovski A. Network Centric Warfare and information Superiority. RUSI. Whitehall, London, 2000.
15. Colas A. International Civil Society: Social Movements in World Politics. Cambridge: Polity Press, 2002. 232 p.
16. Committee on National Security Systems Structure. URL: http://www.cnss.gov/CNSS/about/structure.cfm.
17. Communique on Principles for Internet Policy-Making 2011. OECD. URL: http://www.oecd.org/dataoecd/33/ 12/48387430.pdf.
18. Construire l`autonomie strategique europeenne pour la securite du numerique. URL: https://www.ssi.gouv.fr/agence/missions/lanssi-a-linternational/construire-lautonomie-strategique-europeenne-pour-la-securite-du-numerique/.
19. Cyber Security Strategy Documents. URL: https://ccdcoe.org/ strategies-policies.html.
20. Cyber Security Strategy for Germany. Berlin : Federal Ministry of the Interior. 2011. 15 p.
21. Cybersecurity Law of the People's Republic of China Passed November 6, 2016. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
22. Cyber-security: France Leads the Way in Europe, Media Econocom Blog, May 7, 2015. URL: http://blog.econocom.com/en/ blog/cyber-security-france-leads-theway-in-europe.
23. Cyberspase United States Faces Challenges in Addressing Global Cybersecurity and Governance, Washington, July 2010. http://web.ebscohost.com.
24. CYBERSPASE United States Faces Challenges in Addressing Global Cybersecurity and Governance, Washington, July 2010. http://web.ebscohost.com;
25. Décret № 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information». URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212&dateTexte=&categorieLien=id.

26. DoDD 8000.01. Management of the Department of Defense Information Enterprise, dated February 10. 2009. P. 11. URL: http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf
27. Dr. Mike McGuire and Samantha Dowling Cybercrime: A review of the evidence Summary of key findings and implications. Home Office Research Report 75. University of Surrey, October, 2013. P. 29.
28. Eng James. Consumer Watchdog: Google Should Extend 'Right To Be Forgotten' to U.S. NBC News. URL: https://www.nbcnews.com.
29. EU vs Disinformation campaign. URL: https://euvsdisinfo.eu/about.
30. Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term. URL: www.infosecisland.com/blogview/23287-Cybersecurity-vs-CyberSecurity-When-Why-and-How-to-Use-the-Term.html
31. French National Digital Security Strategy, 2015. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy.
32. Garstka J. Network Centric Warfare: An Overview of Emerging Theory. PHALANX. 2000. Vol. 33. №. 4.
33. Giddens A. The thirdway: the renewal of social democracy. Anthony Giddens. Cambridge: PolityPress, 1998. 166 p.
34. Goldsmith J. Who controls the Internet: illusions of a borderless world. New York: Oxford University Press, 2006. 240 p.
35. Golovko O. M. Media victimization issue: paradox of modern society. Legea si Viata. 2016. № 9/2 (297). P. 31–33.
36. Google sets up 'right to be forgotten' form after EU ruling. BBC News, 30 May 2014.
37. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2014. Рішення ЄСПЛ. URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.
38. Gramm-Leach-Bliley Act or Financial Services Modernization Act of 1999. Public Law 106-102. 113 Stat. 1338. URL: http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN00900.
39. Greenberg A. CISA Security Bill: An F for Security But an A+ for Spying. (20 Mar 2015). URL: https://www.wired.com/2015/03/cisa-security-bill-gets-f-security-spying/.
40. Grundgesetz für die Bundesrepublik Deutschland. Deutscher Bundestag. URL: https://www.bundestag.de/grundgesetz.
41. Hutchins S.G., Kleinman D.L., Hocevar S.P., Kemple W.G. and Porter G.R. Enablers of Self-synchronization for Network-Centric Operations: Designof

a Complex Command and Control Experiment. Proceedings of the 6 the international command and control research and technology symposium, CCRP, Annapolis, MD, USA, 2001. URL: www.dtic.mil/cgi-bin/ GetTRDoc?AD

42. Information Operations. Directive TS 3600.1. Washington D.C.: U.S. Department of Defense. August 14, 2006. P.2. URL: https://www.fas.org/irp/doddir/dod/info_ops.pdf.
43. Information Operations. Joint Publication 3-13. Washington D.C.: Joint Chiefs of Staff. November, 27. URL: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
44. Information Security Agency. 2011. C. 23. URL: //www.gouvernement.fr/sites
45. Information Systems Defence and Security: France's Strategy, 2011. URL: http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_ system_ defence_and _security_-_France_s_strategy.pdf.
46. Information systems defence and security: France's strategy. French Network and Information Security Agency. 2011. C. 23.: //www.gouvernement.fr/sites/ default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf
47. Information Warfare. Directive TS 3600.1. Washington D.C.: U.S. Department of Defense. December 21, 1992. URL: http://www.dod.mil/pubs/foi/administration_and_Management/admin_matters/14- F-0492_doc_01_Directive_TS-3600-1.pdf.
48. International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. URL: http:// www.whitehouse.gov/ sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
49. International Strategy for Cyberspace.White House. URL: http:// www.whitehouse.gov/sites/default/files/rss_viewer/international_
50. Is Russian social media giant VKontakte sidestepping the GDPR? One user is trying to find out. Advox, 30.08.2018. URL: https://advox.globalvoices.org/2018/08/30/is-russian-social-media-giantvkontakte-sidestepping-the-gdpr-one-user-is-trying-to-find-out.
51. IT-Sicherheitsgesetz (IT-SiG) 2.0 – die wichtigsten Änderungen des Referentenentwurfs im Schnellüberblick. Beck-community. Abgerufen am 3. April 2019. URL: https://community.beck.de/2019/04/03/it-sicherheitsgesetz-it-sig-20-die-wichtigsten-aenderungen-des-referentenentwurfs-im-schnellueberblick.

52. Jayasuriya K. Globalization, Law, and the Transformation of Sovereignty: The Emergence of Global Regulatory Governance. Indiana Journal of Global Legal Studies. Spring 1999. Vol. 6. Issue 2. Article 3. Pp. 425-455.
53. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington D.C.: Joint Chiefs of Staff. October 9, 1998. URL: http://www.c4i.org/jp3_13.pdf
54. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington D.C.: Joint Chiefs of Staff. February 13, 2006. Chapter IV. URL: http://www.bits.de/NRANEU/others/jpdoctrine/jp3_13(06).pdf.
55. Kaldor M. Governance, Legitimacy, and Security: Three Scenarios for the Twenty-first century. Principled World Politics: The Challenge of Normative Relations/ ed. Wapner P. and Ruiz L. New York: Rowman & Littlefield Publishers Inc., 2000. 284 p.
56. Kaminska N. Trends in the Development of International Legal Personality and Subjects of International Law: Theoretical Analysis. OPCION. Universidad del Zulia 2018. Vol.34 , Num.87-2. P. 507-520.
57. Kaminska N., Patricha N. Protection of the human rights in armed conflict. Науковий вісник Національної академії внутрішніх справ. 2016. Т. 99. №. 2. С. 19-28.
58. Karvalics L.Z. Information Society – what is it exactly? The meaning, history and conceptual framework of an expression. Information Society: From Theory to Political Practice. Budapest: Gondolat-Uj Mandatum, 2008. Pp. 29-47.
59. Kushakova N. Impact of the newest information technology on the juridical methodology. Ukraniain law revew. 2004. Issue № 7(12). P. 23-24.
60. Libicki M. What is Information Warfare? URL: http:// www.iwar. org.uk/iwar/resources/ndu/infowar/ a003cont.html
61. Loi № 2013-1028 du 15 novembre 2013 relative à l'indépendance de l'audiovisuel public. URL: https:// www.legifrance.gouv.fr/affichTexte. do?cidTexte=JORFTEXT000028199587&dateTexte=&categorieLien=id.
62. Loi № 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. URL: https://www.legifrance.gouv.fr/ affichTexte.do?cidTexte=JORFTEXT000028338825.
63. Loi № 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article8.
64. Lulu Xia and Zhao Leo. China's Cybersecurity Law: An Introduction for Foreign Businesspeople. China Briefing. 2018. URL: https://www.china-briefing.com.

65. McCormick P. Private sector influence in the International Telecommunication Union. The journal of policy, regulation and strategy for telecommunications, information, and media. 2007. № 9. Pp. 70–80.
66. Metz Steven, Kievit James. Strategy and the Revolution in Military Affairs: From Theory to Policy. Strategic Studies Institute. June 27, 1995. URL: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm? PubID=236.
67. Mitrani M. Global Civil Society and International Society: Compete or Complete? Alternatives: Global, Local, Political. 2013. Vol. 38. Issue 2. Pp. 172-188.
68. National Cyber Strategy of the United States of America (September 2018). URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
69. National Security Strategy of the United States of America (December 2017). URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
70. National Strategy to Secure Cyberspace. February 2003. URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace strategy.pdf;
71. NIST Computer Security Division, 2008. Report. URL: http://www.Csrc.nist.gov.
72. Okinawa Charter on Global Information Society 2000. Okinawa Summit. URL: http://www.ioc.u-tokyo.ac.jp/~worldjpn/ documents/texts/summit/20000722.O1E.html.
73. Organisations übersicht des BSI. Aufgaben. URL: https://www.bsi.bund.de/DE/DasBSI/DerPraesident/derpraesident.
74. Pickard V. Neoliberal visions and revisions in global communications policy from NWICO to WSIS. Journal of Communication Inquiry. 2007. Vol. 31. Pp. 118-139.
75. Powell Rose. Google receives 12,000 requests to be ‘forgotten’ on first day. Sydney Morning-Herald. (31 May 2014).
76. President Executive Order 13800 «Strengthening of Federal Networks and Critical Infrastructure. URL: https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.
77. Price R. Reversing the Gun Sights: Transnational Civil Society Targets Land Mines. International Organization. Vol. 52. No. 3. MIT Press, 1998. Pp. 613-644.
78. Rannenberg Kai. The Future of Identity in the Information Society: Challenges and Opportunities/ Kai Rannenberg, Denis Royer, André Deuker. Springer, 2009 524 p.

79. Rayward W. Boyd. Information Revolutions, the Information Society, and the Future of the History of Information Science. Article in Library Trends, 2014. Vol. 10. P. 681 – 713.
80. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.
81. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act. Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0881.
82. Remarks by (he President on securing our nation's cyber infrastructure). White House. URL: whitehouse.gov/ihe_press_ofIicc/ Remarks-by-the-Presidcni-on-Sceuriiy-Nations-Cyber-Infrusimcture.
83. Remove complaints from Google: Right to Be Forgotten. URL: http://removingcomplaints.com/right-to-be-forgotten.
84. Report to Congress on Implementation of The Federal Information Security Management Act of 2002. URL: https://www. whitehouse.gov/ sites/whitehouse.gov/files/omb/assets/reports/fy2008_fisma.pdf.
85. Revue stratégique: une analyse lucide et volontariste pour préparer la prochaine loi de programmation militaire. 2017. URL: https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.
86. Robertson R. Globalization: Social Theory and Global Culture.. London: Sage Publications Ltd, 1992. 224 p.
87. S.2521 – Federal Information Security Modernization Act of 2014. Library of Congress. URL: https://www.congress.gov.
88. Scholte J.A. Global Civil Society: Changing the World? CSGR Working Paper. University of Warwick, UK. 1999. Issue 31. Pp. 1-35.
89. Shevchenko A., Kalhanova O., Kudin S., Kravchenko O. Guarantees of realization of the rights and freedoms of the person in the national legal system: teaching technique. Asian Life Sciences. The Asian International journal of the Life Sciences. 2019. Supplement 21 (2). №. 2.
90. Socta 2013. EU Serious and Organised Crime Threat Assessment. URL: https://www.europol.europa.eu/sites/default/files/publications/socta 2013.

91. Socta 2013. EU Serious and Organised Crime Threat Assessment. URL: https://www.europol.europa.eu/sites/default/files/publications/socta 2013.pdf.strategy_for_cyberspace.pdf;
92. The Administration's Priorities on Cybersecurity. White House. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity# section-protect-critical-infrastructure;
93. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg Businessweek. October, 2018. URL: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.
94. The Cybcrsecurity Act of 2009. URL: https://www.whiiehouse.gov/ihe_press_ofllce.
95. The Department of Defense Cyber Strategy. URL: https://www.strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pd;
96. The Federal Information Security Management Act of 2002 («FISMA"). URL: https://www.congress.gov/bill/107th-congress/house-bill/3844/text.
97. The national strategy to secure cyberspace. Washington, 2003. 60 c.
98. The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights. 2014. June 30. URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
99. The Secure Information Society: Ethical, Legal and Political Challenges. Springer, 2012. 223 p.
100. Treaty on European Union. URL: http://www. eurotreaties.com/maastrichtext.html.
101. Understanding China's Cybersecurity Law. Information for new zealand businesse. Ministry of Foreign Affairs and Trade, and New Zealand Trade and Enterprise. Sep 2017.URL: https://www.mfat.govt.nz.
102. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. (USA PATRIOT Act) Public Law 107-56. 115 Stat. 272. URL: http://www.gpo.gov/fdsys/pkg/BILLS107hr3162enr/pdf/BILLS107hr3162enr.pdf.
103. Updating U.S. Federal Cybersecurity Policy and Guidance. October 2012. URL: http://csis.org/files/publication/121019_Reeder_A130_Web.pdf;
104. US-CERT: Understanding Hidden Threats: Rootkits and Botnets. URL: https://www.us-cert.gov/ncas/tips.
105. World Summit on the Information Society (WSIS). URL: http://www.internetsociety.org/wsis.

106. Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? Strategic Studies Institute, U.S. Army War College. 43 p.
107. Your right to know. The Government's proposals for a Freedom of Information Actfile. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/272048/3818.pdf.
108. Абакумов В.М. Правове регулювання протидії інформаційним війнам в Україні: автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 − адміністративне право і процес; фінансове право; інформаційне право. Запоріжжя, 2011. 22 с.
109. Авдошин І.В. Проблеми правового регулювання інформаційних відносин в Україні. Актуальні проблеми управління інформаційною безпекою держави : збір. матер.наук.-практ. конф. (Київ, 24 трав. 2017 р.). Київ : Нац. акад. СБУ, 2017.С. 5–7.
110. Авраменко А.В., Гасеський В.К. Інформаційна безпека в Україні як складова національної безпеки // зб. наук. праць УАДУ. 2012. № 18. С. 9-18.
111. Адрианова Н.С. Интернет-коммуникация – реальность или симулякр? URL: http://www.nbuv.gov.ua/portal/natural/vdpu/Movozn/2010_16/article/1.pdf. С. 17–18.
112. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ.: Атіка, 2007. 304 с.
113. Актуальні проблеми конституційного права України : підручник / за заг. ред. проф. Олійника А.Ю. Київ : Центр учбової л-ри. 2013. 554 с.
114. Актуальні проблеми теорії держави та права : навч. посіб. / С.М. Тимченко, С.К. Бостан С.М. Легуша, Н.М. Пархоменко Т.О. Пікуля, Н.В. Пронюк. Київ.: КНТ, 2007. Ч. 1. 288 с.
115. Алещенко В., Сербін В. Проблеми захисту від негативного інформаційно-психологічного впливу противника // Математичні машини і системи. 2010. № 1. С. 77–86.
116. Амелін О. Визначення кіберзлочинів у національному законодавстві // Науковий часопис Національної академії прокуратури України. 2016. № 3. URL: http://www.chasopysnapu.gp.gov.ua/ua/pdf/11-2016/ amelin.pdf.
117. Андрейцев В.І. Право екологічної безпеки: навч. та наук.-практ. посіб. Київ.: Знання-Прес, 2002. 331 с.

118. Антонов В.О. Конституційно-правові засади національної безпеки України : монографія / наук. ред. Ю.С. Шемшученко. Київ: ТАЛКОМ, 2017. 576 с.
119. Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України : дис. ... канд. н. з державного управління. Київ, 2017. 218 с.
120. Антошина І.В. Інформаційна функція українського права : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Одеса, 2015. 20 с.
121. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : дис. ... д-ра юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Харків, 2002. 476 с.
122. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти : монографія / за заг. ред. О.М. Бандурки. Харків : Вид-во ун-ту внутр. справ, 2000. 368 с.
123. Арнаутова Л.М. Правове забезпечення інформаційної політики сучасної України в аспекті процесів європейської інтеграції : автореф. дис. ... канд. юрид. н. за спеціальністю: 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2014. 20 с.
124. Арнольд Р., Банашак Б., Вдовіченко С., Гайс М.-Е., Головань І., Гультай М., Кампо В., Овчаренко В., Савчин М. Права і свободи людини і громадянина в Україні : монографія. Київ : Юрінком Інтер, 2013. 374с.
125. Бабаєва Н.Р. Глобалізація сучасного світу // Гілея. 2012. № 59. С. 362–366.
126. Балахонцев Н., Кондратьев А. Влияние концепции «сетецентрическая война» на эффективность разведывательного обеспечения вооруженных сил США // Зарубежное военное обозрение. 2011. № 2. С. 14–18.
127. Баранов А. Информационный суверенитет или информационная безопасность // Національна безпека і оборона. 2001. № 1. С. 70 –76.
128. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» // Правова інформатика. 2014. № 2(42). С. 54–62.
129. Барчук В.Б. Уповноважений Верховної Ради України з прав людини як суб’єкт забезпечення національної безпеки України : дис. ... канд. юрид. н. за спеціальністю 12.00.02 – конституційне право. Київ, 2006. С.204.

130. Баскаков В.Ю. Інформація з обмеженим доступом: поняття та ознаки. Актуальні проблеми державотворення: матеріали науково-практичної конференції (м. Київ, 28 червня 2011 р.). Київ : ФОП О.С. Ліпкан, 2011. С. 47–49.
131. Батурин Ю.М. Право и политика в компьютерном круге. Москва, 1987. С. 27–34.
132. Безпека. Міжнародна поліцейська енциклопедія : у 10 т. / відп. ред. Ю. І. Римаренко, Я. Ю. Кондратьєв, В. Я. Тацій, Ю. С. Шемшученко. Київ : Вид. Дім «Ін Юре», 2003. Т.1 : Теоретико-методологічні та концептуальні засади поліцейського права та поліцейської деонтології. С. 41–46.
133. Бек У. Что такое глобализация? Ошибки глобализма – ответы на глобализацию. Москва : Прогресс-Традиция, 2001. 304 с.
134. Бельський Ю. Щодо визначення поняття кіберзлочину // Юридичний вісн. 2014. № 6. С. 414–418.
135. Березовська І.Р. Суб'єкти у сфері забезпечення інформаційної безпеки в України // Наук. записки Львів. ун-ту бізнесу та права. 2013. № 10. С. 148–153.
136. Бермічева О.В. Соціальна функція держави в Україні : автореф. дисер. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Харків, 2002. 18 с.
137. Берназюк І.М. Конституційно-правовий статус та механізми реалізації стратегічних (програмних) актів :. автореф. дис. ... д-ра юрид. н. за спеціальністю 12.00.02 – конституційне право; муніципальне право. Ужгород, 2017. 36 с.
138. Бєляков К.І. Вступ до інформаційно-правової конфліктології // Право та державне управління. 2013. № 2. С. 19–24.
139. Бєляков К.І. Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики :. автореф. дис. канд..юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2009. 38 с.
140. Бизнес попросил Путина отклонить закон о предустановке российского софта на гаджеты / Ведомости. 2019 URL: https://www.vedomosti.ru/technology/articles/2019/11/29/817525-biznes.
141. Біленчук П.Д., Борисова Л.В., Неклонський І.М., Собина В.О. Правові засади інформаційної безпеки України : монографія. Харків, 2018. 289 с.
142. Біленчук П.Д., Котляревський О.І. Портрет комп'ютерного злочинця: навч. посіб. Київ, 1997. 48 с.

143. Білоусов Є.М. Юридична природа економічної безпеки як категорії господарського права // Європейські перспективи. 2013. № 12. С. 88–93.
144. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека : Термінологічний навчальний довідник / за ред. Кривуци В.Г. К., 2004. 508 с.
145. Богуш В.М. Інформаційна безпека держави. Київ : МК-Прес, 2005. 431 с.
146. Большая энциклопедия. Словарь общедоступных сведений по всем отраслям знания. Санкт-Петербург : Просвещение, 1896. Т. 17. 794 с. URL: https:// ru.wikisource.org/w/index.php?title=Страница: Yuzhakov_Big_ Encyclopedia_Book_17. djvu/317&action=edit&redlink=1
147. Бринчук М.М. Комплексность в экологическом праве // Экологическое право. 2004. № 6. С. 19 – 28.
148. Бурило Ю.П. Правове регулювання інформаційної діяльності у сфері господарювання : автореф. дис. ... д-ра юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2014. 36 с.
149. Буряк В.В. Глобальное гражданское общество и сетевые революции. Симферополь : Диайпи, 2011. 152 с.
150. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спец. техніка. 2011. № 3. С. 104–114.
151. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ : НАУ, 2013. 432 с.
152. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350
153. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КНТ, 2010. 148 с.
154. Валлерстайн І. Глобалізація або вік змін? Довгостроковий погляд на шлях розвитку світової системи. Глобалізація. Регіоналізація. Регіон. політика. Луганськ : Альма-матер – Знання, 2002. С. 49–67.
155. Валюшко І.О. Інформаційна безпека України в контексті російсько-українського конфлікту : дис. ... канд. політ. н. за спеціальністю: 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку. Миколаїв, 2018. 210 с.

156. Варич О.Г. Економічні функції сучасної держави: природа, зміст, тенденції розвитку в Україні: автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2006. 20 с.
157. Васильева Е.Н. Гражданская правоспособность государства. Субъекты гражданского права : сб. науч. тр. / отв. ред. Т.Е. Абова. М. : Ин-т государства и права РАН, 2000. С. 53−60.
158. Вашкович В.В. Адміністративно-правове забезпечення волонтерства як складова соціальної функції держави : дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Ужгород, 2019. 220 с.
159. Ващук О.П. Антроподжерельна невербальна інформація в кримінальному провадженні: криміналістичні засади : дис. ... д-ра юрид. н. за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. Одеса, 2018. 506 с.
160. Великий тлумачний словник сучасної української мови / гол. ред. В.Т. Бусел, редактори-лексикографи: В.Т. Бусел, М.Д. Василега-Дерибас, О.В. Дмитрієв та ін. Київ.: Ірпінь: ВТФ «Перун», 2005. 1728 с.
161. Великий тлумачний словник сучасної української мови / укл. О. Єрошенко. Донецьк : ТОВ «Глорія Трейд», 2012. 864 с.
162. Венгеров АБ. Теория государства и права: учебник для юрид. вузов. Москва : Юриспруденция, 2000. Изд . 3-е. 528 с.
163. Венедиктов А.В. Организация государственной промышленности в СССР : в 2 т. Т. 1. Ленинград : Изд-во Ленингр. ун-та, 1957. 764 с.
164. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. Москва, 1996. С. 31–36.
165. Военная мысль античности: сочинения древнегреческих и византийских авторов. Москва : Изд-во АСТ, 2002. 665 с.
166. Война и мир в терминах и определениях / под общ. ред. Д. Рогозина. Москва: Изд. дом «ПоРог», 2004. URL: www. royallib.ru/book/rogozin_dmitriy.html
167. Волинець В. Забезпечення міжнародної інтеграції та співпраці як функція сучасної української держави: правові аспекти // Юридична Україна. 2013. № 2. С. 8–14.
168. Волинець В.В. Проблеми правового забезпечення інформаційної функції держави у сучасній Україні // Юридична Україна. 2012. №10. С.4–10.

169. Волинець В.В. Функції сучасної держави: теоретико-правові проблеми : монографія. Київ : Логос, 2012. 512 с.
170. Воронкова В.Г. Філософія глобалізації: соціоантропологічні, соціоекономічні та соціокультурні виміри : монографія. Запоріжжя : Вид-во ЗДІА, 2010. 272 с.
171. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора 23-28.02.2013 р. URL: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4 _2013_2_R.pdf.
172. Гаєць В.М., Кваснюк Б.Є. та ін. Концепція економічної безпеки України. Київ : Логос, 1999. 56 с.
173. Гафнер В.В. Информационная безопасность. URL: http://информационная-безопасность.гафнер.рф/chitat-posobie/glava-1/1-1-ponyatie-informacii-i-informacionnoy-bezopasnosti/principy-obespecheniya-informacionnoy-bezopasnosti/
174. Гетьман А.П. Екологічна функція держави в сучасних глобалізаційних процессах. Проблеми законності : зб. наук. пр. Харків, 2015. Вип. 128. С. 145–153.
175. Глазунова С. Інформаційна функція сучасної держави // Інформація і право. 2014. № 2(11).
176. Гнатюк С.Л., Гуцал С.А. Європейський досвід нормативно-проектного забезпечення розвитку інформаційного суспільства: висновки для України: аналіт. доп.; Нац. ін-т стратег. дослідж. Київ : НІСД, 2014. 58 с.
177. Головка А.А. Громадянське суспільства як суб’єкт протидії загрозам національній безпеці в інформаційній сфері : дис. ... канд. політ. н. Київ, 2018. 237 с.
178. Головко О.М. Інформаційна віктимізація у медіа просторі // Інформація і право. 2015. № 3 (15). С. 49–55.
179. Головко О.М. Інформаційна віктимізація як наслідок формування медіа-аддикцій // Право України. 2016. № 4. С. 167–173.
180. Головко О.М. Інформаційно-правова політика України в сфері безпеки людини у медіа просторі : монографія. Київ : Видавничий дім «АртЕк». 2019. 168 с.
181. Головко О.М. Інформаційно-правова політика України у сфері безпеки людини у медіапросторі : дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2018.

182. Головко О.М. Міждисциплінарні підходи до визначення дефініції «медіапростір» // Юридична Україна. 2016. № 9–10. С. 87–95.
183. Головко О.М. Право людини на безпечне інформаційне середовище в контексті природних прав людини // Правова інформатика. 2014. № 4 (44). С. 79–85.
184. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. Ресурсний центр ГУРТ URL: http://www.gurt.org.ua/articles/34602.
185. Горбенко А. СМИ в сфере информационного противоборства // Власть. 2008. № 11. С. 23–26.
186. Горінецький Й.І. Правоохоронна функція держав Центральної Європи: теоретичні і практичні аспекти : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2005. 20 с.
187. Горлинський В.В. Феномен безпеки як об'єкт аксіологічної рефлексії. URL: https://www.filosof. com.ua/Jornel/M_40/Gorlynsky.htm:
188. Горпинюк О.П. Кримінально-правова охорона інформаційного аспекту приватності в Україні : дис. ... канд. юрид. н. за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Львів, 2011. 242 с.
189. Горун О.В., Камінська Н.В., Фатхутдінова О.В. Теорія держави та права : навч. посіб. Київ : КНТ, 2011. 216 с.
190. Государственное управление в сфере национальной безопасности : словарь-справочник / сост. Г.П. Сытник, В.И. Абрамов, В.Ф. Смолянюк и др.; под общ. ред. Г.П. Сытника. Киев: НАДУ, 2012. 496 с.
191. Грабар Н.С. Механізм інформаційної безпеки України в умовах інформаційного глобалізму // Право та державне управління, 2019. № 3. С. 168–173.
192. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки. Теоретичні і прикладні проблеми фізики, математики та інформатики : матер. XIII Всеукр. наук-практ. конф. (м. Київ, 21–23 травня 2015 р.). Київ : НТУУ «КПІ», 2015. С. 10–17.
193. Грицай Т.О. Захист суспільної моралі як функція сучасної держави: теоретико-правові аспекти : дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Львів, 2017. 236 с.
194. Грубінко А. Інформаційна безпека україни: правове гарантування та реалії забезпечення // Актуальні проблеми правознавства. 2019. Вип. 1 (17). http://dspace.tneu.edu.ua/bitstream/316497/34129/1/Грубінко.pdf

195. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу : Навч. посіб. Київ : КНТ, 2007 260 с.
196. Гультай М.М. Історичні витоки вітчизняного конституціоналізму: звичаї, традиції, пам'ятки права та філософські концепції : монографія. Київ : Юрінком Інтер, 2017. 240 с.
197. Гультай М.М., Кияниця І.П. Гарантування Конституційним Судом України окремих особистих прав і свобод людини // Вісн. Конституційного Суду України. 2011. № 2. С. 82–92.
198. Гурковський В.Т. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : дис. ... канд. юрид. н. за спеціальністю 25.00.02 − механізми державного управління. Київ, 2004. 225 с.
199. Данилішина К.О. Американський чинник в процесі інформаційної глобалізації : автореф. дис. ... канд. політ. н. за спеціальністю 23.00.04. Одеса, 2004. 18 с.
200. Декларація Комітету Міністрів Ради Європи «Про свободу вираження поглядів та інформації» від 29 квітня 1982 р. URL: http://zakon4.rada.gov.ua/laws/show/994_885
201. Демиденко В.О. Принципи застосування органами місцевого самоврядування законодавства України в сфері кібербезпеки // Юридичний часопис НАВС. 2018. №1. С. 141–153.
202. Демченко П. Кібернетична безпека як новітній напрям інформаційної складової національної безпеки України: конституційно-правовий аспект. URL: http://publications.lnu.edu.ua/bulletins/index.php/law/article/view/9560
203. Джолос С.В. Держава в етатистському вимірі: загальнотеоретичний аспект : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Одеса, 2011. 20 с.
204. Джураєва О.О. Функції сучасної держави : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Одеса, 2006. 20 с.
205. Дзевелюк М.В. Теоретико-правові засади інформаційної функції сучасної держави // Порівняльно-аналітичне право. 2015. № 2. С. 15 – 18.
206. Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. URL : http://nbuv.gov.ua/j-pdf/DeBu_2013_1_3.pdf.
207. Директива про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива

NIS) від 06.07.2016 р. URL: https://zakon.rada.gov.ua/laws/main/984_013-16.
208. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України : дис. ... д-ра. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Запоріжжя, 2018. 521 с.
209. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. URL: http://goal-int.org/ponyattyata-zmist-nacionalnoi-sistemi-kiberbezpeki/.
210. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ : Видавничий дім «АртЕк, 2017.
211. Додонов О.Г., Литвиненко О.В., Янішевський С.О. Інформаційна політика органів державної влади: напрями удосконалення. Стратегії розвитку України: теорія і практика. Київ : НІСД, 2002. С. 637.
212. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2012 – 2013. Управление по вопросам разоружения ГА ООН. URL: http://daccess-dds-ny.un.org/doc/ UNDOC/GEN/N13/371/68/PDF/ N1337168.pdf?OpenElement
213. Доктрина інформаційної безпеки України: Затверджена указом Президента України від 25 лютого 2017 р. №47/2017 // Офіц. вісн. України, 2017. № 20.
214. Доповідь Генерального секретаря ООН (A/58/373) від 17.09.2003 р. URL: https://undocs.org/pdf?symbol=ru/A/58/373.
215. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2011 рік. URL: http://dki.org.ua/node/119
216. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция 56/19, принятая Генеральной Ассамблеей. По докладу Первого комитета (A/56/533).
217. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки // *Політичний менеджмент*. 2010. № 5. С. 19–30.
218. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. Київ: НІСД, 2011. 30 с.
219. Дугин А.Г. Сетевые войны. Доклад на заседании Изборского клуба 08.07.2013. URL: http:// dynacon.ru/content/articles/2318
220. Дуліба Є.В. Фіскальна функція держави: адміністративно-правовий аспект : дис. ... д-ра. юрид. н. за спеціальністю 12.00.07 –

адміністративне право і процес; фінансове право; інформаційне право. Дн., 2019. 380 с.
221. Екологічне право України. Академічний курс: підруч. / Г.І. Балюк, М.В. Краснова, Ю.С. Шемшученко та ін.; за ред. Ю.С. Шемшученка. Київ. Юридична думка, 2008. 856 с.
222. Економіка та економічна безпека держави. Теорія та практика : монографічний навч. посіб. / С. Давиденко, О. Єгорова, В. Приходько, П. Матішак, Я. Голоніч, П. Копінец, М. Мачкінова, М. Доброволска та ін. Ужгород : РІК-У, 2017. 388 с.
223. Економічна енциклопедія : у 3 т. / відп. ред. С.В. Мочерний. Київ : Академія, 2001. Т.2. С. 355–372.
224. Економічна та інформаційна безпека: проблеми та перспективи: матер. Міжнар. наук.-практ. конф. (м. Дніпро, 27 квітня 2018 р.). Д.: ДДУВС, 2018. 276 с.
225. Екстремізм і ксенофобія небезпечніше порнографії. URL: https://www.dobrenok.com/ua/news/4430-ekstremizm-i-ksenofobiya-pornografiyi .html
226. Енциклопедичний словник з державного управління / за ред. Ю.В. Ковбасюка, В.П. Трощинського, Ю.П. Сурміна. Київ : НАДУ, 2010. 820 с.
227. Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. ... канд. н. з державного управління за спеціальністю 25.00.01 − теорія та історія державного управління. Львів, 2011. 20 с.
228. Європіна І.В. Види протиправних діянь у сфері новітніх інформаційних технологій // Вісн. Академії адвокатури України. 2010. № 3 (19). С. 129–136.
229. Єсімов С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки // Наук. зап. Львів. ун-ту бізнесу та права. 2013. Вип. 11. С. 73–76.
230. Жаров М., Шевяков Т. Хроники информационной войны Москва : Европа, 2009. 48 с.
231. Женевська Декларація принципів «Побудова інформаційного суспільства: глобальна задача в новому тисячолітті від 12.12.2003 р. URL: http://www.nkrz.gov.ua/uk/1324628380 /1337763264/1337766423
232. Женевський план дій від 12.12.2003 р. URL: http://www.nkrz.gov.ua/uk/ 1324628380/1337763264/1337765310.
233. Жужа Д.Ю. Теоретико-методологические концепции глобального управления природными ресурсами // Политика и Общество. 2012. № 6.

234. Забара І.М. Свобода інформації: сучасний концептуальний підхід у науці міжнародного права // Правова інформатика. № 1(45), 2015. URL: http://ippi.org.ua/sites/default/files/15zimnmp.pdf
235. Забезпечення інформаційної безпеки держави: підруч. / за заг. ред. О.А. Семченка та В.М. Петрика. Київ : ДНУ «Книжкова палата України», 2015. 672 с.
236. Завидняк М.І. Конституційно-правові засади забезпечення економічної безпеки України : дис. ... канд. юрид.н. за спеціальністю 12.00.02 – конституційне право; муніципальне право. Ужгород, 2016. 190 с.
237. Загайнов Л.И. Экономические функции советского государства. Москва : Юрид. лит., 1968. 264 с.
238. Загальна декларація прав людини від 10.12.1948 р. // Офіц. вісн. України. 2008. № 93. Ст. 3103.
239. Загальна теорія держави і права : підручник для судентів юрид. вищих навч. закладів / М.В. Цвік, О.В. Петришин, Л.В. Авраменко та ін. за ред. М. В. Цвіка, О. В. Петришина. Х. : Право, 2009. 584 с.
240. Загуменна Ю.О. Органи внутрішніх справ України як суб'єкти реалізації правоохоронної функції держави : монографія / за заг. ред. д-ра юрид. наук, проф. Бандурки О.М. Харків, 2012. 251 с.
241. Зайчук О.В. Принципи права в контексті розвитку загальної теорії держави і права // Альманах права. Основоположні принципи права як його ціннісні виміри // Наук-практ. юрид. журн. Вип. 3. Київ: Інст. держави і права ім. В.М. Корецького НАН України, 2012. С. 22–28.
242. Закон України Про Концепцію Національної програми інформатизації // Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.182
243. Закон України Про національну безпеку України // Відомості Верховної Ради (ВВР), 2018, № 31, ст.241
244. Закон України Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки // Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102.
245. Запорожець О.Ю. Кібервійна: концептуальний вимір // Актуальні проблеми міжнародних відносин. Вип. 121. Ч. І. Київ : Ін-т МВ КНУ ім. Тараса Шевченка, 2014. 232 с.
246. Захаренко К.В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі // Гуманітарний вісник ЗДІА. 2018. Випуск 72. С. 44–52.

247. Заява медійників щодо законопроекту про дезінформацію. «Детектор медіа». 2020. URL: https://detector.media/community/article/174234/2020-01-27-zayava-mediinikiv-shchodo-zakonoproektu-pro-dezinformatsiyu-vidkrita-do-pidpisannya/.
248. Звіт СБУ URL: https://glavcom.ua/country/politics/obmin-polonenimi-obsje-spodivajetsya-na-bilshe-pozitivnih-novin-u-2020-roci-649966.html.
249. Зозуля О.С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства : дис. ... канд. н. з держ. упр. Київ, 2017. 251 с.
250. Зозуля О.С. Інституційна система державного управління інформаційною безпекою України: сучасний стан та шляхи удосконалення // Інвестиції: практика та досвід, 2015. № 6. С. 147–153.
251. Золотар О.О. Правові основи інформаційної безпеки людини : дис. д-ра юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2018. 499 с.
252. Ильин И.В. Глобалистика в контексте политических процессов : дисс. ... д-ра полит. наук. Москва, 2011. 428 с.
253. Иноземцев В.Л. Современное постиндустриальное общество: природа, противоречия, перспективы Москва : Логос, 2000. 304с.
254. Информационное противоборство на современном этапе: анализ и тенденции. URL: http://www.molych.ru/ politika/ informatsionnoe-protivoborstvo-na-sovremennom-etape-analiz-i-tendentsii.html
255. Івановський В.В. Структура інформаційної інтервенції в українське суспільство. URL: http://eprints.zu.edu.ua/2444/1/37-40.pdf.
256. Іванченко І. С. Забезпечення інформаційної безпеки держави / І.С. Іванченко, В.О. Хорошко, Ю.Є. Хохлачова, Д.В. Чирков. Київ: ПВП «Задруга», 2013. 170 с.
257. Інтернет речей: проблеми правового регулювання та впровадження: матеріали Третьої наук.-прак. конф.(м. Київ, 21 листопада 2019 р.) / упоряд. : В.М. Фурашев, С.О. Дорогих, С.Ю. Петряєв. Київ : Політехніка. 2019. 180 с.
258. Інформатизація управління соціальними системами: Організаційно-правові питання теорії і практики : навч. посіб. / В.Д. Гавловський, Р.А. Калюжний, В.С. Цимбалюк та ін.; за заг. ред. М.Я. Швеця, Р.А. Калюжного. Київ : МАУП, 2003. 336 с.
259. Інформатика для економістів: / за ред. В. Полякова. URL: https://stud.com.ua/53288/informatika/informatika_dlya_ekonomistiv

260. Інформаційна безпека (соціально-правові аспекти) : підруч. / Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін.; за ред. Є.Д. Скулиша. Київ : КНТ, 2010. 776 с.
261. Інформаційна безпека: сучасний стан, проблеми та перспективи : матер. І наук.-практ. конф. (м. Київ, 20 вересня 2019 р.)/ упоряд.: В.М. Фурашев, С.Ю. Петряєв. Київ : Політехніка. 2019. 124 с.
262. Інформаційна війна і національна безпека : монографія / [П.П. Ткачук, Р.В. Гула, О.І. Сивак та інші]. Львів : АСВ, 2015. 265 с.
263. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ : ДУТ, 2015.288 с.
264. Інформаційна_загроза. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0
265. Інформаційне суспільство. URL: http://jure.in.ua/tema-2-informatsijne-suspilstvo/
266. Інформаційне суспільство. URL: https://uk.wikipedia.org/wiki/Інформаційне_суспільство
267. Інформаційний ресурс «The Wall Street Journal»: http://blogs.wsj.com/developments/2013/12/17/ hamptons-seller-tries-new-pitch-buy-my-house-inbitcoin.
268. Інформаційні війни: теорія, PR, зв'язки із громадськістю, дипломатія. URL: http://politiko.ua/blogpost82707.
269. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. Київ : Інтертехнологія, 2009. 164 с.
270. Історія інформаційно-психологічного протиборства : підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш] ; за заг. ред. д.ю.н., проф. Є.Д. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.
271. Камаралі Г.В. Становлення та розвиток інформаційної цивілізації: автореф. дис. ... канд. філос. н. за спеціальністю 09.00.03. Донецьк, 2007. 19 с.
272. Камінська Н., Бондар І. Протидія кіберзлочинності: міжнародний досвід та новели національного законодавства. Правові реформи в України: реалії сьогодення : матер. міжвуз. наук.-практ. конф. присвяченій Всеукр. тижню права (м. Київ, 28 листопада 2018 р.). Київ: НАВС, 2018. С. 65–67.

273. Камінська Н., Чухно О. Пріоритети міжнародної співпраці у сфері забезпечення інформаційної безпеки // Публічне право. 2015. № 4. С. 25–32.
274. Камінська Н.В. Захист персональних даних: проблеми внутрішньо-державного, наднаціонального і міжнародно-правового регулювання. Наук. вісн. Нац. акад. внутр. справ. 2015. № 3. С. 106-114.
275. Камінська Н.В. Камінський А.І., Куненко І.С. Екологічне право : навч. посіб. Київ, 2012. 253 с.
276. Камінська Н.В. Міжнародна інформаційна безпека в умовах глобалізації та інтеграції. Міжнародне право: виклики сьогодення : матер. міжнар. наук.-практ. інтернет-конф. (м. Київ, 20 грудня 2016 р.). Київ : КНТЕУ, 2016. С. 22–27.
277. Камінська Н.В. Перспективи гармонізації законодавства України в умовах інтеграції в європейський інформаційний простір. Європейська інтеграція України: сучасний стан та перспективи розвитку : тези підсумкової наук.-теор.. конф. (м. Київ, 22 квітня 2016 р.). К., 2016. С.33–35.
278. Камінська Н.В. Правовий статус електронної особи у світлі законодавчих ініціатив ЄС та України Стан дотримання прав людини в умовах сучасності: теор. та практ. аспекти : матер. всеукр. конф. (м. Київ, 22 березня 2018 р.). URL: http://elar.naiau.kiev.ua/ handle/123456789
279. Камінська Н.В. Проблеми імплементації міжнародно-правових стандартів у сфері кібербезпеки. Розвиток науки і практики міжнародного права : матер. міжнар. наук.-практ. конф., присвяченій 25-річчю УАМП. Київ, 2018.
280. Каращук М.Г. Інформаційна влада як чинник демократизації сучасного суспільства : автореф. дис. ... канд. політ. н. за спеціальністю 23.00.02 – політичні інститути та процеси. Київ, 2006. 19 с.
281. Карл фон Клаузевиц. О войне. Москва-АСТ, 2002, 574 с.
282. Карпчук Н.П. Засади комунікаційної політики: досвід країн–членів Європейського Союзу : монографія. Луцьк : Вежа-Друк, 2015. 440 с.
283. Карчевський М.В. До питання визначення інформаційної безпеки як об’єкта кримінальноправової охорони. Боротьба з організованою злочинністю і корупцією (теорія і практика) // Наук.-практ. журн. 2012. № 1 (27). С. 267-272.
284. Каск Л.И. Функции и структура государства. Ленинград. : Изд-во Ленинград. ун-та, 1969. С. 5–16.
285. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе [пер. с англ. А. Матвеева ; под ред. В. Харитонова]

Екатеринбург : У-Фактория (при участии изд-ва Гуманит. ун-та), 2004. 328 с.

286. Кастельс М., Хіманен П. Інформаційне суспільство та держава побуту. Фінська модель [пер. з англ.]. Київ : Ваклер, 2006. 256 с.

287. Кирилюк О.В. Міжнародно-правове забезпечення розвитку глобального інформаційного суспільства) : дис. ... канд. юрид. н. за спеціальністю 12.00.11 – міжнародне право. Київ, 2016. 247 с.

288. Кирилюк О.В. Міжнародно-правові аспекти використання кіберпростору у військових цілях // Український часопис міжнародного права. 2014. Спецвипуск : Нові імена в науці міжнар. права. С. 80–86.

289. Кирилюк О.В., Пазюк А.В. Виклики національній безпеці в добу глобального інформаційного суспільства. Українська Революція гідності, агресія РФ і міжнародне право : колективна монографія. Київ : «К.І.С.», 2014. С. 837–838.

290. Кір'ян В.О. Правові засади розвитку інформаційного суспільства в Україні : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2013. 20 с.

291. Климентьєв О. Інформаційна взаємодія як прояв інформаційної функції держави // Наук. вісн. Ужгор. ун-ту. Серія Право 2014. Вип. 25. С. 154–158.

292. Климентьєв О.П. Інформаційна функція Української держави : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2014. 21 с.

293. Климчук В. Екстремізм в Україні: привід чи реальність? // Щотижнева електронна інформаційно-правова газета «Правовий тиждень», № 1–4 від 27.02.2018 року. URL: http://legalweekly.com.ua/index.php?id=16061&show=60237.

294. Климчук О.О., Кравченко Р.М. Кібервійна у сучасних умовах // Інформаційна безпека. Людина. Суспільство. Держава. 2011. №1 (5). С. 78–84.

295. Князев А.А. Информационная война // Энциклопедический словарь СМИ. Бишкек : Изд-во КРСУ, 2002. URL: http://www.evartist.narod.ru /text16/069.htm:

296. Ковтун В.І. Гарантії державного суверенітету України: конституційні аспекти : монографія. Харків : Фактор, 2014. 216 с.

297. Козак А. Політика баркідів кінця III ст. до н.е. та її вплив на особливості карфагенської стратегії у другій пунічній війні (218–201 рр.

до н. е.). Питання стародавньої та середньовічної історії, археології й етнології. 2016. Т. 1. С. 7–25.
298. Колодій А.М. Конституція і розвиток принципів права України (методологічні питання) : автореф. дис. ... д-ра юрид. н. Київ. нац. ун-т ім. Т. Шевченка. Київ. 1999. С.19.
299. Колодій І.М. Адміністративно-правове забезпечення інформаційної безпеки банківських установ в Україні : дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2014. 200 с.
300. Комісаров О.Г. Інформаційний простір публічно-правової сфери: аспекти формування // Вісн. Запор. юрид. ін-ту ДДУВС. 2010. № 1. С. 97–105
301. Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля URL: http://zakon1.rada.gov.ua/laws/show/994_015
302. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. // Офіц. вісн.України. 2011. № 1, № 58, С. 701.
303. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. // Офіц. вісн. України. 2006. № 32. С. 270.
304. Конвенція про кіберзлочинність від 23 листопада 2011 р. URL: http://zakon5.rada.gov.ua/laws/show/994_575/print1453722395322329.
305. Конвенція Ради Європи про кіберзлочинність 2001 р. URL: http://zakon4.rada.gov.ua/laws/show/994_575.
306. Кондратьев А. Будущее сетецентрических войн. Независимое военное обозрение. 07.09.2012. URL: http://nvo.ng.ru/concepts/2012-09-07/1_web_war.html
307. Кононов А.А. Управление безопасностью региональной информационной инфраструктуры. Проблемы управления информационной безопасностью : Сб. тр. Москва : УРСС, 2002. С. 36–53.
308. Кононов А.А., Стрельцов А.А., Черешкин Д.С. Защита критических секторов региональной информационной инфраструктуры. Информационная безопасность регионов России ИБРР-2001: матер. II межрег. конф. (г. Санкт-Петербург, 26–29 ноября 2001 г.). Т. 2. СПб., 2001. С. 18–25.
309. Конституция КНР от 01.12.1982 г. (Т в редакции 2018 г.). URL: https://chinalaw.center/constitutional_law/china_constitution_revised_2018_russian/.

310. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993). Собрание законодательства РФ. 2014. № 31. Ст. 4398.
311. Конституційне законодавство зарубіжних країн: хрестоматія : навч. посіб. / упоряд. В. О. Ріяка, К. О. Закоморна. Київ: Юрінком Інтер. 2007. 384 с.
312. Конституційне право України / за ред. О.В. Ріяки. Київ : Юрінком Інтер, 2007. 320 с.
313. Конституційне право України : / за ред. В. П. Колісника та Ю. Г. Барабаша. Харків : Право. 2008. 416 с.
314. Конституційне право України. Академічний курс : підруч. : у 2 т. Т. 2 / за заг. ред. Ю. С. Шемшученка. Київ : Юридична думка. 2008. 800 с.
315. Конституційне право України: навч. посіб / Бисага Ю.М., Бисага Ю.Ю., Бєлов Д.М. та ін.; М-во освіти і науки України. Ужгород : Ліра. 2007. 370 с.
316. Конституція України від 28.06.1996 № 254к/96-ВР // Відомості Верховної Ради України.1996. № 30. Ст. 141.
317. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. Відомості Верховної Ради України. 1996. № 30. С. 141. http://zakon5.rada.gov.ua/laws/
318. Конституція Української гетьманської держави. 1710 р. (староукраїнською, латинською, українською та англійською мовами). Видання подарункове. Київ–Львів, 1997. 160 с.
319. Контроль за додержанням вимог законодавства про захист персональних даних. Результати перевірок. URL: http://www.ombudsman.gov.ua/ua/page/zpd/kontrol/rezultati-perevirok/.
320. Конфліктологія. Словник / за заг. ред. Колба О.Г., Буймістера А.І. Київ, Переяслав-Хмельницький : Видавництво КСВ, 2012. 592 с.
321. Концепція (основи державної політики) національної безпеки України. Відомості Верховної Ради України. 1997. № 10. Ст. 85.
322. Концепція реформування законодавства України у сфері суспільних інформаційних відносин. Затверджена та взята за основу рішенням Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади (Протокол № 7 від 06.10.2000 р.) URL: http://ndcpi.org.ua/jurnal/16_12.htm.
323. Корж Є.М. Реалізація інформаційної функції права в діяльності органів внутрішніх справ : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Харків, 2010. 20 с.

324. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посіб. Київ : Кондор, 2008. 382 с.
325. Кормич Б.А. Інформаційне право : підруч. Харків : БУРУН і К., 2011. 334 с.
326. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. ... д-ра юрид. н. за спеціальністю: 12.00.07 − теорія управління; адміністративне право і процес; фінансове право; інформаційне право. Харків, 2004. 42 с.
327. Корнєєва Т. Права людини в інформаційному суспільстві. Комунікаційні права: четверте покоління прав людини / ред. проф. В.С. Калашник. Харків : Прапор, 2002. 992 с.
328. Коровин В. Главная военная тайна США. Сетевые войны. Москва : Яуза : Эксмо, 2009. 86 с.
329. Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве. URL: http://www.vestnik.mgimo.ru/fileserver/19/18_Korotkov-Zinovieva.pdf
330. Косогов О.М. Інформаційна безпека у сфері оборони як складова воєнної безпеки України // Системи обробки інформації, 2016. Вип. 8 (145). С. 115–117.
331. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору // зб. наук. пр. Харків. ун-ту Повітряних Сил. 2014. Вип. 3. С. 127–130.
332. Костецька Т.А. Інформаційна функція держави: конституційні та інституційні аспекти // Держава і право. Вип. 47. С. 113–119. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/32861/01-Kostec%27ka. pdf?sequence=1
333. Костицький М.В., Камінська Н.В. Діяльність Конституційного Суду України на сучасному етапі: здобутки, проблеми та перспективи // Європейські перспективи. 2019, №3. С. 5–14.
334. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... д-ра юрид. н. за на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Харків, 2016. 16 с.
335. Кравченко В.В. Конституційне право України : навч. посіб. Вид. 6-те, випр. та доповн. Київ : Атіка. 2009. 608 с.
336. Кремль объединил усилия с китайскими властями, чтобы усилить государственный контроль Интернета и его пользователей.УНИАН.

2016. URL: https://www.unian.net/world/1650792-soglashenie-o-kiberbezopasnosti-putin-ispolzuet-zolotoy-schit-v-rossii-the-guardian.html.
337. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. 2001. № 25. Ст. 131. URL: http://zakon.rada.gov.ua/laws/show/2341-14.
338. Кримінологія: питання та відповіді / за заг. ред. О.М. Литвинова; О.О. Авдєєв, А.А. Васильєв та ін. Харків: Золота миля, 2015. 324 с.
339. Крутских А.В., Сафронова И.Л. Международное сотрудничество в области информационной безопасности. URL: http://www.cryptography.ru/db/msg.html?mid=1169389
340. Кузенко Л.В. Правове регулювання права громадян на інформацію в сфері державного управління : дис. ... канд. юрид. н. за спеціальністю 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право. Харків, 2003. 173 с.
341. Кузовков В.В. Політичні відносини Візантії з державами мусульманського світу в епоху самостійного правління Костянтина VII Багрянородного (945 – 959) Історичний архів. 2015. Вип. 15. С. 55-62.
342. Кузьмин И. Future Combat System – революция или эволюция? URL: http://www.3dnewsru/ editorial/ future_combat_system
343. Кухтик С.В. Трансформація держави під впливом глобалізації (теоретико-правовий аспект) : дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2015. 199 с.
344. Кушакова-Костицька Н. В. Філософсько-правові засади становлення і розвитку інформаційного суспільства в Україні : дис. ... д-ра юрид. н. за спеціальністю 12.00.12 – філософія права. Київ, 2019. 514 с.
345. Кушакова-Костицька Н.В. Право на інформацію в інформаційну епоху (порівняльне дослідження) : монографія. Київ : Логос, 2018. 271 с.
346. Кушакова-Костицька Н.В. Свобода інформації: філософсько-правовий вимір // Філософські та методологічні проблеми права. 2017. № 2 (14). С. 188–196.
347. Кушнір І.В. Конституційне право особи на доступ до публічної інформації та його забезпечення Уповноваженим Верховної Ради України з прав людини : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.02 – конституційне право; муніципальне право. Київ, 2018. 20 с.
348. Лахно В.А. Побудова адаптивної системи розпізнавання кіберзагроз на основі нечіткої кластерізації ознак // Восточно-Европейский журн. передовых технологий. 2016. № 2(9). С. 18–25.

349. Леваков А. Информационная безопасность в США: проблемы и решения. URL: http://freelance4.narod.ru/IS_USA.htm
350. Легеза Ю.О. Здійснення державної екологічної політики в умовах децентралізації державної виконавчої влади. (2016). URL: www.visnyk-juris.uzhnu.uz.ua › file › part_1/44.pdf
351. Лекарь С.І. Поняття та зміст економічної безпеки. Форум права. 2012. № 2. С. 399–402.
352. Лиддел Гарт. Стратегия непрямых действий. Москва : Изд-во «Иностр. л-ры», 1957. 532 с.
353. Лисенко О.О. Правовий захист суспільства від шкідливої інформації : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Харків, 2011. 20 с.
354. Лисенко С.О. Інформаційна безпека: ґенеза принципів і підходів на прикладі досліджень класиків військової думки. Revista științifică internațională «supremația dreptului» Международный научный журнал «Верховенство права». 2019. № 2.
355. Лисенков С. Л. Загальна теорія держави і права : навч. посіб. Київ : Юрисконсульт : КНТ, 2006.
356. Литвиненко О. Інформація і безпека // Нова політика. 1998. № 1. С. 47-49.
357. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії) : автореф. дис. ... канд. політ. н. Київ, 1997. 18 с.
358. Ліпкан В. А. Національна безпека України : навч. посіб. Вид 2-ге. Київ : КНТ, 2009. 576 с.
359. Ліпкан В.А., Залізняк В.А. Систематизація інформаційного законодавства України : монографія. Київ : ФОП О. С. Ліпкан, 2012. 304 с.
360. Ліпкан В.А., Ліпкан О.С Національна і міжнародна безпека у визначеннях та поняттях. Вид. 2-ге., доп. і перероб. Київ : Текст, 2008. 400 с.
361. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М.. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.
362. Ліпкан В.А., Череповський К.П. Інкорпорація інформаційного законодавства України : монографія / за заг. ред. В.А. Ліпкана. Київ : ФОП О.С. Ліпкан, 2014. 408 с.

363. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2005. 20 с.
364. Логінов О.В. Гносеологічний аспект управління інформаційною безпекою України. // *Наук. вісник Юридичної академії МВС України*. 2004. № 2. С. 153–161.
365. Логунов А. Б. Региональная и национальная безопасность : учеб. пособ. Москва : Вузовский учебник, 2009. 432 с.
366. Логунов А.Б. Региональная и национальная безопасность: учеб. пос. Москва.: Вузовский учебник, 2009. 432 с.
367. Лощихін О.М. Теоретико-правові характеристики економічної функції сучасної держави : автореф. дис. ... д-ра юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2010. 32 с.
368. Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства // зб. наук. пр. ВІТІ НТУУ «КПІ». 2013. № 1. С. 31–39.
369. Магда Є. Гібридна агресія Росії: уроки для Європи. Київ : Каламар, 2017. 268 с.
370. Мазаева Е.С. Социальная функция современного российского государства : автореф. дисс. ... д-ра юрид. н. по специальности 12.00.01. Н. Новгород, 2001. 20 с.
371. Майкельсон Дж. Сунь-Цзы: искусство побеждать : [пер. с англ.] / Дж. Майкельсон, С. Майкельсон. Изд. 2-е. Минск. Попурри, 2008. 464 с.
372. Макаренко А. Введение в сетецентрические информационно-управляющие системы 2010. URL: http://www.rdcn.ru/ estimation/2010/03042010.shtml
373. Макеєва О. М. Інформаційна функція права та її вплив на правову культуру суспільства // Юрид. вісн. 2015, № 3 (36). С. 47–51.
374. Макиавелли Н. Государь. Рассуждения о первой декаде Тита Ливия. О военном искусстве. Минск-Попурри, 2009. 672с.
375. Маклюэн М. Понимание Медиа: Внешние расширения человека / Пер. с англ. В. Николаева. М.; Жуковский: «КАНОН-пресс-Ц», «Кучково поле», 2003. 464 с.
376. Максименко Ю. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2007. 188 с.

377. Макушев П.В., Сибіряков С.О. Громадянська та правова культури як соціокультурний фактор у формуванні системи стримувань і противаг в умовах побудови громадянського суспільства // Право і суспільство. 2006. № 3. С.31–37.
378. Малий словник термінів інформаційного права України : дод. до журн. «Правова інформатика» / уклад. Р.А. Калюжний [та ін.] ; Наук.-досл. центр правової інформатики Академії правових наук. Київ : НДЦПІ АПрН України, 2008. 48 с.
379. Мамедова К.А. Основные принципы обеспечения информационной безопасности страны. URL: https://cyberleninka.ru/article/n/osnovnye-printsipy-obespecheniya-informatsionnoy-bezopasnosti-strany
380. Манойло А.В. Государственная информационная политика в особых условиях. URL: http://razom. znaimo.com.ua/ docs/45/index-18501.html
381. Манойло А.В. Управление психологической войной. URL: http://andreymanoylo. vov. ru/ uprpsiv.html
382. Манойло А.В., Петренко А.И., Фролов Д.П. Государственная информационная политика в условиях информационно-психологической войны. Москва : Горячая линия Телеком, 2009. 541 с.
383. Марущак А.І. Інформаційне право: доступ до інформації : навч. посіб. для вузів. Київ : КНТ, 2007. 532 с.
384. Марущак А.І. Правові основи захисту інформації з обмеженим доступом : курс лекцій. Київ :КНТ, 2007. 208 с.
385. Машненков К.А. Концепт «екологічна держава» в контексті сучасного державотворення . (2014). URL: http://www.dridu.dp.ua/ vidavnictvo/2014/2014_02(21)/5.pdf
386. Медвідь Ф. Інформаційна безпека України в контексті становлення стратегії національної безпеки держави; Інформаційна безпека України: виклики і загрози. URL: https://nato.pu.if.ua/old/journal/2009-2/2009-2-28.pdf
387. Мельничук О.І. Міжнародно-правовий статус всесвітньої культурної і природної спадщини. Київ : Наукова думка, 2008. 288 с.
388. Мельничук С.М. Правові форми реалізації функцій сучасної держави Україна : дис. ... д-ра юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2019.
389. Мендел Т. Свобода информации: сравнительно-правовое исследование [изд 2-е., доп.]. Париж, ЮНЕСКО, 2008. 176 с.

390. Менеджмент інформаційної безпеки: підруч. : у 2 ч. / А. К. Гринь, О. Д. Довгань, В. І. Журавель, С. О. Князєв, Є. Д. Скулиш, О. М. Солодка, Т. Ю. Ткачук ; за заг. ред. Є. Д. Скулиша. Київ : НА СБУ, 2013. Ч. 2. 604 с
391. Міжнародна поліцейська енциклопедія : у 10 т. Т. 1. Теоретико-методологічні та концептуальні засади поліцейського права та поліцейської деонтології / [відп. ред. Ю. І. Римаренко, Я. Ю. Кондратьєв, В. Я. Тацій, Ю. С. Шемшученко]. Київ : Концерн «Видавничий Дім «Ін Юре», 2003. С.131, 139.
392. Міжнародний пакт про громадянські і політичні права від 16 грудня 1966 р. URL: http://zakon0.rada.gov.ua/laws/show/995_043
393. Мірошніченко А.М., Марусенко Р.І. Науково-практичний коментар до Земельного кодексу України. [вид 3-те., змін. і доп.]. Київ : Алерта; ЦУЛ, 2011. 511 с.
394. Морозов А.М. От физической к психологической войне. Эволюция форм войны в процессе развития цивилизации. URL: http://psyfactor.org/biowar.htm
395. Морозов Ю.В. Балканы сегодня и завтра: военно-политические аспекты миротворчества / Ю.В. Морозов, В.Ю. Глушков, А.С. Шаравин. Москва : ЦВСИ ГШ ВС РФ, 2001. 376 с.
396. Морозова Л. А. Влияние глобализации на функции государства // Государство и право. 2006. № 6. С. 101–107.
397. Морозова Л.А. Теория государства и права. URL: https://law.wikireading.ru/50984.
398. Назаров В. В. Обмеження конституційних прав людини в кримінальному провадженні : автореф. дис. ... д-ра. юрид. н. за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. Дн., 2009. 36 с.
399. Наливайко Л.Р. Державний лад України: поняття, система, гарантії : автореф. дис. ... д-ра юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Харків, 2010. 40 с.
400. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект // Вісн. Запор. держ. ун-ту. 2003. №1. С. 60–65.
401. Наполеон Бонапарт. О воинском мастерстве. Избранные сочинения. Москва-Эксмо, 2003. 800 с.
402. Науково-практичний коментар Конституції України /за ред. Мусіяки В.Л. Харків : Право. 2011. 783 с.

403. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Вид. дім «Гельветика», 2017. 168 с.
404. Нерсесянц В.С. Общая теория права и государства : учеб. Москва : НОРМА, 2000. С. 256.
405. Нестерович В. Ф. Іноземне мовлення США у системі американської публічної дипломатії // Віче. 2016. № 7–8. С. 32–36.
406. Нестерович В.Ф. Верховенство права та забезпечення прав людини на тимчасово окупованих територіях України : Наук. зап. НаУКМА. 2017. Т. 200. Юридичні науки. С. 85–92.
407. Нестерович В.Ф. Виборча кампанія: Словник сленгових термінів та виразів. Київ : Вид-во Ліра-К, 2020. 648 с.
408. Нестерович В.Ф. Види впливу громадськості на прийняття нормативно-правових актів // Вісн. Луган. держ. ун-ту внутрішніх справ імені Е.О. Дідоренка. 2014. № 1. С. 33–39.
409. Нестерович В.Ф. Практикум з Конституційного права України. Київ : Вид-во Ліра-К, 2018. 640 с.
410. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. / за заг. ред. П.В. Мельника, Н.Р. Нижник. Ірпінь, 2000. 304 с
411. Никодимов И. Ю. Информационно-коммуникативная функция государства и механизм ее реализации в современной России (теоретический и сравнительно-правовой анализ) : автореф. дисс. ... д-ра юрид. н. по специальности: 12.00.01. СПб., 2001. 40 с.
412. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства // Наше право. 2016. № 1. С. 17–23.
413. Новый энциклопедический словарь. Москва: Большая Российская энциклопедия, 2001.1456 с. С. 968
414. Носач А.В. Загрози національній безпеці як обов'язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність України // Право і суспільство. 2019. №3. С. 50–56. DOI https://doi.org/10.32842/2078-3736-2019-3-1-9
415. Носіков Д.М. Фіскальна функція сучасної держави: теоретико-правовий аспект : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Харків, 2016. 20 с.
416. О безопасности : Закон Российской Федерации. Ведомости Верховного Совета Российской Федерации. 1992. № 15. Ст. 770.

417. О внесении изменения в статью 4 Закона Российской Федерации «О защите прав потребителей»: Федеральный Закон от 02.12.2019 № 425-ФЗ. Российская газета – Федеральный выпуск. 2019. № 275(8033).
418. О Военной доктрине Российской Федерации : Указ Президента Российской Федерации от 5 февраля 2010 г. № 146. URL:https://web.archive.org/web/20100409080826/http://www.mil.ru/849/11873/1062/1347/1818/index.shtml
419. О Стратегии национальной безопасности РФ: Указ Президента РФ от 31.12.2015 № 653. URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html.
420. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: Положение, утвержденное Постановлением Правительства РФ от 16.03.2009 р. № 228. URL: https://rkn.gov.ru/about/p179.
421. О.А. Семченка та В.М. Петрика. Забезпечення інформаційної безпеки держави : підручник. Київ: ДНУ «Книжкова палата України», 2015. 672 с.
422. Об информации, информационных технологиях и о защите информации: Федер. закон от 27.07.2006 № 149-ФЗ. Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.
423. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646. Собрание законодательства РФ. 2016. № 50. Ст. 7074.
424. Об утверждении Концепции национальной безопасности Российской Федерации: Указ Президента РФ от 17.12.1997 № 1300 (ред. от 10.01.2000). URL: http://www.consultant.ru/document/cons_doc_LAW_17186/defb41ab8ba4fdacc0715ce94f552abb03f39aaf/.
425. Окинавская хартия глобального информационного общества от 22.07.2000 р. // Дипломатический вестн. 2000. № 8. С. 51–56.
426. Оксамытный В.В. Теория государства и права : учеб. Москва : ИМПЭ-ПАБЛИШ, 2004. С. 222.
427. Олійник А. Держава (внутрішні та зовнішні напрями діяльності, функції). Міжнар. поліцейська енциклопедія : у 10 т. / відп. ред. Ю.І. Римаренко, Я.Ю. Кондратьєв, В.Я. Тацій, Ю.С. Шемшученко. Київ : Концерн «Видавничій Дім «Ін Юре», 2003. Т.1. С. 131–133.
428. Олійник А., Сущенко В. Внутрішні та зовнішні напрямки (функції) діяльності держави (характеристика). Міжнар. поліцейська енциклопедія : у 10 т. / Відп. ред. Ю.І. Римаренко, Я.Ю. Кондратьєв,

В.Я. Тацій, Ю.С. Шемшученко. Київ : Концерн «Видавничій Дім «Ін Юре», 2003. Т.1. С. 75–77.
429. Олійник А.Ю. Конституційні свободи людини і громадянина та їх забезпечення в Україні : монографія. Київ : КНУТД ; Дніпро : Ліра ЛДТД. 2018.
430. Олійник О.В. Організаційно-правові засади захисту інформаційних ресурсів України: автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2006. 20 с.
431. Олійник О.В. Принципи забезпечення інформаційної безпеки України // Юридичний вісник. Повітряне і космічне право. 2016. № 4. С. 72-78. URL: http://nbuv.gov.ua/UJRN/Npnau_2016_4_14
432. Оніщенко Н.М. Деякі підходи до вивчення комунікативних властивостей права // Комунікація : наук.-практ. зб. 2013. № 3. С. 9–13.
433. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. / [В.М. Болгов, Н.М. Гадіон, О.З. Гладун та ін.]. Київ : Нац. академія Прокуратури України, 2015. 202 с.
434. Основи демократії : підруч.; ред. А. Колодій. вид 3-тє., онов. і доп. Львів : Астролябія, 2009. 832 с.
435. Основи інформаційного права Україн : навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.; за ред. М.Я. Швеця, Р.А. Калюжного, П.В. Мельника. Київ : Знання, 2004. 274 с.
436. Остапенко О.Г. Правознавство. URL: http://dl.khadi.kharkov.ua/mod/book/view.php?id=29662&chapterid=4825
437. Остапенко О.І. Про інформаційну функцію української держави. URL: http://aphd.ua/publication-153/
438. Офіційний сайт «ІТАР-тарс». URL: http://itar–tass.com/ekonomika/783989.
439. Офіційний сайт інформаційного агентства «Russia Today». URL: http://rt.com/usa/bitcoin–sec–shavers–texas–231.
440. Павленко Ж.О. Поняття інформаційної функції держави. Проблеми законності : акад. зб. наук. пр. Харків, 2011. Вип. 117. С. 202–211.
441. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти): дис. ... д-ра юрид. н. за спеціальністю 12.00.11 – міжнародне право. Київ, 2016. 467 с.
442. Пазюк А.В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.11 – міжнародне право. Київ, 2004. 19 с.

443. Панченко В. М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз Інформаційна безпека людини, суспільства, держави : наук.-практ. журн. К. 2012. №3 (10). С. 100–109.
444. Парсонс Т. Система современных обществ ; пер. с англ. Л.А. Седова, А.Д. Ковалева ; под. ред. М.С. Ковалевой. Москва : Аспект Пресс, 1998. 270 с.
445. Пархоменко Н.М. Суверенітет держави: соціально-політична сутність та юридичний зміст // Наук. часопис НПУ ім. М.П. Драгоманова. Серія 18 «Економіка і право». 2011. Вип. 14. С. 113–121.
446. Паспорт спеціальності 21.04.01 – економічна безпека держави (економічні науки) : Президія ВАК України від 15.12.2004 протокол № 11-10/11т. URL: https://zakon.rada.gov.ua/rada/show/va11-33004/ed20041215/findtext=%E5%EA%EE%ED%EE%EC%B3%F7%ED%B3.
447. Паспорт федеральной программы «Информационная безопасность» от 28.05.2019 р. URL: https://digital.gov.ru/uploaded/files/pasport-federalnogo-proekta-informatsionnaya-bezopasnost.pdf.
448. Пендюра М. Національна безпека України в контексті сучасних європейських геополітичних трансформацій : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2006. 16 с.
449. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право Львів, 2019. 268 с.
450. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи // Юрид. журн. 2009. № 5. С. 122– 134.
451. Петров Є.В. Інформація як об’єкт цивільно-правових відносин : дис. ... канд. юрид. н. за спеціальністю 12.00.03. Харків, 2003. 206 с.
452. Петрунько О.В. Соціалізувальні ресурси і ризики агре- сивного медіа середовища. URL: http://elibrary.kubg.edu.ua/2638/1/O_Petunko_%20 RMOVLP_17_SRRAM.pdf.
453. Пилипчук В.Г., Дзьобань О.П. Інформаційне суспільство: філософсько-правовий вимір : монографія / НДІ інформатики і права Нац. акад. прав. наук України. Ужгород : ІВА, 2014. 282 с.
454. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. Стратегічні пріоритети. 2011. № 4 (21). С. 12–17.

455. Побудова націєцентричного культурно-інформаційного простору як шлях подолання соціальної конфліктності та солідаризації суспільства : колект. монографія / [Жулинський М. та ін. ; відп. ред.: Жулинський М., Кравченко А.] ; НАН України, Ін-т літ. ім. Т. Г. Шевченка. Київ : Ін-т літ. ім. Т. Г. Шевченка НАН України, 2017. 216 с.
456. Погорілко В.Ф., Федоренко В.Л. Конституційне право України : підруч. / За заг. ред. проф. В.Л. Федоренка.Вид. 3-тє, перероб. і доопр. Київ : КНТ, В-во Ліра-К, 2011. 532 с.
457. Політологія URL:.https://pidruchniki.com/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi _informat siyniy _sferi
458. Попадинець Н.М. Основні чинники забезпечення економічної безпеки України // Соціально-економічні проблеми сучасного періоду України. 2016. № 2. С. 20–23.
459. Попов В.Д. Информациология и информационная политика. Москва, 2001. 120 с.
460. Попов И.М. Сетецентрическая война Пентагона // Независимое военное обозрение. 2004. № 9 (369). URL: http://nvong.ru/concepts/2004-03-12/1_pentagonhtml
461. Попова Т.В., В.А. Ліпкан. Стратегічні комунікації : словник / за заг. ред. доктора юридичних наук В.А. Ліпкана. Київ : ФОП Ліпкан О.С., 2016. 416 с.
462. Почепцов Г.Г. Информационные войны. Москва.: Рефл-бук, Киев.: Ваклер, 2000. 576 с
463. Почепцов Г.Г. Нові медіа як засіб міжнародних інформаційних інтервенцій.: http://osvita.mediasapiens.ua/material/13955.
464. Почецов Г.Г. Інформаційні війни в закритих і відкритих системах. URL: http:// www.academy.gov.ua/doc/zmi_pro_nas/publ/publ_2013_06_30. pdf.
465. Правова інформатика: (система інформатизації законотворчої, правозастосовної, правоохоронної судочинної та правоосвітньої діяльності в Україні): [монографія]. Ужгород : ІВА, 2003. 168 с.
466. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків : 2018. 289 с. URL:.http://repositsc.nuczu.edu.ua/bitstream/123456789/8484/1/Монография%20Борисова.pdf
467. Предборський В.А. Економічна безпека держави : монографія. Київ: Кондор, 2005. 391 с.

468. Присяжнюк О.А. Основи концепції правового регулювання інтернет-відносин в Україні» (загальнотеоретичні аспекти) : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових вчень. Харків, 2007. 20 с.
469. Пріоритетні напрями досліджень розвитку держави і права в умовах євроатлантичної інтеграції України: монографія / за заг. ред. професора Наталії Камінської. Київ, 2018. 300 с.
470. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. № 638-IV. URL : http://zakon.rada.gov.ua/laws/show/638-15.
471. Про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав – учасниць СНД : Міжнар. документ від 11.09.1998 р. URL: https://zakon.rada.gov.ua/laws/show/997_889.
472. Про державну таємницю : Закон України від 21 січня 1994 р. № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93.
473. Про деякі питання діяльності Міністерства культури, молоді та спорту: Постанова Кабінету Міністрів України від 16.10.2019 р. № 885. Офіційний вісник України. 2019. № 88. Ст. 2942.
474. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 р. № 514/2009 // Офіц. вісн. України. 2009. № 52. С. 7. Ст. 1783.
475. Про доступ до інформації, яка знаходиться в розпорядженні державних органів : Рекомендації Комітету Міністрів Ради Європи від 25 листопада 1981 р. URL:http://www.medialaw.kiev.ua/laws/laws_international/ 116/
476. Про доступ до офіційних документів : Рекомендації Комітету Міністрів Ради Європи № R (2002)2 від 21 лютого 2002 р. URL: http://zakon2.rada.gov.ua/ laws/show/994_a33
477. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI // Відомості Верховної Ради України. 2011. № 32. Ст. 314.
478. Про Загальнодержавну програму формування національної екологічної мережі України на 2000 – 2015 роки : Закон України від 21.09.2000 р. // Відомості Верховної Ради України. 2000. № 47. Ст. 405.
479. Про затвердження Методики розрахунку рівня економічної безпеки України : Наказ Міністерства економіки України від 02.03.2007 р. № 60. URL: https://zakon.rada.gov.ua/rada/show/v006066507/ed20070302/find?Text=%C5%EA%EE%ED%EE%EC%B3%F7%ED%E0+%E1%E5%E7%EF%E5%EA%E0.

480. Про затвердження Методики розрахунку рівня економічної безпеки України: Наказ Міністерства економіки України від 02.03.2007 р. № 60. URL: https://zakon.rada.gov.ua/rada/show/v006066507/ed20070302/find?Text =%C5%EA%EE%ED%EE%EC%B3%F7%ED%E0+%E1%E5%E7%EF% E5%EA%E0
481. Про затвердження Методичних рекомендаціях щодо розрахунку рівня економічної безпеки України : Наказ Міністерства економічного розвитку та торгівлі від 29.10.2013 р. № 1277. URL: https://zakon.rada.gov.ua/ rada/show/v1277731-13.
482. Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру : Закон України від 8 червня 2000 р. // Відомості Верховної Ради України. 2000. № 40. Ст. 337.
483. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.81 р. № 108, Страсбург URL: www.convention.coe.int/treaty/en/Treaties/Html/ 108.htm.
484. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.
485. Про контррозвідувальну діяльність : Закон України від 26.12.2002 р. № 374-IV // Відомості Верховної Ради України, 2003. № 12. Ст.89.
486. Про Концепцію національної інформаційної політики : Проект закону від 13.12.2002 р. № 2526. URL: http://w1.c1.rada.gov.ua/pls/ zweb2/webproc4_1?pf3511=13798.
487. Про Концепцію Національної програми інформатизації : Закон України № 75/98-ВР від 04.02.1998 р. URL: http://zakon4.rada.gov.ua/l.
488. Про міжнародні договори України : Закон України від 29.06.2004 р. № 1906-IV р. URL: https://zakon.rada.gov.ua/laws/show/1906-15
489. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469 VIII. URL: https://zakon.rada.gov.ua/ laws/show/2469-19
490. Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації : Положення, затверджене Указом Президента 23.11.2011 р. № 1067/2011. URL: https://zakon.rada.gov.ua/laws/show/1067/2011.
491. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

492. Про нову редакцію Воєнної доктрини України : затв. Указом Президента від 24.09.2015 р. № 555/2015. URL: https://zakon.rada.gov.ua/laws/show/n0016525-15.
493. Про оборону України : Закон України // Відомості Верховної Ради України. 1992. № 9. Ст. 106. (у редакції від 03.07.2019 р.): URL:http://zakon4.rada.gov.ua/laws/show/1932- 12.
494. Про основи національної безпеки України : Закон України від 1 9 червня 2003 року № 964-IV // Відомості Верховної Ради України. 2003. № 39. Ст. 351. Втратив чинність від 08.07.2018, підстава Закон 2469-VIII https://zakon.rada.gov.ua/laws/show/964-15
495. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII // Офіц. вісн. України. 2017. № 91. Ст. 2765.
496. Про основні засади забезпечення кібербезпеки України. Закон України від 5.10.2017 р. № 2163-VIII. // Відомості Верховної Ради. 2017. № 45. Ст.403.
497. Про охорону навколишнього природного середовища : Закон України від 25.06.1991р. № 1264-XII. URL: https://zakon.rada.gov.ua/laws/term/ 8022/sp?sp=:max15
498. Про передачу третім особам персональних даних, які знаходяться в розпорядженні державних органів : Рекомендації Комітету Міністрів Ради Європи від 9 вересня 1991 р. URL: http://www.medialaw.kiev.ua/laws/laws_ international/104/
499. Про перелік відомостей, що не становлять комерційної таємниці : Постанова Кабінету Міністрів України від 9 серпня 1993 р. № 611. URL: http://zakon5.rada.gov.ua/laws/show/611-93-%D0%BF
500. Про Питання Міністерства цифрової трансформації : Постанова Кабінету Міністрів України від 18.09.2019 р. № 856 // Офіц. вісн. України. 2019. № 80. Ст. 2736.
501. Про правовий режим надзвичайного стану : Закон України від 16 березня 2000 р. // Відомості Верховної Ради України. 2000. № 23. Ст.176.
502. Про Прокуратуру: Закон України від 14.10.2014 № 1697-VII. Відомості Верховної Ради, 2015. № 2–3. Ст.12.
503. Про протидію дезінформації: презентація законопроекту. Міністерство культури, молоді та спорту України. Київ. 2020. URL: http://mkms.gov.ua/files/InformPolityka.pdf.
504. Про протидію дезінформації: презентація законопроекту. Міністерство культури, молоді та спорту України. Київ. 2020. URL: http://mkms.gov.ua/files/InformPolityka.pdf.

505. Про протидію і запобігання сепаратизму та подолання наслідків сепаратистської діяльності на території України (десепаратизація) : проект закону від 17 липня 2014 р. № 4300а. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=4300%D0%B0&skl=8 (дата звернення: 08.05.2019).
506. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 липня 2006 р. № 23-V // Відомості Верховної Ради України. 2006. № 39. С. 1384. Ст. 328.
507. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 р. № 2824-IV // Відомості Верховної Ради України. 2006. № 17. С. 128. Ст. 71.
508. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016 // Офіц. вісн. України. 2016. № 23. Ст. 899.
509. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015 // Офіц. вісн. України. 2015. № 43. Ст. 1353.
510. Про свободу вираження поглядів та інформації: Декларація Комітету міністрів Ради Європи від 29 квітня 1982 р. URL: http://zakon2.rada.gov.ua/ laws/show/994_885
511. Про Службу безпеки України : Закон України від 25.03.1992 р. № 27, ст.382 URL: http://zakon.rada.gov.ua/laws/show/2229-12
512. Про Стратегію національної безпеки України : Указ Президента України від 12.02.2007 р. № 105/2007 (із змінами від 8.06.2012 р. № 389/2012) URL: http://zakon4.rada.gov.ua/laws/show/105/2007
513. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки : Указ Президента України № 276/2015 від 20 травня 2015 р. URL: .http://zakon0.rada.gov.ua/laws/show/ 276/2015.
514. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи : Постанова Пленуму Верховного суду України від 27.02.2009 р. № 1. URL: http://zakon2.rada.gov.ua/laws/show/v_001700-09.

515. Про судоустрій і статус суддів : Закон України від 07.07.2010 № 2453-VI // Відомості Верховної Ради України. 2010. № 41–42, № 43, № 44–45. Ст.529.
516. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації :Розпорядження Кабінету Міністрів України; Концепція, План, Заходи від 17.01.2018 р. № 67-р. // Урядовий кур'єр. 2018. № 88.
517. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінет Міністрів України від 15 травня 2013 р. № 386-р URL: http://zakon5.rada.gov.ua/laws/show/386-2013-р
518. Про Уповноваженого Верховної Ради з прав людини: Закон України від 23 грудня 1997 р. № 776/97-ВР // Відомості Верховної Ради України. 1998. № 20. Ст. 99.
519. Проблеми інформаційного законодавства України в сфері створення, поширення та використання інформації та шляхи їх вирішення : аналітична записка / Національний інститут стратегічних досліджень. URL: http://old2.niss.gov.ua/articles/1189.
520. Проблеми сучасної конституціоналістики : навч. посіб. / Орзіх М.П. та ін. Київ: Юрінком Інтер. 2011. 267 с.
521. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування:. аналітична записка : URL: http://www.niss.gov.ua/articles/454/
522. Проект Закону «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України» URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JF8L100A.html
523. Пронюк Н.В. Впровадження європейських стандартів у законодавство України Міжнародна поліцейська енциклопедія : у 10 т. / відп. ред. Ю.І. Римаренко, Я.Ю. Кондратьєв, В.Я. Тацій, Ю.С. Шемшученко. Київ : «Ін Юре», 2005. Т.2. Права людини у контексті поліцейської діяльності. С. 62–63.
524. Пронюк Н.В. Сучасне міжнародне право: навчальний посібник. Вид. 2-ге, допов. і перероб. Київ : КНТ, 2010. 280 с.
525. Протидія кіберзлочинності в Україні: правові та організаційні засади / [О.Є. Користін, В.М. Бутузов, В.В. Василевич та ін.] ; за заг. ред. В.В. Коваленка. Київ : Вид. дім «Скіф», 2012. 728 с.
526. Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід : монографія / за заг. ред. Сергія Чернова та ін. Запоріжжя : ЗДІА, 2017 602 с

527. Пухтаєвич Г.О. Аналіз національної економіки : навч. посіб. Київ : КНЕУ, 2005. 254 с.
528. Пушкіна О.В. Конституційний механізм забезпечення прав людини і громадянина в Україні: проблеми теорії і практики : автореф. дис. ... д-ра. юрид. н. за спеціальністю 12.00.02 – конституційне право. Харків, 2008. 38 с.
529. Рабінович П.М. Основи загальної теорії права та держави : навч. посіб. [вид. 6-те]. Харків : Консум, 2002. 160 с.
530. Расторгуев С.П. Философия информационной войны. Москва : Московский психолого-социальный ин-т, 2003. 496 с.
531. Резолюция ГА ООН № 66/24 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности от 13.12.2011 р. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/460/28/PDF/N1146028.pdf?OpenElement.
532. Резолюция ГА ООН № 67/27 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности от 11.12.2012 р. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N12/480/24/PDF/N1248024.pdf?OpenElement.
533. Решетников Ф.М. Правовые системи стран мира: справочник. Москва : Юрид. л-ра, 1993. 256 с.
534. Рішення Конституційного Суду від 11.10.2018 р. № 7-р/2018. URL: http://ccu.gov.ua/storinka-knygy/428-pravo-na-nedotorkannist-osobystogo-zhyttya.
535. Рішення Конституційного Суду від 20.01.2012 р. № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#n51.
536. Рішення Конституційного Суду України у справі за конституційним зверненням Київської міської ради професійних спілок щодо офіційного тлумачення частини третьої статті 21 Кодексу законів про працю України (справа про тлумачення терміну «законодавство») // Офіц. вісн.України від 27.08.1998, № 32, ст. 59.
537. Роберт Гейтс. Объязанность, мемуары министра войны. Москва-АСТ, 2014. 798 с.
538. Романенко О.В. Пенітенціарна функція демократичної правової держави та роль громадянського суспільства в механізмі її реалізації : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.08 – кримінальне право та кримінологія, кримінально-виконавче право. Київ, 2004. 21 с.

539. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2015. 247 с.
540. Рудник Л.І. Роль та місце стратегічних комунікацій в сучасному суспільстві знань. URL: http://goal-int.org/rol-ta-mistse-strategichnihkomunikatsij-v-suchasnomu-suspilstvi-znan/
541. Руководство по кибербезопасности для развивающихся стран: URL: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf.
542. Рябовол Л.Т. Державний суверенітет: наукові підходи до визначення поняття і ступеня обмежень в умовах глобалізації // Вісн. НТУУ «КПІ». Політологія. Соціологія. Право. Вип. 3 (43) 2019. С. 262–266.
543. Рябоконь О. Державна інформаційна політика формування інформаційного суспільства: зарубіжний досвід // Наук. пр. Нац. бібл. України ім. В. І. Вернадського : зб. наук. пр. Київ, 2016. Вип. 43. С. 97–114.
544. Савин В.А. Некоторые аспекты экономической безопасности России. Международный бизнес России. 1995. № 9.
545. Савінова Н.А. Кібернетична інтервенція: до питань походження та потреби криміналізації в умовах формування та розвитку інформаційного суспільства. URL : http://justinian.ua/article.php?id=3912.
546. Савінова Н.А. Кримінально-правова політика забезпечення інформаційного суспільства в Україні: дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Львів, 2013. 510 с.
547. Савюк М.Ф. Адміністративно-правові засади інформаційного суспільства : автореф. дис. ... канд. юрид. н. зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2016. 19 с.
548. Сайт Минрегиона был взломан хакерами – пресс-служба ведомства, 27.12.2014 г. URL: http://korrespondent.net/ukraine/3461338-saitmynrehyona-byl-vzloman-khakeramy-press-sluzhba-vedomstva.
549. Сайтарлы Тимофей. Защита критической инфраструктуры – составная часть национальной безопасности и стабильности URL: http://www.crime-research.ru/library/Saytarly_aprl.html
550. Сало В.І. Внутрішні функції держави в умовах членства в Європейському Союзі : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Харків, 2008. 22 с.

551. Самойленко Ю. Економічна безпека України : правовий аспект.URL: http://www.viche.info/ journal/3838/.
552. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012 // Вісн. Книжкової палати. 2013. № 1. С. 40–43.
553. Сасин Г.В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір. Грані. 2015, № 3 (119). С. 18–23.
554. Сахновський Є., Чедолума І. Воєнна теорія Карла фон Клаузевіца на межі XX–XXI ст. (матеріали наукового семінару кафедри історії нового та новітнього часу, 25 листопада 2014 р.) // Історична панорама. 2015. Вип. 20. С. 109 –127.
555. Свобода інформації : навч. посіб. [пер. з англ. Р. Тополевського]. Київ : Тютюкін, 2010. 128 с. https://cedem.org.ua/wp-content/uploads/userimages/book_files/A_19_ freedom_info_signal.pdf
556. Свобода інформації в Україні та світі. Теорія та практика / упор. О. М. Павліченко, Р. І. Стадник; ГО «Харківська правозахисна група». Харків : ТОВ «Видавництво права людини», 2015. 216 с.
557. Свобода інформації та право на приватність в Україні. Т. 1, 2. URL: https://krytyka.com/ua/reviews/svoboda-informatsiyi-ta-pravo-na-pryvatnist-v-ukrayini-tom-1-2
558. Северинчик О.П. Маніпулятивний аспект діяльності ЗМІ. Філософія і соціологія в контексті сучасної культури : зб. наук. пр. ДНУ, 2008. С. 326–329.
559. Селіванов А. Суверенітет народу і його забезпечення публічною владою // Право України. 2009. № 11. С. 66–72.
560. Сепаратизм. URL: https://uk.wikipedia.org/wiki/Сепаратизм.
561. Серебро М.В. Сучасна держава як цінність : загальнотеоретичне дослідження : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01– теорія та історія держави і права; історія політичних і правових учень. Одеса 2012 – 24 с. С.8
562. Серьогін В.О. Право на недоторканність приватного життя у конституційно-правовій теорії та практиці : монографія. Харків : ФІН», 2010. 608 с.
563. Сили спеціальних операцій України: ексклюзивне інтерв'ю із командувачем ССО Ігорем Луньовим. 2019. Радіо Свобода. URL: https://www.radiosvoboda.org/a/sso-lunev-spets-opera/30014073.html.

564. Сироїд Т.Л. Правова основа політики Європейського Союзу в галузі безпеки: від витоків до сучасності // Наук. вісн. Дніпропет. держ. ун-ту внутрішніх справ. 2019. № 3. С. 547– 60.
565. Система. Матеріал з Вікіпедії – вільної енциклопедії. URL. 222 https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0 %BC%D0%B0.
566. Скакун О. Ф. Теория государства и права : учебник. Харків : Консум, 2000. 704 с.
567. Скалацький В.М. Інформаційне суспільство: сучасні теорії та моделі (соціально-філософський аналіз) : автореф. дис. ... канд. філос. н. за спеціальністю 09.00.03 – соціальна філософія та філософія історії. Київ, 2006. 17 с.
568. Сліденко І. Концепт демократії в контексті нових горизонтів української конституції: філософські і концептуальні основи // Вісн. Конституційного Суду України 2019, № 6. С. 128–131.
569. Словник іншомовних слів: 23 000 слів та термінологічних словосполучень / укл. Л. О. Пустовіт та ін. Київ : Довіра, 2000. 1018 с.
570. Словник термінів з кібербезпеки / за заг. ред. О. Копана, Є. Скулиша. Київ : ВБ «Аванпост-Прим», 2012. 214 с.
571. Словник термінів інформаційного права / упор. А.І. Марущак ; заг. ред. М.Я. Швець. Київ : КНТ, 2008. 184 с.
572. Словник української мови: в 11 т. / за ред. І.К. Білодіда. Київ : Наук. думка, 1970– 1980. Т. 3.
573. Совгиря О.В., Шукліна Н.Г. Конституційне право України : навч. посіб. Київ : Юрінком Інтер. 2007. 632 с.
574. Соглашение между правительствами государств–членов Шанхайской организации сотрудничества «О сотрудничестве в области обеспечения международной информационной безопасности» от 16.06.2009 г. URL: http://base.spinform.ru/show_doc.fwx?rgn=28340 .
575. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. URL: http://zakon4.rada.gov.ua/laws/show/997_353
576. Созыв международной конференции по вопросу о свободе информации: Резолюция ГА ООН 59 (I) от 14.12.1946 г. URL: www.daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/033/10/IMG/R003310.pdf?OpenElement

577. Соловйов С.Г. Теоретичні засади інформаційної оборони. Державне будівництво. 2015. № 1. URL: http://www.kbuapa.kharkov.ua/e-book/db/2015-1/doc/1/06.pdf
578. Сопілко І.В. Інформаційні загрози та безпека сучасного українського суспільства. URL: http://jrnl.nau.edu.ua/index.php/UV/article/ viewFile/8181/9770.
579. Сопілко І.М. Правові засади державної інформаційної політики України : автореф. дис. ... д-ра юрид. н. за спеціальністю 12.00.07 − адміністративне право і процес; фінансове право; інформаційне право. Київ, 2014. 38 с.
580. Сорокін О.Л. Інформаційна безпека та її складові: проблеми визначення концепту // Держава та право. 2014. №8. С. 18-22.
581. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду ООН від 26 червня 1945 р. URL: http://zakon4.rada.gov.ua/laws/show/995_010.
582. Степко О.М. Аналіз головних складових інформаційної безпеки держави // Наук. вісн. Ін-ту міжнар. відносин НАУ. 2011. Вип. 1(3). С. 90−99.
583. Стеценко С.Г. Адміністративне право України : навч. посіб. Київ : Атіка, 2007. 624 с.
584. Стратегія кібербезпеки України від 15.03.2016. URL : http://zakon3.rada.gov.ua/laws/show/96/2016
585. Стратегія національної безпеки України : введена у дію Указом Президента від 26.05.2015 р. № 287/2015 // Офіц. вісн. України. 2015. № 43, Ст. 1353.
586. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / ред. В.А. Садовничий, В. П. Шерстюк. Москва : МЦМНО, 2002. 296 с.
587. Стрельцов Є.Л. Державний суверенітет і суверенітет особистості: проблеми взаємовідносин. Правове забезпечення ефективного виконання рішень і застосування практики Європейського суду з прав людини : матер. 2-ї Міжнар. наук.-практ. конф., 20–21 вересня 2013 р. Одеса : Фенікс, 2013. С. 48–60.
588. Субіна Т.В. Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.07 − адміністративне право і процес; фінансове право; інформаційне право. Ірпінь, 2010. 24 с.
589. Сунєгін С. О. Функції сучасної держави: питання аксіологічного осмислення // Альманах права. 2017. Вип.1. С. 269−277.

590. Сунь-Цзи, У-Цзи. Трактати про військове мистецтво. Москва-АСТ, 2003, 558с.
591. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. URL: http://www.niss.gov.ua/articles/294/
592. Талдикін О.В. Нетократія як черговий фактор кризи інституту національної держави: передумови виникнення // Наук. вісн. Дніпропетр. держ. ун-ту внутр. справ. 2012. № 1. С. 149−155.
593. Твердохліб О.С. Інформаційна політика України: концептуальні засади становлення та перспективи розвитку : монографія. Київ : ІПК ДСЗУ, 2019. 239 с.
594. Твердохліб О.С. Формування та розвиток інформаційних державно-управлінських ресурсів України : дис. ... канд. н. з державного управління за спеціальністю 25.00.01 – теорія та історія державного управління. Київ, 2012. 20 с.
595. Теліпко В.Е. Конституційне та конституційно-процесуальне право України : навч. посіб. Київ : Центр учбової л-ри. 2009. 568 с.
596. Теліпко В.Е. Універсальна теорія держави і права : підручник Київ : БІНОТАВР, 2007. С. 221−222.
597. Теория государства и права : курс лекций / Н.И. Матузов, А.А. Воротников, В.Л. Кулапов ; под ред. Н.И. Матузова, А. В. Малько. [3-е изд., перераб. и доп.] Москва : Юр. Норма : НИЦ ИНФРА-М, 2018. 640 с.
598. Теорія держави і права : навч. посіб. / заг. ред. В.В. Копєйчикова. Київ.: Юрінформ, 1995. С. 65.
599. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, 1999.
600. Тисянчин В.М. Правові форми здійснення економічної функції держави: теоретичні і практичні аспекти : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Львів, 2011. 16 с.
601. Тихомиров О. О. Забезпечення інформаційної безпеки як функція держави : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Київ, 2011. 19 с.
602. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / заг. ред. Р. А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

603. Тихомиров О.О. Інформаційний делікт як підстава «інформаційної» юридичної відповідальності : відмітні ознаки Інформація і право. 2019, №1(28) С. 37−44.
604. Тихомиров О.О. Класифікації забезпечення інформаційної безпеки. URL: http://web.znu.edu.ua/herald/issues/2011/ur_2011_1/164-168.pdf
605. Тихомиров О.О. Перспективні зміни розуміння інформаційної безпеки // Правова інформатика. 2010. № 4(28).
606. Тихомирова Є.Б. Комунікативна політика ЄС: інформаційна безпека vs транспарентність. Актуальні проблеми міжнародних відносин. 2011, Вип. 102, (ч. І). С. 22−28. URL: journals.iir.kiev.ua/index.php/apmv/article/viewFile/2112/1875
607. Ткаченко В.В. Кирієнко О.Ю. На варті інформаційної безпеки: до історії протидії шпигунській діяльності в Російській імперії в роки Першої світової війни // Наука і правоохорона. 2017. № 4. С. 303−311.
608. Ткачова Н.Н., Чернов С.А. Экономический механизм регулирования инновационных процес сов /зб. наук. пр. ІЕП НАН України «Экономика промышленности». Донецк, 2000. С. 188−193.
609. 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.
610. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України : правовий вимір : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 422 с.
611. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. ... д-ра юрид. н. за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Ужгород, 2019. 487 с.
612. Толль Ф.Э. Настольный словарь для справок по всем отраслям знаний. Санкт-Петербург : В. Безобразов. и др., 1864. Т. 3. 1172 с. URL: https://www.prlib.ru/item/428718 (дата звернення 11.05.2019).
613. Тоффлер Э. Война и антивойна. Что такое война и как с ней бороться ?. Как выжить на рассвете XXI века ? / Э. Тоффлер, Х. Тоффлер. М.: Аст: Транзиткнига, 2005. 412 с.
614. Туніська програма для інформаційного суспільства від 18.11.2005 р. URL: http://www.nkrz.gov.ua/uk/1324628380/1337763264/ 1337767389/.
615. У Держспецзв'язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози. URL :

http://www.dsszzi.gov.ua/dsszzi/
control/uk/publish/article?art_id=286338&cat_id=284576/
616. У США викрили створену українцем міжнародну мережу кіберзлочинців. URL : https://zaxid.net/u_ssha_vikrili_stvorenu_ukrayintsem_mizhnarodnu_merezhu_kiberzlochintsiv_n1448553.
617. Уголовное законодательство зарубежных стран (Англии, США, Франции, Германии, Японии) : Сб. законодательных материалов / Н.А. Голованова, В.Н. Еремин, И.Д. Козочкин и др. ; под ред. И.Д. Козочкина. Москва : Зерцало, 1999. 352 с.
618. Українська Революція гідності, агресія РФ і міжнародне право : колект. монографія. Київ : «К.І.С.», 2014. С. 837−838.
619. Управління боротьби з кіберзлочинністю / Мін. внутр. справ України. URL: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754
620. Уряд запускає мобільний застосунок з е-правами, який заміняє паспорт під час подорожей. URL: https://hmarochos.kiev.ua/2020/01/29/uryad-zapuskaye-mobilnyj-zastosunok-z-e-pravamy-yakyj-zaminyaye-pasport-pid-chas-podorozhej/.
621. Уфимцев Ю.С. Методика информационной безопасности / Ю.С. Уфимцев, В.П. Буянов, Е.А. Ерофеев и др. Москва : Экзамен, 2004. 544 с.
622. Федоренко В. Л. Теоретичні основи системи конституційного права України : автореф. дис. ... д-ра юрид. н. за спеціальністю 12.00.02 – конституційне право; муніципальне право. Харків. 2010. 40 с.
623. Філософський енциклопедичний словник. Київ : Абрис, 2002. С. 519.
624. Фісун А.О. Ґенеза поняття «інформаційна війна». Гілея. 2011. № 49. С. 534–538.
625. Фоміна М.В., Мішина І.Г. Глобальна економічна безпека: сутність і тенденції. URL: http://trade.donduet.edu.ua/download/2011/32/Fom_Mish.pdf.
626. Фрицький О. Ф. Конституційне право України : підруч. Вид 3-тє, перероб. і доп. Київ : Юрінком Інтер, 2006. 512 с.
627. Фулей Т.І. Сучасні загальнолюдські принципи права та проблеми їх впровадження в Україні : автореф. дис. ... канд. юрид. н. Київ. Нац. ун-т ім. Т. Шевченка. Київ. 2003. 16 с.
628. Функції держави URL: https://lawbook.online/ukraine-gosudarstva-prava-teoriya/osoblivosti-vnutrishnih-zovnishnih-funktsiy-72128.htmlстор
629. Функції держави. URL: https://ips.ligazakon.net/document/view/TS001811

630. Хакери з ЄСМ заявляють, що слідом за сайтом Ющенка «положать» сайт СБУ. URL: http://www. unian.ua/politics/73946-hakeri-z-esm-zayavlyayut-scho-slidomza-saytom-yuschenka-polojat-sayt-sbu.html.
631. Хамадун И.Т. В поисках кибермира. Декларация Эриче по принципам киберстабильности и кибермира. Всемирная федерация ученых (World Federation of Scientists). URL: https://www.itu.int/ dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-MSW-R.docx:
632. Хантингтон С. Столкновение цивилизаций / под общ. ред. К. Королева ; пер. с англ. Т. Велимееева, Ю. Новикова. Москва : АСТ, 2003. 603 с.
633. Хартія основних прав Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/994_524
634. Харченко Л.С., Ліпкан В А., Логінов О.В. Інформаційна безпека України : Глосарій / за заг. ред. Р.А. Калюжного. Київ: Текст, 2004. 180 с.
635. Хорошко В.О., Хохлачова Ю.Є. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Ч. 1. Безпека інформації. Т. 22. № 3 (2016).
636. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : монографія. Київ : Освіта Україн», 2010. 388 с.
637. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства. Київ : Освіта України, 2011. 426 с.
638. Цимбалюк В.С. Концепція кодифікації законодавства України про інформацію. Інформаційні технології в глобальному управління : Матер. Міжнарод. наук.-практ. конф. (м. Київ, 29.10.2011 р.). К.: ФОП О.С. Ліпкан С. 73–91.
639. Цимбалюк В.С. Науково-доктринальні положення щодо методологічних установок систематизації законодавства про інформацію // Інформація і право. 2015. № 2. С. 76−83.
640. Червяковский А.В. Информационная функция права и деятельность органов внутренних дел по ее реализации : автореф. дисс. ... канд. юрид. н. по специальности: 12.00.01. Москва, 2002. 21 с.
641. Череповський К. Інкорпорація як етап кодифікації інформаційного законодавства України // Підприємництво, господарство і право. 2012. № 5. С. 47−49.
642. Череповський К.П. Інкорпорація інформаційного законодавства України : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.07 –

адміністративне право і процес; фінансове право; інформаційне право. Запоріжжя, 2013. 19 с.
643. Черноголовкин Н.В. Теория функции социалистического государства. Москва : Юрид. лит., 1970. 215 с.
644. Четверик Г.Г. Напрямки реалізації державної політики у сфері кібернетичної безпеки // Вісн. Дніпропетр. ун-ту. 2012. Вип. 22. С. 240–245.
645. Чорнобай О.Л. Комунікативна функція права: інформаційно-орієнтаційний вимір // Наук. вісн. Львів. держ. ун-ту внутр. справ 2013. №1. С. 496−507.
646. Чуйко З.Д. Конституційні основи національної безпеки України : дис. ... канд. юрид. н. за спеціальністю 12.00.02 – конституційне право. Харків, 2008. 209 с.
647. Чукут С. Інформаційна політика : навч. посіб. Київ : Вид-во УАДУ, 2003. Ч.2. 99 с.
648. Шаблистий В.В. Теоретико-прикладні засади кримінально-правового забезпечення безпеки людини в Україні : автореф. дис. ... д-ра юрид. н. за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Харків, 2016. 36 с.
649. Шай Р.Я. Правоохоронна функція правової держави: теоретико-практичний аспект : автореферат дис. ... канд. юрид. н. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Львів, 2012. 20 с.
650. Шамрай В.О. Інформаційна безпека як складова національної безпеки України. URL: http://www.crime-research.ru/library/Shamray.htm.
651. Шаптала Н.К. Загальнолюдські цінності у конституційному судовому процесі : аксіологічні виміри // Публічне право : наук.-практ. юрид. журн. Спецвип. 2018. С. 206 – 212.
652. Шаптала Н.К. Співвідношення конституційних прав і свобод людини і громадянина та забезпечення національної безпеки України // Вісн. Конституційного Суду України. 2016, № 6, С. 181–186.
653. Шаптала Н.К., Задорожня Г.В. Конституційне право України : навч. посіб. Дніпропетровськ : ЛізуновПрес, 2012. 471 с.
654. Шариков П., Степанова Н.. Подходы США, ЕС и России к проблеме информационной политики. Современная Европа, 2019. № 2. С. 73-83.
655. Шахбазян К.С. Міжнародно-правові основи регулювання відносин в мережі Інтернет : автореф. дис. ... канд. юрид. н. за спеціальністю 12.00.11 – міжнародне право. Київ, 2009. 19 с.

656. Швець С.В., Швець У.С. Основи системного аналізу : навч. посіб. Суми: Сумськ. держ. ун-т, 2017. 126 с.
657. Шевчук О.Б., Голобуцький О.П.. E-Ukraine: Інформаційне суспільство: бути чи не бути. Київ : Атлант UMS, 2001. 102 с.
658. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 2. С. 299–309.
659. Шемчук В.В. Глобальне інформаційне суспільство: основні підходи та сутнісні характеристики // Верховенство права. Кишинев, Молдова, 2019. № 2.С. 177−183.
660. Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави // Порівняльне-аналітичне право. 2019. Вип. № 2. С. 188−191.
661. Шемчук В.В. Захист інтернет-середовища як складова інформаційної безпеки держави : досвід Франції // Наук. вісн. УжНУ. Серія «Право», 2019. № 57.
662. Шемчук В.В. Інформаційна безпека та інформаційна оборона у контексті розвитку вітчизняної доктрини і законодавчої основи // Вісн. Таврій. наці. ун-ту ім. В.І. Вернадського. Серія юрид. науки. 2019. № 4.
663. Шемчук В.В. Інформаційна функція та її місце в системі функцій сучасної держави // Вісн. Таврій. нац. ун-ту ім. В.І. Вернадського. Серія юрид. науки. 2018. №4. С. 39−45.
664. Шемчук В.В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні // Вісн. Таврій. нац. ун-ту ім. В.І. Вернадського. Серія юрид. науки. 2018. № 6. С.119−124.
665. Шемчук В.В. Конституційна та правова держава в умовах сучасних реформ : теоретичні і практичні проблеми / Верховенство права як гарантія конституційного ладу: матер. наук.-практ. круглого столу (м. Київ, 5 грудня 2019 р.). Київ, 2019. С.179−181.
666. Шемчук В.В. Конституційно-правові основи розвитку інформаційного суспільства в Україні // Наук. вісн. НАВС. 2018. № 3. С.133−144.
667. Шемчук В.В. Концептуальні підходи розуміння інформаційної війни в сучасному світі // Вісн. Таврій. нац. ун-ту ім. В.І. Вернадського. Серія юрид. науки. Том 30 (69) № 3 2019. С.29−35.
668. Шемчук В.В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи // Філософські та методологічні проблеми права. 2019. № 1. С. 51−59.

669. Шемчук В.В. Принципи інформаційної безпеки // Наук. зап. Ін-ту законодавства Верховної Ради України. 2018. Вип.4. С. 50−56.
670. Шемчук В.В. Проблеми концептуального визначення свободи інформації // Верховенство права. Кишинев, Молдова, 2019. № 1. С. 36−41.
671. Шемчук В.В. Соціально-правова природа інформаційного суспільства. Вчені зап. Таврій. нац. ун-ту імені В. І. Вернадського. Серія : Юридичні науки. 2018. Т. 29(68), № 3. С. 109−113.
672. Шемчук В.В. Тенденції і напрями міжнародно-правового регулювання інформаційної сфери // Вісник Південного регіон. центру Нац. академії правових наук України. 2019. № 19. С.106−114.
673. Шемчук В.В. Теоретико-правові засади дослідження інформаційної безпеки // Європейські перспективи. 2019. № 2. С.5−11.
674. Шемчук В.В. Термінологічна різноманітність інформаційної сфери. Українська мова в юриспруденції : стан, проблеми, перспективи: матеріали XV Всеукр. наук.-практ. конф. (Київ, 28 листопада 2019 р.) : у 2 ч. / [редкол.: В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2019. Ч. 1. С. 90−92.
675. Шлемко В.Т., Бінько І.Ф. Економічна безпека України: сутність і напрямки забезпечення : монографія. Київ: НІСД, 1997. 144 с.
676. Шляхтун П.П. Політологія (теорія та історія політичної науки) : навч. посіб. Київ: Либідь, 2005. 576 с.
677. Шумка А.В., Черник П.П. Теоретичні аспекти інформаційних війн та національна безпека // Грані. 2015. № 9. С. 10 –16.
678. Энциклопедический словарь русского библиографического Института Гранат. Москва : Русский библиографический Институт Гранат, б.г. Т. 21. 640 с. URL: http://futura.ru/granat/Энциклопедический словарь Гранат 021.pdf (дата звернення 10.05.2019).
679. Юридическая энциклопедия / отв. ред. Б. Н. Топорнин. Москва : Юристъ, 2001. 1272 с.
680. Юридична енциклопедія : в 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. Київ : Укр. енциклопедія, 1998. – 1999. Т. 2.: Д – Й. 744 с.
681. Я оприлюднював дані зі зламаного сайту Міноборони Росії – очільник «кібер військ». Радіо Свобода. 2014. URL: https://www.radiosvoboda.org/a/26770307.html.
682. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві // Наук. вісн. Львів. держ. ун-ту внутр. справ. Серія Право. Львів, 2016. № 2. С. 244−252.

683. Яременко О. Інформаційна функція української держави : поняття, мета та форми здійснення. Підприємництво, господарство і право. 2005. № 7. С. 66 – 69.
684. Ярочкин В.И. Информационная безопасность : учеб. Москва : Академический Проект; Гаудеамус, 2 -е изд. 2004. 544 с.