

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Соціально-гуманітарний факультет
Кафедра інформаційної та соціокультурної діяльності

КУРИЛО Дмитро Володимирович

**Правове забезпечення інформаційної безпеки при побудові
інформаційного суспільства в Україні / Legal support of
information security in building an information society in
Ukraine**

спеціальність: 029 – Інформаційна, бібліотечна та архівна справа
освітньо-професійна програма – Документознавство та інформаційна діяльність

Кваліфікаційна робота

Виконав студент групи
ДІДм-21
Д.В. Курило

Науковий керівник:
д.іст.н., проф. Л.І. Біловус

Кваліфікаційну роботу допущено
до захисту:

« ____ » _____ 20__ р.

Завідувач кафедри

_____ І.Р. Недошитко

ТЕРНОПІЛЬ - 2022

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. Стан правового регулювання в області забезпечення інформаційної безпеки.....	8
1.1. Міжнародно-правове регулювання у сфері забезпечення інформаційної безпеки	8
1.2. Системний аналіз правового забезпечення інформаційної безпеки в Україні	17
РОЗДІЛ 2. Теоретичні та методологічні основи правового забезпечення інформаційної безпеки в системі органів державної влади та управління	24
2.1. Особливості інформаційних правовідносин при побудові інформаційного суспільства	24
2.2. Поняття інформаційної безпеки та її місце у системі національної безпеки	29
2.3. Проблеми методології правового забезпечення інформаційної безпеки	33
РОЗДІЛ 3. Основні напрямки розвитку правового регулювання в області забезпечення інформаційної безпеки системи органів державної влади та управління	38
3.1. Інформаційне забезпечення державної політики у сфері забезпечення інформаційної безпеки	38
3.2. Заходи щодо реалізації концептуальних та доктринальних документів забезпечення інформаційної безпеки	44
3.3. Система міжнародної інформаційної безпеки	47
ВИСНОВКИ	53
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	57

ВСТУП

Актуальність проблеми. Початок ХХІ століття характеризується новим етапом науково-технічної революції, впровадженням у всі сфери життя інформаційно-комунікаційних технологій, що створюють необхідний фундамент для переходу до інформаційного суспільства та надають величезний вплив на всі аспекти життя суспільства, особистості та держави. Як зазначається у Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» [13], такі технології відкривають нові перспективи задля досягнення вищих рівнів розвитку.

Проте зростаюча роль інформаційної сфери, що є системотворчим чинником життя суспільства, активно впливає на стан політичної, економічної, військової та інших складових національної безпеки України. У зв'язку з цим інформаційна безпека набуває все більшого значення в загальній системі забезпечення національної безпеки України в цілому.

Як впливає із указу Президента України «Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки» від 27.09.2021 р. [38] та рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [44] удосконалення правового забезпечення інформаційної безпеки є одним із пріоритетів при побудові глобального інформаційного суспільства.

Завдання розвитку правового регулювання у сфері забезпечення інформаційної безпеки та напрями його розвитку визначено у Стратегії національної безпеки, затвердженої указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» [43], а також Стратегією інформаційної безпеки, схваленої Президентом України в указі 28.12.2021 року № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [44].

Актуальність дослідження пов'язана з прагненням не лише вивчити проблеми правового забезпечення розвитку інформаційного суспільства, які поки що не знайшли оптимального рішення та потребують застосування

сучасних підходів, а й запропонувати шляхи їх вирішення. При цьому слід зазначити, що теоретичні питання створення інформаційного суспільства та правового забезпечення інформаційної безпеки досліджено недостатньо. Визначення напрямів правового забезпечення інформаційної безпеки потребує системного підходу та правових оцінок з урахуванням опрацювання на основі аналізу особливостей інформаційних відносин, що пов'язані із забезпеченням інформаційної безпеки, впливом на них процесів глобалізації. Багатогранність інформаційних відносин та необхідність їх врегулювання вимагають розробки кодифікованого законодавчого акту, а також проекту засад забезпечення інформаційної безпеки. Вдосконалення правового регулювання у сфері протидії новим викликам та загрозам національній безпеці, їх особливості, а також важлива складова безпеки у сучасному світі – інформаційна безпека та проблеми боротьби з кібертероризмом, теж визначають актуальність проблеми дослідження.

В останні роки процес розробки національної стратегії, необхідної для реалізації зазначених завдань, значно активізувався. Широкий спектр проблем забезпечення інформаційної безпеки особистості, суспільства та держави, розвитку культури кібербезпеки, забезпечення недоторканності приватного життя та захисту прав на доступ до інформації, захисту інформаційних систем, ресурсів та мереж, розширення застосування інформаційних технологій у державному управлінні та при наданні державних послуг, а також інші проблеми інформаційної безпеки потребують системного правового регулювання на основі ретельного аналізу міжнародних правових норм, закордонного законодавства, чинного законодавства України та правозастосовної практики.

Правові підходи до визначення інформаційного суспільства поки що обмежувалися перерахуванням його ознак, завдань, однак не було дано його юридичне поняття, що впливає з теорії права та інформаційного права.

Теоретичним та методологічним дослідженням у галузі правового регулювання інформаційної безпеки присвячені наукові праці, включаючи і дисертаційні дослідження.

Аналіз останніх досліджень та наукових праць. Теоретичною основою міждисциплінарної курсової роботи були наукові праці І. Бачило, В. Цимбалюка, А. Венгерова, М. Швеця, С. Єсімова, А. Яременко, О. Копана, О. Баранова, В. Копилова, І. Арістової, В. Ліпкана, А. Марущака, Р. Калюжного, К. Белякова, А. Новицького, Н. Новицької.

Важливе значення для розробки юридичного поняття інформаційного суспільства, визначення ступеня впливу глобалізації на його розвиток мають роботи зарубіжних авторів теорії інформації, глобалізації (К. Шеннона, Е. Тоффлера, П. Дракера, М. Кастельса, Д. Сайчела, Т. Форестера), так і вітчизняних дослідників у цій галузі В. Гурковський, Л. Кочубей, О. Ніщименко, Б. Кормич, Ю. Коваленко, Р. Калюжний, І. Корж та інші.

Мета дослідження – наукове осмислення фундаментальних теоретичних питань щодо визначення юридичного поняття інформаційного суспільства, особливостей інформаційних правовідносин у галузі забезпечення інформаційної безпеки при побудові інформаційного суспільства в період глобалізації. Вирішення актуальних теоретичних та методологічних питань правового забезпечення інформаційної безпеки необхідне для розробки концептуальних положень правових основ розвитку інформаційного суспільства України.

Відповідно до мети визначимо такі **завдання**:

- проведено порівняльно-правовий аналіз законодавства України, міжнародних та зарубіжних правових актів у галузі правового забезпечення інформаційної безпеки в системі органів державної влади та управління;
- обґрунтовано теоретичні та методологічні питання правового забезпечення інформаційної безпеки в системі органів державної влади та управління в Україні;
- визначено місце та роль правового забезпечення інформаційної безпеки в Україні;
- проаналізовано нові виклики та загрози інформаційній безпеці в умовах глобалізації в системі органів державної влади та управління;

– розглянуто питання формування державної політики та визначення основних напрямів удосконалення законодавства в галузі, що розглядається, у тому числі у сфері Інтернету, спрямованих на реалізацію Національну стратегію сприяння розвитку громадянського суспільства в Україні.

Об'єктом дослідження є місце та роль, а також стан правового забезпечення інформаційної безпеки в системі органів державної влади та управління.

Предметом дослідження виступає коло питань, що стосуються суспільних відносин щодо правового забезпечення інформаційної безпеки в системі органів державної влади та управління в Україні.

Теоретичною основою дослідження були наукові праці Р. Яргера, В. Горбуліна, І. Панової, Б. Герга, О. Баранова, Є. Мануйлова, В. Брижка, В. Пилипчука, С. Ларіна, Г. Ситника та інших вчених.

Методи дослідження. Методологічну основу дослідження становлять такі загальнонаукові методи: діалектичний та дедуктивний методи, системний підхід та аналіз, методи гносеології, формальної логіки, політології, соціології, юриспруденції, соціального управління. Крім того, у роботі застосовувалися і спеціальні методи дослідження правових явищ: порівняльно-правовий аналіз, методи порівняльного правознавства, експертних оцінок, конкретно-соціологічний та формально-юридичний методи.

Обґрунтованість і достовірність результатів дослідження базуються на використанні наукової логіки, широкому застосуванні конкретних методів дослідження, широкій інформаційній базі дослідження, що включає наукову літературу та правові акти, що дозволило вивчити питання у взаємозв'язку, цілісності, всебічно і об'єктивно.

Правова база дослідження ґрунтується на принципах та теоретичних положеннях теорії права та держави, інформаційного, конституційного, цивільного, кримінального, кримінально-процесуального та адміністративного права. При підготовці міждисциплінарної курсової роботи використовувалися положення Конституції України, укази Президента України, постанови

Верховної Ради України, рішення Ради національної безпеки і оборони України, міжнародні правові акти та зарубіжного законодавства.

Апробація роботи. Матеріали кваліфікаційної роботи обговорювалися на засіданні кафедри інформаційної та соціокультурної діяльності. Основні положення роботи пройшли апробацію на конференції (1 доповідь).

Кваліфікаційна робота складається з вступу, трьох розділів та висновків. У вступі обґрунтована актуальність обраної теми дослідження. У першому розділі визначені теоретичні основи правового регулювання в області забезпечення інформаційної безпеки. Другий розділ курсової роботи відображає результати аналізу теоретичних та методологічних основ правового забезпечення інформаційної безпеки в системі органів державної влади та управління. У третьому розділі роботи окреслено заходи напрямків розвитку правового регулювання в області забезпечення інформаційної безпеки системі органів державної влади та управління.

РОЗДІЛ 1

СТАН ПРАВОВОГО РЕГУЛЮВАННЯ В ОБЛАСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Міжнародно-правове регулювання у сфері забезпечення інформаційної безпеки

Дослідження правового забезпечення інформаційної безпеки в Україні пов'язані з необхідністю проаналізувати міжнародні правові акти і зарубіжний досвід правового регулювання у цій сфері.

Одним із першочергових завдань, що стоять перед світовим співтовариством у XXI столітті, є побудова інформаційного суспільства. Значну роль об'єднанні світової спільноти навколо формування інформаційного суспільства займають питання правового забезпечення інформаційної безпеки. Важливим чинником координації зусиль держав є узгоджений та комплексний розвиток правового регулювання цієї сфери суспільних відносин.

Наразі йдуть активні процеси формування міжнародного досвіду у сфері забезпечення інформаційної безпеки в рамках діяльності таких міжнародних організацій, як ООН, Ради Європи, Європейського Союзу, та інших.

Створення інформаційного суспільства стало розглядатися як першорядне завдання Ради Європи з кінця 1993 року, коли було випущено Білу книгу «Економічне зростання, конкуренція, зайнятість – завдання та шляхи їх вирішення на порозі XXI століття». Дій «Шлях Європи в інформаційне суспільство», що передбачає низку механізмів, що дозволяють створити умови для вільного доступу до інформації та одночасно оберігають особу та суспільство.

Основні принципи законодавчого регулювання суспільних відносин у сфері міжнародної інформаційної безпеки сформульовані в основних міжнародних документах і, як показує їх аналіз, є загальновизнаними та пріоритетними у розвитку інформаційного законодавства та для України.

Найважливішим кроком для розвитку законодавства як в інформаційній сфері в цілому, так і в галузі забезпечення інформаційної безпеки було прийняття та проголошення 10 грудня 1948 р. Генеральною асамблеєю ООН Загальної

декларації прав людини [17], у статтях 12, 19, 26 якої встановлено право кожної людини на свободу переконань, думки, совісті, релігії, право на освіту, а також право на вільне вираження цих переконань та право шукати, отримувати та поширювати інформацію та ідеї будь-якими засобами, незалежно від державних кордонів.

Положення, що закріплюють інформаційні права та свободи, були розвинені в Конвенції Ради Європи про захист прав людини та основоположних свобод [20] 1950 року та Міжнародного пакту про громадянські та політичні права [23] 1966 року.

У зазначених актах встановлено, що свобода отримання та розповсюдження інформації реалізується без будь-якого втручання з боку державних органів, незалежно від державних кордонів та поширюється на будь-яку інформацію (стаття 10 Конвенції, стаття 19 Міжнародного пакту).

Таким чином, право на свободу інформації в тому вигляді, в якому воно закріплене в міжнародних документах з прав людини, не є новим суб'єктивним правом людини в галузі інформації, а проявом традиційних свобод думки та слова. Фактично вплив поглядів на свободі як втілення інформаційних прав громадян позначилося становленні принципу свободи інформації.

Основні принципи встановлення меж втручання у приватне життя з боку держави, організацій, юридичних та фізичних осіб також встановлені Загальною декларацією прав людини, Конвенціями ООН та Ради Європи.

Особливо важливим є застосування у законодавстві України загальних принципів, закріплених у Резолюції 2450 (XXIII) від 12.12.1968 р. Генеральної Асамблеї ООН: принцип свободи обміну інформацією; принципи та процедури інформування громадськості про діяльність державних структур, а також принцип контролю держав над комунікаційною діяльністю, що здійснюється під їхньою юрисдикцією, регламентація порядку діяльності та здійснення контролю за телекомунікаціями, включаючи комплексну розробку державної політики у цій сфері. Для розвитку українського інформаційного законодавства важливим є вивчення міжнародного досвіду регулювання суспільних відносин, пов'язаних із забезпеченням інформаційної безпеки.

У рамках ООН триває активний переговорний процес щодо правового режиму інформаційної безпеки. Починаючи з 1998 р. проблеми інформаційної безпеки обговорювалися на всіх сесіях Генеральної Асамблеї ООН, зокрема питання формування понятійного апарату в даній сфері суспільних відносин, а також розробки міжнародно-правового режиму інформаційної безпеки.

Про актуальність розвитку міжнародного співробітництва у сфері забезпечення інформаційної безпеки свідчать також заяви Глав держав-членів Шанхайської організації співробітництва. Лише скоординовані та взаємодоповнюючі заходи на двосторонньому, регіональному та міжнародному рівнях дозволять адекватно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері. При цьому серед можливих напрямів співробітництва передбачається сприяння розробці міжнародної правової бази співробітництва та вироблення єдиного понятійного апарату у сфері забезпечення інформаційної безпеки.

Починаючи з 2000 року в інформаційній сфері прийнято низку основоположних міжнародних документів, таких як Окінавська хартія глобального інформаційного суспільства [25] (далі – Окінавська хартія), підсумкові документи Всесвітньої зустрічі на найвищому рівні з питань інформаційного суспільства (2003 р. у Женеві та 2005 р.), які є політико-правовими документами, спрямованими на прискорення формування постіндустріальних тенденцій в економічній, соціально-політичній та духовній сферах життя суспільства.

Завдання формування нормативної правової бази в інформаційно-комунікаційній сфері визначено як одне із пріоритетних при побудові глобального інформаційного суспільства, проголошеного в Окінавській хартії.

Відповідно до її положень, держави зобов'язуються здійснювати керівництво у просуванні зусиль урядів щодо зміцнення відповідної політики та нормативної бази, що стимулюють конкуренцію та новаторство, забезпечення економічної та фінансової стабільності, сприяють співпраці з оптимізації глобальних мереж, боротьбі зі зловживаннями, які підривають цілісність.

цифрових технологій, інвестування в людей та забезпечення глобального доступу та участі у цьому процесі.

Побудова інформаційного суспільства як глобальне завдання у новому тисячолітті проголосила Декларація принципів із питань інформаційного суспільства, прийнята на Всесвітній зустрічі на найвищому рівні в Женеві в 2003 році, в якій підкреслено, що, будуючи інформаційне суспільство, необхідно забезпечувати, підвищувати довіру та безпеку при використанні інформаційних технологій, що є одним із ключових принципів побудови відкритого для всіх інформаційного суспільства.

Декларація визначила інформаційну та комунікаційну інфраструктуру як необхідний фундамент інформаційного суспільства.

Розвиваючи національне законодавство в галузі забезпечення доступу до інформації необхідно враховувати рекомендації Ради Європи № R (81) 19 «Про доступ до інформації, що є у розпорядженні державних органів» та № R (2002) 2 «Про доступ до офіційних документів», якими встановлено основний принцип доступу до таких документів. Відповідно до останнього, держави повинні гарантувати право кожного громадянина на доступ до офіційних документів, за запитом.

У прийнятих 15.11.2005 року на Всесвітній зустрічі на найвищому рівні з питань інформаційного суспільства Туніському зобов'язанні та Туніській програмі для інформаційного суспільства наголошується, що інформаційно-комунікаційні технології є ефективним інструментом сприяння справі миру, безпеки та стабільності, посиленню демократії, соціальної згуртованості верховенства права на національному, регіональному та міжнародному рівнях. Для досягнення цієї мети ключове значення має розвиток інфраструктури, створення людського потенціалу, інформаційна безпека. Визнається також необхідність ефективної протидії проблемам і загрозам, що виникають внаслідок використання ІКТ, з метою, яка несумісна із завданнями щодо підтримки міжнародної стабільності та безпеки і може негативно вплинути на цілісність інфраструктури в рамках окремих держав на шкоду їхній безпеці. Особливо наголошується на важливості запобігання зловживанням інформаційними

ресурсами та технологіями у злочинних та терористичних цілях, дотримання прав людини.

Особливо важливим є те, що Туніське зобов'язання закликає уряди, використовуючи потенціал ІКТ, створювати державні системи інформації про закони та нормативні положення, що передбачають ширший розвиток мережі пунктів колективного доступу та забезпечують достатню наявність цієї інформації.

Для рівноправного та постійного доступу до інформації потрібне здійснення стратегій довгострокового зберігання цифрової інформації, що створюється.

Сучасні умови потребують комплексного підходу до формування законодавства у сфері автоматизованої обробки персональних даних.

У 1981 році Радою Європи було прийнято Конвенцію про захист особистості у зв'язку з автоматизованою обробкою персональних даних, метою якої є посилення захисту персональних даних, а також правовий захист особи при автоматизованій обробці персональної інформації. Крім того, зазначена Конвенція встановлює вимоги до персональних даних, а також визначає принципи їх справедливого та законного збору та використання.

Конвенція стала першим міжнародним актом, що захищає фізичних осіб від зловживань, які можуть мати місце при збиранні та обробці персональних даних, і водночас ставить завдання регулювання транскордонного потоку персональних даних.

Особливу увагу міжнародні організації приділяють питанням міжнародної торгівлі та здійснення угод з використанням електронних повідомлень та інших засобів зв'язку.

23 листопада 2005 року Генеральною Асамблеєю ООН прийнято Конвенцію про використання електронних повідомлень у міжнародних договорах. З 16 січня 2006 року вона відкрита для підписання державами та спрямована на підвищення ефективності комерційної діяльності, відкриває нові можливості у взаємній торгівлі для раніше віддалених один від одного сторін та ринків, створює однакові правила, спрямовані на усунення бар'єрів для

використання електронних повідомлень у міжнародних договорах. Конвенція має забезпечити можливість державам із різними правовими, соціальними та економічними системами отримати рівний доступ до сучасних каналів торгівлі.

Однією з основних цілей Конвенції є усунення можливих правових перешкод на шляху розвитку електронної торгівлі, які існують у міжнародних документах. Для цього передбачається, що поняття електронного повідомлення, закріплене в тексті Конвенції, застосовується щодо цілого ряду договорів і конвенцій у сферах міжнародної купівлі-продажу товарів та визнання та виконання іноземних арбітражних рішень.

Найбільш повно зазначений вище підхід втілений у Директиві Європейського Парламенту з електронних підписів 1999 р., що виходить, перш за все, з цілей та завдань Римського Договору: забезпечення нормального функціонування внутрішнього ринку Європейського Союзу, вільного переміщення товарів та капіталу, а також вільного пересування фізичних осіб по всій території Євросоюзу.

Директива встановлює рамкове регулювання застосування електронних підписів та надання послуг з надання сертифікатів ключів електронного підпису. Вона не поширюється на укладення та виконання договорів чи інших зобов'язань, що підпорядковуються вимогам національного законодавства держав-учасниць Євросоюзу (ст. 1).

Необхідно зазначити, що основні вимоги Директиви щодо законодавства держав-учасниць щодо використання коштів електронного підпису полягають у добровільній акредитації постачальників даних послуг (ст. 3); гарантії їхнього вільного звернення; транснаціональне використання (ст. 4); гарантії захисту приватних осіб щодо використання персональної інформації, яка надається для отримання сертифікатів ключів електронного підпису (ст. 8); прийняття державами-учасницями нормативних правових актів, що відповідають цій Директиві.

Радою Європи та її Комітетом міністрів було прийнято низку актів щодо забезпечення прозорості діяльності публічної адміністрації, щодо забезпечення свободи думок у ЗМІ. У 1970 році Консультативною Асамблеєю Ради Європи

було прийнято Європейську декларацію про засоби масової інформації та права людини. Ще раніше 1967 р. на Стокгольмській конференції було прийнято Конвенцію про заснування Всесвітньої організації інтелектуальної власності (ВОІВ), яка набула чинності 1979 р.

З метою міжнародного обміну законодавством було прийнято Європейську конвенцію про інформацію щодо іноземного законодавства від 07.06.1968 р., яка передбачає, що сторони зобов'язуються надавати одна одній інформацію щодо свого законодавства та процедур у цивільній та комерційній сферах, а також судову систему.

8 травня 1979 р. Європейський Парламент ухвалив «Резолюцію про захист прав особистості у зв'язку з прогресом інформатики». До цієї резолюції були підготовлені рекомендації парламенту Комісії та Раді про принципи, на яких мають ґрунтуватися норми спільноти щодо захисту даних про особу у зв'язку з технічним прогресом у галузі інформатики.

Слід також наголосити на Директиві Євросоюзу 90/313 про свободу доступу до інформації з навколишнього середовища. Вона надає право доступу до екологічної інформації, що є у розпорядженні державної влади, для всіх юридичних та фізичних осіб.

У сфері розширення доступу до інформації, що є у розпорядженні державних відомств, Комітет міністрів держав-членів Ради Європи 25 листопада 1981 року прийняв Рекомендацію № R (81) 19 «Про доступ до інформації, яка є у розпорядженні державних відомств», у якій визначено принципові підходи отримання інформації із суспільно значущих питань.

Виняткову важливість для правового регулювання відносин в інформаційній сфері мають рекомендації, прийняті Комітетом Міністрів Ради Європи 28 лютого 2001 року, № 2 та № 3, якими регламентуються питання використання правових інформаційних систем, надання судами інформації та надання інших правових послуг громадянам за допомогою нових технологій, передбачено обов'язок держави забезпечити доступ до правової інформації в електронній формі, до електронних реєстрів у правовій галузі, у тому числі через використання мережі Інтернет, а також автоматизацію судових технологій.

Рекомендацією Комітету Міністрів Ради Європи від 21 лютого 2002 року № 2 про доступ до офіційних документів встановлено основний принцип доступу до зазначених документів, згідно з яким державам слід гарантувати право кожного на доступ до офіційних документів, що запитуються, що знаходяться у публічної влади.

У сфері полегшення доступу до правосуддя Комітет Міністрів держав-членів Ради Європи 14 травня 1981 року ухвалив Рекомендацію № R (81) 7 щодо полегшення доступу до правосуддя, в якій рекомендує урядам держав-членів вжити або посилити всі заходи з метою поступової реалізації принципів полегшення доступу громадян до правосуддя та їх інформування про засоби захисту своїх прав у суді, а також спростити, прискорити та здешевити судовий розгляд у цивільних, торгових, адміністративних, соціальних чи податкових справах.

У 1999р. було видано Директиву Європарламенту та Ради Європи «Про електронні підписи», відповідно до якої електронна інформація щодо процедур суду має бути доступна публіці.

Інформація повинна поширюватися з використанням широко доступних технологій (нині Інтернету), і в цьому випадку держава є гарантом справжності та цілісності інформації, поширеної цим способом. При цьому термін «правова інформація» включає всі офіційні тексти законів, правил та відповідних міжнародних угод, а також важливі рішення суду.

У Рекомендаціях R (2001)2 Комітету Міністрів державам – членам Ради Європи щодо влаштування та перебудови судових систем та правових інформаційних систем у рентабельній манері від 28.02.2001 відзначається роль електронних технологій для модернізації систем правосуддя та правових інформаційних систем та забезпечення гарантій безпеки доступу до даних , використання електронних підписів з метою гарантування цілісності даних у системі.

Не менш важливим міжнародним правовим документом є Рекомендації Комітету Міністрів державам-членам Ради Європи від 11. 09.1995 № 11 щодо відбору, обробки, подання та архівації судових рішень у правових інформаційно-

пошукових системах, у них зазначається, що автоматизовані пошукові системи інформації про судову практику мають охоплювати банки даних, незалежно від організації їхнього змісту чи методу поширення, а також нові магнітні та оптичні інформаційні носії.

Завдання автоматизованих пошукових систем полягають, зокрема, у тому, щоб полегшувати роботу юристів шляхом оперативного отримання повної та сучасної інформації; надання інформації всім особам, які виявляють інтерес до судової практики; поширення інформації про нові судові рішення та сприяють єдності судової практики.

Питання конфіденційності та захисту особистих даних при цьому мають регулюватися національним правом відповідно до принципів, закріплених у Конвенції про захист фізичних осіб під час автоматизованої обробки персональних даних та допоміжних документів до неї.

Важливе місце серед міжнародних актів в інформаційній сфері займають питання прозорості засобів масової інформації.

Європейська Конвенція про транскордонне телебачення (ЄКТТ) від 5 травня 1989 р. визначає основні принципи регулювання транскордонного телебачення з урахуванням існуючих Рекомендацій щодо аудіовізуальної масової інформації, її поширення засобами телемовлення та включає загальні норми, спрямовані на гармонійний розвиток програм транскордонного телебачення, включаючи захист прав особистості.

На межі XX-XXI століть у сферу правового забезпечення електронної торгівлі були включені юридичні норми та правила, що регламентують так звані «послуги інформаційного суспільства», а також правовий статус, обов'язки та відповідальність осіб, які надають подібні послуги: електронних магазинів, інформаційних посередників, юридичних чи фізичних осіб, які надають послуги, що належать до електронних підписів, у тому числі випускають сертифікати ключів електронних підписів тощо.

Зазначені питання найбільш повно висвітлено у Директиві Європарламенту «Про електронну торгівлю», положення якої багато зарубіжних держав сприйняли в національному законодавстві.

Формування правової основи єдиного інформаційно-телекомунікаційного простору України тісно пов'язане з міжнародним та зарубіжним досвідом і має здійснюватися на основі принципу системності та збалансованості правових норм з урахуванням загальновизнаних принципів та норм міжнародного права.

Основні принципи законодавчого регулювання суспільних відносин у сфері міжнародної інформаційної безпеки сформульовані в основних міжнародних документах і, як показує їх аналіз, є загальновизнаними та пріоритетними у розвитку інформаційного законодавства та для України.

На основі вивчення міжнародних правових актів, що стосуються протидії новим викликам та загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного суспільства, очевидним є висновок про необхідність подальшої імплементації положень міжнародних правових актів та гармонізації законодавства держав, Лише використання скоординованих та взаємодоповнюючих заходів на двосторонньому, регіональному та міжнародному рівнях дозволить адекватно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері. При цьому серед можливих напрямів співробітництва передбачається сприяння розробці міжнародної правової бази співробітництва та вироблення єдиного понятійного апарату у сфері забезпечення інформаційної безпеки.

1.2. Системний аналіз правового забезпечення інформаційної безпеки в Україні

В даний час в Україні сформувалися необхідні умови для переходу до інформаційного суспільства і, звичайно, однією з таких умов є розвиток системи нормативного правового регулювання відносин у галузі інформаційної безпеки, хоча буде справедливим також визнати, що саме суспільні відносини щодо інформаційної сфери є імпульсом, що впливає на розвиток інформаційного законодавства в цілому та його підгалузі - законодавства у сфері забезпечення інформаційної безпеки.

У цьому дослідженні є доцільним проведення системного аналізу законодавства України у сфері забезпечення інформаційної безпеки з урахуванням його структури «по вертикалі» (принцип субординації) і «по горизонталі» (принцип координації).

Відповідно до загальних для всіх галузей законодавства принципів, виходячи з теорії права, акти законодавства в галузі забезпечення інформаційної безпеки та їх окремі норми відповідно до принципу субординації різняться за своєю юридичною силою.

При вертикальному структуруванні галузі законодавства у аналізованій області в основі ієрархії нормативних правових актів лежить Конституція України, як такі рівні можна назвати рівень законів і рівень підзаконних актів – указів Президента України і постанови Верховної Ради України.

У Конституції України [21] міститься понад 20 правових норм, пов'язаних із забезпеченням інформаційної безпеки, які є основоположними і мають вищу юридичну силу.

У числі основних конституційних правових норм у галузі слід зазначити те, що закріплено право на інформацію, передбачена охорона відомостей, що становлять державну таємницю.

Вивчення конституційного закріплення правових норм, пов'язаних із забезпеченням інформаційної безпеки, показує, що це питання є настільки багатограним та багатоаспектним, що кожна з лише зазначених правових норм може стати темою окремого наукового дослідження. Але навіть такий короткий аналіз окремих положень Конституції України, пов'язаних із забезпеченням захисту інформаційних прав та свобод, підтверджує, що в Основному законі держави міститься значна кількість норм, що становлять основу законодавства у сфері забезпечення інформаційної безпеки.

Конституцією України [21] передбачено прийняття законів, що мають пряму дію на всій території України. У зв'язку з цим як наступний структурний блок у системі законодавства в галузі забезпечення інформаційної безпеки можна виділити норми чинних конституційних законів.

Важливе місце серед нормативних правових актів у зазначеній області займає Кримінальний кодекс України, в якому встановлюється відповідальність за порушення недоторканності приватного життя (стаття 137), таємниці листування та телефонних переговорів (стаття 138), відмова у наданні громадянину інформації (стаття 140), незаконний експорт науково-технічної інформації (стаття 189), розголошення державної таємниці (стаття 283) та інші злочини у цій сфері. Окрема глава Кримінальний кодекс України вперше в українському законодавстві присвячена злочинам у сфері комп'ютерної інформації (глава 28).

Митний кодекс України (статті 186, 214, 344) та Податковий кодекс України (статті 84, 90, 313) також містять норми, що встановлюють режим захисту різних видів конфіденційної інформації.

У Законі України «Про друковані засоби масової інформації (пресу) в Україні» [29] закріплено норми про неприпустимість зловживання свободою масової інформації (стаття 4), конфіденційність інформації (статті 41, 49), обов'язки журналіста отримувати згоду на поширення у ЗМІ відомостей про особисте життя громадянина (стаття 49) та інші.

У Законі України «Про національну безпеку України» [38] міститься поняття безпеки, під якою розуміється стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз. Під життєво важливими інтересами при цьому розуміється сукупність потреб, задоволення яких надійно забезпечує існування та можливості прогресивного розвитку особистості, суспільства та держави (стаття 1), а під загрозами безпеки - сукупність умов та факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства та держави. стаття 3).

Як видно з перелічених визначень, в українському законодавстві поняття «інформаційна безпека» включає значне коло суспільних відносин в інформаційній сфері, крім безпеки безпосередньо інформації, проте більшість норм у зазначеній сфері пов'язана саме із захистом інформації.

Закон «Про захист інформації в інформаційно-комунікаційних системах» [35] є базовим в інформаційній сфері. У ньому містяться визначення

основних понять: інформація – відомості (повідомлення, дані) незалежно від форми їх подання; інформаційні технології – процеси, методи пошуку, збору, зберігання, обробки, надання, розповсюдження інформації та способи здійснення таких процесів та методів; інформаційна система – сукупність інформації, що міститься в базах даних і забезпечує її обробку інформаційних технологій та технічних засобів; інформаційно-телекомунікаційна мережа – технологічна система, призначена для передачі по лініях зв'язку інформації, доступ до якої здійснюється з використанням засобів обчислювальної техніки; власник інформації – особа, яка самостійно створила інформацію або отримала на підставі закону або договору право дозволяти або обмежувати доступ до інформації, яка визначається за будь-якими ознаками; доступ до інформації – можливість отримання інформації та її використання; конфіденційність інформації – обов'язкова для виконання особою, яка отримала доступ до певної інформації, вимога не передавати таку інформацію третім особам без згоди її власника; надання інформації – дії, спрямовані на отримання інформації певним колом осіб чи передачу інформації певному колу осіб; поширення інформації – дії, спрямовані на отримання інформації невизначеним колом осіб або передачу інформації невизначеному колу осіб; електронне повідомлення – інформація, передана чи отримана користувачем інформаційно-телекомунікаційної мережі; документована інформація – зафіксована на матеріальному носії шляхом документування інформація з реквізитами, що дозволяють визначити таку інформацію або у встановлених законодавством України випадках її матеріальний носій; оператор інформаційної системи – громадянин або юридична особа, які провадять діяльність з експлуатації інформаційної системи, у тому числі з обробки інформації, що міститься в її базах даних.

Правове регулювання відносин, що виникають у сфері інформації, інформаційних технологій та захисту інформації, відповідно до зазначеного закону ґрунтується на наступних принципах:

- 1) свобода пошуку, отримання, передачі, виробництва та розповсюдження інформації будь-яким законним способом;
- 2) встановлення обмежень доступу до інформації лише законом;

3) відкритість інформації про діяльність державних органів та органів місцевого самоврядування та вільний доступ до такої інформації, крім випадків, встановлених законом;

4) забезпечення безпеки України при створенні інформаційних систем, їх експлуатації та захисті міститься в них інформації;

5) достовірність інформації та своєчасність її надання;

6) недоторканність приватного життя, неприпустимість збору, зберігання, використання та розповсюдження інформації про приватне життя особи без її згоди;

7) неприпустимість встановлення нормативними правовими актами будь-яких переваг застосування одних інформаційних технологій перед іншими, якщо обов'язковість застосування певних інформаційних технологій до створення та експлуатації державних інформаційних систем не встановлених законом.

Найбільш важливою при розгляді питання про вдосконалення правового регулювання у цьому переліку є проблема категорії персональних даних. Найважливіше значення у розвитку інформаційного законодавства у сфері забезпечення інформаційної безпеки має приведення законодавства у відповідність до ратифікованої Україною Європейської Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних.

Таким чином, багатогранність інформаційних відносин дозволяє зробити висновок про те, що до системи законодавства у сфері забезпечення інформаційної безпеки включаються норми конституційного, адміністративного, цивільного, кримінального, трудового та інших галузей законодавства.

Аналіз українського законодавства в аналізованій сфері дозволяє дійти невтішного висновку, що його структура багато в чому визначається основними напрямками захисту об'єктів інформаційної сфери та інформаційного законодавства: захист інформаційних права і свободи; захист інформації, інформаційних ресурсів та інформаційних систем від неправомірного впливу сторонніх осіб; захист інтересів особи, суспільства та держави від впливу шкідливої, небезпечної, недоброякісної інформації.

На основі системного аналізу законодавства в галузі забезпечення інформаційної безпеки можна зробити висновок про необхідність упорядкування законодавства в галузі, що розглядається, визначення принципів реалізації державної політики та розробки концепції правових основ інформаційного суспільства.

Концепція національної безпеки України відносить забезпечення єдності правового простору до національних інтересів України у внутрішньополітичній сфері та розглядає цю діяльність як одну із складових захисту конституційного ладу в Україні. В даний час суб'єкти України мають величезні інформаційні ресурси, в областях активно здійснюється інформатизація, в діяльності органів державної влади широко впроваджуються сучасні інформаційні технології, прийнято значну кількість нормативних правових актів, що регулюють ці питання.

У сфері забезпечення інформаційної безпеки у суб'єктах України приймаються концепції у сфері інформації, інформатизації (включаючи правову інформатизацію), інформаційних технологій та інформаційної безпеки; формуються та експлуатація державних інформаційних ресурсів; державного обліку та реєстрації баз та банків даних; правові акти, спрямовані на реалізацію законів «Про захист інформації в інформаційно-комунікаційних системах» та «Про персональні дані» в частині забезпечення конфіденційності інформації обмеженого доступу, включаючи персональні дані; забезпечення доступу до інформації, включаючи Інтернет; забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, розподілу та від неправомірних дій; реалізацію ФЦП «Електронне урядування» на регіональному рівні.

Таким чином, системний аналіз чинного законодавства в галузі забезпечення інформаційної безпеки в Україні дозволяє зробити такі висновки, що воно характеризується:

- суперечливістю;

– декларативністю (наприклад, у законодавстві перераховуються понад 40 видів таємниць, а в кодексах згадується лише п'ять, за розголошення яких передбачено відповідальність);

– нерегульованістю низки ключових питань.

Проблеми правового регулювання законодавства про інформаційну безпеку розглядаються у розділі 4 цієї роботи.

Звісно ж, що з розробкою основних напрямів вдосконалення законодавства в аналізованій сфері важливо визначити предметну галузь законодавства і побудову цілісної системи законодавства у сфері забезпечення інформаційної безпеки. Як основні можна виділити три групи об'єктів захисту: інформації та прав на неї, інформаційних ресурсів (право на доступ до інформації, право на таємницю, право на об'єкти інтелектуальної власності); громадянина та суспільства від впливу «шкідливої» інформації; інформаційних систем та прав на них (прав та інтересів держави щодо збереження єдиного інформаційного простору в країні).

Правове регулювання відносин, що виникають у сфері інформації, інформаційних технологій та захисту інформації, нерозривно пов'язане із завданнями побудови інформаційного суспільства.

РОЗДІЛ 2

ТЕОРЕТИЧНІ ТА МЕТОДОЛІЧНІ ОСНОВИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ ТА УПРАВЛІННЯ

2.1. Особливості інформаційних правовідносин при побудові інформаційного суспільства

Інформаційне суспільство у своїй основі формує особливого роду інформаційні відносини, які становлять інтерес для досліджень. В умовах розвитку інформаційного суспільства в Україні інформаційні правовідносини визначаються об'єктивними економічними відносинами, заснованими на різноманітні форм власності, зокрема і інформаційні технології, і є суспільні відносини вільних громадян, засобів, підприємств, фірм, інших суб'єктів права; вони є засобом вирішення завдань у сфері формування єдиного інформаційно-правового простору країни, захисту конституційних прав на інформацію, інформаційного обміну, забезпечення інформаційної безпеки та багатьох інших.

Визначаючи правовідносини як суспільні зв'язки, які виникають на основі норм права, їх учасники набувають суб'єктивних прав та обов'язків, забезпечених державою, ми розглядаємо інформаційні правовідносини як однорідну групу суспільних відносин в інформаційній сфері.

Інформаційна сфера останнім часом розглядається як середовище, в якому створюється, зберігається, обробляється та поширюється інформація та здійснюються всі форми інформаційної взаємодії в суспільстві, що забезпечують його існування та функціонування як єдиного соціального організму. Таке визначення інформаційної сфери (середовища) наголошує на глобальному, всеосяжному характері суспільних відносин та предмету правового регулювання у зазначеній сфері. На основі викладеного, однак, можна дійти невтішного висновку, що інформаційне право, предметом якого є інформаційні правовідносини, є «супергалуззю» українського права.

Кожна галузь права є важливим компонентом правової системи. За своєю роллю у регулюванні суспільних відносин, за своїм соціальним значенням кожна з них займає своє місце у зазначеній системі. Питанням співвідношення

галузей права та його генетичним, і навіть функціональним зв'язкам присвячено безліч монографічних досліджень. Останніми роками критерії виділення галузі права та її місця у системі права отримали достатнього теоретичного обґрунтування.

Інформаційне право є комплексною галуззю права. Розглядаючи інформаційні правовідносини як предмет правового регулювання інформаційного права, можна дійти невтішного висновку: більшість громадських відносин у інформаційній сфері, що є предметом інформаційного права, не збігається з предметом будь-якої іншої галузі права.

Системоутворюючий чинник, що концентрується головним чином на предметі правового регулювання, в інформаційному праві полягає (відбивається) в особливостях суспільних відносин в інформаційній сфері (своєрідність умов збору, обробки, зберігання, поширення, використання, цивільно-правового обороту інформації та пов'язаних з ними процесів інформатизації). Інформаційне право складається не лише з норм та інститутів низки основних гілок права, але й великої кількості інформаційних норм, оскільки в період побудови інформаційного суспільства до правового поля включаються об'єкти, які мають не лише економічну цінність, а й нематеріальні блага, як право на інформацію, спрямовані на вільний та повний розвиток особистості.

Об'єднуючими елементами суспільних відносин в інформаційній сфері як предмета інформаційного права є, насамперед, інформація та інформаційні об'єкти, які мають специфіку при здійсненні прав, виконанні обов'язків та встановленні відповідальності з їх приводу в інформаційній сфері. Однорідність та особливості інформаційних відносин визначаються особливостями та юридичними властивостями цих об'єктів. До таких об'єктів, окрім інформації та інформаційних об'єктів, належать також інформаційні технології, засоби їх забезпечення, засоби зв'язку та телекомунікацій, елементи інформаційної безпеки.

Аналіз особливостей поведінки суб'єктів в інформаційній сфері з приводу інформації, інформаційних та інших об'єктів дає можливість виявити інформаційні відносини щодо окремих видів діяльності, проаналізувати

структуру та склад інформаційних правовідносин, провести класифікацію з об'єктів захисту та за основними напрямками забезпечення інформаційної безпеки.

Правовідносини у сфері забезпечення інформаційної безпеки, як інформаційні правовідносини, виділяються за такими об'єктами захисту як об'єктами інформаційного права:

- правам особи, інтересам суспільства та держави при використанні інформаційно-телекомунікаційних систем та мереж; інформації;
- постійному функціонуванню інформаційно-телекомунікаційних систем та мереж;
- міжнародному співробітництву у сфері безпеки функціонування глобальних інформаційних систем та мереж.

Поряд із вище зазначеними до об'єктів захисту інформаційних правовідносин, що виникають при створенні та застосуванні засобів та механізмів інформаційної безпеки, відносяться:

- інтереси громадянина, суспільства, держави у інформаційній сфері;
- конституційний устрій, суверенітет;
- документована інформація;
- машинні носії з інформацією;
- бази даних у складі автоматизованих інформаційних систем;
- програмні засоби у складі ЕОМ, їх мереж.

Цивільно-правовий аспект інформаційних правовідносин обумовлюється особливостями реалізації інформаційних прав та свобод, насамперед майнових та немайнових прав, а також прав власності на інформаційні ресурси, інші об'єкти в інформаційній сфері, здійснення яких визначається особливостями інформації як об'єкта цивільних прав.

Публічно-правовий аспект інформаційних правовідносин обумовлюється, головним чином, необхідністю формування та здійснення державної політики, що гарантує свободу масової інформації в Україні, управління інформаційними процесами, формування та використання державних інформаційних ресурсів, створення та застосування державних

автоматизованих інформаційних систем та засобів їх забезпечення, в тому числі інформаційної безпеки, для досягнення головної мети – забезпечення гарантій здійснення інформаційних прав та свобод.

Інформаційне суспільство відрізняється від суспільства, в якому домінують традиційна промисловість та сфера послуг, тим, що інформація, знання, інформаційні послуги та всі галузі, пов'язані з їх виробництвом (телекомунікаційна, комп'ютерна, телевізійна), зростають швидшими темпами, є джерелом нових робочих місць, стають домінуючими в економічному розвитку. На шляху до інформаційного суспільства змінюється функція фахівців, які беруть участь у формуванні та організації використання інформації про ситуацію та події у політиці, економіці, законотворчості, науці, культурі, освіті та інших сферах суспільної діяльності.

Це відбувається під впливом різкого збільшення ролі інформації у економічно розвинених країнах і кількості людей, основним заняттям яких є створення, збирання, обробка, поширення, зберігання інформації, продаж інформаційних продуктів та надання інформаційних послуг з використанням сучасних інформаційних технологій.

Автоматизація інформаційних технологій призводить до поступового витіснення паперових носіїв, що доводить їхню роль до розумних (зручних людині) меж. Так, створення системи розрахунків у режимі реального часу передбачає у найближчому майбутньому відмовитися від застосування у роботі банківської системи держави паперових носіїв первинної інформації та перейти до роботи з електронними документами. Складність таких технологій, звісно, породжує і складні суспільні відносини, які потребують спеціального правового регулювання. Особливість цих відносин у тому, що безпосереднім їх об'єктом стає, з усього сказаного, інформація у електронно-цифровій формі. Звідси випливає, що основним предметом правового регулювання необхідно визнати соціальні (суспільні) відносини, що виникають у процесі створення, перетворення та споживання інформації на основі застосування автоматизованих інформаційних технологій. Ці відносини становлять особливий різновид інформаційних відносин. Такі відносини деякі автори називають інформаційно-

комп'ютерними, а зазначену діяльність відносять до сфери комп'ютерної інформації. Їх специфіка, в такий спосіб, зумовлена особливостями самої природи інформації на машинних носіях і безпосередньою технологією її обробки. Тепер інформація – об'єкт права.

Процес впровадження інформаційних технологій дозволяє виявити основні суспільні відносини, які при цьому виникають та потребують правового врегулювання. До них можна віднести відносини, що виникають при:

- забезпеченні конституційних прав на інформацію, що обробляється за допомогою автоматизованих інформаційних технологій;
- розроблення, впровадження та експлуатації комп'ютерних систем та мереж, а також телекомунікаційних мереж;
- створення, поширення, передачу, купівлю-продаж програмного забезпечення для ЕОМ та інших засобів забезпечення автоматизованих інформаційних систем;
- формування та використання інформаційних ресурсів, що включають електронні банки даних;
- встановлення та дотримання режиму доступу до комп'ютерної інформації та проведення інших заходів інформаційної безпеки;
- міжнародний обмін комп'ютерною інформацією.

Суспільні відносини – це різноманітні зв'язки між соціальними групами, націями, релігійними громадами, а також усередині них у процесі економічної, соціальної, політичної, культурної та іншої діяльності. Таким чином, інформаційні відносини та особливості їх регулювання визначаються таким видом діяльності, як інформаційна.

У структуру предмета правового регулювання теорії права прийнято включати такі елементи: суб'єкти і об'єкти регульованих громадських відносин; юридичні факти, що сприяють виникненню відповідних правовідносин; практичну діяльність людей.

Світова практика свідчить про те, що на рівні законів зазначені відносини регулюються за трьома основними напрямками:

- 1) захист прав громадян на доступ до інформації;

- 2) захист інформації (інформаційна безпека);
- 3) охорона авторських прав на програми для ЕОМ та бази даних.

Теоретично права прийнято вважати, що з виникнення нової галузі права необхідні щонайменше чотири умови:

- 1) наявність державного інтересу у створенні конкретної галузі права;
- 2) чітке вираження специфіки регульованих суспільних відносин, що становлять предмет самостійного правового регулювання;
- 3) потреба у особливому методі правового регулювання;
- 4) наявність чи потреба у спеціальних правових нормах.

Всім цим умовам, безперечно, повністю відповідає інформаційне право як нова самостійна галузь російського права, яка фактично давно об'єктивно існує та активно розвивається. Щодо питання диференціації права на галузі права досі немає єдиної думки.

Інформаційна безпека суб'єктів інформаційних відносин (особистості, суспільства, держави) у цій роботі розглядається як одна з цілей правового режиму інформації. Аналіз правових відносин щодо забезпечення інформаційної безпеки дозволяє зробити висновок, що структура зазначених відносин багато в чому визначається основними напрямками захисту об'єктів інформаційної сфери та інформаційного законодавства: захист інформаційних права і свободи; захист інформації, інформаційних ресурсів та інформаційних систем від неправомірного впливу сторонніх осіб; захист інтересів особи, суспільства та держави від впливу шкідливої, небезпечної, недоброякісної інформації.

2.2. Поняття інформаційної безпеки та її місце у системі національної безпеки

Поняття інформаційної безпеки доцільно визначити як стан захищеності національних інтересів України в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства та держави, від внутрішніх та зовнішніх загроз.

Перехід до інформаційного суспільства становить основний зміст національних інтересів. Прийнято низку концептуальних, доктринальних та

програмних документів щодо розвитку окремих складових інформаційної інфраструктури, удосконалення системи управління наукою та системи освіти, впровадження інформаційних технологій у діяльність органів державної влади, використання інформаційних технологій у важливих сферах діяльності людини, суспільства та держави.

Удосконалюється інформаційна інфраструктура як складова глобальної інформаційної інфраструктури, швидкими темпами розвивається ринок послуг зв'язку.

Інформаційні технології вже використовуються в економічному, політичному, соціальному та духовному житті суспільства, у науково-технічній сфері та сфері освіти.

Розвивається система правового регулювання відносин, яка пов'язана із створенням та використанням інформаційних технологій.

Однак зберігається залежність української інформаційної інфраструктури від зарубіжних інформаційних технологій внаслідок невисокої конкурентоспроможності продукції вітчизняної мікроелектронної промисловості, українського телекомунікаційного обладнання, засобів обчислювальної техніки та програмних продуктів. Більше 95% всіх інформаційних та телекомунікаційних систем, що експлуатуються в Україні, створено на базі зарубіжних інформаційних технологій.

У перспективі реальна загроза подальшого зниження конкурентоспроможності вітчизняної продукції як на внутрішньому, так і на зовнішніх ринках. У той самий час імператив інформаційної глобалізації для України – інноваційна конкурентоспроможність.

Слід також зважати на те, що інтенсивний розвиток інформаційних технологій призводить до появи нових загроз національній безпеці. Збільшення масштабів соціальної небезпеки протиправних діянь в інформаційній сфері обумовлює необхідність підвищення захищеності критично важливих об'єктів інформаційної інфраструктури, посилення протидії загрозі розповсюдженню комп'ютерної злочинності та її крайньої форми – кібертероризму.

Як показує світовий досвід постіндустріального розвитку, важливим фактором інтенсифікації формування інформаційного суспільства є об'єднання зусиль та ресурсів держави, суспільства та бізнесу для досягнення загальновизнаних цілей – підвищення конкурентоспроможності країни, добробуту та якості життя її громадян, зміцнення обороноздатності та безпеки.

У цих умовах було необхідно прийняття політичного документа, який би, з одного боку, інтегрально визначив основні напрямки діяльності з формування інформаційного суспільства, а з іншого – дозволив підключити на основі партнерства можливості та потенціал приватного капіталу та громадянського суспільства, без яких це завдання вирішено бути не може.

Оскільки суспільні відносини, що виникають у зв'язку із забезпеченням інформаційної безпеки відносяться до інформаційної сфери, і до сфери забезпечення національної безпеки в цілому, в даній роботі є необхідним проаналізувати його основні характеристики, визначити, що є законодавством у сфері забезпечення інформаційної безпеки.

Для визначення поняття законодавства у сфері забезпечення інформаційної безпеки, безумовно важливим є визначення таких понять, як «інформація» та «безпека». Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особистості у зазначеній сфері, зміцненні демократії, створенні правової соціальної держави, досягненні та підтримці суспільної згоди, у духовному відновленні Росії, а інтереси держави у створенні умов для гармонійного розвитку російської інформаційної інфраструктури для реалізації конституційних права і свободи людини і громадянина в галузі отримання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності Росії, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

На нашу думку, стан захищеності не є в сучасних умовах статичним, а навпаки, вимагає постійного вдосконалення у зв'язку з глобальними викликами та загрозами, що виникають у наш дуже динамічний «інформаційний вік»,

їхньою транскордонністю, надзвичайно швидким розвитком, трансформацією, коли інформаційні технології стрімко розвиваються і приносять суспільству як благо, а й безліч проблем і використовуються, на превеликий жаль, й у злочинних цілях.

При розгляді в рамках даного дослідження проблеми формування законодавства в галузі забезпечення інформаційної безпеки є важливим його визначення з позиції теорії права та з урахуванням його стану. При цьому неможливо абстрагуватися від поняття інформаційного законодавства, оскільки їх взаємозв'язок очевидний, так само як і не викликає сумніву необхідність вивчення формування інформаційного законодавства та пов'язаних із нею питань визнання інформаційного права як самостійна галузь права.

В рамках цього дослідження автор вважає, що забезпечення інформаційної безпеки, так само як і забезпечення національної безпеки в цілому, слід розглядати як складну багаторівневу функціональну складову системи національної безпеки в інформаційній сфері, що включає сукупність взаємопов'язаних складових, що розвиваються, таких як національні інтереси, виклики і загрози національним інтересам; система забезпечення інформаційної безпеки.

Для забезпечення інформаційної безпеки при побудові інформаційного суспільства найважливіше значення має розробка нового стратегічного документа про національну безпеку України концептуального характеру та розробка законопроекту про національну безпеку, оскільки сучасна правова система потребує законодавчого закріплення глибоко опрацьованих, науково обґрунтованих сучасних понять: «національна безпека», «національні інтереси», «загрози національної безпеки», «забезпечення національної безпеки», «система національної безпеки», а також необхідні правові механізми протидії новим викликам та загрозам інформаційній безпеці держави. Крім того, потребують законодавчого закріплення у відповідному федеральному законі про Раду Безпеки України її правовий статус та повноваження щодо вироблення державної політики в галузі національної безпеки, включаючи забезпечення інформаційної безпеки.

2.3. Проблеми методології правового забезпечення інформаційної безпеки

Розглядаючи в рамках даного дослідження теоретичні та методологічні проблеми в галузі правового забезпечення інформаційної безпеки, важливим є позначити проблеми, пов'язані з фундаментальними змінами в системі життєвих цінностей, способі життя. З впровадженням інформаційних технологій у правовій сфері виникає «подвійна» проблема: інформатизація у праві та право в інформації. Крім того, в умовах побудови інформаційного суспільства виникає потреба зміни принципів правового регулювання у всіх сферах людської діяльності. З'являються нові галузі права, нові способи виникнення правовідносин та, головне, інформаційні технології суттєво впливають на правову систему. Не можна побудувати інформаційне суспільство в окремо взятій країні, з'явився віртуальний простір, якому вже дано визначення як сукупності інформаційних відносин. Ці відносини набули нової характеристики – вони часто стають «наддержавними», «наднаціональними», змінюються традиційні підходи до їх правового регулювання. Виникли нові види загроз у сфері інформаційної безпеки. Процеси, пов'язані зі становленням основ інформаційного суспільства, змінять і форму права.

Взаємозв'язок права та інформації, їх взаємозалежність від інформаційних технологій вимагають розвитку основ теорії інформаційного права, пов'язаних, передусім, зі зміною розуміння методів і механізмів, і навіть принципів правового регулювання.

Історична своєрідність української дійсності полягає в тому, що довгий час в інформаційних відносинах основне місце займала інформаційна діяльність держави, яка полягала як в інформаційному обслуговуванні громадян, так і в інформаційному забезпеченні самої держави, її органів, організацій, установ та посадових осіб. У цьому інформаційне забезпечення грало роль не функціональної, а допоміжної підсистеми системи соціального управління, представляючи певну інформаційну базу, необхідну державі реалізації всіх його функцій. Оскільки будь-який процес управління, що здійснюється в соціальних

системах, по своїй суті є інформаційним процесом, пов'язаним з отриманням, переробкою і передачею інформації, то інформація як така виступала безпосереднім інструментом управління.

Принципи та методи як самої науки інформаційного права, так і методи дослідження його предмета, а також окремих його структурних частин продиктовані його специфікою, яка має на увазі як поєднання загальнонаукових методів, які притаманні всім або більшості юридичних наук, міжгалузевих, характерних для кількох галузей науки, так і суто спеціальних, характерних лише даного предмета дослідження – інформаційного права. Таке різноманіття пояснюється лише тим, що галузь інформаційного права носить комплексний характер, вона побудована за предметним ознакою, і у неї може бути єдиного методу ні регулювання, ні вивчення.

Процес формування інформаційного права та інформаційного законодавства є складним та тривалим. Наукові дослідження в галузі інформаційного права вперше з'явилися у юридичній науці у 60-70 роки ХХ століття. У науковій літературі того часу можна зустріти різні назви інформаційного права: комп'ютерне право, правова кібернетика, програмне право, програмна інформатика, інформаційно-комп'ютерне право, телекомунікаційне право і, нарешті, «інформаційне право». Однак не можна не визнати, що правове регулювання суспільних відносин в інформаційній сфері здійснювалося в основному класичними галузями права, насамперед адміністративним.

Поділяючи висновки деяких учених про те, що інформаційне право виділяється в самостійну галузь права, враховуючи безліч об'єктивних для цього факторів (наявність загального предмета правового регулювання, конституційних положень, базових законів та великої кількості норм, що стосуються даної сфери та містяться в інших нормативних правових актах) у різних галузях правничий та законодавства, зокрема, норм міжнародного права, актуальність завдань економічного, соціального та політичного розвитку та інших), можна стверджувати сьогодні, що інформаційне право сформувалося як самостійна галузь права.

Право забезпечення інформаційної безпеки також сформувалося як його підгалузі, хоча у великих і складних за складом галузях права (цивільному, кримінальному, трудовому праві) виділяються такі компоненти, як підгалузі, які є цілісним утворенням, яке регламентується специфічним видом відносин у межах сфери правового регулювання відповідної галузі права. Не можна не враховувати, що воно вже має структуру і складається з базових, спеціальних, комплексних галузей. Профілюючими, базовими галузями є конституційне право, три матеріальні галузі – цивільне, адміністративне та кримінальне право, що відповідають їм процесуальній галузі. Саме в цій групі сконцентровані головні юридичні режими та засоби регулювання, тому у сфері саме базових галузей виявляються дуже складні та тонкі зв'язки та залежності, які є предметом теорії права. Крім того, він виділяє спеціальні галузі, де правові режими модифіковані та пристосовані до особливих сфер життя суспільства (трудове, земельне, фінансове, сімейне право тощо).

Так звані класичні галузі права формують найповнішу гаму методів правового регулювання в інших галузях. Зазвичай, комплексні чи вузькоспеціалізовані галузі виникають у результаті вичленування їх предмета з базових галузей за збереження методу правового регулювання. Така справа і з інформаційним правом. Базові галузі створюють свої сімейства спеціалізованих галузей.

З позиції теорії права у межах предметної галузі права чи комплексної галузі права не формується у сенсі самостійний метод правового регулювання. Такі галузі акумулюють усі методи правового регулювання не більше свого предмета, тобто. одна й та область громадських відносин регулюється методами різних базових галузей права.

Акумулювання норм різних галузей права та законодавства навколо одного предметного комплексу суспільних відносин особливо помітно – в результаті виділення галузі права на самостійну, яка отримує свій статус у системі права і перетворюється на комплексну галузь права саме на тій підставі, що більш активно взаємодіє з усіма іншими галузями.

Багатофункціональність та специфіка інформації, суспільних відносин, пов'язаних з її збиранням, обробкою та зберіганням, а також забезпеченням інформаційної безпеки, призводять до необхідності застосовувати у законодавстві у сфері забезпечення інформаційної безпеки весь відомий спектр методів правового регулювання залежно від виду та призначення інформації.

Відносини у сфері забезпечення інформаційної безпеки регулюються методами адміністративного, цивільного та інших галузей права. Наприклад, збирання та обробка персональних даних проводиться з дотриманням конституційних прав і свобод громадян, а порядок діяльності структур, що обробляють таку інформацію, регулюється нормами як конституційного, так і адміністративного права, так само як і надання статистичної, звітної інформації та інших державних інформаційних ресурсів. При створенні інформації, що представляє результат творчості, застосовуються цивільно-правові методи, так само регулюються питання комерційної, банківської таємниці та інші питання, пов'язані з інформацією. Статті Цивільного кодексу закріплюють таку форму відносин, як інформаційні послуги, визнаючи електронний підпис або інший аналог власноручного підпису як засіб, що засвідчує справжність підпису.

Аналіз законодавства в даній галузі дозволяє зробити висновок про поєднання всіх зазначених методів правового регулювання, що свідчить про їх комплексний характер, що виражається у поєднанні конституційного регулювання, адміністративних способів забезпечення інформаційної безпеки, залучення всього арсеналу регулюючих, контрольних, примусових, каральних та стимулюючих заходів.

Метод правового регулювання включає спосіб взаємозв'язку прав і обов'язків між учасниками правовідносин, сукупність юридичних фактів, що служать підставою для виникнення, зміни або припинення правовідносин, способи формування змісту прав і обов'язків суб'єктів права, санкції, способи і процедури їх застосування.

Дозвільний метод передбачає такий характер інформаційної діяльності, при якому учасникам суспільних відносин надається свобода у реалізації своїх прав, цілей та завдань.

При цьому в ході реалізації зазначеного методу можуть використовуватися інші методи – делегуючий, рекомендаційний і санкційний.

При делегуючому методі правового регулювання законодавець, відповідний орган державної влади або уповноважена особа надає конкретні права та свободи учасникам правовідносин у сфері забезпечення інформаційної безпеки у межах конкретного розділу інформаційного законодавства.

Рекомендаційний спосіб виявляється у тому, що учасникам правовідносин надано право самим вибирати ті чи інші варіанти поведінки і відповідно до цього діяти.

Санкційний метод правового регулювання – це такий спосіб, при якому законодавець надає тому чи іншому учаснику відносин у галузі забезпечення інформаційної безпеки право самому приймати рішення з питань, що його цікавлять, але ці рішення в той же час повинні бути санкціоновані в установленому законом порядку.

У законодавчій сфері забезпечення інформаційної безпеки використовують і обмежувально-заборонні методи. Особливо це характерно для правових норм, що містяться в адміністративному та кримінальному праві.

Протягом минулого десятиліття масштаби інформаційних загроз значно зросли. Агресивне інформаційне середовище здатне порушити і навіть знищити цивілізацію. Події останніх дають підстави вважати, що інформація може бути сильнішою за будь-який з раніше відомих знарядь масового ураження.

РОЗДІЛ 3

ОСНОВНІ НАПРЯМКИ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ В ОБЛАСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ ОРГАНІВ ВЛАДИ ТА УПРАВЛІННЯ

3.1. Інформаційне забезпечення державної політики у сфері забезпечення інформаційної безпеки

Система інформаційного забезпечення державної політики у сфері забезпечення інформаційної безпеки є основою для координації управління з метою сталого розвитку та захисту національних інтересів в інформаційній сфері від внутрішніх та зовнішніх викликів і загроз та репрезентує сукупність державних органів та інших уповноважених суб'єктів, які беруть участь у здійсненні інформаційного супроводу забезпечення державної політики та регульованих нормативними правовими актами відповідних суспільних відносин.

У рамках цього дослідження доцільно розглядати державну політику в галузі забезпечення інформаційної безпеки в широкому сенсі, оскільки інформаційна безпека при побудові інформаційного суспільства пронизує всі сфери життєдіяльності особистості, суспільства та держави.

Державна політика у сфері використання інформаційних технологій у державному управлінні спрямована на забезпечення координації діяльності органів у структурі державної влади щодо створення державних інформаційних систем, ресурсів і надання громадських послуг, і навіть підвищення ефективності бюджетних витрат у цій сфері.

Інформаційне забезпечення державної політики має здійснюватися на основі таких принципів:

- відкритості державної політики – всі основні заходи, пов'язані з державною політикою, відкрито обговорюються суспільством і держава враховує громадську думку;
- рівності інтересів усіх суб'єктів, які беруть участь у формуванні державної політики;

- системності – при реалізації прийнятих рішень щодо зміни стану одного з об'єктів регулювання повинні враховуватися його наслідки для стану інших та всіх у сукупності;
- соціальної орієнтації – основні заходи державної політики мають бути спрямовані на забезпечення соціальних інтересів громадян України;
- пріоритетності права – розвиток та застосування правових та економічних методів має пріоритет перед будь-якими формами адміністративних рішень.

Основними завданнями системи інформаційного забезпечення державної політики є: ефективне формування та використання національних інформаційних ресурсів та забезпечення широкого, вільного доступу до них; забезпечення громадян суспільно значущою інформацією та розвиток незалежних засобів масової інформації; створення необхідної нормативної правової основи формування системи інформаційного забезпечення державної політики.

Однорідні, суттєво взаємопов'язані компоненти системи інформаційного забезпечення державної політики мають консолідуватись у єдині загальнодержавні системи та структури, що об'єднують інформаційний простір держави у єдине ціле для забезпечення формування державної внутрішньої та зовнішньої політики. Основні напрями державної політики України реалізуються через систему державних органів, що має сприяти координації управління.

Державні органи, органи місцевого самоврядування відповідно до своїх повноважень беруть участь у розробці та реалізації цільових програм застосування інформаційних технологій, а також створюють інформаційні системи та забезпечують доступ до інформації, що в них міститься, державною мовою України.

Багато в чому завдяки діяльності системи інформаційного забезпечення державної політики вдалося досягти громадської підтримки заходів щодо реалізації національних проектів, проведення адміністративної реформи, а також забезпечити певний рівень довіри населення до діяльності державних органів та

розпочати створення системи державних гарантій реалізації прав людини та громадянина на отримання достовірної та об'єктивної інформації про діяльність державних органів.

Водночас слід визнати обґрунтованою критику недостатньо широкого інформування державними органами громадян про свої дії, що становлять значний суспільний інтерес, особливо на етапі підготовки рішень, виконання прийнятих рішень. Зберігається недостатній рівень координації діяльності об'єктів інформаційного супроводу державної політики.

У рекомендаціях Ради Європи № R (81) 19 «Про доступ до інформації, що є у розпорядженні державних органів» та № R (2002) 2 «Щодо доступу до офіційних документів» також наголошується на необхідності забезпечення широкого доступу громадськості до офіційних документів державних органів.

Правові норми, що стосуються правового забезпечення державної політики, державне регулювання у сфері застосування інформаційних технологій визначено у Законі України «Про захист інформації в інформаційно-комунікаційних системах»:

1) регулювання відносин, пов'язаних з пошуком, отриманням, передачею, виробництвом та поширенням інформації із застосуванням інформаційних технологій (інформатизації), на підставі принципів, встановлених цим законом;

2) розвиток інформаційних систем різного призначення для забезпечення громадян (фізичних осіб), організацій, державних органів та органів місцевого самоврядування інформацією, а також забезпечення взаємодії таких систем;

3) створення умов ефективного використання інформаційно-телекомунікаційних мереж, зокрема мережі Інтернет та інших подібних інформаційно-телекомунікаційних мереж [35].

Основною метою формування системи інформаційного забезпечення державної політики та використання інформаційних технологій у діяльності федеральних органів державної влади є підвищення ефективності механізмів державного управління на основі створення загальної інформаційно-

технологічної інфраструктури, що включає державні інформаційні системи та ресурси, а також засоби, що забезпечують їх функціонування, взаємодію між собою, населенням та організаціями у межах надання державних послуг з метою реалізації прав громадян, у інформаційній сфері.

Як основні напрями державної політики у інформаційній сфері можна назвати такі:

- забезпечення умов для ефективного реалізації та захисту конституційних прав та свобод людини в інформаційній сфері;
- створення політичних, економічних, правових та інших засад побудови інформаційного суспільства;
- розвиток національної інформаційної інфраструктури; забезпечення економічних та правових умов для розвитку ринку та інформаційних технологій та інформаційних послуг;
- сприяння застосуванню інформаційних технологій у державному управлінні, економіці, обороні, охороні здоров'я, освіті, екології тощо;
- забезпечення рівноправної інтеграції країни до глобального інформаційного простору, дотримання міжнародних договорів та угод в інформаційній сфері.

Однією з головних функцій держави є зовнішньополітична діяльність – взаємодія на офіційному рівні з іншими державами та світовою спільнотою в особі її міждержавних інституцій та організацій.

З метою вдосконалення системи інформаційного забезпечення державної політики вона має ґрунтуватися на системі та структурі органів державної влади, проте нині роль координуючого органу у цій сфері визначена недостатньо чітко.

Нормативне правове забезпечення, що регламентує питання взаємодії громадян та організацій з державними інститутами та прийняття рішень в органах державної влади, включаючи нормативні правові акти всіх рівнів від законодавства до посадових інструкцій, також пов'язане з реалізацією державної політики, що вимагає забезпечення інформаційної безпеки, має здійснюватися на основі системності, усунення прогалин та необхідності врегулювання на

законодавчому рівні ключових питань про право на інформацію, забезпечення доступу до інформації тощо.

Крім основних законодавчих та інших нормативних правових актів для регулювання структури системи органів влади, формування зв'язків, визначення правил та порядку роботи, встановлення взаємодії між різними гілками, рівнями та окремими елементами всередині самої системи для інформаційного забезпечення державної політики мають бути прийняті відповідні управлінські рішення. як адміністративно-розпорядчих, так і нормативних правових актів.

Реалізація державної політики у сфері забезпечення формування державних інформаційних ресурсів має здійснюватися з урахуванням розвитку системи загальнодоступних інформаційних ресурсів із застосуванням сучасних інформаційних технологій, зокрема, з використанням мережі Інтернет. Вирішення зазначених завдань пов'язане зі створенням, формуванням, обробкою, обміном та поданням інформаційних ресурсів в електронній формі, забезпеченням їх достовірності та цілісності, забезпеченням прав громадян та організацій на отримання інформації з усіх загальнодоступних інформаційних систем, посиленням контролю за інформаційною безпекою, використанням засобів криптографії при передачу інформаційних ресурсів.

Важливу роль при цьому відіграє кадрове забезпечення, яке пов'язане з визначенням та прогнозуванням потреби у фахівцях у галузі формування системи інформаційного забезпечення державної політики та підвищенням якості підготовки відповідних наукових та технічних кадрів.

Одним із пріоритетних напрямів державної політики у сфері, що розглядається, має стати вдосконалення механізмів правового регулювання суспільних відносин, що виникають у галузі забезпечення інформаційної безпеки.

Розвиток законодавства в галузі забезпечення інформаційної безпеки України має базуватися, перш за все, на дотриманні таких загальноправових принципів, як законність, справедливість, юридична рівність громадян, гуманізм, демократизм, єдність прав та обов'язків, міжгалузевих принципів, наприклад, невідворотності відповідальності, а також таких галузевих

принципів, як дотримання балансу інтересів особистості, суспільства та держави та їхньої взаємної відповідальності, інтеграції в рамках міжнародної інформаційної безпеки.

На підставі викладеного системний метод дослідження дозволяє автору визначити як основні фактори реалізації державної політики у зазначеній сфері формування та розвиток відповідної системи законодавства, системи інформаційних ресурсів, інформаційно-комунікаційної інфраструктури, науково-технічного та виробничого комплексу інформаційної індустрії, ринку інформаційної продукції та послуг, системи масової інформаційної освіти, освіти та підготовки професійних кадрів для інформаційної сфери.

Для інформаційного забезпечення державної політики та розробки основних напрямів удосконалення законодавства в галузі, що розглядається, важливим є визначення предметної галузі законодавства та побудови цілісної системи законодавства в галузі забезпечення інформаційної безпеки та в якості основних можна виділити три групи об'єктів захисту: інформація та права на неї, інформаційні ресурси (право на доступ до інформації, декларація про таємницю, декларація про об'єкти інтелектуальної власності); громадянина та суспільства від впливу «шкідливої» інформації; інформаційні системи та права на них (права та інтереси держави щодо збереження єдиного інформаційного простору в країні).

Звісно ж, що у галузі нормативно-правового забезпечення безпеки інформаційно-телекомунікаційних систем та мереж, необхідні реалізації державної інформаційної політики, основними напрямками регулювання є:

- захист прав особистості, інтересів суспільства та держави при використанні інформаційно-телекомунікаційних систем та мереж;
- захист інформації в інформаційно-телекомунікаційних системах та мережах;
- забезпечення стійкого функціонування інформаційно-телекомунікаційних систем та мереж;
- розвиток міжнародного співробітництва у сфері безпеки функціонування глобальних інформаційних систем та мереж.

Систему інформаційного забезпечення державної політики у сфері інформаційної безпеки представляє сукупність державних органів та інших уповноважених суб'єктів, які беруть участь у здійсненні інформаційного супроводу забезпечення державної політики та встановлених нормативними правовими актами відповідних суспільних відносин.

У галузі нормативно-правового забезпечення інформаційної безпеки можна виділити такі основні напрями регулювання:

- захист особистості, інтересів суспільства та держави при використанні інформаційно-телекомунікаційних систем та мереж;
- захист інформації;
- забезпечення стійкого функціонування інформаційно-телекомунікаційних систем та мереж;
- розвиток міжнародного співробітництва у сфері безпеки функціонування глобальних інформаційних систем та мереж;
- правова рівність всіх учасників процесу інформаційної взаємодії незалежно від їхнього політичного, соціального та економічного статусу, що ґрунтується на конституційному праві громадян на вільний пошук, отримання, передачу, виробництво та розповсюдження інформації будь-яким законним способом.

3.2. Заходи щодо реалізації концептуальних та доктринальних документів забезпечення інформаційної безпеки

Відповідно до Декларації принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003., питання забезпечення національної безпеки в інформаційній сфері віднесені до основних завдань, що вимагають вирішення для досягнення поставленої мети розвитку інформаційного суспільства в Україні [13].

Зазначений документ є не лише політичною основою, а й певною мірою правовою підставою для підготовки та уточнення наявних, а також розробки нових доктринальних, концептуальних, програмних та інших документів, що

визначають цілі та напрямки діяльності органів державної влади, принципи та механізми їх взаємодії з організаціями та громадянами у галузі розвитку інформаційного суспільства в Україні.

У зазначеній Декларації також враховано основні положення Окінавської хартії глобального інформаційного суспільства, Декларації принципів побудови інформаційного суспільства, Плану дій Туніського зобов'язання та інших міжнародних документів, ухвалених на Всесвітній зустрічі на найвищому рівні з питань розвитку інформаційного суспільства.

Очевидна актуальність питань, пов'язаних з правовим забезпеченням інформаційної безпеки при побудові інформаційного суспільства в Україні.

На основі системного аналізу законодавства в галузі забезпечення інформаційної безпеки автор даного дослідження приходить до висновку про необхідність упорядкування законодавства в галузі, що розглядається, визначення принципів реалізації державної політики та розробки з цією метою концепції розвитку та вдосконалення законодавства.

Дотримання одного з основних принципів права – принципу законності вимагає від органів державної влади при вирішенні конфліктів, що виникають в інформаційній сфері, неухильно керуватися законодавчими та іншими нормативними правовими актами, що регулюють відносини в цій сфері.

Особливістю правового забезпечення інформаційної безпеки є необхідність дотримання принципу балансу інтересів особистості, суспільства та держави в інформаційній сфері, що передбачає законодавче закріплення пріоритету цих інтересів у різних сферах життєдіяльності суспільства, а також використання форм громадського контролю у діяльності органів державної влади та органів місцевого самоврядування. Реалізація гарантій конституційних права і свободи людини і громадянина інформаційної сфері є найважливішим завданням держави у сфері інформаційної безпеки.

На жаль, неврегульованість правовідносин, пов'язаних з розвитком інформатизації та забезпеченням інформаційної безпеки, формуванням та використанням державних інформаційних ресурсів, реалізацією права всіх суб'єктів на інформацію, захистом інтересів користувачів та власників

інформаційних ресурсів від внутрішніх та зовнішніх загроз можуть викликати непоправні негативні наслідки.

Потрібні концептуальні підходи щодо забезпечення стану захищеності від внутрішніх та зовнішніх загроз в інформаційній сфері, таких як: «інформаційна зброя»; інформаційно-психологічний вплив на здоров'я, свідомість та поведінку людини; комп'ютерні злочини; використання глобальних інформаційних систем та мереж: широке розповсюдження електронної пошти, електронної торгівлі, освітньої, комерційної діяльності з використанням Інтернету та ін.

Стан захищеності, який визначається інформаційна безпека не є в сучасних умовах статичним, а, навпаки, вимагає постійного вдосконалення у зв'язку із зазначеними вище викликами та загрозами нашого дуже динамічного «інформаційного століття», їх транскордонністю, надзвичайно динамічним розвитком, трансформацією, коли інформаційні технології стрімко розвиваються і приносять суспільству як благо, а й безліч проблем і використовуються, на превеликий жаль, й у злочинних цілях.

Для забезпечення інформаційної безпеки необхідний розвиток та вдосконалення законодавства в цій галузі на основі комплексного, міждисциплінарного, системного наукового теоретико-правового дослідження, що включає вивчення особливостей суспільних відносин в інформаційній сфері, нових викликів та загроз, розробку нових концептуальних документів.

Також вимагають вироблення загальних концептуальних підходів питання внесення змін до низки чинних нормативних правових актів, зокрема федеральних законів, спрямованих на врегулювання спільних питань власності в інформаційній сфері, охорони прав на об'єкти інтелектуальної творчості, що має важливе значення для боротьби з таким видом комп'ютерних злочинів як незаконний обіг об'єктів інтелектуальної власності на електронних носіях (контрафактної продукції).

Істотні прогалини спостерігаються у правовому регулюванні суспільних відносин, що виникають в інформаційних мережах. Вимагають законодавчого вирішення питання: - підвищення потенціалу інформації як ресурсу; розподілу

компетенції державних органів щодо формування інформаційних ресурсів, що мають державне значення, та забезпечення користування ними; ліцензування та сертифікації інформаційних систем, технологій та продукції; ліквідації монополізму; захисту інформації, автоматизованих інформаційних систем та засобів їх забезпечення як об'єктів власності; захисту авторських прав на автоматизовані інформаційні системи та засоби їх забезпечення; гарантії права на інформацію; встановлення відповідальності за порушення у роботі з інформацією.

З розвитком інформаційного суспільства та виникненням у зв'язку з цим нових суспільних відносин особливої гостроти та соціальної значущості набуває проблема їх адекватного правового регулювання. Правова основа розвитку єдиного інформаційного простору України при побудові інформаційного суспільства має сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та засобів інформаційного виробництва в країні у процесі її руху до створення інформаційного суспільства. Важливість проблеми вироблення концептуальних підходів до розвитку законодавства в інформаційній сфері визначається також тією обставиною, що норми законів цієї сфери істотно впливають на якість регулювання відносин суб'єктів у всіх сферах життя країни.

3.3. Система міжнародної інформаційної безпеки

В рамках цього дослідження, враховуючи глобалізацію інформаційних процесів, транскордонність інформаційного простору, нові виклики та загрози в інформаційній сфері, а також формування міжнародного досвіду у сфері забезпечення інформаційної безпеки у діяльності таких міжнародних організацій, як Рада Європи, Європейський Союз, ООН, ШОС необхідне дослідження проблем створення системи міжнародної інформаційної безпеки.

Побудова інформаційного суспільства почала розглядатися як першорядне завдання Ради Європи з кінця 1993 р., коли було випущено Білу книгу «Економічне зростання, конкуренція, зайнятість – завдання та шляхи їх

вирішення на порозі XXI століття». У червні 1994 року Радою Європи було ухвалено план дій «Шлях Європи в інформаційне суспільство», що передбачає низку механізмів, що дозволяють створити умови для вільного доступу до інформації та одночасно оберігають особу та суспільство.

Переговорний процес щодо правового режиму міжнародної інформаційної безпеки в рамках ООН, починаючи з 1998 р., і проблеми, пов'язані із забезпеченням інформаційної безпеки, не втрачають своєї актуальності. На міжнародному рівні очевидна необхідність формування понятійного апарату у цій сфері суспільних відносин, визначення міжнародно-правового режиму інформаційної безпеки. Відповідні пропозиції України щодо переліку загроз, а також визначення термінів та понять були направлені до Секретаріату ООН.

Тільки вживання скоординованих та взаємодоповнюючих заходів на двосторонньому, регіональному та багатосторонньому міжнародному рівнях дозволить адекватно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері, при цьому серед можливих напрямків обов'язковим має бути вдосконалення міжнародної правової бази співробітництва та вироблення єдиного понятійного апарату у сфері забезпечення міжнародної інформаційної безпеки.

Роль узгодженого та комплексного розвитку правового регулювання суспільних відносин у галузі забезпечення інформаційної безпеки при побудові світовою спільнотою глобального інформаційного суспільства відзначається практично у всіх міжнародних правових актах, що стосуються цієї сфери, і є важливим фактором координації зусиль держав при побудові системи міжнародної інформаційної безпеки у глобальному інформаційному суспільстві.

Про актуальність розвитку міжнародного співробітництва у сфері забезпечення інформаційної безпеки свідчать також досвід такого співробітництва, спрямований на вироблення узгодженого понятійного апарату, розроблення міжнародних правових актів, просування ініціатив у галузі міжнародної інформаційної безпеки в рамках Шанхайської організації співробітництва (м. Шанхай, КНР).

Відповідно до Заяви глав держав-членів Шанхайської організації співробітництва (ШОС) з міжнародної інформаційної безпеки 15 червня 2006 року було прийнято рішення про створення Групи експертів держав – членів ШОС з міжнародної інформаційної безпеки (МІБ) для вироблення плану дій держав-членів ШОС у цій галузі та визначення можливих шляхів та засобів вирішення проблем у всіх її аспектах.

На виконання зазначеного рішення міжнародною Групою експертів було розроблено План дій держав-членів ШОС щодо забезпечення міжнародної інформаційної безпеки, затверджений главами держав 16 серпня 2007 р., який передбачає співпрацю за такими напрямками з метою створення системи міжнародної інформаційної безпеки:

- вироблення єдиного понятійного апарату, що включає перелік відповідних термінів та понять у сфері інформаційної безпеки для підвищення ефективності практичної взаємодії в галузі МІБ на просторі ШОС з метою забезпечення сумісності законодавств держав-членів ШОС;

- аналіз загроз у галузі міжнародної інформаційної безпеки (існуючих та потенційних у зв'язку з розвитком інформаційних технологій та вироблення пропозицій щодо визначення та застосування адекватних заходів протидії їм);

- вироблення пропозицій щодо створення практичних механізмів моніторингу загроз та координації дій щодо забезпечення інформаційної безпеки на просторі ШОС, враховуючи транскордонний характер інформаційно-комунікаційних технологій та загроз МІБ;

- вивчення та зіставлення національних законодавств у сфері забезпечення інформаційної безпеки, що є важливою складовою розвитку співробітництва у цій сфері та основою для координації протидії загрозам МІБ, у тому числі для боротьби з використанням інформаційно-комунікаційних технологій у ворожих, злочинних терористичних та екстремістських цілях;

- дослідження питання про міжнародно-правове регулювання та стан міжнародно-правової бази сфери МІБ (на думку більшості експертів держав-членів ШОС, наявних міжнародно-правових документів, що так чи інакше

стосуються сфери забезпечення МІБ, недостатньо, вони не скоординовані, допускають різні трактування основних понять);

– участь у міжнародних організаціях та форумах, проведення консультацій експертів, у тому числі з правових питань забезпечення інформаційної безпеки;

– розробка та здійснення заходів довіри між державами-членами ШОС у сфері забезпечення інформаційної безпеки (включаючи розробку механізму обміну інформацією, методиками протидії використанню інформаційно-комунікаційних технологій у ворожих, злочинних та терористичних цілях);

– вивчення можливих шляхів надання взаємної допомоги, у сфері запобігання деструктивним інформаційним впливам та надзвичайним ситуаціям у сфері інформаційної безпеки;

– вивчення доцільності розробки та укладання міжнародних угод про співробітництво у сфері забезпечення МІБ.

Право на свободу інформації в тому вигляді, в якому ми зустрічаємо його в міжнародних документах з прав людини, не є новим суб'єктивним правом людини в галузі інформації, а проявом традиційних свобод думки і слова в міжнародному інформаційному обміні. Фактично вплив поглядів на свободі як втілення інформаційних прав громадян позначилося становленні принципу міжнародного інформаційного обміну, принципу вільного потоку інформації, який продовжує панувати у сфері відносин.

Основні засади встановлення меж втручання у приватне життя з боку держави, організацій, юридичних та фізичних осіб, встановлені Загальною декларацією прав людини, Конвенціями ООН та Ради Європи.

Основні принципи законодавчого регулювання суспільних відносин у сфері міжнародної інформаційної безпеки сформульовані в основних міжнародних документах і, як показує їхній аналіз, є пріоритетними у розвитку інформаційного законодавства та для України.

Особлива увага має бути приділена участі у міжнародних дослідницьких проектах з пріоритетних напрямів розвитку науки, технологій та техніки, а також, що з точки зору забезпечення інформаційної безпеки має ключове

значення при побудові глобального інформаційного суспільства, участь у розробці міжнародних стандартів у сфері інформаційних та телекомунікаційних технологій, гармонізація національної системи стандартів та сертифікації у цій сфері з міжнародною системою.

Такий системний підхід відображає мету державної політики в галузі міжнародної інформаційної безпеки, оскільки без потенціалу міжнародного співробітництва у цій сфері для ліквідації чи суттєвого зниження шкоди національним інтересам, а також інтересам міжнародної спільноти, пов'язаних із підтриманням миру та стабільності від прояву загроз злочинного чи агресивного використання інформаційно-комунікаційних технологій.

Надається необхідним для формування системи міжнародної інформаційної безпеки створення механізмів забезпечення довіри у сфері використання інформаційно-комунікаційних технологій задля забезпечення стійкості інформаційної сфери; формування міжнародної системи розслідування злочинів, що скоюються з використанням інформаційно-комунікаційних технологій, виявлення та припинення кібертероризму.

Продовжуються дискусії щодо проблем анонімності в Інтернеті, можливості у зв'язку з цим безперешкодно порушувати авторські права, здійснювати протиправні дії (поширювати шкідливі програми, наклеп, незаконно отримувати інформацію тощо). Однак, незважаючи на те, що в Декларації про свободу комунікацій в Інтернеті, прийнятої Радою Європи 28.05.2003, як один із принципів проголошено гарантії права користувача на анонімність, це не позбавляє можливості держав вживати заходів і співпрацювати з метою встановлення осіб, які вчинили кримінальні злочини. діяння, відповідно до національного законодавства, Конвенцією про захист прав людини та основних свобод та іншими міжнародними угодами.

Вирішення завдання обмеження анонімності при транскордонному електронному обміні та використання його як механізму забезпечення міжнародної інформаційної безпеки досить складне не лише в технічному та організаційному плані, а й у політичному та міжнародно-правовому аспекті. В умовах надійної ідентифікації користувачів, яка, на думку фахівців у цій галузі,

може бути створена, міждержавна взаємодія за фактами порушення міжнародної інформаційної безпеки при транскордонному електронному обміні, має бути переведена в площину міжнародного права з визначенням механізмів компенсації фінансової та іншої шкоди державою. території якого здійснено порушення.

При побудові інформаційного суспільства пошук шляхів вирішення цих проблем має суттєве значення, оскільки є важливою, базовою ланкою в механізмі забезпечення міжнародної інформаційної безпеки щодо запобігання таким загрозам, як заподіяння шкоди інформаційній, телекомунікаційній, критично важливій інфраструктурі держави, інформаційний вплив, що підриває економічну, політичну та інші системи держави, терористична та екстремістська діяльність.

ВИСНОВКИ

Парадигма розвитку людського суспільства, що стрімко змінюється, глобалізація економіки, перехід до постіндустріальних форм розвитку, поява нових викликів і загроз військово-політичного, кримінального, терористичного характеру – ці тенденції впливають на динамічний прогрес у галузі техніки та технологій, серед яких особливо виділяються інформаційні технології. Сьогодні вже неможливо собі уявити відсутність мобільного зв'язку, персональних комп'ютерів та мережі Інтернет, які міцно увійшли до повсякденного життя. Проте розвиток інформаційних технологій значно випереджає їхнє гуманітарне осмислення, насамперед у галузі права. Це підтверджується як міжнародними актами, без постійних посилянь куди у цьому дослідженні просто неможливо обійтись, і дуже динамічним розвитком зарубіжного законодавства та інформаційного законодавства України.

Найважливішими принципами побудови інформаційного суспільства, які є основним вектором у цій діяльності, не випадково визначено зміцнення довіри та безпеки, верховенства права при використанні інформаційно-комунікаційних технологій, що значною мірою визначило дослідницьку мотивацію автора та вироблення конкретних пропозицій.

Інформаційні війни, інформаційний тероризм та кіберзлочинність стали, на жаль, реальністю нашого часу. Сьогодні міжнародне співтовариство усвідомило загрозу національній та глобальній інформаційній безпеці та готує до практичних кроків щодо її нейтралізації. У багатьох країнах вживаються часом дуже жорсткі заходи у цій сфері, але вони виявляються малоефективними, насамперед, внаслідок транскордонного характеру нових загроз та анонімності порушників. Ніхто не може почуватися надійно захищеним, самотужки борючись із інформаційними загрозами.

Система інформаційної безпеки в Україні покликана забезпечувати збереження державної та інших таємниць, захищати інформаційні ресурси та інформаційно-телекомунікаційну інфраструктуру від впливу інформаційної зброї, загроз інформаційного тероризму та інформаційного криміналу.

Необхідність системного методологічного підходу до дослідження зазначених питань пов'язана з тим, що інформаційна безпека відіграє дедалі значнішу роль загальної системи забезпечення національної безпеки України.

Удосконалення правового забезпечення інформаційної безпеки є одним із пріоритетів при побудові глобального інформаційного суспільства, проголошеного в Окінавській хартії глобального інформаційного суспільства, підписаної Президентом України 22.12.2000 року, а також впливає зі Декларації принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003 року.

Визначення напрямків правового забезпечення інформаційної безпеки потребує системного підходу та правових оцінок з урахуванням опрацювання на основі аналізу законодавства у галузі забезпечення інформаційної безпеки особливостей інформаційних відносин, пов'язаних із забезпеченням інформаційної безпеки, а також впливу на них процесів глобалізації. Багатогранність інформаційних відносин та необхідність їх урегулювання дозволяє автору зробити висновок про необхідність розробки кодифікованого законодавчого акта – Інформаційного кодексу, а також проекту Основ законодавства України про інформаційну безпеку.

У цій роботі сформульовано поняття інформаційного суспільства, пропозиції щодо вдосконалення чинного інформаційного законодавства, доповнено принципи правового забезпечення інформаційної безпеки, відзначено особливості інформаційних правовідносин при побудові інформаційного суспільства, пов'язані з комплексним характером інформаційно-правової діяльності, а також приватно-публічні методи правового регулювання інформаційної сфери.

Широкий спектр проблем інформаційної безпеки особистості, суспільства та держави, розвитку культури кібербезпеки, забезпечення недоторканності приватного життя та захисту прав на доступ до інформації, захисту інформаційних систем, ресурсів та мереж, розширення застосування інформаційних технологій у державному управлінні та при наданні державних послуг, а також цілий ряд інших проблем інформаційної безпеки потребують

системного правового регулювання на основі ретельного аналізу міжнародних правових норм, закордонного законодавства, чинного законодавства України та правозастосування.

У цьому дослідженні також розглянуто актуальні питання просування ініціатив у галузі міжнародної інформаційної безпеки, зокрема у рамках Шанхайської організації співробітництва. Проблеми правового регулювання в цій галузі викликають занепокоєння у всіх держав-учасниць цієї організації з урахуванням глобалізації викликів та загроз, розробляється понятійний та термінологічний апарат, визначаються виклики та загрози, їх ознаки, вирішується питання щодо розробки міждержавної угоди.

Проблеми врегулювання відносин в Інтернеті, встановлення відповідальності за зміст інтернет-сайтів та інтернаціоналізації управління Інтернетом також мають міжнародний характер, у зв'язку з чим ця проблема потребує додаткового вивчення для вироблення взаємоузгоджених пропозицій та їх реалізації. Враховуючи роль ООН у сучасному світі як безпрецедентну, автор вважає, що сьогодні немає інших таких універсальних майданчиків, як ООН, для узгодження інтересів учасників глобального інформаційного суспільства та вирішення питань, пов'язаних із забезпеченням міжнародної інформаційної безпеки, включаючи інтернаціоналізацію управління Інтернетом. ООН накопичила багатий більш ніж піввіковий досвід, виробила систему міжнародного права, і жодна країна сама не здатна вирішити міжнародні проблеми інформаційної безпеки. Тому так важливим є створення та розвиток системи міжнародної інформаційної безпеки на основі міжнародного інформаційного права, і автором обґрунтовується необхідність створення такого органу (організації) при ООН.

Як пріоритетні обґрунтовуються такі напрями правового забезпечення інформаційної безпеки України як:

- законодавче закріплення механізмів реалізації державної підтримки вітчизняних виробників інформаційних та комунікаційних технологій;
- розвиток та впорядкування законодавства про різні види інформації обмеженого доступу, у тому числі визначення принципів співвідношення видів

таємниць та формування відповідних правових режимів конфіденційності; законодавче врегулювання режиму службової таємниці;

➤ законодавче регулювання доступу до інформації органів державної влади та органів місцевого самоврядування, питань формування відкритих державних інформаційних ресурсів з метою створення умов для роз'яснення основних напрямів державної політики, обґрунтування прийнятих рішень, підтримання інформаційної взаємодії суспільства та держави, надання громадянам своєчасної та об'єктивної інформації щодо найважливіших подій суспільного життя;

➤ ухвалення нормативних правових актів, що забезпечують реалізацію концепції електронного уряду, у тому числі надання державних послуг із використанням інформаційно-комунікаційних технологій, розвиток довіреного електронного документообігу та електронної комерції на основі використання загальнодоступних інформаційно-телекомунікаційних мереж;

➤ вдосконалення законодавства у частині посилення захисту прав користувачів та суб'єктів, що представляють послуги зв'язку та інформаційні послуги, створення ефективних механізмів контролю за дотриманням законодавства України у сфері інформаційних технологій та зв'язку;

➤ розвиток законодавства, що забезпечує технічне регулювання застосування інформаційних технологій, інформаційних систем та інформаційно-телекомунікаційних мереж у критично важливих галузях життя суспільства та держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Antiroikko A. V. Introduction to democratic E governance //E transformation in Governance: new directions in government and politics. Idea Group Publishing. 2004. P. 22-51.
2. Breton F., Proux S. Explosion de la communication. Naissance de la nouvelle idéologie, p. 12.
3. Daniel T. Lasica. Strategic Implications of Hybrid War: A Theory of Victory – School of Advanced Military Studies, 2009. URL: <https://doi.org/10.1037/e505392012-001>
4. Fountain J. Towards a Theory of Federal Bureaucracy for the Twenty-First Century// Governance.com: Democracy in the information age, Washington D.C.: Brookings institution press, 2002.
5. Pardo T. Realizing the Promise of Digital Government: It's more than Building a Web Site. *Information Impacts Magazine*. 2000. October.
6. Yarger Richard H, George Barber. The U.S. Army War College Mehtodology for Determining Interests and Levels of Intensity. Carlisle Barracs, U.S. Army War College, 1997. URL: <http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm>; <http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm>
7. Yong J. Sl. E government in Asia: enabling public service innovation in the 21st century. Singapore: Times Editions. 2003.
8. Yuriy Kuniev, Iryna Sopilko, Valerii Kolpakov: Object and subject of information law. Journal of law and political sciences scientific and academy journal. 2020. Vol. 23. Issue 2. P. 9-41.
9. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. № 9. С. 100-108.
10. Бугайчук К. Функції публічного адміністрування в органах Національної поліції України: поняття та класифікація. *Підприємництво, господарство і право*. 2018. № 5. С.112-117.
11. Горбулін В. На захист національних інтересів. *Політика і час*. 1995. № 2. С. 3-8.

12. Горбулін В.П. Засади національної безпеки України. К. : Інтер-технологія, 2009. 272 с.
13. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003. URL: https://zakon.rada.gov.ua/laws/show/995_c57#Text
14. Демкова М.С., М. В. Фігель. Доступ до інформації та електронне урядування К.: Факт, 2004. 336 с.
15. Державне агентство з питань науки, інновацій та інформації України. URL: <http://www.dknii.gov.ua/index.php/uk/component/content/article/189-1-1>
16. Деякі питання реалізації в Україні Ініціативи «Партнерство «Відкритий Уряд»»: Постанова Кабінету Міністрів України від 13 черв. 2012 р. № 671 URL: <http://www.kmu.gov.ua>
17. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. Неофіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
18. Зарубіжний досвід публічного адміністрування: метод. рек. / за заг. ред. Н. М. Мельтюхової. К.: НАДУ, 2010. 28 с.
19. Зарубіжний досвід упровадження електронного врядування / Авт. кол.: Т. Камінська, А. Камінський, М. Пасічник та ін.; за заг. ред. д-ра наук з держ. упр., проф. С. А. Чукут. К.: Вид-во НАДУ, 2008. 200 с.
20. Конвенція про захист прав людини і основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
21. Конституція України: Із змінами, внесеними Законами України від 07 лютого 2019 року, N 2680-VIII. URL: <https://www.president.gov.ua/documents/constitution>
22. Мануйлов Є.М., Калиновський Ю.Ю. Аксіологічний вимір інформаційної безпеки української держави. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. № 3 (34) 2017. С. 13-30
23. Міжнародний пакт про громадянські і політичні права. Ратифіковано Указом Президії Верховної Ради Української РСР N 2148-VIII (2148-08) від 19.10.73 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

24. Міненко М. А. Трансформація системи державного управління в сучасні моделі регулювання суспільства. Державне управління: удосконалення та розвиток. URL: <http://www.dy.nauka.com.ua/?op=1&z=581>

25. Окінавська Хартія Глобального Інформаційного Суспільства. URL: https://zakon5.rada.gov.ua/laws/show/998_163#Text

26. Перун Т. Значення адміністративної відповідальності в системі заходів забезпечення інформаційної безпеки. Право України. 2017. № 10. С. 202-209.

27. Про державне прогнозування та розроблення програм економічного і соціального розвитку України: Закон України // Відом. Верхов. Ради України. 2000. № 25. Ст. 195. URL: <http://www.rada.gov.ua>

28. Про державні цільові програми: Закон України // Відом. Верхов. Ради України. 2004. № 25. Ст. 352. URL: <http://www.rada.gov.ua>

29. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.92. № 2783-XII. URL: <https://zakon.rada.gov.ua/laws/show/2782-12#Text>

30. Про затвердження плану заходів з виконання завдань, передбачених Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» : Розпорядження Кабінету Міністрів України від 15 серп. 2007 р. №653-р URL: <http://www.kmu.gov.ua>

31. Про затвердження плану заходів з виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку «Україна – 2020» у 2015 році: Розпорядження Кабінету Міністрів України від 04.03.2015 р. №213-р. URL: <http://zakon5.rada.gov.ua/laws/show/213-2015-%D1%80>

32. Про затвердження плану заходів з впровадження Ініціативи «Партнерство «Відкритий Уряд»»: Розпорядження Кабінету Міністрів України від 18 лип. 2012 р. № 514-р URL: <http://www.kmu.gov.ua>

33. Про затвердження плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 26 верес. 2011 р. №1014-р URL: <http://www.kmu.gov.ua>

34. Про затвердження Порядку розроблення та затвердження державних цільових програм : Постанова Кабінету Міністрів України від 31 січ. 2007 р. №106. URL: <http://www.kmu.gov.ua>

35. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.94, № 81/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

36. Про Концепцію Національної програми інформатизації: Закон України // Відом. Верхов. Ради України. 1998. № 27-28. Ст. 182. URL: <http://www.rada.gov.ua>

37. Про Концепцію Національної програми інформатизації: Закон України // Відом. Верхов. Ради України. 1998. № 27-28. Ст. 182. URL: <http://www.rada.gov.ua>

38. Про національну безпеку України: Закон України. Відомості Верховної Ради, № 31, ст.241, 2018. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

39. Про Національну програму інформатизації: Закон України // Відом. Верхов. Ради України. 1998. №27-28. Ст. 181. URL: <http://www.rada.gov.ua>

40. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки : Указ Президента України від 27.09.2021 р. № 487/2021. URL: <https://zakon.rada.gov.ua/laws/show/487/2021#Text>

41. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. №537-V. URL: <http://zakon2.rada.gov.ua/laws/show/537-16>

42. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України // Відом. Верхов. Ради України. 2007. № 12. Ст. 102. URL: <http://www.rada.gov.ua>

43. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037>

44. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 року № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>

45. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12.01.2015 р. № 5/2015. URL: <http://zakon0.rada.gov.ua/laws/show/5/2015#n10>

46. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ*. Серія юридична. 2016. Випуск 2. С. 244-252.