ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
Факультет міжнародних економічних відносин, управління і бізнесу
Кафедра державного управління і місцевого самоврядування

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: **ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ**

Виконала: здобувачка другого (магістерського)
рівня вищої освіти групи 6зУА
спеціальності 281 «Публічне управління та адміністрування»
освітньо-професійної програми
«Публічне управління та адміністрування»
Літвінова Ю.В.
_____
(прізвище та ініціали)
Керівник Половцев О.В.
_____
(прізвище та ініціали)

Хмельницький 2024 року

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *міжнародних економічних відносин, управління і бізнесу*
Кафедра *державного управління і місцевого самоврядування*
Рівень вищої освіти *другий (магістерський)*
Спеціальності *281 Публічне управління та адміністрування*
Освітньо-професійна програма: *Публічне управління та адміністрування*

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри,
д. держ. упр., професор
_____ ***Вікторія ФІЛІППОВА***
«_____» _____ 2024 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Літвінова Юлія Артурівна
(прізвище, ім'я, по батькові)

1. Тема роботи *Шляхи забезпечення інформаційного суверенітету України.*
керівник роботи *Половцев Олег Валентинович, д.держ.упр., професор.*
затверджена наказом закладу вищої освіти від *18.01.2024 р. № 69-с*
2. Строк подання студентом роботи *грудень 2024 року*
3. Вихідні дані до роботи *Законодавчі та нормативні документи, підручники, навчальні посібники, періодичні видання, планові та звітні показники діяльності.*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): *Теоретико-методологічні основи розуміння інформаційного суверенітету. Аналіз існуючих інформаційних загроз, місце гібридної війни та впив дезінформації та маніпуляції на громадську думку. Рекомендації щодо концепції нової моделі кібербезпеки та інформаційного суверенітету країни.*
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) *Робота містить 5 рисунків та 1 таблицю.*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Консультант з написання І-ІІІ розділів	*Олег ПОЛОВЦЕВ, Професор*	*19.01.2024* р	
Консультант з нормоконтролю	*Наталія КРЕТОВА, провідний фахівець*		

7. Дата видачі завдання *19.01.2024 р*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Огляд літературних джерел з теми	*19.01.2024 -25.02.2024*	*Виконано*
2.	Складання і затвердження плану роботи	*27.02.2024 - 11.03.2024*	*Виконано*
3.	Написання І розділу	*26.09.2024 - 09.10.2024*	*Виконано*
4.	Написання ІІ розділу	*10.10.2024 - 24.10.2024*	*Виконано*
5.	Написання ІІІ розділу	*25.10.2024 - 11.11.2024*	*Виконано*
6.	Формулювання висновків за темою дослідження	*12.11.2024 - 21.11.2024*	*Виконано*
7.	Оформлення роботи	*22.11.2024 - 25.11.2024*	*Виконано*
8.	Надання роботи керівнику для перевірки та написання подання	*26.11.2024 - 30.11.2024*	*Виконано*
9.	Подання роботи для перевірки у КСПНП	*01.12.2024*	*Виконано*
10.	Захист роботи в ЕК		

Здобувач _____ *Юлія ЛІТВІНОВА*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Олег ПОЛОВЦЕВ*
(підпис) (прізвище та ініціали)

Літвінова Ю.В. Шляхи забезпечення інформаційного суверенітету України. – Рукопис.

Кваліфікаційна робота магістра за спеціальністю 281 «Публічне управління та адміністрування». Херсонський національний технічний університет. Хмельницький, 2024.

У дослідженні з’ясовано зміст проблеми забезпечення інформаційного суверенітету в Україні. Охарактеризовано сутність інформаційного суверенітету, місце суверенітету у національній безпеці держави. Розкрито міжнародний досвід реалізації інформаційного суверенітету, також описано правову основу інформаційного суверенітету.

У роботі розглянуто інформаційні загрози та їхні джерела в Україні, гібридні війни та інформаційна безпека. Даною роботою узагальнено вплив дезінформації та маніпуляцій на громадську думку. Розроблено нову модель кібербезпеки та інформаційного суверенітету країни.

Матеріали роботи будуть корисними для стратегічного планування у сфері інформаційної безпеки, розвитку національних інформаційних ресурсів і технологій, а також можуть бути використані для аналізу співпраці з міжнародними організаціями в контексті інформаційної безпеки.

Ключові слова: інформаційний суверенітет, інформаційна безпека, інформаційне суспільство, інформаційний простір, кібербезпека.

ЗМІСТ

ВСТУП

Актуальність: у сучасних умовах розвитку інформаційного суспільства та процесів глобалізації змінюється роль держави як політико-територіальної організації суспільства, причому ці зміни стосуються не лише її функціонального призначення. Формується новий правовий простір, що має наддержавний характер.

Одночасно реальний географічний простір, визначений державними кордонами, зазнає трансформацій, доповнюючись віртуальним простором Інтернету. Це суттєво впливає на розширення розуміння інформаційної складової державного суверенітету, який набуває нових рис у вигляді інформаційного суверенітету.

Разом із тим стрімкий розвиток цифрових технологій, глобальна доступність мережі Інтернет, а також прогрес у створенні нейронних мереж і штучного інтелекту викликають неоднозначні реакції щодо ефективності правового регулювання інформаційного простору на національному та міжнародному рівнях.

Зростає розуміння важливості вирішення питань регулювання суспільних інформаційних відносин, зокрема необхідності узгодження різних підходів до визначення та формулювання поняття "інформаційний суверенітет", а також уточнення його основних характеристик. Це дозволяє знайти ефективні методи й засоби для його захисту та подальшого розвитку.

Для України ця правова категорія є надзвичайно актуальною, оскільки гібридна війна, розв'язана Росією, ставить питання збереження суверенітету української держави в пряму залежність від ефективного забезпечення її інформаційного суверенітету.

Вибір теми "Шляхи забезпечення інформаційного суверенітету України" *обґрунтовано* її актуальністю в контексті сучасних викликів, пов’язаних із глобалізацією інформаційних процесів, зростанням впливу

цифрових технологій та інформаційною війною. У сучасних дослідженнях значна увага приділяється проблемам інформаційної безпеки, регулювання інформаційного простору та протидії дезінформації, проте питання інформаційного суверенітету держави потребує глибшого вивчення, зокрема в аспекті розробки дієвих механізмів його забезпечення.

Критичний аналіз наукових праць дозволяє визначити сутність проблеми як протистояння між необхідністю захисту національного інформаційного простору та загрозами, що виникають у результаті зовнішнього впливу, таких як маніпуляції громадською думкою, поширення фейкових новин і кібератаки. Особливої ваги це питання набуває для України, яка в умовах гібридної війни стикається із прямими загрозами її суверенітету, зокрема в інформаційній сфері.

Це завдання передбачає не лише аналіз існуючого міжнародного досвіду, а й визначення його придатності до національного контексту, розробку стратегій захисту інформаційного простору та формування дієвих механізмів співпраці на державному й міждержавному рівнях. Таким чином, дослідження спрямоване на вирішення нагальної наукової та практичної проблеми, що має стратегічне значення для збереження державного суверенітету України.

Мета даної кваліфікаційної роботи магістра полягає у тому, щоб запропонувати нову модель кібербезпеки та інформаційного суверенітету країни, адже сучасні реалії в інформаційній сфері визначають необхідність глибокого осмислення проблеми інформаційного суверенітету, щоб результати цього аналізу могли бути застосовані у практичній діяльності. Це важливо як для забезпечення інтересів націй, держав і суспільних структур, так і для врахування загально-цивілізаційних тенденцій розвитку інформаційного простору.

Поставлена мета зумовила необхідність розв'язання таких головних *завдань*:

– охарактеризувати поняття, види і значення інформаційний суверенітет;

– оцінити яка правова основа забезпечення інформаційного суверенітету України;

– проаналізувати як можна використати міжнародний досвід для забезпечення інформаційного суверенітету України;

– здійснити аналіз існуючих інформаційних загроз та їхніх джерел для України;

– з'ясувати місце гібридної війни та інформаційної безпеки у інформаційному суверенітеті;

– навести вплив дезінформації та маніпуляції на громадську думку;

– обґрунтувати стратегічне планування у сфері інформаційної безпеки;

– охарактеризувати розвиток національних інформаційних ресурсів і технологій;

– дослідити співпрацю України з міжнародними організаціями в контексті інформаційної безпеки;

– синтезувати нову модель кібербезпеки та інформаційного суверенітету країни.

Об'єктом роботи є інформаційний суверенітет України як складова національної безпеки держави.

Предметом даної роботи є шляхи, методи та механізми забезпечення інформаційного суверенітету України в умовах сучасних інформаційних загроз і глобалізації.

Методологічна основа:

- *Історико-правовий метод* застосовано під час аналізу розвитку правового регулювання інформаційного суверенітету в Україні;
- *Системний, нормативний та формально-юридичний методи* сприяли дослідженню юридичного змісту правових актів законодавства

України та міжнародно-правових актів, в яких закріплено регулювання інформаційного суверенітету;

- Використання *порівняльно-правового методу* дозволило провести порівняння шляхів регулювання та захисту інформаційного суверенітету в Україні з міжнародним досвідом;
- Метод *узагальнення* для визначення загального поняття, в якому відображається основне, що характеризує предмет дослідження;
- Метод моделювання, що застосований для синтезу нової моделі кібербезпеки та інформаційного суверенітету країни.

Науково-практична новизна дослідження полягає в систематизації та комплексному аналізі сучасних методів та механізмів забезпечення інформаційного суверенітету на національному рівні в умовах глобальних інформаційних загроз. У результаті проведеного дослідження розроблено нову модель кібербезпеки та інформаційного суверенітету країни, що може бути застосована в контексті національної стратегії інформаційного суверенітету України.

Практична значущість дослідження полягає в тому, що запропоновані рекомендації та рішення можуть бути використані органами державної влади для розробки та вдосконалення політики в галузі інформаційної безпеки, законодавчих ініціатив, а також у формуванні стратегій і програм національного рівня, спрямованих на захист критичної інформаційної інфраструктури та боротьбу з кіберзагрозами.

Структура магістерської роботи складається з титульного аркушу, змісту, вступу, трьох розділів: в першому розділу – підпункти, в другому – 3 підпункти, третьому - 4 підпункти, висновків, списку використаних джерел. Загальний обсяг кваліфікаційної роботи магістра становить 89 сторінок

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ

1.1. Сутність інформаційного суверенітету: поняття, види і значення

«Суверенітет держави вимагає поваги до її права визначати власні закони та захищати внутрішній порядок, який гарантує свободу її громадян» (Іммануїл Кант).

Поняття «суверенітет» (від давньофранцузького «soveranite», що у свою чергу походить від латинського «suprematis», або «suprema potestas» – «вища влада») набуло значимості в епоху середньовіччя [1]. У класичному розумінні суверенітету як такого слід виокремити три його основні види: «державний», «народний», та «національний». Складником державного суверенітету є інформаційний суверенітет, що є питанням дослідження даної роботи [2].

Порівняємо визначення поняття «інформаційного суверенітету» від різних науковців. Олексій Онищенко, Валерій Горовий та ін. у своїй монографії визначають інформаційний суверенітет як здатність держави зберігати та захищати свої інформаційні ресурси від зовнішніх впливів і контролю, забезпечувати незалежність та самостійність у використанні інформаційної інфраструктури [3]. Можна зробити висновок, що науковці підкреслюють значення цього суверенітету для стабільності та безпеки в умовах глобалізації інформаційних потоків, особливо на тлі розвитку сучасних технологій.

Зокрема, Дмитро Дубов зазначає, що інформаційний суверенітет пов’язаний з правом держави на незалежну інформаційну політику, яка дозволяє реалізувати інтереси безпеки та розвитку національної інформаційної інфраструктури [4]. Іншими словами, в умовах зростаючого впливу інформаційних технологій інформаційний суверенітет стає критично важливим елементом національного суверенітету в цілому.

Ще одне ключове визначення пропонує Олександр Радутний, де розглядає інформаційний суверенітет як право суспільства на збереження своєї культурної та духовної ідентичності у глобальному інформаційному просторі [5]. Концепція його погляду полягає у тому, що велике значення має роль інформаційного суверенітету у забезпеченні прав і свобод громадян на отримання й поширення інформації.

Власну точку зору висловлює В. Гонг щодо інформаційного суверенітету, підкреслюючи, що його внутрішня складова передбачає верховну владу держави при прийнятті рішень, реалізації інформаційної політики і підтримці інформаційного порядку в країні, тоді як зовнішня полягає в повній юридичній рівності держав і їх незалежності від зовнішнього контролю при виробництві і використанні інформації. На його думку, інформаційний суверенітет – це повнота влади щодо встановлення інформаційного порядку всередині держави і незалежне право держав створювати, передавати і використовувати інформацію без втручання ззовні [6]. Тобто, цей тип суверенітету є динамічним і характеризується відносною, відкритою, прогресивною та прагматичною природою, що відрізняє його від класичного суверенітету, який має більш абсолютний, закритий, оборонний і риторично-захисний характер.

Враховуючи ці різні підходи, можна зробити висновок, що інформаційний суверенітет має бути збалансованим, адже надмірний контроль може призвести до обмеження розвитку, а надмірна відкритість – до втрати стратегічної незалежності. Важливо знаходити оптимальну точку між глобальними інформаційними потоками та національними інтересами, що дозволить країнам бути конкурентоспроможними в умовах сучасних викликів і загроз.

Інформаційний суверенітет досліджується багатьма науковцями, і в літературі його можна класифікувати за кількома основними типами, що відображають різні підходи до захисту та контролю інформаційного простору.

Розглянемо основні види інформаційного суверенітету та підходи до них (рисунок 1.1).

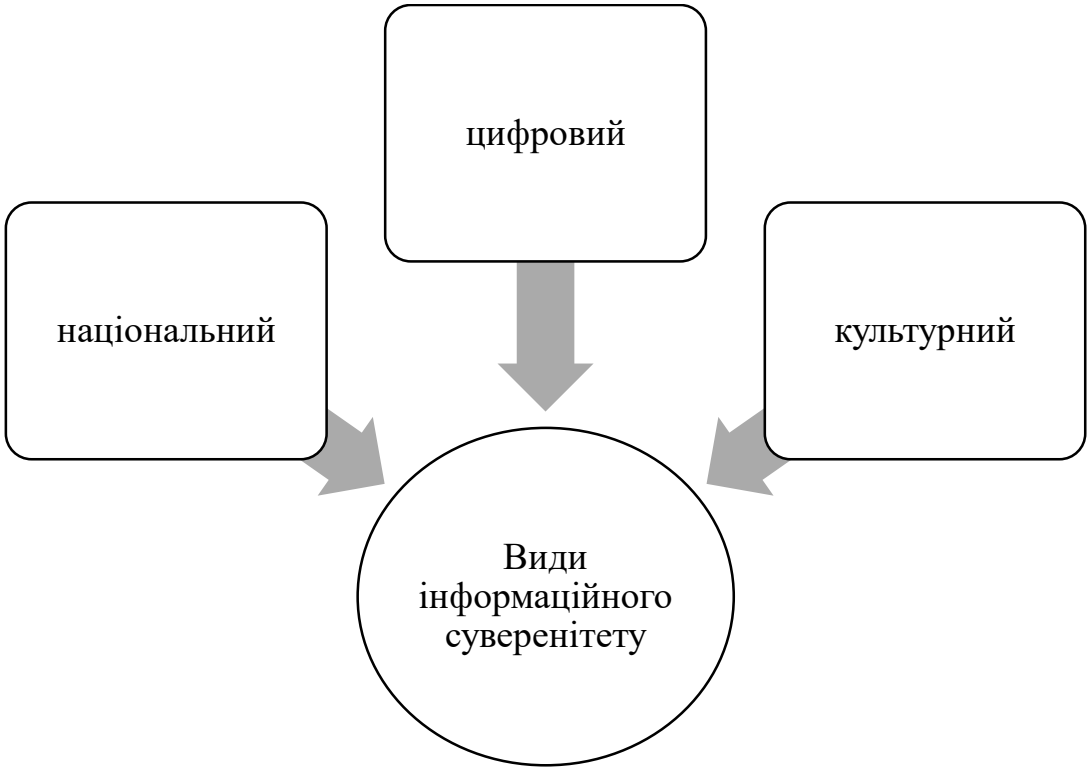

Рис. 1.1 – Види інформаційного суверенітету

За визначенням В. О. Березневич-Ломанюк, національний тип суверенітету зосереджений на здатності держави забезпечувати контроль над внутрішнім інформаційним простором та обмежувати зовнішній вплив на інформаційну сферу. Метою є захист громадян від інформаційної агресії та пропаганди інших держав. Березневич-Ломанюк зазначає, що держава повинна мати право регулювати інформаційні потоки, зокрема через законодавчі обмеження на іноземні медіа та технологічний контроль.

Національний інформаційний суверенітет є важливим інструментом для забезпечення безпеки держави, її громадян і національних інтересів в епоху цифрових технологій. Це не тільки захист від зовнішніх загроз, а й контроль за власними інформаційними потоками та правами громадян на приватність. Водночас важливо забезпечити баланс між безпекою і свободою інформації, щоб не порушувати основні права людини на доступ до інформації [7].

Зокрема, в умовах цифровізації зростає увага до суверенітету в кіберпросторі, що передбачає контроль над національними інтернет-ресурсами та даними. Д. В. Дубов визначає цифровий суверенітет як здатність держави незалежно регулювати цифрові платформи та захищати дані своїх громадян від іноземних компаній. Він також підкреслює, що цифровий суверенітет забезпечує безпеку національної інформаційної інфраструктури, включаючи сервери, телекомунікаційні мережі та бази даних [8].

Культурний інформаційний суверенітет охоплює зусилля держави щодо збереження культурної ідентичності через медіа та інші інформаційні ресурси. На думку В. О. Березневич-Ломанюк, культурний суверенітет спрямований на підтримку національних цінностей та традицій, протистоячи глобалізації культурного впливу. Зокрема, він вважає, що держави мають право підтримувати національну культуру через фінансування медіа та освітніх проєктів, спрямованих на розвиток національної ідентичності [7].

Інформаційний суверенітет є ключовим елементом забезпечення національної безпеки і стабільності в умовах глобалізації цифрового середовища. Здатність держав контролювати потік інформації, що циркулює через національні кордони, дозволяє їм мінімізувати загрози, пов'язані з кібератаками, пропагандою і маніпуляціями з боку іноземних суб'єктів. В умовах, коли інформація стала основним інструментом геополітичного впливу, для підтримки політичної стабільності та національної ідентичності необхідно оберігати інформаційний простір від зовнішніх маніпуляцій, що особливо важливо в контексті кризових ситуацій, коли інформація може бути використана як потужний інструмент впливу, здатний підірвати внутрішні процеси держави.

Інформаційний суверенітет базується на національних інформаційних ресурсах, забезпечується контролем держави за станом та наповнюванням інформаційних потоків. Видом інформаційного суверенітету вважається цифровий суверенітет, пов’язаний з «забезпеченням пріоритетних завдань щодо забезпечення ІКТ-незалежності держави» [9].

Враховуючи бурхливий розвиток інформаційно-комунікаційних технологій, повну комп'ютеризацію, створення глобального інформаційного простору, сформувалися принципово нові першооснови – інформаційне суспільство, кіберпростір, які мають необмежений потенціал і значний вплив на політичну, економічну, соціальну і культурний розвиток держави. Власне створення інформаційного суспільства спричинило появу багатьох кіберзагроз у важливих сферах життєдіяльності суспільства (банківська, військова, критична інфраструктура тощо), для яких держави справедливо відносять інформаційну безпеку як самостійний елемент національної безпеки до національної безпеки.

Глобалізація сучасного інформаційного простору призводить до послаблення інформаційного суверенітету держави, а рівень розвитку та безпеки інформаційного простору впливає на стан безпеки будь-якої держави загалом [11].

Враховуючи вище зазначене, впевнено можна стверджувати, що інформаційний суверенітет відіграє важливу роль у забезпеченні національної безпеки сучасних країн. В умовах глобалізації, збільшення інформаційних потоків та розвитку цифрових технологій питання захисту національного інформаційного простору стало одним із пріоритетних напрямків національної політики. Це пояснюється тим, що інформаційний суверенітет є не лише елементом управління, а й необхідністю захисту країни від зовнішніх інформаційних загроз, таких як інформаційна війна, пропаганда та злочинні кіберманіпуляції.

Доречно зазначити, що інформаційний суверенітет забезпечує кілька важливих функцій, необхідних для забезпечення національної безпеки. По-перше, це контроль національного інформаційного простору, контролюючи потоки інформації, держава може запобігти поширенню деструктивної інформації, яка підриває суспільну єдність і стабільність. Держава має регулювати потік інформації, щоб захистити суспільств від вторгнень і

пропаганди. Цей контроль забезпечується внутрішнім законодавством, яке визначає правила поширення інформації на території країни.

По-друге, інформаційний суверенітет допомагає зберегти стратегічну інформацію, яка може бути використана для шантажу або маніпулювання іншими державами або недержавними суб'єктами лише військово-політична інформація, але також включає економічні дані, які впливають на стабільність економічних умов країни [12].

Підсумовуючи, інформаційний суверенітет є необхідною умовою для забезпечення національної безпеки в умовах сучасних масштабних викликів. Завдяки контролю за інформаційним простором, захисту стратегічної інформації та протидії зовнішнім інформаційним загрозам держава може зберігати стабільність, незалежність та безпеку. Ефективне забезпечення інформаційного суверенітету потребує використання законодавчих, технічних та дипломатичних механізмів, що дозволяють державі реагувати на сучасні загрози та підтримувати захищеність інформаційного простору.

1.2. Міжнародний досвід забезпечення інформаційного суверенітету

Без сумніву, боротьба за інформаційний простір не залишає топових позицій світових безпекових чартів та змушує держави шукати балансу між здобутками інформаційного суспільства та забезпеченням інформаційної безпеки і збереженням власного інформаційного суверенітету. Зазначене підтверджується тим, що серед ключових питань 56-ї Мюнхенської конференції з безпеки 2020 року стали загроза Росії та експансія Китаю.

Особливістю забезпечення цифрового суверенітету країн Західної Європи та США є те, що акцент робиться на державно-приватне партнерство (йдеться про пріоритет компаній, які займаються розробкою інформаційних технологій), а у таких країнах як Росія, Китай цифровий суверенітет реалізується виключно за рахунок створення національних сил і засобів в

галузі інформаційно-комунікаційних технологій, проте це здійснюється під чітким контролем держави (в умовах відсутності конкуренції) [14].

Зупинімося докладніше на досвіді забезпечення інформаційного суверенітету Сполучених Штатів Америки. Розробки науковців показують, що першість у забезпеченні інформаційної безпеки у світі належить США. Так, навіть Японія, яка вважається меккою виробництва цифрової техніки та використання найсучасніших ІТ-технологій, відстає від США більше ніж на п'ять років у сфері розповсюдження персональних комп'ютерів, кабельного телебачення, цифрової телефонії та в інших аспектах інформаційної політики.

Необхідність наукового аналізу форм і методів інформаційної безпеки, захисту населення від негативних впливів як у воєнний час, так і в мирний, що використовується США, дозволить критично оцінити американський досвід у побудові інформаційної стратегії, в цілому розглянути її систему, роль і повноваження різних відомств з урахуванням специфіки їх діяльності. Вивчення теорії та практики інформаційних операцій, інформаційного протиборства, інформаційних війн, що проводяться США, необхідно для аналізу можливих загроз Україні [12].

Розглядаючи положення законодавства США в інформаційній сфері, вони, з одного боку, спрямовані на забезпечення права громадян на інформацію та конфіденційність їхнього приватного життя, а з іншого – на зовнішню інформаційну безпеку. Це свідчить про збалансованість у законодавствах інтересів особи, суспільства та держави.

«Національна стратегія захисту кіберпростору США» 2003 р. спрямована на захист складних і взаємопов'язаних інформаційних систем, які мають життєво важливе значення для сучасного інформаційного суспільства. Загальна мета цього документа – виокремити організаційні завдання й пріоритетність зусиль задля їх досягнення; визначити напрями так роки, які мають зробити як урядові структури, так і підприємства й приватні користувачі для досягнення безпеки кібернетичного простору США. Визначено основне завдання у сфері кібернетичної безпеки: «запобігання

кібернетичним нападам на критичну інфраструктуру, зниження вразливості нації до таких нападів і мінімізацію збитків та часу відновлення».

29 травня 2009 р. оприлюднено «Огляд з кібербезпеки» (Cyber Security Review), що мав на меті «виробити стратегічну основу кіберініціатив Уряду США». У цьому Огляді ключових завдань керівництва США у сфері кібербезпеки віднесено забезпечення центральної ролі Білого Дому у формуванні кібербезпекової політики, аби продемонструвати аудиторії як усередині США, так і міжнародним партнерам серйозність намірів американського керівництва у сфері кібербезпеки; перегляд законодавства та політики у сфері кібербезпеки; посилення федерального законодавства та відповідальності у сфері кібербезпеки; просування інформаційних проектів державного, регіонального та локального рівнів [13].

Інформаційна індустрія є основним стратегічним фактором конкуренції і вважається основним сектором економіки країни. Інформаційна політика – це політика, спрямована на створення інформаційних технологій і управління ними, пов'язана з потоком інформації, пов'язана з впливом інформаційних технологій і потоку інформації на певні установи і громадську діяльність. Як і в інших країнах, одним із ключових напрямків розвитку інформаційної безпеки є забезпечення безпеки інформаційних систем національної безпеки, тобто «правоохоронних» структур: збройних сил, іноземних розвідок тощо.

Американська політика інформаційної безпеки спрямована на досягнення і закріплення переваги США в світовому інформаційному просторі Враховуючи саму важливість інформаційних ресурсів практично у всіх сферах безпеки, Інформаційна перевага є важливим аспектом технічної, економічної, військової та політичної переваги США над іншими державами.

За останні 35 років у США сформувалася чітка система забезпечення інформаційної безпеки, яка характеризується поступовими тенденціями та, разом з тим, кардинальними заходами. Тож американський досвід державної політики в сфері інформаційної безпеки уявляється важливим для української зовнішньої та внутрішньої політики. Найціннішим є дієвий підхід до

регулювання ринку інформаційних технологій в умовах ринкової економіки [12].

Нормативно-правове регулювання, мабуть, є найважливішим фактором ефективності в забезпеченні інформаційної безпеки в будь-якій державі. Американський уряд приділяє значну увагу питанню забезпечення інформаційної безпеки в державних комп'ютерних системах (закони США «Про комп'ютерну безпеку» та «Про удосконалення інформаційної безпеки»), протидії комп'ютерній злочинності (закони «Про комп'ютерне шахрайство та зловживання» і «Про зловживання комп'ютерами»), регулювання співвідношення прав громадян на отримання інформації (закони «Про свободу інформації» та «Про висвітлення діяльності уряду») та конфіденційності їхнього приватного життя (закон «Про охорону персональних даних»)

Державні установи відіграють важливу роль у забезпеченні інформаційної безпеки. Структура інформаційної безпеки в США настільки обширна, що складається зі значної кількості компонентів, на які покладені відповідні завдання і функції з урахуванням можливостей кожного з них [13].

Далі розглянемо не менш важливий міжнародний досвід для України на прикладі Японії, що зарекомендувала себе як одна з найбільш передових інформаційних країн у світі. Групи, які постраждали від кібератак – від окремих осіб та окремих сімей до компаній зі складною соціальною інфраструктурою – це швидко розширюються. Попри всі зусилля японського уряду, ризик інформаційних атак зростає. Японська промисловість відстає від американської та європейської промисловості в оцінці кіберзагроз [16].

10 червня 2013 року Рада з політики інформаційної безпеки Японії прийняла Стратегію кібербезпеки. Урядом Японії раніше було використовано формулювання «інформаційна безпека» для своєї 54 політики і основоположних планів.

Однак із зростанням кіберзагроз, що виходять за рамки інформаційної безпеки, таких, наприклад, як диверсія щодо об'єктів життєзабезпечення

населення, в Токіо було прийнято рішення використовувати термін «кібербезпека» для того, щоб вперше розглянути всі ці проблеми.

Стратегія спрямована на розвиток «провідного в світі», «сталого» і «динамічного» кіберпростору і перетворення Японії у світового лідера в області кібербезпеки. Для реалізації цих цілей в документі передбачені чотири основні принципи (рисунок 1.2) [17].

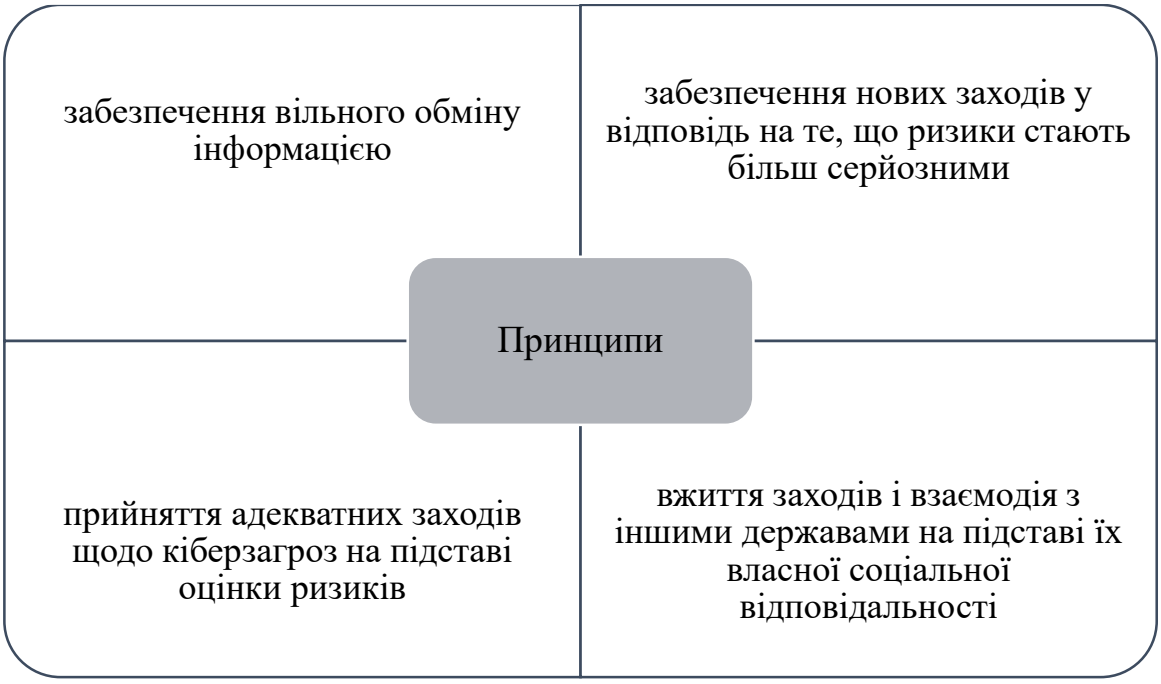

Рис. 1.2 – Принципи Стратегії кібербезпеки Японії

На противагу уже зазначеним країнам, для прикладу побудови зовсім іншого бачення та підходу до інформаційного суверенітету потрібно описати політику Китаю. Китай має один із найсуворіших підходів до забезпечення інформаційного суверенітету, відомий під назвою «Великий китайський фаєрвол». Ця система блокує доступ до іноземних медіа, соціальних мереж (таких як Facebook і Twitter) та західних інформаційних ресурсів, що дозволяє уряду контролювати контент, доступний громадянам Китаю. Крім цього, Китай активно розвиває власні інформаційні платформи (WeChat, Weibo), які повністю підконтрольні державі. Такий підхід дозволяє Китаю обмежити зовнішній інформаційний вплив та підтримувати державну ідеологію через національні медіа.

Основні завдання в сфері кіберзахисту, які ставить перед собою Китай:

- Захист суверенітету кіберпростору;
- Захист критичної інформаційної інфраструктури (ICI);
- Створення здорової онлайн-культури;
- Боротьба з кіберзлочинністю, шпигунством і тероризмом;
- Поліпшення кібер-управління;
- Підвищення базової кібербезпеки;
- Зміцнення міжнародного співробітництва.

Щоб забезпечити ще більший захист даних громадян, Китай прийняв Закон про кібербезпеку, який зобов'язує всі міжнародні компанії зберігати персональні дані китайських користувачів на серверах, розташованих у Китаї. Таким чином, Китай підсилює свій контроль над інформаційними потоками, захищаючи національні інтереси в цифровій сфері [18].

Таким чином, проаналізувавши дані країни, можна дійти до таких висновків, що міжнародний досвід США, Японії та Китаю у сфері інформаційного суверенітету надає Україні важливі уроки для зміцнення національної безпеки та інформаційної незалежності.

Будучи провідною країною в галузі технологій і комунікацій, США продемонстрували важливість суворої політики, що регулює цифровий простір, і активно продовжують працювати щодо захисту своєї інформаційної інфраструктури від зовнішніх загроз. Запозичуючи досвід США в області кібератак, Україна може захистити свій інформаційний простір від зовнішнього втручання, особливо в напрямку поліпшення кібербезпеки і вдосконалення правової бази для боротьби з дезінформацією.

Японія, яка активно використовує сучасні технології для забезпечення національної безпеки, може стати прикладом для України у створенні надійної цифрової інфраструктури та розробці інноваційних систем моніторингу потоку інформації. З досвіду Китаю можна навчитися суворому контролю за інформаційними потоками і забезпеченню інформаційної стабільності, хоча у

ньому є свої особливості, але він може бути адаптований до контексту національної безпеки України. Водночас Україна має уникати надмірних обмежень свободи слова та враховувати етичні та правові аспекти.

1.3. Правова основа забезпечення інформаційного суверенітету України

Нормативно-правове забезпечення інформаційного суверенітету в Україні є важливою складовою національної безпеки та стратегічного розвитку країни. Це забезпечення включає низку законів, указів, постанов і міжнародних угод, які спрямовані на захист інформаційного простору від зовнішніх і внутрішніх загроз, забезпечення стабільного функціонування засобів масової інформації та ефективного використання інформаційних технологій.

Зростання глобального інформаційного потоку, залежність розвитку держави від сучасних інформаційних технологій, а також значний тиск цих факторів щодо реалізації "суверенітету" вже на початку 90-х років призвели до усвідомлення необхідності сформулювати дефініцію "інформаційний суверенітет держави".

Поняття "інформаційний суверенітет" вперше з'являється в правовій практиці України в Законі України «Про інформацію», де в статті 53 зазначено, що основою інформаційного суверенітету України є національні інформаційні ресурси. До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами [19]. Змінами, внесеними до цього закону 09.05.2011 р. ця стаття була виключена.

Згодом, нормативна дефініція «інформаційний суверенітет держави» була передбачена Законом України «Про Національну програму

інформатизації» від 1998 р., в якому було зазначено, що – це здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави [10]. Однак цей закон було втратив чинність відповідно до Закону України «Про Національну програму інформатизації» від 01.12.2022 р., де більше не було визначення даної категорії.

Нормативно-правове забезпечення інформаційного суверенітету України охоплює широкий спектр законодавчих актів, які регулюють захист інформаційного простору, протидію дезінформації та кібербезпеці. Проаналізувавши нормативну базу, була сформована таблиця, в якій викладені основні акти і сфера застосування інформаційного суверенітету (табл. 1.1):

Табл. 1.1 Нормативно-правове забезпечення інформаційного суверенітету України

Назва нормативно-правового акту	Сфера регулювання
Конституція України	Закріплює права громадян на доступ до інформації, свободу слова, а також встановлює принципи національної безпеки, до яких належить і захист інформаційного простору
Європейська конвенція про транскордонне телебачення (ETS N	Сприяє розвитку телекомунікацій та захисту інформаційного простору від незаконного впливу з інших країн.
Закон України "Про доступ до публічної інформації"	Сприяє розвитку прозорості та відкритості органів влади, що є важливою частиною забезпечення інформаційного суверенітету. Він регулює права громадян на доступ до публічної інформації, що підвищує рівень контролю за діяльністю держави.
Закон України "Про захист інформації в інформаційно-комунікаційних системах"	Встановлює правові та організаційні основи захисту інформації в електронних інформаційно-комунікаційних системах, що є важливим для забезпечення цілісності

Назва нормативно-правового акту	Сфера регулювання
	та безпеки національних інформаційних ресурсів.
Закон України "Про інформацію"	Визначає загальні засади інформаційної діяльності в Україні, регулює права громадян на отримання та поширення інформації, а також забезпечує національний інформаційний простір від зовнішніх загроз.
Закон України "Про медіа"	Регулює діяльності у сфері медіа, зокрема в контексті захисту інформаційного простору від пропаганди та маніпуляцій.
Закон України " Про основні засади забезпечення кібербезпеки України"	Визначає правові та організаційні засади кібербезпеки в Україні, що є важливою частиною інформаційного суверенітету, зокрема щодо захисту від кіберзагроз, захисту інтересів держави та громадян в інформаційній сфері.
Указ Президента України «Про Раду національної безпеки і оборони України»	Указ створює Раду національної безпеки та оборони, яка серед інших завдань займається питаннями забезпечення інформаційної безпеки країни, у тому числі інформаційного суверенітету.
Постанова Верховної Ради України «Про затвердження завдань Національної програми інформатизації на 2022-2024 роки»	Програма включає інвестиції в розвиток інформаційно-комунікаційних технологій, впровадження національних стандартів захисту інформації, а також підтримку українського контенту в Інтернеті та в засобах масової інформації.
Про Стратегію інформаційної безпеки (затверджена Указом Президента України № n0080525-21)	Документ, який визначає основні напрями та завдання для розвитку національного інформаційного простору, забезпечення його безпеки та захисту від зовнішніх інформаційних загроз. Стратегія акцентує увагу на боротьбі з інформаційною агресією, зокрема з боку Росії та інших держав.

Джерело: складено автором на основі [20, 21, 22, 23, 19, 24, 25, 26,27,28]

Висновки до першого розділу

Отже, підсумовуючи вище зазначене, інформаційний суверенітет є важливим аспектом загального суверенітету держави, що забезпечує її здатність контролювати власний інформаційний простір, захищати національні інтереси та зберігати культурну ідентичність в умовах глобалізації. Держави повинні мати можливість здійснювати незалежну інформаційну політику, регулювати інформаційні потоки та захищати своїх громадян від зовнішнього впливу, що особливо важливо в умовах зростання цифрових загроз і геополітичної напруженості.

Міжнародний досвід США, Японії та Китаю у сфері інформаційного суверенітету надає важливі уроки для України щодо зміцнення національної безпеки та захисту інформаційного простору. США демонструють ефективність суворого регулювання цифрового простору та створення потужної інфраструктури кібербезпеки, що може стати основою для поліпшення захисту українських інформаційних систем. Адаптація кращих практик цих країн може допомогти Україні зміцнити свій інформаційний суверенітет та протистояти зовнішнім загрозам у цифровому середовищі.

Нормативно-правове забезпечення інформаційного суверенітету в Україні є критично важливим для національної безпеки та стабільного розвитку країни, оскільки воно визначає основи для захисту інформаційного простору від різноманітних загроз. Україна закріпила це поняття в законодавчих актах, зокрема у Законі «Про інформацію» та «Про Національну програму інформатизації», проте з часом зміни в законодавстві призвели до втрати чіткої дефініції. Попри це, нормативно-правова база країни залишається важливою для регулювання інформаційного простору, протидії дезінформації та забезпечення кібербезпеки.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

2.1. Інформаційні загрози та їхні джерела в Україні

Сучасний етап розвитку цивілізації визначається переходом від індустріального суспільства до інформаційного. Поняття «інформація», яке раніше мало переважно філософський характер, дедалі більше набуває рис правової категорії, перетворюючись на ресурс і товар сучасного світу, а також стаючи об’єктом правовідносин. Це значною мірою зумовлює актуальність обраної тематики дослідження.

Відомо, що внаслідок інформаційної революції, яка відбулася наприкінці XX – на початку XXI століття, інформація набуває ключового значення у суспільних відносинах, стаючи основою соціально-економічного прогресу. Швидкий розвиток технічних і технологічних засобів збору, зберігання, використання та поширення інформації сприяв динамічному формуванню інформаційних відносин у суспільстві.

Після повномасштабного вторгнення Російської Федерації в Україну спостерігається активне використання російських засобів масової інформації для маніпуляції даними. Вони подають події виключно у вигідному для себе світлі, називаючи війну "військовою операцією", спотворюють інформацію про загиблих військових та мирних жителів, а також систематично генерують нові інформаційні вкиди для виправдання своїх дій і створення ілюзії загрози з боку України [29].

Формування глобального інформаційного простору збільшило ризики для безпеки, особливо з боку стратегічних супротивників і міжнародного тероризму. Боротьба з такою загрозою - основне завдання, що стоїть перед Збройними силами і фахівцями в області безпеки.

Є очевидним, що сучасні військові конфлікти відбуваються не лише за допомогою традиційних методів, але й із застосуванням інформаційних технологій (рис. 2.1) [30].

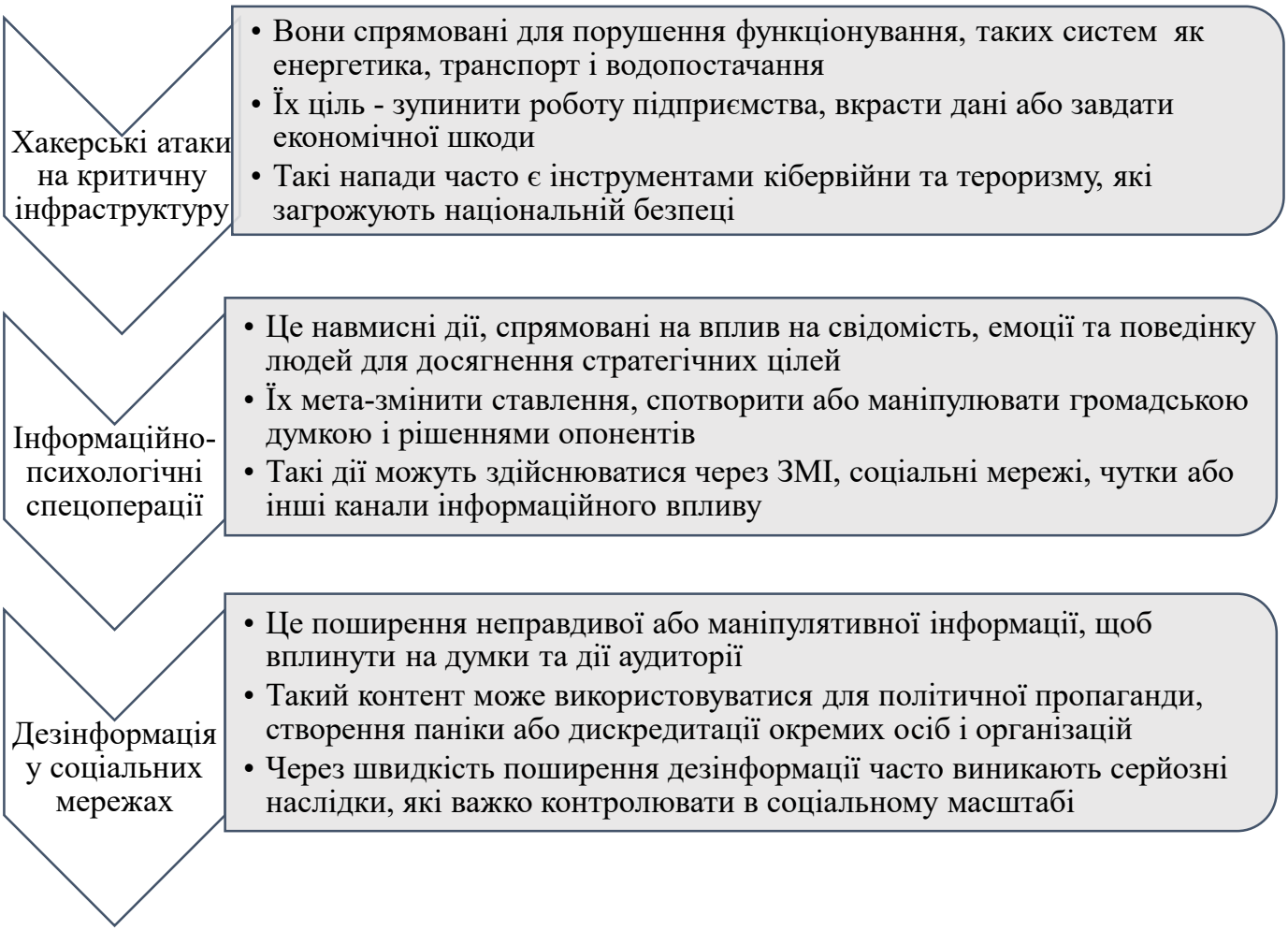

Рисунок 2.1. – Види інформаційні технологій

Інформаційна загроза – це комплекс чинників, що становлять небезпеку для конституційних прав і свобод особи, державних секретів, а також важливої для суспільства інформації, захищаючи її від несанкціонованого доступу та поширення.

Необхідно зазначити, що сучасні виклики інформаційної безпеки в Україні обумовлені як внутрішніми, так і зовнішніми факторами:

Внутрішні фактори – це ті чинники, які відбуваються в одній країні. Відмінною рисою є: відсталість інформаційних технологій в Україні від

найбільших країн світу, низький рівень комп'ютеризації, роздробленість влади державних органів і законів в інформаційній сфері [31].

Україна значно відстає у розвитку інформаційних технологій від провідних країн світу. Зокрема, за міжнародними індексами ІКТ, Україна посідає низькі позиції, наприклад, у 2022 році вона опинилася на 81 місці у світі. Це відставання спричинене недостатньою комп’ютеризацією в регіонах, особливо в сільській місцевості, де технологічна інфраструктура розвивається повільно, а доступ до інтернету обмежений [32].

Ситуація ускладнюється також роздробленістю законодавства у сфері інформаційних технологій, де регулювання часто застаріле і фрагментоване. Відсутність єдиної державної політики у сфері цифрової безпеки й інформатизації гальмує процес інтеграції сучасних технологій в управління державними органами та захист даних. На додаток, у різних органів влади є свої процедури та вимоги, що утруднює створення єдиної цифрової стратегії на національному рівні [33].

Зовнішніми факторами є глобальні процеси розвитку та використання інформаційних технологій, а також спроби іноземних суб’єктів втручатися у національний інформаційний простір для досягнення своїх інтересів [31].

Зовнішні фактори, які впливають на інформаційний простір України, включають глобальні технологічні зміни та використання цифрових технологій іншими державами для досягнення власних інтересів. Глобально швидке впровадження новітніх технологій, таких як штучний інтелект, 5G-мережі та хмарні сервіси, встановлює високі стандарти для розвитку IT-сектору. Ці технології стають основою економічної конкурентоспроможності, соціальної взаємодії та навіть військових операцій, що підвищує потребу в їх інтеграції в інфраструктуру України для уникнення технологічного відставання [32].

Водночас, іноземні держави та корпорації можуть прагнути контролювати чи впливати на інформаційний простір України,

використовуючи кіберпростір для досягнення політичних або економічних цілей. Це може включати втручання у внутрішні процеси, маніпуляції суспільною думкою через соціальні медіа, або спроби зламати інформаційні системи державних органів. Наприклад, різні кібератаки, спрямовані на стратегічні інфраструктурні об’єкти та державні установи України, свідчать про спроби отримати вплив на національну безпеку або дестабілізувати політичну ситуацію [33].

Таким чином, зовнішні фактори створюють виклики для національної інформаційної безпеки України, що вимагає постійного вдосконалення кіберзахисту, розробки відповідних законів та залучення інновацій для протидії цим загрозам.

Також, варто звернути увагу, що основними загрозами для розвитку інформаційної індустрії в Україні можуть бути:

1. Обмежений доступ до новітніх технологій, що призведе до технологічного відставання і збільшить залежність від зарубіжних ринків;

2. Витіснення національних виробників, що перешкоджатиме розвитку внутрішнього ринку та економічної незалежності країни;

3. Загрози для інформаційної та телекомунікаційної безпеки, які включають незаконний збір і використання даних, порушення технологічних процесів обробки інформації, впровадження шкідливих програм та несанкціонований доступ до конфіденційної інформації [34].

Проаналізувавши праці науковців, було з’ясовано, що інформаційні загрози в Україні виникають із кількох ключових джерел, кожне з яких має свої особливості, механізми дії та наслідки (рис. 2.2)

Рисунок 2.2 Джерела інформаційних загроз

Першим розглянемо джерело інформаційний загроз, а саме іноземні держави. На даний час триває повномасштабне вторгнення Російської Федерації до України, тому доречно буде дослідити дане джерело на цьому прикладі, адже Росія є найбільшим джерелом інформаційних загроз для України. Її інформаційна стратегія включає:

1. Пропаганду через медіа;

2. Дезінформаційні кампанії;

3. Кібероперації.

Детальніше зупинимось на кожній з вище зазначених чинників. Пропаганда через медіа – це форма спілкування, головна мета якої вплив на ставлення суспільства до проблем, ситуацій чи явищ. Кремль використовує власні ЗМІ, такі як RT, "Спутник" та інші, для поширення маніпулятивних

наративів, спрямованих на дискредитацію української влади, підрив єдності в суспільстві та міжнародної підтримки України [35].

Наведемо найяскравіший приклад пропаганди Росії, він стосується архетипу Другої світової війни, зокрема образ ворога-нациста, використовуються у пропаганді як виправдання для ворожнечі. Спершу ця ідея була спрямована на нацистів, але згодом у свідомості багатьох росіян утвердився наратив, що «українці – нацисти», а отже, вважаються ворогами, яких треба знищити. Цей наратив став основою більшості російської пропаганди.

Протягом останніх десяти років, коли в Росії активно поширювалася ідея, що «українці – нацисти», багато хто сприймав це як абсурд. Однак, з часом цей стереотип закріпився, і зараз значна частина суспільства переконана у необхідності «боротьби з українцями» [36].

Перейдемо до другого чинника, що є дезінформаційними кампаніями. Це систематичне створення та поширення неправдивої інформації з метою викликати паніку, зневіру або політичну нестабільність. Приклади включають поширення фейків про події в зоні бойових дій або міжнародну ізоляцію України. Прикладом є кампанія проти українських мігрантів, біженців [35].

Кампанія з дискредитації українських біженців почалася майже одразу після початку повномасштабного вторгнення. У країнах, де українські біженці отримали прихисток, пропаганда активно поширює антимігрантські гасла, наголошуючи на соціальному паразитизмі, нібито зростанні злочинності, демпінгу на ринку праці та «нездоланних» культурних відмінностях, що можуть спричинити конфлікти. Оскільки ці твердження часто не відповідають реальності, для їхньої підтримки активно використовуються фейки. У країнах Глобального Півдня російська пропаганда просуває ідею «білого расизму», протиставляючи українських біженців мігрантам із Африки та Близького Сходу [37].

Третім чинником є кібероперації, завдяки яким російські хакерські групи, такі як Fancy Bear і Sandworm, здійснюють атаки на українські інформаційні системи для викрадення даних, блокування роботи інфраструктури та поширення деструктивного програмного забезпечення [35].

Цікавим кейсом є , коли хакерська група, відома під кодом UAC-0165 З 11 травня до 29 вересня 2023, здійснила кібернапади на інформаційно-комунікаційні системи принаймні 11 провайдерів. Це призвело до перебоїв у послугах інтернет-доступу, хостингу та електронної пошти. Фахівці CERT-UA заздалегідь попереджали телекомунікаційні компанії про можливі атаки, які мали ознаки цілеспрямованої кампанії. Після детального аналізу було встановлено зв’язок цих атак з групою Sandworm [38].

Далі розглянемо такий вид джерела як локальні деструктивні групи. У межах країни діють групи чи окремі особи, які свідомо або випадково сприяють поширенню деструктивних наративів. Це може відбуватися через політичну заангажованість [39].

Деякі політичні сили використовують дезінформацію для дискредитації опонентів або для створення конфліктів у суспільстві. Політичні сили в Україні інколи використовували дезінформацію для дискредитації опонентів. Наприклад, під час виборчих кампаній було зафіксовано випадки, коли політичні партії або їх прихильники поширювали неправдиву інформацію про опонентів, аби викликати недовіру в суспільстві. У 2019 році перед президентськими виборами дезінформація активно поширювалася з метою знизити підтримку певних кандидатів, особливо в соціальних мережах, де контролювати достовірність інформації складніше.

Зокрема, у грудні 2018 року спостерігачі Громадянської мережі ОПОРА зафіксували сім друкованих матеріалів у волинських ЗМІ, що мали ознаки «чорного піару» проти ймовірного кандидата в президенти Володимира Зеленського. У той же час в інтернет-виданнях було виявлено по одному випадку антиреклами стосовно потенційних кандидатів Анатолія Гриценка (партія «Громадянська позиція») та Юлії Тимошенко (ВО «Батьківщина»). У

друкованих виданнях були розміщені матеріали із назвою «Вова Зеленський – зоряний час Ігоря Коломойського!». У цих матеріалах розповідалось про те, що вже 27 років українцями правлять олігархи, а також наголошувалось, що Володимир Зеленський – це маріонетка Ігоря Коломойського [40].

Також, другим складником локальних деструктивних груп є вплив зовнішніх агентів. В Україні діють проросійські групи та особи, що активно поширюють вигідні для Кремля наративи. Наприклад, під час подій на сході України, організації та особи з проросійськими поглядами поширювали ідею «руського мира» та дискредитували українські урядові структури. Крім того, багато фейкових новин, зокрема в соціальних мережах, підтримували російську версію конфлікту, відкидаючи офіційні українські заяви про агресію. Деякі громадські діячі та медійні ресурси, які мають проросійські позиції, продовжують поширювати дезінформацію, щоб підтримати російські інтереси на українському інформаційному полі [41].

Нарешті, перейдемо до останнього критерію вище зазначеного джерела, а саме до наслідків недовіри до офіційних джерел. Через низький рівень довіри до державних інституцій в Україні часто виникають ситуації, коли громадяни охоче приймають недостовірну або маніпулятивну інформацію. Наприклад, під час пандемії COVID-19 частина населення не довіряла офіційним рекомендаціям Міністерства охорони здоров'я, що сприяло поширенню дезінформації про вакцини, лікування та саму загрозу вірусу. Багато українців схильні шукати альтернативні джерела, в тому числі соціальні мережі, де неправдиву інформацію поширюють значно.

«Конспірологічні теорії, плітки та зловмисне дезінформування може швидко набути вірусного поширення в соціальних мережах, особливо за низького рівня довіри громадськості до державних інституцій», — на думку Ґерчевої [42].

Останнім, проте не менш важливим джерелом є недостатній рівень інформаційної грамотності. Брак навичок критичного мислення та вміння

аналізувати інформацію створює сприятливий ґрунт для маніпуляцій. Особливо вразливими три верстви населення:

1. Люди старшого віку в Україні є вразливими до дезінформації, оскільки часто отримують інформацію з традиційних медіа, які можуть бути джерелом маніпулятивних повідомлень. Наприклад, на регіональних телеканалах і в деяких друкованих виданнях можуть поширюватися новини, що містять пропагандистські наративи. Літні люди активно використовують месенджери, як-от Viber, де через групи часто поширюються фейкові новини та маніпулятивний контент. Це підсилює їхню уразливість до дезінформації, зокрема під час політичних подій або криз, таких як пандемія COVID-19;

2. Молоді люди, хоча й мають краще володіння цифровими навичками, також часто стають жертвами маніпуляцій через соціальні медіа. Наприклад, у період виборів або під час суспільно-політичних криз (як під час повномасштабного вторгнення РФ в Україну) соцмережі переповнені неправдивою інформацією, зокрема в TikTok, Instagram, Telegram. Поширюються відео з маніпулятивними заголовками та емоційно забарвленими повідомленнями, що впливають на думку молоді. За даними досліджень, молоді користувачі часто сприймають такий контент без критичного аналізу, що робить їх легкою мішенню для дезінформаційних кампаній;

3. Відсутність освіти з медіаграмотності, у багатьох школах і на робочих місцях в Україні не вистачає програм, які б розвивали медіаграмотність та критичне мислення. Лише кілька проєктів намагаються навчати школярів і студентів розпізнавати фейки та аналізувати інформацію. Наприклад, проєкт "Вивчай та розрізняй" від IREX, який реалізується за підтримки МОН, охоплює частину шкіл, але ця ініціатива не є обов'язковою та доступною для всіх. Це залишає багатьох громадян без базових навичок перевірки джерел, що підвищує їхню вразливість до фейків і маніпуляцій в інформаційному просторі [43].

Отже, є всі підстави зробити такий висновок, поєднання зовнішнього впливу, внутрішніх деструктивних сил і низького рівня інформаційної грамотності створює для України серйозні проблеми в інформаційному просторі. Ефективне реагування на ці загрози вимагає систематичної роботи, включаючи законодавчі ініціативи, освітні програми та інноваційні технічні рішення.

Проаналізувавши вище зазначену інформацію, доречно запропонувати шляхи забезпечення розвитку таких напрямів:

1. Законодавче регулювання, тобто, потрібно посилити нормативну базу, яка спрямована на контроль інформаційної діяльності в кризових умовах;

2. Підвищення інформаційної грамотності, а саме організації освітніх програм, відповідно до яких громадяни набудуть навички критичної оцінки інформації та розпізнання дезінформації;

3. Технологічні рішення, за допомогою розробки систем моніторингу і протидії кіберзагрозам, а також використання штучного інтелекту буде виявлено фейки.

2.2. Гібридні війни та інформаційна безпека

Рівень розвитку суспільства та технологій безпосередньо впливає на характер збройного протистояння, а також на значення та функції військових інструментів у політичних процесах. Удосконалення озброєнь і тактики ведення бойових дій відбувається поступово, з урахуванням еволюції суспільної організації та зміни колективної свідомості.

В результаті, з’явилась така дефініція як «hybrid warfare» – гібридна війна. Цей термін має на меті дати розуміння нових явищ та феноменів на полях боїв XXI ст. Гібридна війна, яка є новітньою формою багатовекторного протистояння, стала однією з головних загроз сучасності.

Варто звернути увагу, що теоретичне осмислення поняття гібридного протистояння, особливо в Україні, досі перебуває на стадії активного

розвитку. У цьому контексті важливим кроком є спроба глибше зрозуміти природу цього явища та проаналізувати його ключові складові [44].

Термін "гібридна війна" вперше ввів у науковий обіг підполковник Корпусу морської піхоти США Френк Г. Хоффман. За його визначенням, гібридні війни охоплюють широкий спектр методів ведення бойових дій, включаючи традиційні (конвенційні) засоби, нерегулярну тактику, терористичні акти із застосуванням примусу та насильства, а також кримінальні заворушень [45].

Науковець Г.Г. Динис стверджує, що «гібридна війна / гібридний конфлікт» – це несформовані правовідносини, учасниками, яких є державні та недержавні актори, регулярні збройні сили, нерегулярні воєнізовані формування, що поєднують традиційні та нетрадиційні методи, терористичні засоби ведення війни з використанням новітніх видів озброєнь та високих інформаційно-комунікаційних технологій для дезорганізації, деморалізації збройних сил противника та населення на території державного утворення з метою отримання воєнно-політичної перемоги над противником [46].

Необхідно зазначити, що Г.Г. Динис звертає увагу на можливість ототожнення понять "гібридна війна" та "гібридний конфлікт", що викликає певні дискусії, оскільки конфлікт має ширше значення і не обов’язково включає збройне протистояння. Війна ж є найгострішою фазою конфлікту, тоді як самі конфлікти можуть існувати без використання військової сили.

Також, цінна думка кандидата політичних наук Є. М. Магди, про те, що гібридна війна – це сукупність заздалегідь підготовлених і оперативно реалізованих дій військового, дипломатичного, економічного, інформаційного характеру, спрямованих на досягнення стратегічних цілей [47].

На наш погляд, Є. М. Магда визначає гібридну війну як сукупність різноманітних впливів на цільовий об'єкт, спрямованих на досягнення конкретної мети. Він акцентує на тому, що дії в межах гібридної війни завжди мають чітке цілепокладання, адже участь у таких конфліктах без визначених

стратегічних цілей є нелогічною. Це стосується як видимих, так і прихованих форм конфлікту.

Переконливо у своїй праці зазначає К.Н. Сабрі, що гібридна війна являє собою сучасну військову стратегію, яка поєднує одночасне застосування конвенційних, мілітарних сил з використанням іррегулярних утворень, веденням дій у кіберпросторі, а також інформаційних операцій та засобів економічного і дипломатичного тиску на противника [48].

Ми погоджуємось із думкою К.Н. Сабрі, що обмеження гібридної війни лише до "сучасної військової стратегії" звужує її концепцію. Вона є не тільки військовим феноменом, а й продовженням політичної стратегії, яку застосовують держави або квазідержавні суб'єкти для досягнення поставлених, не завжди військових, цілей.

Підсумовуючи, можна стверджувати, що специфіка гібридної війни, особливо у контексті агресії Росії проти України, залишається недостатньо вивченою науковцями та фахівцями з безпеки.

Гібридна війна включає в себе певний набір компонентів і характеристик, які впливають на ворога одночасно в різних напрямках. Головними компонентами гібридної війни є: інформаційний, ідеологічний, психологічний, економічний, політичний, дипломатичний, військовий, технологічний, ресурсний, енергетичний. Зупинимось на найбільш важливих.

Один з найважливіших аспектів гібридної війни є економічний компонент, цей термін набув поширення після переходу від самозабезпечення і локальних економік до глобальної економічної системи з міжнародним розподілом праці та світовою торгівлею. Прикладом давнього історичного методу є підробка банкнот під час наполеонівських воєн, коли Франція підробляла Британські, австрійські та російські банкноти. Звичайно, даний метод, вже не є актуальним через розвиток цифрової економіки. Сучасним прикладом може слугувати заборона на транзит коштів через "треті країни" в 2018 році або блокування доступу іранських банків до системи SWIFT.

Варто звернути увагу на те, що ще одним елементом гібридної війни для України є енергетичний аспект. Політичне використання енергетичних ресурсів безпосередньо пов'язане з міжнародним впливом держави. Сучасні технологічні можливості та різноманітність економічних зв’язків породжують нові види протистояння: транспортні, енергетичні та водні блокади, які можуть спричинити екоцид цілих регіонів. Для ілюстрації даного аспекту можна зазначити спробу відокремити воду з річки Йордан від Ізраїлю, які стали однією з причин "шестиденної війни" 1967 року, або кібер-саботаж, зроблений в 2019 році для знищення енергетичної галузі Венесуели.

Далі поговоримо про складові інформаційної, які включають отримання розвідувальних даних, дезінформацію, психологічні операції, фізичне знищення інформаційних ресурсів, зараження комп’ютерними вірусами та доступ до мережевих систем противника.

Особливо важливо відзначити, що в гібридних конфліктах інформаційна війна відіграє вирішальну роль, адже дозволяє впливати на суспільну думку, порушувати комунікаційні системи та змінювати сприйняття подій.

Доцільно зупинитись також на культурі, культурно-цивілізаційних цінностях та чутливості населення країни впливу. У цьому контексті основна увага приділяється формі із змінним зображенням, але вміст втрачає пріоритет і може піддаватися довільним маніпуляціям. Сучасна популярна культура також характеризується зниженням культурної та інтелектуальної складності подання матеріалів аудиторії. Щоб забезпечити доступність, інформація для громадськості не повинна вимагати значних інтелектуальних зусиль з боку аудиторії або слухачів, в значній мірі залежних від емоційного впливу контенту на споживачів.

Завершуючи, розглянемо ще психологічний аспект гібридної війни. Психологічний тиск також є одним із популярних методів впливу на людську свідомість. Він включає шантаж, погрози, переслідування, репресії, фізичну загрозу, повідомлення про реальні або вигадані небезпеки, а також терористичні та диверсійні акти. В Україні особливо розповсюджено

телефонний тероризм — дзвінки з повідомленнями про хибне замінування громадських об’єктів, таких як вокзали. Основні способи тиску включають шахрайство, блеф, провокації, маніпуляції, містифікації, чутки, психологічні операції та дезінформацію. Провокація, зокрема, часто використовується для підбурювання опонента до невигідних для нього рішень [49].

Проведене дослідження дало можливість сформулювати такі висновки, що гібридну війну можна описати як поєднання стратегічно спрямованих дій, що включають військові, дипломатичні, економічні й інформаційні інструменти для досягнення поставлених цілей. У ній використовуються як звичні, так і новітні методи, включаючи терористичні та підривні дії, які дозволяють протистояти перевагам супротивника на військовому рівні.

Загалом, гібридна війна поєднує риси традиційних збройних конфліктів та міждержавних протистоянь. До її основних елементів належать економічний тиск, інформаційні кампанії, політичне оформлення конфліктів, приховані методи ведення війни, а також діяльність спецслужб.

Зв’язок між гібридною війною та інформаційною безпекою є надзвичайно актуальним для України, особливо з огляду на загрози, які виникли під час конфлікту з Росією. Гібридна війна поєднує традиційні військові методи з інформаційними та кібер-атаками, економічними тисками, пропагандою та дезінформацією. Ці аспекти відзначають науковці, вказуючи, що маніпулювання інформацією і контроль над нею стали важливими інструментами гібридної агресії, що спрямовані на дестабілізацію держави.

Одним із головних проявів гібридної війни є вплив на інформаційну сферу. Сучасні методи, такі як дезінформація, сприяють руйнуванню довіри до державних інституцій та посилюють паніку в суспільстві. Росія використовує інформаційні атаки для того, щоб викликати у громадян України сумніви у власному уряді, підриваючи національну єдність та створюючи негативне сприйняття національної політики [50].

Водночас, інформаційна безпека стала важливою складовою національної безпеки, адже захист національного інформаційного простору допомагає забезпечити стабільність політичної системи і запобігти впливу пропаганди. За даними українських науковців, важливим аспектом інформаційної безпеки є не тільки боротьба з дезінформацією, але й розвиток критичного мислення та підвищення медіаграмотності серед громадян. Це дозволяє знизити вразливість суспільства до фейків і маніпуляцій, що є основними інструментами гібридної агресії.

В умовах гібридної війни Україна також активно модернізує свої кіберзахисні системи, що допомагає протистояти несанкціонованим вторгненням та спробам проникнення у державні системи. Наукові дослідження наголошують, що тільки країни з розвинутою інформаційною інфраструктурою можуть ефективно протистояти зовнішнім загрозам у кіберпросторі, зберігаючи національний суверенітет та незалежність [51].

Додатково, нам слід детальніше розглянути сутність інформаційної безпеки. Інформаційна безпека — це багатогранна область, де для досягнення успіху необхідний системний і комплексний підхід. Проблеми, пов’язані з використанням інформаційних систем, можна розділити на кілька основних категорій: забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів і підтримуючої інфраструктури.

Інформаційна безпека виходить за межі простого захисту від несанкціонованого доступу і є більш широким поняттям. Суб’єкт інформаційних відносин може постраждати не тільки від несанкціонованого доступу, але й через системні збої, що призводять до перебоїв у роботі.

У сучасних умовах життя в Україні питання безпеки набуває нового значення. До лютого 2022 року світ здавався стабільним і безпечним, але теперішні загрози є набагато серйознішими. Вплив російської пропаганди спрямований не лише на окремих осіб або групи, а й на цілі народи. Психологічні маніпуляції здійснюються через засоби масової інформації, де важливу роль відіграє сприйняття та поверхневе засвоєння інформації.

Сучасні інформаційні атаки, використання ботів і фейків є ефективними інструментами для заплутування, залякування та маніпуляцій з метою створення паніки серед населення. Спеціально сформовані джерела інформації глибоко впливають на підсвідомість людей, змушуючи їх вірити в нав'язувану інформацію.

Інформаційна безпека є ключовою функцією держави, яка вимагає створення відповідних органів для розробки політики та механізмів забезпечення інформаційної безпеки. Важливу роль у цьому процесі відіграють державні установи, що виконують організаційні, правові, матеріально-технічні та фінансові функції для впровадження національної політики в сфері інформаційної безпеки [52].

Питання інформаційної безпеки та культури в умовах війни є критично важливими для виживання індивіда, суспільства та держави. Забезпечення цієї безпеки охоплює не лише державні інтереси, але й права та свободи особи. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, її конфіденційність і надійність збереження.

Інформаційна безпека включає не тільки нормативно-політичні аспекти, але й інституційну складову, яка передбачає діяльність органів, що її забезпечують, а також застосування програмно-технічних засобів для досягнення цих цілей.

Однією з найбільших проблем є недостатня розвиненість законодавчої бази щодо захисту інформації та протидії новим загрозам. Багато аспектів інформаційного простору ще не класифіковані і не врегульовані в нормативно-правових актах, що ускладнює застосування відповідальності за дії, які можуть завдати шкоди інформаційній безпеці Збройних Сил та їх військовослужбовцям.

Проте ці питання поступово вирішуються: приймаються нові нормативні акти, які регулюють використання іноземних технологій в техніці, що надходить до війська. З початком воєнного стану в Україні були внесені

зміни до законодавства, які враховують реалії війни. Це стосується таких аспектів, як заборона розповсюдження небезпечної інформації, регулювання технічного запису даних у воєнних умовах, посилення відповідальності за поширення небезпечної інформації та встановлення чітких процедур для отримання інформації.

Так, Верховна Рада ухвалила законопроект, що передбачає кримінальну відповідальність за незаконну фото- та відеофіксацію пересування Збройних Сил та міжнародної військової допомоги під час воєнного стану.

Маємо зауважити, що згідно з доктриною інформаційної безпеки України, серед основних загроз національним інтересам та безпеці в інформаційній сфері виділяються кілька важливих аспектів:

1. Проведення інформаційних операцій, які спрямовані на ослаблення обороноздатності, деморалізацію військових, створення панічних настроїв, а також на загострення соціально-політичної ситуації в країні.
2. Спеціальні інформаційні операції, організовані державою-агресором, з метою дискредитації України на міжнародній арені.
3. Інформаційна експансія країн-агресорів, зокрема через розвиток власної інформаційної інфраструктури на території України та інших країн.
4. Інформаційний контроль з боку держави-агресора на тимчасово окупованих територіях.
5. Недостатній розвиток національної інформаційної інфраструктури, що ускладнює ефективну реакцію на інформаційні атаки і реалізацію національних інтересів.
6. Проблеми в національній інформаційній політиці, включаючи неповноту законодавства та невизначеність стратегічного наративу.

7. Поширення радикальних ідей, таких як ізоляціонізм та автономія, в окремих регіонах країни [53].

Результати здійсненого аналізу дозволяють зробити висновок про те, що інформаційна безпека є ключовою складовою у протистоянні гібридній агресії, і її важливість у рамках національної безпеки зростає з кожним роком. Суспільство і державні інституції повинні адаптуватися до нових викликів, що допоможе Україні ефективніше захищати свою інформаційну сферу та забезпечувати стабільність на національному рівні.

2.3. Вплив дезінформації та маніпуляцій на громадську думку

В умовах війни дезінформація набуває унікального значення, оскільки вона суттєво впливає на громадську думку і поведінку людей. У цьому контексті критично важливо розуміти природу та механізми дезінформації. Часто маскуючись під правдиву інформацію, вона може маніпулювати сприйняттям подій, формувати стереотипи і викликати паніку та страх. У цьому розділі ми дослідимо, як дезінформація впливає на суспільство в умовах війни та які існують способи боротьби з цим явищем.

Вплив маніпуляцій на суспільство відіграє велику роль у становленні держави, її розвитку та подальшому існуванні. Впливати за допомогою слів не складно, для цього використовуються різні методи, які надають вербальний вплив як на одну людину, так і на велику групу людей. Маніпулювання громадською думкою шляхом використання безлічі прийомів психологічного та інформаційного впливу є поширеним явищем в засобах масової інформації. Зокрема, вплив на інформацію здійснюється у політичних цілях. Політичне маніпулювання громадською думкою – це перешкода основним принципам демократичного суспільства і серйозна загроза психологічної безпеки громадян.

У зв’язку з викладеним вище, постає необхідність зрозуміти дефініцій «дезінформація» та «маніпуляція».

Дезінформація має глибоке історичне коріння, початок якої береться у 17 столітті термін, і де вислів "газетна качка" вперше почав використовуватися для позначення фейкових новин. У 20 столітті дезінформація активно використовувалася під час військових дій, особливо кампанії дезінформації нацистської Німеччини та Радянського Союзу, які використовувалися для пропаганди і приховання своїх злочинів [54].

Розглянемо, як інтерпретується поняття «дезінформація» у словниках. "Cambridge Advanced Learner’s Dictionary & Thesaurus" визначає дезінформацію як неправдиву інформацію, яка поширюється з метою ввести людей в оману.

Водночас, "Oxford Living Dictionary" пропонує більш розширене визначення, яке включає не тільки неправдиві відомості, що вводять в оману, а й підкреслює роль пропаганди, що розповсюджується державними структурами з метою впливу на опозицію або ЗМІ. Цей словник також зазначає, що поняття дезінформації стало поширеним у Європі з 1950-х років і має російське походження.

У свою чергу, радянський "Контррозвідувальний словник" не наводить визначення терміну «дезінформація», але фіксує поняття «дезінформаційні відомості», під якими маються на увазі спеціально підготовлені дані, що використовуються для створення у супротивника хибних уявлень про реальність, на основі яких він може приймати рішення, вигідні дезінформуючій стороні.

З цього можна зробити висновок, що в наведених визначеннях дезінформація розглядається саме як вид інформації, а не як процес її створення та поширення. Варто зазначити, що в радянському словнику не йдеться про хибність або неправдивість дезінформаційних відомостей. Натомість акцент робиться на їх спеціальній підготовленості та меті — формувати хибні уявлення про дійсність. Ця характеристика є надзвичайно актуальною й сьогодні, оскільки практика показує, що дезінформація може

ґрунтуватися не лише на спотворених чи неповних даних, але й на навмисно створених фактах [55].

З іншого боку, поняття "дезінформація" неодноразово ставало предметом наукових досліджень. Наприклад, Д.Х. Фетцер визначав дезінформацію як розповсюдження неповної, неточної чи іншим чином оманливої інформації, метою якого є свідоме введення в оману щодо правди.

Шлапаченко В. М. трактував дезінформацію як метод інформаційно-психологічного впливу, при якому об'єктом впливу є особа або група осіб, уповноважених приймати рішення, а засобом – модифікована інформація, що сприяє формуванню хибних уявлень про події чи явища, що, в свою чергу, призводить до прийняття вигідних для суб'єкта впливу рішень.

Кіца М. О. також розглядала дезінформацію як інструмент психологічного впливу, що полягає в наданні об'єкту інформації, яка створює викривлену реальність, але при цьому не акцентувала увагу на спеціальних вимогах до об'єкта впливу чи кінцевій меті дезінформації – прийнятті бажаного рішення.

Натомість Саєнко О. Г., досліджуючи механізми інформаційно-психологічного впливу в умовах гібридної війни, підкреслював, що дезінформація тісно пов'язана з маніпуляцією, і визначав її як інформацію, яка спрямована на введення в оману та нав'язування спотвореного або неправдивого уявлення про реальність. Тобто він розглядав дезінформацію не як тип впливу, а як інструмент, який застосовується для цього впливу. Крім того, він виділяв такі форми дезінформації, як сенсації, стереотипи, образи та новини [55].

Сучасні методи боротьби з дезінформацією включають міжнародні ініціативи, спрямовані на її усунення. Наприклад, Європейська Комісія створила Кодекс поведінки для великих технологічних платформ (Google, Facebook, Twitter), щоб обмежити поширення фейкових новин.

До сучасних форм дезінформації належать:

− Текстовий контент: статті, новини, блоги.

− Фейкові новини: неправдиві повідомлення, що видаються за достовірну інформацію.

− Діпфейки: маніпульовані відео або аудіо за допомогою штучного інтелекту.

− Координована неавтентична діяльність: створення фальшивих акаунтів для масового розповсюдження дезінформації.

Основними методами боротьби є фактчекінг та моніторинг джерел інформації для виявлення анонімних чи фальшивих повідомлень.

Багато країн створили законодавчі ініціативи для боротьби з дезінформацією. Наприклад, у Німеччині існує закон NetzDG, який вимагає від соціальних мереж видаляти неправдиві повідомлення протягом 24 годин. У Франції закон проти дезінформації дозволяє уряду блокувати фейкові новини під час виборчих кампаній.

На міжнародному рівні організації, такі як ООН та Рада Європи, працюють над розробкою глобальних стандартів для боротьби з дезінформацією. Проте важливо зберігати баланс між захистом громадян та правом на вільне висловлювання, оскільки боротьба з фейковими новинами може впливати на свободу слова [54].

Проілюструємо викладене вище яскравими прикладами російської дезінформації про Україну. Відповідно до даних Державного департаменту, який працює з іншими урядовими відомствами США, російські військові та розвідувальні структури проводять інформаційну кампанію проти України. Російська пропаганда активно поширює дезінформацію з метою представити Україну та її уряд як агресора в конфлікті між Росією та Україною. Такі маніпуляції спрямовані на західні країни, щоб створити враження, що дії України можуть призвести до глобальної війни, а також переконати громадян Росії в необхідності військових дій проти України.

Ось кілька прикладів російської пропаганди та реальних фактів:

1. Дезінформація «Україна та її урядовці є агресорами в російсько-українському конфлікті». Насправді, Росія, на чолі з режимом Путіна, звинувачує жертву агресії, Україну, у провокаціях. Росія вторглася в Україну у 2014 році, окупувала Крим, підтримує бойовиків на Донбасі і зараз зосереджує понад 100 000 військових на кордоні з Україною, погрожуючи «відповідними військово-технічними» заходами, якщо її вимоги не будуть виконані;

2. Дезінформація «Захід спонукає Україну до конфлікту». Реальність – поточну кризу спровокувала саме Москва, розмістивши більше 100 000 солдатів на кордоні з Україною, без аналогічних військових рухів з боку України. Російські військові та спецслужби розповсюджують дезінформацію, щоб представити Україну як агресора. Росія намагається обдурити світ, змусивши його повірити, що Україна може спровокувати глобальний конфлікт, і переконати своїх громадян у доцільності військових дій в Україні. Москва звинувачує інших у своїй агресії, однак саме Росія має виконати свої зобов'язання щодо мирного врегулювання через дипломатичні засоби;

3. Дезінформація «Розміщення російських військ — це просто передислокація військ на її території». Насправді, розміщення більше 100 000 російських військових на кордоні з Україною, включаючи досвідчені бойові підрозділи і наступальні озброєння, — це не проста ротація. Це явна загроза Україні, яке зберігає свою територіальну цілісність. Паралельно з військовими заходами Росія веде кампанію з дезінформації, щоб підривати довіру до української влади і створювати умови для подальшої агресії;

4. Дезінформація «США планують напади з використанням хімічної зброї на Донбасі». Реальність – США, як і Росія, є підписантами Конвенції про заборону хімічної зброї та не використовують її. Натомість Росія двічі застосовувала хімічну зброю для атак на опонентів, зокрема за межами Росії. Водночас США з 2014 року надали гуманітарну допомогу Україні на суму

понад $351 млн для постраждалих від російської агресії. Росія, в свою чергу, маніпулює інформацією, щоб виправдати свої військові дії;

5. Дезінформація «Росія захищає етнічних росіян в Україні». Насправді, немає жодних підтверджень, що етнічні росіяни чи російськомовні громадяни зазнають переслідувань з боку української влади. Проте в окупованому Росією Криму і на Донбасі українці стикаються з утисками, репресіями та обмеженнями своїх прав. У Криму Росія змушує українців приймати російське громадянство або втрачати своє майно, доступ до медичних послуг і роботу. Ті, хто виступає проти російської окупації, піддаються арештам, обшукам, дискримінації та навіть катуванням. Росія активно переслідує релігійні та етнічні меншини, звинувачуючи їх у "екстремізмі" і "тероризмі" [56].

Отже, можна зробити висновок, що в умовах цифрової епохи дезінформація досягла нового рівня і стала одним із найбільших викликів як для окремих країн, так і для глобальної спільноти. Тому розробка правових механізмів для боротьби з цим явищем є надзвичайно актуальною. Однією з головних труднощів у впровадженні нормативно-правових заходів щодо боротьби з дезінформацією є відсутність єдиного підходу до її визначення та розуміння основних її ознак.

Перспективи подальшого вивчення заявленої проблеми вбачаємо у дослідженні сутності «маніпуляції», адже питання вивчення даного терміну є досить дискусійним. Маніпуляція суспільною свідомістю є основною інформаційною загрозою національній безпеці, яка проявляється через можливість іншої сторони впливати на інформаційну інфраструктуру країни, її ресурси, суспільство, а також свідомість і підсвідомість громадян. Метою цього впливу є нав'язування системи цінностей, поглядів, інтересів і рішень у ключових сферах державного та суспільного життя, щоб спрямувати поведінку та розвиток суспільства в потрібному для іншої сторони напрямі.

Етимологія слова «маніпуляція» походить від латинського manipulus – пригорща, жменя (від manus – рука і ple – наповнювати). У різних словниках

європейської мови це поняття визначається як «Поводження з об’єктами, що мають певні наміри, цілі».

У сучасній науковій та публіцистичній літературі існує багато тлумачень терміну «маніпуляція». Це демонструє неоднозначність цього поняття і вказує на різноманіття підходів до його аналізу. Важливо зазначити, що маніпуляцію часто асоціюють із такими явищами, як інформаційна війна, пропаганда, зомбування, «макіавеллізм», дезінформація, політичні інтриги тощо [57].

Маніпулювання може бути як результатом, так і методом неправильних міркувань. Водночас у науковій літературі існують різні точки зору щодо оцінки маніпуляцій. А. Шопенгауер зазначав, що немає чіткої межі між правильними та неправильними міркуваннями, оскільки головним є досягнення правди. Тому з його погляду маніпулювання може бути виправданим. Це підтверджують сучасні психологи, які вважають, що в деяких ситуаціях маніпуляція не є негативною.

Наприклад, Шехерезада маніпулює владним Шахріаром, розповідаючи йому казки, і це не засуджується, оскільки таким чином вона протягом трьох років рятувала не лише себе, але й інших дівчат своєї країни. В повсякденному житті маніпуляція може виконувати функцію захисту від авторитарних керівників, важких колег чи родичів, а також від недружніх ситуацій у спілкуванні з іншими людьми.

В.П. Шейнов звертає увагу на те, чи є мотиви маніпулятора егоїстичними або альтруїстичними. Якщо маніпуляція має егоїстичний характер, то вигоду отримує лише той, хто здійснює вплив. Однак, якщо вигоду отримує адресат маніпуляції, а не ініціатор, то це можна розглядати як альтруїстичний прихований вплив.

Проте сучасні філософи не погоджуються з цією думкою, вважаючи, що "перемога, здобута за допомогою отруєної зброї, не принесе задоволення, а лише викличе сором". О. М. Лисанюк прагне визначити межі між легітимними

та нелегітимними аргументами в дискусіях. Вона вважає, що еристика та пейрастіка (мистецтво ведення бесіди без маніпуляцій) є допустимими соціальними практиками [58].

З одного боку, технології впливу на свідомість людей є різноманітними, але важливою метою суб'єкта інформаційної війни стає здатність кодувати повідомлення, що поширюються під час цієї війни. Завдання такої маніпуляції зазвичай включають:

- зниження рівня усвідомленості населення на конкретній території;
- руйнування усталених світоглядних цінностей і заміна їх на інші стимули;
- знищення культурної та родової пам'яті, що призводить до психічних розладів у суспільстві, появи керованих осіб із маніакальними тенденціями;
- розрив традиційних механізмів самоідентифікації та впровадження нових через створення різних «груп участі»;
- підрив суб'єктності цілих етнічних груп і народів;
- здійснення цивілізаційної переорієнтації етносів і народів [59].

З іншого боку, основна мета інформаційних війн полягає у впливі на масову свідомість. Часто така маніпуляція націлена на:

- впровадження в суспільну та індивідуальну свідомість негативних і шкідливих ідей;
- дезінформацію та дезорієнтацію населення;
- ослаблення певних переконань і традицій;
- залякування власного населення образом ворога;
- демонстрацію своєї сили з метою налякати опонента [60].

Отже, важливим завданням на сучасному етапі є захист прав і свобод людини, що стає більш досяжним за умов підвищення рівня правової

свідомості громадян та їхнього розуміння основних прав і свобод, а також законних способів їх захисту у випадку порушення.

В Україні лише починає формуватися практика масштабних соціологічних опитувань громадян, що відбувається поряд із маніпуляцією політиків суспільними настроями та цінностями потенційних виборців. Люди дедалі уважніше оцінюють роботу влади й дають власну оцінку ситуації, що вказує на поступове формування «антиманіпуляційного імунітету». Показовим є загальнонаціональне опитування, проведене соціологічною службою Центру Разумкова з 23 березня по 6 квітня 2007 року в межах моніторингу діяльності влади.

На запитання «чи є в країні політична криза» 73 % респондентів відповіли позитивно, а лише 9 % заперечили. На думку 61 % опитаних, ситуація в країні погана, тоді як лише 5 % мають іншу думку. З серпня 2006 року до квітня 2007 року, після формування коаліційного уряду під керівництвом В. Ф. Януковича, 49 % громадян вважають, що ситуація погіршилася. При цьому 61 % респондентів переконані, що президент не захищає інтереси громадян, а 59 % вважають, що В. Ф. Янукович дбає лише про власні інтереси [60].

Для протидії впливу дезінформації та маніпуляції на громадську думку, ми пропонуємо такі заходи, які в подальшому можуть бути використані державою:

1. Підвищення рівня медіаграмотності населення. Організація освітніх програм і тренінгів, які сприятимуть формуванню критичного мислення у громадян та здатності оцінювати достовірність інформації. Такі заходи допоможуть населенню розпізнавати дезінформацію і маніпуляцію та знижувати її вплив на суспільну думку.

2. Створення платформ для швидкого спростування фейків. Розробка онлайн-ресурсів, де фахівці перевіряють інформацію на достовірність і

оперативно публікують спростування недостовірних повідомлень. Це може бути інтерактивний портал або розділ на офіційних сайтах урядових структур.

3. Партнерство з соціальними мережами для виявлення та маркування фейків. Спільні ініціативи з соціальними платформами, спрямовані на позначення або видалення неправдивого контенту, можуть зменшити охоплення дезінформації. Це дасть можливість швидше виявляти загрози та обмежувати їх поширення.

4. Розвиток незалежних медіа та підтримка якісної журналістики. Створення умов для роботи незалежних засобів масової інформації та підвищення стандартів журналістики сприяють поширенню об'єктивної інформації. Підтримка таких медіа зміцнює довіру громадян до перевірених джерел.

5. Проведення інформаційних кампаній, що роз'яснюють механізми дезінформації. Інформаційні кампанії, що пояснюють, як працюють методи маніпуляції та дезінформації, можуть підвищити обізнаність населення. Це допоможе людям краще розуміти й оцінювати інформаційні потоки, зменшуючи вразливість до маніпулятивних повідомлень.

Висновки до другого розділу

Підбиваючи підсумки, можна зазначити, що сучасні інформаційні виклики для України значною мірою обумовлені поєднанням внутрішніх і зовнішніх факторів. Зокрема, глобальний розвиток інформаційних технологій і військові конфлікти, такі як повномасштабне вторгнення Росії, підвищують роль інформації як важливого ресурсу і засобу маніпуляції. Це створює численні загрози для національної безпеки, зокрема через пропаганду, дезінформацію та кібероперації, які активно застосовуються як зовнішніми державами, так і внутрішніми деструктивними групами. Водночас, низький рівень інформаційної грамотності серед населення ускладнює боротьбу з маніпуляціями. Тому, для ефективної протидії цим загрозам необхідно

посилити законодавче регулювання інформаційної сфери, розвивати освітні програми для підвищення медіаграмотності громадян та впроваджувати інноваційні технологічні рішення, такі як штучний інтелект для виявлення фейків та кіберзагроз.

Ключовим елементом є інформаційна безпека, оскільки маніпуляції з інформацією можуть дестабілізувати суспільство, підривати довіру до державних інститутів і посилювати внутрішні розбіжності. Захист національного інформаційного простору є критичним для забезпечення державного суверенітету, а також для протидії гібридній агресії. Важливим аспектом є розвиток медіаграмотності серед громадян, модернізація кіберзахисту та вдосконалення законодавчої бази

РОЗДІЛ 3. ШЛЯХИ ТА МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

3.1. Стратегічне планування у сфері інформаційної безпеки

Глобалізація спричинила серйозні зміни не лише в міжнародному безпековому середовищі, але й у внутрішніх процесах держави. Планування національної безпеки — це управлінський процес, у якому важливо враховувати можливі сценарії розвитку подій, адже кризові ситуації зазвичай супроводжуються високим рівнем напруги, ризиком насильства, браком часу та невизначеністю.

Основне завдання стратегічного планування — створення чіткого алгоритму дій для визначення мети, уточнення завдань, розподілу ресурсів і прийняття рішень. Його перевага полягає у фокусуванні на ключових питаннях національної безпеки. Для досягнення найкращих результатів стратегічне планування вимагає ефективного збору інформації, вивчення стратегічних альтернатив і посиленої уваги до можливих ризиків, що виникають під час прийняття рішень.

Пітер Лоранж описує стратегічне планування як процес, який сприяє інноваціям і змінам в організації на необхідному рівні. Він визначив чотири ключові напрямки цього процесу:

1. Розподіл ресурсів (фінансових фондів, дефіцитних управлінських талантів, технологічної експертизи);
2. Адаптація до зовнішнього середовища (налагодження взаємовідносин організації з оточенням);
3. Внутрішня координація;
4. Організаційно-стратегічне прогнозування [61].

Зміни в законодавстві, що стосуються правового регулювання національної безпеки України, були запроваджені у 2018 році із прийняттям Закону України "Про національну безпеку України". Це створило підґрунтя

для подальшого вдосконалення нормативної бази у цій сфері. Основними напрямами таких змін стали реформування системи державних органів, що забезпечують національну безпеку, уточнення їхніх функцій і повноважень, оптимізація координації діяльності, а також встановлення механізмів контролю. Закон також унормував систему стратегічного планування, зокрема через поділ його на довгострокове, середньострокове й короткострокове, що відображено в Розділі IV.

Стаття 25 Закону визначає мету планування у сферах національної безпеки та оборони як реалізацію державної політики через створення стратегій, концепцій, програм і планів розвитку. Водночас, аналіз практичного впровадження цих положень вказує на проблеми, пов’язані з неузгодженістю між окремими документами та недостатнім науковим обґрунтуванням ухвалених рішень.

Суб’єкти забезпечення національної безпеки – це учасники правовідносин, які мають встановлені законом права та обов’язки щодо забезпечення національної безпеки. Згідно з Конституцією України, до них належать: Президент України, Верховна Рада, Кабінет Міністрів, Рада національної безпеки і оборони, міністерства та центральні органи виконавчої влади, Національний банк, суди загальної юрисдикції, прокуратура, місцеві державні адміністрації та органи місцевого самоврядування, а також Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки, Державна прикордонна служба та інші військові формування, створені відповідно до законодавства. Крім того, суб’єктами національної безпеки є громадяни України та об’єднання громадян.

Регулювання діяльності цих суб’єктів здійснюється через низку нормативно-правових актів, зокрема закони України "Про Збройні Сили України", "Про Службу безпеки України", "Про державну прикордонну службу України", "Про Раду національної безпеки і оборони України", а також укази Президента, постанови Кабінету Міністрів і нормативні акти відомств. [62].

Варто зазначити, що програма або план – це структурований набір рішень, який базується на аналізі актуальної глобальної ситуації та спрямований на реалізацію масштабних цілей. Під час створення плану на майбутнє слід враховувати як спонтанні фактори, так і природний ритм розвитку подій. Якщо план передбачає зміну цього напряму, важливо, щоб це сприяло певному покращенню. Водночас необхідно забезпечити відповідність завдань плану реальним умовам і обставинам.

Розробка програми є результатом аналізу поточних даних і прогнозування, оскільки кожен план передбачає можливість вибору. Цей вибір значною мірою визначається ідеологією та політичною стратегією, а не лише об'єктивними обставинами. Також, стратегічне планування виконує низку функції (рис. 3.1) [61].

Рисунок 3.1 Переваги стратегічного планування

Стратегічне планування включає кілька послідовних етапів, процедур і деталізованих дій, які потрібно виконати. Перед початком роботи над стратегічним планом важливо усвідомити його значущість, уточнити

відповідні організаційні повноваження та забезпечити підтримку цього процесу. Для досягнення поставлених завдань необхідно:

- визначити ключових зацікавлених осіб, які мають інтерес у реалізації цілей і сприятимуть їх виконанню;
- забезпечити ефективний зворотний зв’язок, залучаючи компетентних фахівців;
- створити умови для доступу до інноваційних рішень та ідей;
- сформувати атмосферу згоди щодо визначених цілей, що збільшить ймовірність їх успішного досягнення[63].

Стратегія національної безпеки займає ключове місце в системі планування у сфері національної безпеки України. Її ухвалення неодноразово здійснювалося протягом історії країни, відображаючи зміни в політичному курсі та державній політиці. Головним завданням цієї стратегії є визначення актуальних загроз національній безпеці, встановлення відповідних цілей, завдань та механізмів захисту національних інтересів. Вона слугує основою для планування і реалізації державної політики у цій сфері.

Згідно із Законом України "Про національну безпеку України", Стратегія національної безпеки є базою для розробки інших документів у сфері національної безпеки й оборони, включаючи низку спеціалізованих стратегій і програм, таких як:

– Стратегії воєнної безпеки України;

– Стратегії громадської безпеки та цивільного захисту України;

– Стратегії розвитку оборонно-промислового комплексу України;

– Стратегії кібербезпеки України;

– Національної розвідувальної програми;

– Державних програм у сферах національної безпеки і оборони.

Міністерства та центральні органи виконавчої влади створюють державні цільові програми, спираючись на галузеві стратегії реалізації державної політики, у порядку, визначеному законодавством.

Законодавством передбачено обов’язкову розробку чотирьох стратегій, Національної розвідувальної програми та державних цільових програм у певних сферах. Проте частина цих документів досі не оприлюднена, що ускладнює визначення, чи містять вони інформацію з обмеженим доступом. Якщо їх метою є визначення стратегічних цілей державної політики, то забезпечення публічного доступу до таких документів є доцільним. Крім того, усі зазначені документи повинні бути взаємно узгодженими, щоб забезпечити ефективність державної політики [62].

Інформаційна безпека України є ключовим елементом її стратегії збереження суверенітету та стабільності, що реалізується через впровадження структурованої та продуманої політики, спрямованої на захист національних інтересів від загроз як внутрішнього, так і зовнішнього характеру.

Національне стратегічне планування передбачає раціональне використання ресурсів і потенціалу держави, включаючи людські, інформаційні, фінансові, телекомунікаційні, технологічні й інженерні. Це спрямовано на забезпечення безпеки, стабільності соціально-економічного розвитку та цифрової трансформації громадянського суспільства.

Досягнення цієї мети вимагає високого рівня управлінської культури, застосування системного аналізу та прогнозування в процесі забезпечення інформаційної безпеки. Ефективність державного управління у цій сфері може бути значно підвищена завдяки стратегічному плануванню.

Цей підхід має стати універсальним інструментом для всіх органів влади, що дозволить вирішувати актуальні завдання в сфері інформаційної безпеки, зокрема із залученням державно-приватного партнерства.

На сьогодні суспільство, особливо ІТ-сектор, стикається із гібридною агресією з боку російської федерації, яка завдає значних збитків через проникнення в інформаційний простір. РФ активно використовує сучасні технології, такі як соціальні мережі та мікроблоги, для маніпулювання

громадською свідомістю, посилення соціальної напруги та поширення забороненої інформації.

Гібридна війна стає дедалі складнішою, тому необхідно адаптуватися до нових форм загроз і розробляти механізми їх нейтралізації. Спецслужби мають враховувати інноваційні методи гібридної агресії РФ, зокрема з метою запобігання сценаріям «керованого хаосу». Для цього потрібне посилення контррозвідувальних можливостей та ефективна протидія підривній діяльності, що загрожує державі.

Також, важливим елементом для України є досвід зарубіжних країн у формуванні стратегічного планування у сфері інформаційної безпеки, розглянемо на прикладі США.

Системи стратегічного планування у провідних країнах світу відрізняються за підходами: від чітко регламентованої нормативно-правової бази, як у США, до менш формалізованих і необов’язкових систем, характерних для інших держав.

Попри різницю в структурах стратегічних документів і особливостях державного управління, загальна логіка побудови системи стратегічного планування залишається сталою. Наприклад, значна кількість стратегічних документів у сфері безпеки та оборони в США не означає, що Велика Британія має труднощі через меншу кількість подібних документів.

Основним фактором, що визначає ефективність стратегічного планування, є культура функціонування цієї системи, яка формується протягом тривалого часу.

США демонструють системний підхід до розробки керівних документів стратегічного рівня у сфері національної безпеки, активно застосовуючи сучасні методи стратегічного планування. Основним законодавчим актом, який регулює ці процеси, є закон "Про ефективність та результати діяльності уряду". Цей документ встановлює ієрархію стратегічного планування

виконавчої влади, визначає перелік необхідних документів і конкретні терміни їх підготовки.

Система стратегічного планування в США має чітку структуру з розподілом документів за функціональною та галузевою класифікацією. На кожному рівні формуються загальні, галузеві та функціональні стратегії, які узгоджуються між собою.

На вершині ієрархії стратегічних документів після Конституції розташована Стратегія національної безпеки, яка є основою для розробки Національної стратегії оборони та інших галузевих стратегій, що формують другий рівень системи.

Національна воєнна стратегія США, створена на основі положень Національної стратегії оборони, належить до третього рівня. Вона визначає завдання для збройних сил і концепції взаємодії складових сектору безпеки, слугуючи ключовим керівним документом у цій сфері [61].

Отже, враховуючи вище зазначену інформацію, важливо запропонувати такі можливі варіанти удосконалення стратегічного планування у сфері безпеки та оборони:

1.Чітке регламентування ієрархії стратегічного планування через законодавчі акти. Це передбачає ухвалення законодавства, подібного до закону про стратегічне планування США, який встановлює основні засади, принципи, порядок та механізми роботи системи стратегічного планування. Також необхідно створити ієрархічну систему стратегічних документів, таких як Стратегія національної безпеки України, Стратегія діяльності уряду, Стратегія воєнної безпеки чи Стратегія розвитку оборонно-промислового комплексу. Діючі нормативно-правові акти слід узгодити із Законом України "Про стратегічне планування", який має стати базовим документом у цій сфері.

2. Удосконалення нормативно-правової бази стратегічного планування. Це включає розробку Закону України "Про стратегічне планування", який встановлюватиме загальні принципи роботи системи стратегічного

планування, а також модернізацію існуючої нормативної бази для її ефективного функціонування.

3.2. Розвиток національних інформаційних ресурсів і технологій

В сучасному світі інформація набуває статусу ключової цінності, а сфера її створення, обробки та поширення стає однією з провідних галузей, куди постійно інвестують значні ресурси. Інформатизація суспільства є важливим чинником економічної модернізації на ринкових засадах та сприяє інтеграції України в глобальну спільноту. Інформаційні ресурси та сфера їхнього використання відіграють системо-утворюючу роль у функціонуванні суспільства і держави, впливаючи на всі аспекти їхнього розвитку — політичний, економічний, соціокультурний, оборонний тощо.

Стаття 17 Конституції України зазначає, що захист суверенітету, територіальної цілісності, економічної та інформаційної безпеки є пріоритетними завданнями держави та всього народу. Це підкреслює важливість захисту інформаційного простору як одного з головних аспектів забезпечення національної безпеки. Фраза "Хто володіє інформацією, той володіє світом" яскраво ілюструє силу інформації. Знання використовуються як потужний інструмент для реалізації національних інтересів і вирішення конфліктів у різних сферах, що обумовлює виникнення специфічної боротьби методами інформаційного впливу.

Новітні інноваційні процеси значною мірою базуються на використанні інформаційних систем і технологій, які здатні створювати, зберігати, передавати й аналізувати великі обсяги даних, а також генерувати нові знання. Ці технології відіграють ключову роль як у національних, так і в міжнародних економічних системах. Швидкий розвиток глобального ринку інформаційних технологій суттєво впливає на світову економіку, адже впровадження інновацій у цій галузі підвищує ефективність виробничих процесів, оптимізує використання ресурсів і прискорює обмін даними.

У сучасних реаліях управління стає одним із основних ресурсів організації нарівні з матеріальними, фінансовими та людськими. Інтенсивний розвиток комп'ютерних технологій, вдосконалення технічного обладнання й поява нових типів програмного забезпечення зумовили кардинальні зміни у підходах до автоматизації управління виробничими процесами.

Підприємства активно впроваджують інформаційні та комунікаційні технології для підвищення ефективності своєї роботи та збільшення прибутків. Завдяки Інтернету компанії отримують можливість залучати клієнтів не лише в межах країни, а й на міжнародному рівні. Маркетинг також активно інтегрується в цифрове середовище, зокрема через Інтернет. Більшість великих компаній створюють власні веб-сайти, які служать платформою для інформування потенційних клієнтів про їхню діяльність, рекламні кампанії та важливі події.

Соціальні мережі стають ще одним потужним інструментом для розширення клієнтської бази. Особливо популярним є використання платформи "Facebook", де компанії створюють профілі для взаємодії з аудиторією, поширення інформації та аналізу зацікавленості потенційних споживачів [64].

Згідно з електронним словником, інформаційні технології (IT) та інформаційно-комунікаційні технології (Information and Communication Technologies, ICT) – це комплекс методів, виробничих процесів, а також програмно-технічних засобів, спрямованих на збирання, обробку, збереження, поширення, відображення та використання інформації в інтересах користувачів.

Сучасні інформаційні технології поділяються на кілька основних видів:

- технології обробки даних,
- технології управління,
- системи підтримки прийняття рішень,
- технології експертних систем,

- та інші.

У 2024 році Україна зайняла 81-ше місце у світі за рівнем розвитку інформаційно-комунікаційних технологій (ІКТ) за даними Global Innovation Index. Хоча країна покращила свої позиції в окремих напрямках, таких як експорт ІТ-послуг (5-те місце), загальний рівень розвитку інфраструктури та використання технологій залишається відносно середнім, що вказує на необхідність подальшого вдосконалення [65].

За даними ООНівського рейтингу Online Services Index, що є частиною дослідження E-Government Development Index і охоплює 193 країни, Україна посіла 5-е місце за рівнем цифрових державних послуг. Про це повідомив Михайло Федоров, міністр цифрової трансформації України.

У 2018 році Україна займала лише 102-гу позицію, але за шість років піднялася на 97 сходинок, опинившись серед світових лідерів. Попереду залишилися Корея, Данія, Естонія та Саудівська Аравія.

За даними Федорова, на сьогодні порталом "Дія" користуються майже 21 мільйон громадян. "Першими прирівняли електронні документи до паперових і четвертими в Європі запустили цифрові водійські права. Реєстрація ФОП в Україні — найшвидша в усьому світі, усього 4 секунди. Крім 5-го місця за рівнем розвитку цифрових послуг, ми на першому місці щодо залученості громадян до державних процесів через онлайн", — повідомив міністр.

Федоров також відзначив, що українську платформу "Дія" планують інтегрувати в інших країнах. Крім того, він поставив мету до 2026 року підняти Україну на перше місце в цьому рейтингу. [66].

Інформаційні ресурси — це сукупність документів і їх масивів, які зберігаються в інформаційних системах, таких як бібліотеки, архіви, фонди, бази даних, депозитарії чи музейні сховища.

Виділяють такі типи інформаційних ресурсів:

1. Інформаційні ресурси спільного користування – це сукупність інформаційних ресурсів, які належать державним органам, установам, що займаються науково-технічною інформацією, науковим і технічним бібліотекам, а також комерційним організаціям, залученим до науково-технічної діяльності. Використання таких ресурсів регламентується угодами між їх власниками.

2. Інформаційні ресурси науково-технічної інформації – це впорядковані зібрання науково-технічної літератури та документації, до яких належать книги, брошури, журнали, патенти, нормативно-технічні акти, промислові каталоги, конструкторська документація, звіти про наукові й дослідно-конструкторські роботи, а також переклади та депоновані рукописи. Ці матеріали можуть бути доступні як у друкованій формі, так і на інших носіях. [67].

Закон України "Про національну програму інформатизації" містить універсальне визначення поняття "інформаційний ресурс". Відповідно до статті 1 цього закону, інформаційний ресурс – це сукупність документів, збережених в інформаційних системах, таких як бібліотеки, архіви, чи бази даних.

Проте це визначення не враховує низки важливих аспектів, які характеризують інформацію як ресурс. До основних характеристик належать: "інформація" як категорія змісту, "інформаційний ресурс" як продукт людської діяльності, об'єкт права власності фізичних і юридичних осіб, держави, а також елемент товарно-ринкових відносин. Інформаційний ресурс може мати статус національного чи державного надбання, виступати системо-утворювальним і керованим елементом, що впливає на розвиток суспільства, економіки та національної безпеки.

Дефіцит цього ресурсу, його низька якість або вплив зовнішніх негативних факторів можуть призвести до значної шкоди для суспільства й держави. Інформаційні ресурси, через їхню цінність, стають об’єктом злочинних посягань, що вимагає спеціальних заходів захисту. Крім того, вони

мають властивості, характерні для інших видів ресурсів, і за своєю важливістю поділяються на національні та державні. Розглянемо ці категорії детальніше. [68].

Національні інформаційні ресурси включають всю інформацію, що належить Україні, незалежно від її змісту, форми, дати створення чи форми власності. Це також результати інтелектуальної та творчої діяльності, закріплені на будь-яких носіях і доступні через засоби масової інформації, телекомунікації, архіви, бібліотеки, музеї, фонди, бази даних, публічні виступи чи мистецьку діяльність.

Головною метою національних інформаційних ресурсів є підтримка національних інтересів України, захист інформаційних прав громадян, суспільства, державних і місцевих органів влади, а також юридичних осіб різних форм власності. Вони слугують основою для забезпечення суверенітету та інформаційної безпеки країни, сприяючи розвитку економіки, науки, культури та інших сфер. До їх складу входять дані різного походження і форм власності.

Слід мати на увазі, що Державні інформаційні ресурси – це впорядкована інформація, яка доступна завдяки інформаційним технологіям і права на яку належать державним органам, військовим формуванням, створеним за законами України, а також державним підприємствам, установам і організаціям. До них також належить інформація, створена чи оброблена фізичними або юридичними особами за дорученням державних органів відповідно до законодавства.

Основні вимоги до державних інформаційних ресурсів включають актуальність, достовірність, повноту, компактність подання та швидкість доступу. Їхня структура поділяється на обов’язкову частину (основні дані й вихідна інформація) та додаткову частину (довідкові матеріали, бібліографічний апарат і допоміжна інформація) [68].

Серед головних досягнень України у формуванні інформаційно-комунікативного суспільства можна виділити такі:

- Високий кадровий потенціал: Україна входить до п’ятірки країн із найбільшою кількістю фахівців у галузі комп’ютерних наук і лідирує за якістю підготовки кадрів для сфери інформаційних технологій.
- Розвиток перспективних напрямів: У країні активно розвиваються штучний інтелект, теорія самоорганізації та системний аналіз, засновані на моделюванні роботи людського мозку для вирішення складних завдань. Ці дослідження стали значним проривом у кібернетиці.
- Історична роль у створенні ЕОМ: У Києві академіком Лебедєвим була створена перша в СРСР і третя у світі електронно-обчислювальна машина.
- Ініціатива в системах управління: У 1964 році академік Віктор Глушков, перший директор Інституту кібернетики НАН України, запропонував проект Загальнодержавної системи збору та обробки інформації для управління економікою. Цей проект започаткував розвиток інформаційно-комп’ютерних технологій.

Фактори, що ускладнюють формування «сильного» іміджу України в міжнародному інформаційному співтоваристві, включають:

1. Неповна законодавча база у сфері інформаційних технологій.

2. Відсутність комплексної стратегії розвитку: немає цілісної національної програми соціально-економічного прогресу, що базується на принципах інформаційного суспільства.

3. Непріоритетний статус інформаційного суспільства: розвиток цієї сфери розглядається як міжвідомча задача, а не як стратегічний напрямок для всієї країни.

4. Недостатня координація на державному рівні: слабка інтеграція елементів інформаційної інфраструктури, включаючи загальнодержавні, корпоративні та відомчі інформаційно-телекомунікаційні мережі.

5. Повільне впровадження інтернет-технологій: низький рівень державної координації у впровадженні інтернет-послуг [67].

Отже, можна зробити висновки, що інформаційні технології мають вирішальне значення для розвитку сучасного суспільства. Використання комп'ютерних систем, комунікаційних мереж та інноваційних технологій значно впливає на різні сфери, зокрема освіту, бізнес, медицину, політику та загальне сприйняття світу. Наразі не існує єдиного стандарту чи моделі для формування інформаційного суспільства, до якого має прагнути наша країна. Кожен регіон має свої унікальні особливості, які визначають характер цього процесу. Однак, без належної державної підтримки наші спеціалісти будуть змушені працювати за кордоном. Тому чим швидше і активніше розвиватимуться ці процеси, тим більше можливостей для підвищення рівня розвитку суспільства.

Тому, ми вважаємо, що вкрай актуальним є створення національної стратегії для побудови інформаційно-комунікаційного суспільства. Доцільно побудувати стратегію, яка повинна включати кілька ключових аспектів:

1. Підвищення рівня інформованості громадян і зміцнення соціальної відповідальності щодо інформаційної безпеки.
2. Раціональне використання наявних ресурсів та активізація взаємодії між державою, бізнесом і громадянським суспільством для забезпечення сталого розвитку цієї сфери.
3. Консолідація зусиль і ресурсів для проведення політичних і інституційних реформ в інформаційному секторі.
4. Визначення чітких ролей і відповідальності кожного учасника процесу — держави, бізнесу і громадськості — для ефективного партнерства в розвитку цієї сфери.

5. Орієнтація ресурсів на досягнення національних стратегічних цілей, включаючи залучення додаткових інвестицій в інформаційно-комунікаційні технології.

Тільки через комплексний підхід до вирішення цих завдань можна забезпечити успішну інтеграцію України в глобальне інформаційне середовище та створити стійку інформаційну інфраструктуру.

3.3. Співпраця з міжнародними організаціями в контексті інформаційної безпеки

Інформаційна безпека займає ключову позицію в загальній системі міжнародної безпеки, оскільки нові виклики в інформаційному просторі призвели до виникнення нових методів ведення конфліктів і загроз для глобального порядку. Реалізація таких загроз може серйозно вплинути як на національну, так і на міжнародну безпеку.

Сучасні виклики у сфері глобальної інформаційної безпеки змусили переосмислити підходи до міжнародної співпраці, зокрема щодо створення спільних стандартів і правил відповідальності. Основними характеристиками системної кризи інформаційної безпеки є вразливість, взаємозв'язок, доступність і незахищеність учасників міжнародних відносин. Це обумовлює необхідність розробки дієвих механізмів для забезпечення глобальної інформаційної безпеки.

Для подолання кіберзагроз та проблем інформаційної безпеки міжнародна співпраця має базуватися на пошуку спільних рішень у межах міжнародних організацій. Це включає розробку загальних стратегій боротьби з кібервійнами, інформаційним тероризмом та кіберзлочинністю. Лише колективні зусилля та дотримання норм міжнародного права дозволять ефективно відповісти на виклики, які виникають у політичній, економічній та безпековій сферах [69].

Сучасні виклики в області інформаційної безпеки вимагають скоординованих зусиль і інтегрованих підходів на міжнародному рівні. Організації, як-от ООН, НАТО, ОБСЄ та інші, виконують важливу роль у формуванні політики безпеки та сприянні міжнародній співпраці у цій сфері.

Рішення, які ухвалюються в рамках цих міжнародних безпекових структур, спрямовані на забезпечення стабільності в умовах постійно зростаючих загроз у інформаційному просторі. Вони ґрунтуються на принципах міжнародного права і спільних інтересах учасників, визначаючи стратегії, ініціативи та механізми реагування на новітні виклики, що виникають у галузі інформаційної безпеки.

Завдяки широкому представленню та врахуванню різноманітних позицій і інтересів міжнародних акторів ці організації розробляють ефективні механізми для колективної боротьби з інформаційними загрозами, сприяючи тим самим збереженню миру і стабільності на глобальному рівні [70].

Найбільшим впливом на модернізацію політики в сфері інформаційної безпеки має НАТО, яке, визнаючи кіберпростір як середовище інформаційного протиборства, зробило кібербезпеку головним пріоритетом своєї діяльності. Альянс створив спеціалізовані центри в країнах-членах, які є багатонаціональними інститутами для розробки доктрин кібербезпеки, удосконалення міжнародної співпраці, впровадження теоретичних розробок у боротьбі з кіберзагрозами, а також для обміну досвідом у галузі кіберзахисту серед фахівців держав-членів і партнерів.

Один із таких центрів розташований в Естонії, де він був заснований завдяки ініціативі естонської влади та перших країн-спонсорів, які підписали меморандум щодо діяльності і акредитації Центру. Важливо зазначити, що цей центр не є частиною військової структури НАТО, а його фінансування та персонал забезпечуються державами-спонсорами та учасниками [71].

Під час повномасштабного вторгнення РФ в Україну, а також в умовах конфлікту на Сході та окупації Криму, міністр оборони Естонії закликав

країни НАТО надавати фінансову підтримку Україні у зв'язку з агресивними кібератаками з боку Росії. Естонія також внесла 100 тисяч євро до трастового фонду НАТО для зміцнення інформаційної безпеки України та організувала навчання для українських фахівців з кіберзахисту.

Зазначено, що досвід України у протидії російським кіберзагрозам і інформаційній агресії може зробити її важливим партнером для Центру кібербезпеки НАТО. Це питання є актуальним не тільки для демократичних процесів в Європі, а й для глобальної безпеки.

Наведемо найбільш важливі вагомі співпраці України з міжнародними організаціями. Перша з них, є приєднання України до ініціативи "Партнерства розширених можливостей НАТО" відкриває нові перспективи для посилення співпраці в сфері інформаційної безпеки, що може бути корисним під час вирішення кризових ситуацій та проведення миротворчих операцій. В рамках цієї програми Україна отримає можливість брати участь у плануванні на ранніх етапах конфліктів, посилити обмін розвідувальною інформацією.

Співпраця України з НАТО в рамках Комплексного пакету допомоги є важливим кроком для підвищення стандартів військово-політичної організації в країні, включаючи підтримку через трастові фонди та реалізацію Річної національної програми, що є інструментом для впровадження реформ [72].

Тобто, після даної співпраці Україна отримає досвід посилення взаємодії з провідними країнами альянсу, передовий досвід в кібербезпеці, візьме участь у розробці стандартів і стратегії безпеки на міжнародному рівні.

Наступна програма, на яку варто звернути увагу — Комплексний пакет допомоги НАТО (CAP) — це ініціатива, спрямована на надання підтримки країнам-партнерам НАТО для зміцнення їхніх можливостей у сфері безпеки, зокрема в розбудові оборонних інституцій, покращенні співпраці з альянсом та інтеграції у спільну безпекову систему. Програма включає фінансову та технічну допомогу через трастові фонди НАТО, а також надання

консультаційної підтримки в різних сферах, зокрема кібербезпеки, військової реформи та управління кризами.

Для України Комплексний пакет допомоги має стратегічне значення, оскільки країна стикається з численними викликами в сфері безпеки, зокрема з агресією з боку Росії та загрозою кіберзавоювань. Програма дозволяє Україні отримати конкретну допомогу в зміцненні національної обороноздатності, розвитку інфраструктури кібербезпеки та удосконаленні процедур реагування на кризові ситуації. Одним із ключових аспектів є підвищення оперативної спроможності Збройних сил України, а також інтеграція в більш широку систему колективної безпеки[73].

Отже, Україна зможе покращить кіберзахист критичних інфраструктур, матиме доступ до передових технологій та експертних знань НАТО, зможе реалізувати національні реформи у сфері інформаційної безпеки.

Доцільно, проілюструвати Програму Європейського Союзу "Східне партнерство" — це ініціатива ЄС, що була запущена в 2009 році для сприяння політичному та економічному зближенню з шістьма пострадянськими країнами Східної Європи: Україною, Молдовою, Грузією, Вірменією, Азербайджаном і Білоруссю. Метою програми є підтримка розвитку демократичних інститутів, зміцнення економічних зв'язків, покращення управління та належного врядування, а також посилення безпеки в регіоні. Програма передбачає не лише технічну та фінансову допомогу, а й розширену співпрацю в таких сферах, як енергетика, транспорт, екологія та, зокрема, кібербезпека.

Для України "Східне партнерство" має стратегічне значення, оскільки програма надає Україні можливість зміцнити свої відносини з Європейським Союзом, сприяючи реалізації реформ і інтеграції у європейські структури. Одним із важливих аспектів є посилення співпраці в сфері інформаційної та кібербезпеки, що особливо актуально в умовах гібридної війни з Росією. Програма також сприяє економічній стабільності, розвитку інфраструктури та

зниженню енергетичної залежності від Росії, відкриваючи для України нові ринки та інвестиційні можливості [74].

Можемо зробити висновок, що для України зазначена вище програма є корисною, адже відбувається розвиток кіберзахисту в державному секторі, удосконалення правових норм у сфері інформаційної безпеки, інтеграція в європейські системи обміну інформацією про кіберзагрози.

Потрібно звернути увагу на таку програму як Програма ОБСЄ з кібербезпеки. Це ініціатива, яку Організація з безпеки і співробітництва в Європі (ОБСЄ) запустила для підтримки своїх держав-членів у розвитку національних можливостей в галузі кібербезпеки. Програма зосереджена на створенні умов для ефективного захисту інформаційних систем, протидії кіберзагрозам і зміцненні довіри між державами в кіберпросторі.

Для України програма ОБСЄ є надзвичайно важливою в умовах постійної загрози з боку кіберзлочинців і агресивних кібероперацій з боку Росії. Співпраця з ОБСЄ допомагає Україні зміцнити свою національну кібербезпеку, зокрема через обмін досвідом, участь у спільних навчаннях та отримання технічної підтримки для розвитку систем кіберзахисту. Це сприяє підвищенню готовності українських органів влади та підприємств до кіберінцидентів [74].

Остання програма, яку також варто охарактеризувати — Програма Центру кібербезпеки НАТО (NATO CCD COE). Це спеціалізований орган НАТО, створений для розвитку та вдосконалення співпраці між країнами-учасниками альянсу в галузі кібербезпеки. Центр забезпечує обмін знаннями та досвідом, проводить дослідження в сфері кіберзахисту, а також організовує навчання та симуляції, щоб підвищити ефективність реагування на кіберзагрози. Окрім цього, Центр розробляє концепції та доктрини кібербезпеки, пропонує інструменти для держав та організацій з покращення національних систем кіберзахисту, а також сприяє міжнародному співробітництву у боротьбі з кіберзлочинністю.

Для України участь у діяльності Центру кібербезпеки НАТО є важливою, оскільки вона дає доступ до передових методів захисту інформаційних систем і технологій. В умовах постійних кіберзагроз з боку Росії, участь у Центрі дозволяє Україні розвивати свою національну стратегію кібербезпеки, удосконалювати практики реагування на кіберінциденти, а також інтегруватися в міжнародні механізми кіберзахисту. Крім того, співпраця з НАТО допомагає українським фахівцям підвищувати свою кваліфікацію через участь у навчаннях та отримання доступу до міжнародних стандартів у сфері кібербезпеки [76].

Тобто, Україна має доступ до передових технологій і стратегій кіберзахисту, бере участь у міжнародних навчаннях, має можливість брати участь у розробці міжнародних стандартів кібербезпеки.

Таким чином, на основі проаналізованої інформації, можна зробити такі висновки, що міжнародне та європейське співробітництво в сфері кібербезпеки має вирішальне значення для забезпечення глобальної безпеки, оскільки кіберзагрози не визнають кордонів і можуть миттєво впливати на держави та критичну інфраструктуру по всьому світу. Таке співробітництво сприяє обміну інформацією, розробці спільних стандартів і підвищенню стійкості глобальних інтернет-мереж до кіберзагроз. Україна, маючи значний досвід у цій сфері та активно залучена до міжнародних ініціатив, продовжує відігравати важливу роль у зміцненні кібербезпеки на світовому рівні, сприяючи створенню безпечнішого кіберпростору для всіх країн.

3.4 Шляхи і механізми практичного впровадження органами публічної влади нової моделі інформаційного суверенітету країни

На основі проведеного дослідження, доцільним синтез и впровадження нової моделі кібербезпеки та інформаційного суверенітету країни, концепція і шляхи реалізації якої розроблено автором роботи, які в подальшому можуть бути використані органами публічної влади для вдосконалення системи

інформаційного суверенітету України. Окреслено два підходи до синтезу та впровадження пропонованої нової моделі.

1 варіант. Пропонується створити Національний центр кібербезпеки та медіа-інформаційної політики (далі – НЦКМІП), який координуватиме всі заходи щодо захисту інформаційних ресурсів України. Цей центр об'єднає представників органів державної влади, кібербезпекових структур, а також експертів у сфері медіа та інформаційних технологій. Шлях реалізації: ухвалення законодавчих змін, що передбачатимуть створення та діяльність НЦКМІП. Центр матиме міжвідомчий статус, у ньому працюватимуть експерти з кібербезпеки, фахівці з інформаційної політики та аналітики в галузі медіа. Потрібно створити інфраструктуру для роботи центру, зокрема забезпечити його технічними та людськими ресурсами.

Створення правового механізму для діяльності НЦКМІП передбачатиме прийняття ряду нормативно-правових актів, зокрема законів, що регулюють діяльність кібербезпеки, інформаційного захисту та медіа-простору. Ці закони повинні визначати правила для медіа, що поширюють інформацію на національному рівні, а також стандарти безпеки для інформаційних систем, що містять стратегічні дані. Шлях реалізації: прийняття та імплементація законів, таких як "Про кібербезпеку", "Про захист інформаційних ресурсів" та "Про медіа та інформаційні технології". Для цього необхідно організувати робочі групи з юридичних експертів, представників органів влади та громадських організацій, які сприятимуть створенню нових нормативних актів.

Для фінансування НЦКМІП та інших ініціатив потрібно передбачити в державному бюджеті спеціальний фонд, що буде направлений на забезпечення інформаційного суверенітету. Фонд має фінансувати заходи з кібербезпеки, створення нових платформ для моніторингу інформаційного простору, а також розробку систем для перевірки фактів у медіа. Шлях реалізації: пропозиція щодо внесення змін до державного бюджету, створення окремого фінансового резерву для розбудови інформаційної безпеки країни. Окрім цього, залучення

міжнародних грантів і фондів для розвитку інформаційних ініціатив і підтримки стартапів у галузі кібербезпеки та медіа.

Детальніше охарактеризуємо саме шлях реалізації зазначеного варіанту, адже для виконання даного механізму потрібно дотримуватись створення таких умов:

1. Інтегрована платформа для моніторингу інформаційного простору. Ідея створення інтегрованої платформи для моніторингу інформаційного простору базується на необхідності посилення безпеки держави в умовах гібридної війни та інформаційних атак. Така платформа буде спрямована на виявлення, аналіз та реагування на загрози в реальному часі. Вона використовуватиме алгоритми штучного інтелекту та технології великих даних (Big Data) для автоматизованої ідентифікації шкідливого контенту, дезінформації та кібератак. Це дозволить створити інтегровану базу даних про загрози, полегшуючи роботу державних структур і підвищуючи ефективність інформаційного захисту

2. Автоматизовані системи для виявлення загроз. Центральним елементом цієї платформи стане впровадження автоматизованих систем для виявлення кіберзагроз, зокрема фішингових атак, шкідливого програмного забезпечення та спроб компрометації даних. Ці системи будуть оснащені сучасними технологіями кіберзахисту, зокрема інструментами для аналізу інтернет-трафіку та моніторингу соціальних мереж. Також буде передбачено інтеграцію зі світовими базами кіберзагроз, що дозволить оперативно реагувати на нові виклики. Результати таких технологій вже демонструє успішне функціонування CERT-UA, яка працює як на державному, так і на міжнародному рівнях.

3. Освітні курси для медіа-спеціалістів та політиків. Важливим компонентом програми є організація навчальних курсів, спрямованих на підвищення рівня медіаграмотності серед фахівців ЗМІ та політиків. Навчання включатиме теми кібербезпеки, фактчекінгу, протидії маніпуляціям у ЗМІ та безпечного використання інформаційних технологій. Такі ініціативи

сприятимуть формуванню стійкої інформаційної культури та зменшенню впливу дезінформації на суспільство. Курси можуть проводитися у співпраці з університетами, міжнародними організаціями та технологічними компаніями.

4. Підтримка стартапів у сфері технологій і кібербезпеки. Ще одним пріоритетом є розвиток екосистеми стартапів у сфері кібербезпеки та інноваційних технологій. Це передбачає створення грантових програм, технологічних хабів та інкубаторів, де молоді підприємці зможуть розвивати свої ідеї. Така підтримка дозволить створювати нові продукти, які підвищать загальний рівень кіберзахисту. Наприклад, за сприяння державних і приватних структур можуть бути розроблені інструменти для автоматизованої перевірки фактів або платформи для захисту персональних даних.

5. Стратегічне значення ініціативи. Загалом, створення інтегрованої платформи та впровадження супутніх заходів є стратегічним пріоритетом України в умовах сучасної війни, яка має значний кіберкомпонент. Ці ініціативи спрямовані не лише на захист державних ресурсів, але й на формування нового інформаційного середовища, яке буде менш вразливим до зовнішніх загроз. Реалізація цих проєктів дозволить Україні посилити свій кіберзахист та стати світовим лідером у боротьбі з інформаційними викликами.

2 варіант. Пропонується запровадити програму розвитку національних медіа та кіберінфраструктури. Для забезпечення інформаційного суверенітету необхідно створити державну агенцію з розвитку національних медіа та кіберінфраструктури. Ця агенція займатиметься підтримкою українських медіа та ІТ-компаній, а також здійснюватиме контроль за кіберзахистом критичних інформаційних ресурсів. Шлях реалізації: створення агентства на базі Міністерства цифрової трансформації та Міністерства інформаційної політики України. Визначення його повноважень щодо контролю за інформаційними потоками та кіберінфраструктурою, а також забезпечення інформаційної безпеки.

Для розвитку національних медіа та кіберінфраструктури потрібно ухвалити нові законодавчі ініціативи, які стимулюватимуть інвестиції в українські медіа-платформи та інформаційні технології. Законодавство має включати підтримку українських виробників технологій, захист даних громадян та засадничі принципи інформаційної безпеки. Шлях реалізації: розробка законів, що забезпечують захист даних, підтримку українських інформаційних технологій, а також надають державні субсидії для стартапів у сфері кібербезпеки та медіа. Ухвалення змін до законів, що регулюють діяльність ЗМІ та інформаційних платформ.

Для реалізації проектів необхідно залучити фінансування як із державного бюджету, так і від приватних інвесторів та міжнародних партнерів. Це включатиме створення фінансових інструментів для підтримки медіа-проектів, а також інвестиційних фондів для розвитку кібербезпеки та інформаційних технологій. Шлях реалізації: розробка фінансових механізмів для залучення інвестицій, включаючи створення венчурних фондів для стартапів у сфері кібербезпеки та медіа. Ухвалення рішень щодо державного фінансування та створення окремих грантових програм для медіа та IT-компаній.

Для реалізації зазначеного механізму слід детальніше розглянути шляхи його виконання, адже досягнення мети потребує створення таких умов:

1. Впровадження національної системи кіберзахистую. Для підтримки українських IT-компаній та медіа у контексті посилення кібербезпеки важливо впровадити національну систему кіберзахисту, яка забезпечуватиме захист інфраструктури та даних від зовнішніх і внутрішніх загроз. Така система включатиме інструменти для автоматизованого виявлення загроз, аналізу інцидентів та координації дій між державними структурами й приватними компаніями. Вона також передбачає сертифікацію компаній відповідно до стандартів кібербезпеки, що сприятиме підвищенню їхньої конкурентоспроможності на міжнародному ринку

2. Розвиток цифрових платформ. Українські цифрові платформи, зокрема ті, що працюють у сфері медіа та технологій, потребують підтримки у вигляді державних грантів, інвестицій та податкових пільг. Ці заходи сприятимуть створенню нових інноваційних проєктів, які будуть конкурентними на світовому рівні. Наприклад, розробка програмного забезпечення для фактчекінгу чи аналізу великих даних може стати вагомим внеском у глобальну кібербезпеку. Крім того, підтримка місцевих платформ зміцнює інформаційний суверенітет України, зменшуючи залежність від іноземних технологічних компаній

3. Підвищення медіаграмотності населення. Одним із ключових напрямів є активна просвіта населення в аспектах медіаграмотності. Враховуючи масштаби інформаційних атак, важливо навчити громадян ідентифікувати фейкову інформацію, захищати свої дані онлайн та уникати маніпуляцій. Для цього варто впровадити інтерактивні курси, тренінги та створити доступні навчальні матеріали в інтернеті. Крім того, доцільно інтегрувати основи медіаграмотності у шкільну програму, аби формувати навички критичного мислення з раннього віку

4. Інтеграція держави і приватного сектору. Співпраця між державними структурами, приватним сектором та міжнародними партнерами стане важливим кроком у розвитку кіберзахисту. ІТ-компанії можуть отримати доступ до національних кіберцентрів для перевірки своїх систем і продуктів, тоді як медіа отримають захист від атак, спрямованих на компрометацію їхньої діяльності. Це також сприятиме створенню нових партнерств у розробці програмного забезпечення для кібербезпеки та медіаплатформ

5. Соціальний ефект від реалізації ініціатив. Комплексний підхід до впровадження національної системи кіберзахисту, підтримки цифрових платформ та підвищення медіаграмотності допоможе створити захищене та стійке інформаційне середовище. Це не лише зміцнить економічні позиції України на міжнародному ринку, але й підвищить довіру громадян до медіа,

знизивши ризики впливу дезінформації. Зрештою, такі ініціативи сприятимуть інтеграції України у світову кібербезпекову спільноту.

Таким чином, зазначені варіанти є важливими та корисними при створенні нової системи інформаційного суверенітету України.

Висновки до третього розділу

Стратегічне планування у сфері національної безпеки є важливою складовою управлінських процесів, що сприяють ефективному реагуванню на кризові ситуації та загрози. В Україні розвиток цієї системи регулюється через Закон "Про національну безпеку України", який забезпечує структуроване планування на різних рівнях — від довгострокових до короткострокових стратегій. Однак, незважаючи на вдосконалення нормативно-правової бази, існують проблеми з узгодженістю документів і недостатнім науковим обґрунтуванням рішень. Враховуючи досвід зарубіжних країн, таких як США, Франція та Німеччина, Україні необхідно вдосконалити систему стратегічного планування, впровадивши чітке регламентування ієрархії стратегічних документів і розробивши Закон про стратегічне планування, що дозволить досягти більшої ефективності в управлінні національною безпекою.

У сучасному світі інформаційні технології займають ключову роль у розвитку економіки, суспільства та національної безпеки. Вони не тільки стимулюють економічний ріст, але й активно впливають на всі сфери життя, від бізнесу до освіти. Для успішної інтеграції в глобальне інформаційне середовище необхідно створити національну стратегію, яка передбачатиме злагоджену взаємодію між державою, бізнесом та громадянським суспільством, а також раціональне використання наявних ресурсів

Інформаційна безпека стала важливою складовою міжнародної безпеки, адже нові кіберзагрози і методи ведення конфліктів вимагають розробки спільних стратегій і стандартів для забезпечення стабільності в глобальному просторі. Міжнародне співробітництво, зокрема через організації, такі як

НАТО, ООН, ОБСЄ та ЄС, сприяє ефективному обміну знаннями, розробці стратегії кіберзахисту та інтеграції національних систем безпеки з міжнародними стандартами.

Розроблено нову модель кібербезпеки та інформаційного суверенітету країни.

ВИСНОВКИ

У сучасних умовах глобалізації та цифровізації забезпечення інформаційного суверенітету є критично важливим завданням для будь-якої країни, оскільки інформаційні загрози можуть суттєво впливати на національну безпеку, економіку та політичну стабільність. Важливими шляхами досягнення цього суверенітету є розробка національних стратегій в сфері інформаційної безпеки, створення та вдосконалення механізмів захисту критичної інформаційної інфраструктури, а також розвиток технологічної незалежності через підтримку вітчизняних IT-індустрій.

Не менш важливим є укріплення міжнародного співробітництва, зокрема через участь у глобальних ініціативах з кібербезпеки та створення спільних стандартів інформаційної безпеки. Для ефективного забезпечення інформаційного суверенітету країнам необхідно посилити внутрішні законодавчі та правові механізми, удосконалювати співпрацю між державними органами, приватним сектором і громадськими організаціями.

В Україні цей процес набуває особливої актуальності в умовах гібридних загроз і агресії, що вимагає розробки комплексних заходів для забезпечення стабільності інформаційного простору та захисту національних інтересів у кіберпросторі.

В ході магістерського дослідження (розділ 1) було здійснено о теоретико-понятійний аналіз явища інформаційного суверенітету, а також досліджено різні підходи та аспекти явища інформаційного суверенітету. Було констатовано, що дефеніція «інформаційний суверенітет» залишається дискусійним питанням як для держави, так і для багатьох науковці. Проте ми підтримуємо саме думку науковців Олексія Онищенко, Валерія Горовий та ін., де у своїй монографії визначають інформаційний суверенітет як здатність держави зберігати та захищати свої інформаційні ресурси від зовнішніх впливів і контролю, забезпечувати незалежність та самостійність у

використанні інформаційної інфраструктури. Також, було проаналізовано основні види інформаційного суверенітету та підходи до них.

Нами було проаналізовано і описано, що міжнародний досвід США, Японії та Китаю у забезпеченні інформаційного суверенітету є цінним для України, оскільки ці країни демонструють різні підходи до захисту національних інтересів в інформаційному просторі. США акцентують увагу на розвитку сучасних технологій, кібервійськ і регулюванні діяльності технологічних компаній, щоб зменшити вплив зовнішніх загроз. Японія спрямовує зусилля на співпрацю між державними органами та приватним сектором, впроваджуючи жорсткі заходи проти кіберзлочинів. Китай, зі свого боку, активно створює власну цифрову екосистему, захищаючи внутрішній інформаційний простір через суворі державні механізми контролю.

Наступним було доведено важливість, що нормативно-правове забезпечення інформаційного суверенітету в Україні є важливою складовою національної безпеки та стратегічного розвитку країни. Це забезпечення включає низку законів, указів, постанов і міжнародних угод, які спрямовані на захист інформаційного простору від зовнішніх і внутрішніх загроз, забезпечення стабільного функціонування засобів масової інформації та ефективного використання інформаційних технологій.

В розділі 2 магістерської роботи було досліджено поняття «інформаційні загрози» та описано джерела їх виявлення. Було запропоновано шляхи забезпечення розвитку врегулювання інформаційних загроз:

1. Законодавче регулювання, тобто, потрібно посилити нормативну базу, яка спрямована на контроль інформаційної діяльності в кризових умовах;

2. Підвищення інформаційної грамотності, а саме організації освітніх програм, відповідно до яких громадяни набудуть навички критичної оцінки інформації та розпізнання дезінформації;

3. Технологічні рішення, за допомогою розробки систем моніторингу і протидії кіберзагрозам, а також використання штучного інтелекту буде виявлено фейки.

Було розглянуто в історичному контексті виникнення такого поняття як «гібридна війна» та проаналізовано думки науковців з приводу цього поняття. Було охарактеризовано та виявлено головні компоненти гібридної війни є: інформаційний, ідеологічний, психологічний, економічний, політичний, дипломатичний, військовий, технологічний, ресурсний, енергетичний. Зупинимось на найбільш важливих.

Завдяки проведеному аналізу загроз національним інтересам та безпеці в інформаційній сфері, було виявлено виділяються кілька важливих аспектів. В ході дослідження, було наведено реальні приклади російської пропаганди.

Було сформовано заходи для протидії впливу дезінформації та маніпуляції на громадську думку: 1. Підвищення рівня медіаграмотності населення; 2. Створення платформ для швидкого спростування фейків; 3. Партнерство з соціальними мережами для виявлення та маркування фейків; 4. Розвиток незалежних медіа та підтримка якісної журналістики; 5. Проведення інформаційних кампаній, що роз’яснюють механізми дезінформації.

В ході магістерського дослідження (розділ 3) було виявлено основне завдання стратегічного планування — створення чіткого алгоритму дій для визначення мети, уточнення завдань, розподілу ресурсів і прийняття рішень.

Було проілюстровано досвід зарубіжних країн формуванні стратегічного планування у сфері інформаційної безпеки та запропоновано варіанти удосконалення стратегічного планування у сфері безпеки та оборони таких як:

1.Чітке регламентування ієрархії стратегічного планування через законодавчі акти.

2. Удосконалення нормативно-правової бази стратегічного планування.

Було виявлено, що міжнародне та європейське співробітництво в сфері кібербезпеки має вирішальне значення для забезпечення глобальної безпеки,

оскільки кіберзагрози не визнають кордонів і можуть миттєво впливати на держави та критичну інфраструктуру по всьому світу. Таке співробітництво сприяє обміну інформацією, розробці спільних стандартів і підвищенню стійкості глобальних інтернет-мереж до кіберзагроз.

Розроблено нову модель кібербезпеки та інформаційного суверенітету країни, що в подальшому можуть бути впровадженні органами публічної влади для покращення інформаційного суверенітету України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бондар Н.О. Історична еволюція концепту суверенітету. *Право і суспільство*. 2021. С.17-21.

2. Діміч А.В., Єрьоміна Л. В. Сучасні наукові підходи до визначення «Інформаційний суверенітет України». *Інформаційна безпека людини, суспільства, держави*. 2022. № 1–3 (34–36). С.13-19.

3. О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.. НАН України, Нац. б-ка України ім. В. І. Вернадського. – К. : НБУВ, 2011. – 154 с.

4. Дубов Д.В. Проблеми нормативно-правового забезпечення інформаційного суверенітету Україні. *Вісник Національної академії керівних кадрів культури і мистецтв*. 2014. № 1. С.233-238.

5. “Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні". Аналітична записка. Національний інститут стратегічних досліджень, 2014 URL: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/problemi-normativno-pravovogo-zabezpechennya-informaciynogo.

6. Солодка О. Інформаційний суверенітет та інформаційна безпека України: діалектика понять. *Європейська політика та право*. 2020. №7. С.233-239.

7. Березневич-Ломанюк В. О. Суверенітет сучасної держави в умовах глобалізації: дис. доктора філос. / Березневич-Ломанюк, Влада Олексіївна ; Національний університет «Одеська юридична академія» – Одеса, 2024. – 229 с.

8. Дубов Д.В. «Цифровий суверенітет» у сучасному світі: виклики та можливості для України. *Вісник Національної академії керівних кадрів культури і мистецтв.* 2015. № 1. С.205-209.

9. Куцепал С.В. Інформаційний суверенітет та інформаційна безпека України: виклики та реалії війни. *Полтавський правовий часопис*. 2023. № 1. С.78-88.

10. Про Національну програму інформатизації: Закон України від 04.02.98 р. № 74/98-ВР. Відомості Верховної Ради України, № 27-28, ст.181 (втратив чинність).

11. Горулько В. Роль і місце інформаційної безпеки в загальній системі національної безпеки держави. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»,* 2022. № 34. С.103-108.

12. Голод К. Інформаційна безпека США: сучасний стан та уроки для України. *Геополітика України: історія і сучасність*. 2017. № 2. С. 91-107.

13. Ничипорчук Н. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2018. № 1. С. 66-71.

14. Олійник О. В. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки України. *Наукові записки Інституту законодавства Верховної Ради України*. 2015. № 1. С. 54-59.

15. Шемчук В.В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник Національної академії внутрішніх справ*. 2019. № 4 (113). С. 119-124.

16. Хлапонін Ю. І. Аналіз стану кібербезпеки в провідних країнах світу. *Кібербезпека: освіта, наука, техніка*. 2019. № 4. С. 6-13.

17. Моренчук А., Вознюк Є. Кіберпротистояння Японії (досвід України). *Мультидисциплінарні підходи до аналізу суспільно-політичних проблем в умовах російсько-української гібридної війни : матеріали міжнародного круглого столу (28 квітня 2022 р.)*. Львів, 2022. С.53–56.

18. Глосарій: навч. енцикл. слов.-довід. із питань інформ. безпеки / за заг. ред. д-ра політ. наук, проф. А. М. Шуляк. – Київ : МПБП «Гордон», 2019. 580 с.

19. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради України, 1992, № 48, ст.650.

20. Конституція України: Закон України від 08.06.1996 р. № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

21. Європейська конвенція про транскордонне телебачення (ETS N 132). Прийнята Радою Європи 05.05.1989 р. № 994_444.

22. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. Відомості Верховної Ради України, 2011, № 32, ст. 314.

23. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України, 1994, № 31, ст.286.

24. Про медіа: Закон України від 13.12.2022 № 2849-IX. Відомості Верховної Ради України, 2023, №№ 47-50, ст.120.

25. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. Відомості Верховної Ради, 2017, № 45, ст.403.

26. Про Раду національної безпеки і оборони України : Указ Президента України від 30.08.1996 р. № 772/96.

27. Про затвердження завдань Національної програми інформатизації на 2022-2024 роки : Постанова Верховної Ради України від 15.02.2022 р. № 2079-IX.

28. Про Стратегію інформаційної безпеки : затверджена Указом Президента України від 15.03.2021 р. № 98/2021.

29. Музика О.-З., Крикавська І. Інформаційні загрози в мережі Інтернет в умовах війни в Україні. *зб. матер. III Міжнар. наук.-практ. конф.* (м. Львів, 5 травня 2023 р.). С. 237-239.

30. Тарасюк А.В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право*. 2019. № 4(31). С. 73-82.

31. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці України. Економічний простір. 2021. № 176. С. 155-158.

32. Україна посіла 81-ше місце в світі за рівнем розвитку інформаційно-комунікаційних технологій. Уніан інформаційне агенство, 2014 URL: https://www.unian.ua/science/913007-ukrajina-posila-81-she-mistse-v-sviti-za-rivnem-rozvitku-informatsiyno-komunikatsiynih-tehnologiy.html.

33. Розвиток IT в Україні: поточна ситуація та перспективи. Блог YC.Market, 2024. URL: https://blog.youcontrol.market/rozvitok-it-v-ukrayini-potochna-situatsiia-ta-pierspiektivi/.

34. Котляров В. Аналіз сучасного стану інформаційної безпеки в Україні. Механізм Регулювання Економіки. 2024. № 2. С. 101-104.

35. Мельник, Д. С. Актуальні загрози національній безпеці України в інформаційній сфері: питання визначення та протидії. *Інформаційна безпека людини, суспільства, держави*. 2022. № 1-3. С. 31–33.

36. Шість найпоширеніших наративів російської пропаганди, які допомагають убивати українців. УКРІНФОРМ, 2024. URL: https://www.ukrinform.ua/rubric-ato/3875878-sist-najposirenisih-narativiv-rosijskoi-propagandi-aki-dopomagaut-ubivati-ukrainciv.html.

37. Фейки та дезінформація терористичної Росії: українська діаспора під прицілом. СТОЖАРИ САЙТ УКРАЇНСЬКОЇ ДІАСПОРИ, 2024. URL:

38. Огляд подій в сфері кібербезпеки, жовтень-листопад 2023. URL: https://ufss.com.ua/wp-content/uploads/2024/01/Cyber-digest_Oct-Nov_2023_UA.pdf.

39. Виздрик В.С., Мельник О.М. Інформаційна безпека в Україні: сучасний стан. Міжнародний науковий журнал «Грааль науки». 2023. № 24. С. 196-202.

40. Волинь: у грудні ОПОРА зафіксувала 9 публікацій з елементами «чорного піару» стосовно імовірних кандидатів. ОПОРА, 2018. URL: https://www.oporaua.org/vybory/46082-volyn-u-hrudni-opora-zafiksuvala-9-

publikatsii-z-elementamy-chornoho-piaru-stosovno-imovirnykh-kandydativ-15817.

41. Українські медіа і російська дезінформація: точки дотику і як протидіяти. Національна рада України з питань телебачення і радіомовлення, 2024. URL: https://webportal.nrada.gov.ua/ukrayinski-media-i-rosijska-dezinformatsiya-tochky-dotyku-i-yak-protydiyaty/.

42. «Інфодемія» дезінформації про COVID-19 шкодить здоров'ю українців — з'ясовано в дослідженні на замовлення ООН. UNICEF Україна, 2021. URL: https://www.unicef.org/ukraine/press-releases/infodemic-covid-19-disinformation-bad-ukrainians-health-study-un-finds.

43. Килимник І.І Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2023. № 76 (2). С. 53-57.

44. Магда Є. В. Гібридна війна: вижити і перемогти. — Х.: Віват, 2015. — 304 с.

45. Білявський Д.С. Визначення та проблематика терміна «Гібридна війни». *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. :* матеріали Міжнар. наук.- практ. конф. (19 травня 2023 р.). Одеса. 2023. С. 380-382.

46. Динис Г. Г. Сучасні гібридні збройні конфлікти: правові аспекти (приклад агресії Російської Федерації проти України) : збірник наукових праць «Геополітика України: історія і сучасність». Вип. 2 (17). Київ, 2016. С. 103–111.

47. Магда Є.М. Гібридна війна: сутність та структура феномену International relations, part "Political sciences". 2014. URL: https://d1wqtxts1xzle7.cloudfront.net/62782149/2489-9062-1-PB20200403-109004-1yp6mp5-libre.pdf?1585996827=&response-content-

disposition=inline%3B+filename%3D62782149.pdf&Expires=1732038699&Signature=Yk5bWLQuLhKTZs3gENsXtfDDyvhPfbH96bYGYmLg~7DsGtwxnQDhkSbkgbM0pIZ16brueLy9ll4axveXvheJfy8-T5nCYVSWuO7bmcXhieLFppMmRGT6pv2gV2-RNoet2VzIqubOwFw4UZKlJyn6RCgovadmDu2oRJh5SBb96fOr3LUGOupj1OxHScUp4czUuDFDUEki0SJIchCcl~Nc-fjUYIBGV2WNyJTc1gozOtZxXz9h6TST6WWy398Jvviv-N4E~oGY4FwH1zq1UG~FcCA3c96HTrCI9McJoSsLV8qtVbBlxXB1Q-tFr7RS0l3mk3hx7L1ApsQrptAvxAyrjw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA.

48. Сабрі К. Н. Інформаційно-іміджевий аспект гібридної. *Молодий вчени*й. 2018. № 5(1). С. 206–210.

49. Концепція «гібридної» війни та її складові. Центр безпекових досліджень “СЕНСС”, 2024. URL: https://censs.org/concept-of-hybrid-warfare-and-its-components/.

50. Захаренко К.В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дис…кандидата пол. / Захаренко Костянтин Володимирович; Національний педагогічний університет імені М.П. Драгоманова –Київ, 2021. – 423 с..

51. Запорожець С. А Інформаційна безпека України в умовах гібридної війни. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. 2019. № 17. С. 52–63.

52. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

53. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Том 2 № 77. С. 121-127.

54. Муровицький А.А. Дезінформація та методи боротьби з нею. *ІІ науково-практична конференція*. м. Ужгород, 25-26 жовтня 2024 р. С. 58-60.

55. Самчинська О. А. Дезінформація: поняття та сутність. *Адміністративне право і процес*. 2022. № 3 (38). С. 32–45.

56. Факти проти вигадок: російська дезінформація про Україну. U.S. DEPARTAMENT of STATE, 2022 URL: https://www.state.gov/%D1%84%D0%B0%D0%BA%D1%82%D0%B8-%D0%BF%D1%80%D0%BE%D1%82%D0%B8-%D0%B2%D0%B8%D0%B3%D0%B0%D0%B4%D0%BE%D0%BA-%D1%80%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0-%D0%B4%D0%B5%D0%B7%D1%96%D0%BD%D1%84/.

57. Шевчук О. В. Політична маніпуляція: поняття, концепції, механізм реалізації. *Актуальні проблеми політики*. 2021. №.68. С. 83-89.

58. Невельська-Гордєєва О. П., Нечитайло В. О. Маніпуляції як засіб інформаційно-психологічного впливу у інформаційній війні. *Вісник НЮУ імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. 2021. Том 3 № 50. С. 71-83.

59. Арабаджиєв Д. Ю. Маніпулювання свідомістю суспільства в умовах інформаційної та гібридної війни в Україні. Гілея: науковий вісник. 2019. № 146(3). С. 12-15.

60. Задорожна М. І. Державне управління в умовах гібридної війни: маніпуляція суспільною свідомістю. Публічне адміністрування: теорія та практика. 2017. №. 2 (18). С.1-17.

61. Шипілова Л.М. Стратегічне планування у сфері національної безпеки: курс лекцій / Л.М.Шипілова. К: ВПЦ "Київський університет", 2023. – 143 с.

62. Гордієнко С.Г., Доронін І.М. Стратегічне планування у сфері державної безпеки як прикладна проблема. *ІНФОРМАЦІЯ І ПРАВО*. 2023. № 1(44). С.168-176.

63. Соломіцький А., Семененко О., Толок П., Ремез А., Мельничу Ю., Миненко А. Організація прогнозування воєнно-політичної обстановки для забезпечення військової та економічної безпеки держави. *Соціальний розвиток та безпека*. 2024. № *14*(1). С. 28-36.

64. Климчук О.В. Сучасні аспекти використання інформаційних систем і технологій в управлінні. *ІІ Міжнародна науково-практична конференція «Бізнес, інновації, менеджмент: проблеми та перспективи».* 2021, Секція 2. С. 170-171.

65. Позиції України в Global Innovation Index 2024: аналіз і тенденції. Technology Center, 2024. URL: https://entc.com.ua/uk/gollovna.

66. Україна посідає 5 місце у світі за розвитком цифрових держпослуг. Суспільне новини, 2024. URL: https://suspilne.media/840493-ukraina-posila-5-misce-u-sviti-za-rozvitkom-cifrovih-derzposlug/.

67. Лекція 3 ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО ІНФОРМАЦІЙНІ РЕСУРСИ. URL: https://moodle.znu.edu.ua/pluginfile.php?file=/721431/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%203%20%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96%20%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%B8.pdf.

68. Нестеренко О. Національні інформаційні ресурси: минуле і сьогодення, або двадцять років потому. *Суспільство. Економіка. Діджиталізація*. 2024. № 1(1). С. 45–59.

69. Котляров В. Система забезпечення інформаційної безпеки України. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління*. 2024. № 2 (74). С.45-49.

70. Стратегічні комунікації в міжнародних відносинах. Монографія, К.:Вадекс,2019, с.348-368.

71. Копійка М. В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя*. 2020. № 1. С. 102-109.

72. Україна стала учасником Партнерства розширених можливостей НАТО, орієнтованої на взаємозамінюваність важливих партнерів Альянсу // Міністерство оборони України, 2020. URL: https://www.mil.gov.ua/news/2020/07/24/programarozshirenih-mozhlivostej-nato-dlya-ukraini/.

73. Комплексний пакет допомоги НАТО - це 13 галузей співпраці та 40 цільових напрямків, які дозволяють вирішувати завдання щодо обороноздатності // Міністерство оборони України. URL: https://www.kmu.gov.ua/news/249185923.

74. Політика ЄС. EU NEIGHBOURS EAST. URL: https://euneighbourseast.eu/ru/policy/.

75. Сливка М.М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. Юридичний науковий електронний журнал. 2022. № 10. С. 489-491.

76. НАТО на кіберзахисті: як Альянс допомагає Україні вберегтися від хакерських атак РФ. ЄВРОПЕЙСЬКА ПРАВДА, 2022. URL: https://www.eurointegration.com.ua/articles/2022/07/6/7142651/.