Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Навчально-науковий інститут державного управління
Кафедра державного управління і місцевого самоврядування

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

Студента *Лук'янченко Анни Василівни*

академічної групи *281м-22з-4 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

на тему: *«Напрями удосконалення системи забезпечення інформаційної безпеки України»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Матвєєва О.Ю.			
розділів:				

Рецензент				

Нормоконтролер	Вишневська О.В.			

Дніпро
2023

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи ступеня магістра на тему «Напрями удосконалення системи забезпечення інформаційної безпеки України».

66 с., 3 рис., 70 використаних джерел.

ПУБЛІЧНЕ УПРАВЛІННЯ, ДЕРЖАВНА ПОЛІТИКА, ІНФОРМАЦІЙНА СИСТЕМА, ІНФОРМАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ДЕЗІНФОРМАЦІЯ, КІБЕРБЕЗПЕКА.

Об’єкт дослідження – суспільні відносини у сфері публічного управління інформаційною безпекою України.

Предмет дослідження – процес удосконалення системи забезпечення інформаційної безпеки України.

Мета дослідження – визначення напрямів удосконалення системи забезпечення інформаційної безпеки України.

У першому розділі досліджено теоретичні засади публічного управління у сфері забезпечення інформаційної безпеки. Другий розділ присвячено аналізу вітчизняного та світового досвіду публічного управління у сфері забезпечення інформаційної безпеки. У третьому розділі обґрунтовано напрями удосконалення системи забезпечення інформаційної безпеки України.

Сфера практичного застосування результатів дослідження – центральні та місцеві органи виконавчої влади, органи місцевого самоврядування.

ABSTRACT

The explanatory note of the qualifying work for the master's degree on the topic «Directions for improving the Information Security System of Ukraine».

66 pages, 3 pictures, 70 used sources.

PUBLIC ADMINISTRATION, PUBLIC POLICY, INFORMATION SYSTEM, INFORMATION, INFORMATION SECURITY, DISINFORMATION, CYBER SECURITY.

The object of research – is public relations in the field of public information security management of Ukraine.

The subject of research – is the process of improving the information security system of Ukraine.

The purpose of research – is to determine ways for improving the information security system of Ukraine.

In the first chapter, the theoretical foundations of public administration in the field of ensuring information security are explored. The second chapter is devoted to the analysis of domestic and global experience of public administration in the field of ensuring information security. In the third chapter, directions for improving the information security system of Ukraine are substantiated.

The sphere of practical application of the research results – is central and local authorities of executive power, authorities of local self-government.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЄС	–	Європейський Союз (EU)
ЗМІ	–	Засоби масової інформації
ІПСО	–	Спеціальна інформаційно-психологічна операція
НАТО	–	Організація Північноатлантичного договору (NATO)
США	–	Сполучені Штати Америки (USA)
ШІ	–	Штучний інтелект
BST	–	Чорноморський фонд регіонального співробітництва
EDMO	–	Європейський центр спостереження за цифровими медіа (The European Digital Media Observatory)
KPI	–	Ключові показники ефективності (Key performance indicators)
MDF	–	Фонд розвитку медіа (Media Development Foundation)
USAID	–	Агентство США з міжнародного розвитку

ВСТУП

Сьогодні ми не уявляємо свого життя без інформації – вона стала невід'ємним атрибутом діяльності держав, юридичних осіб, громадських організацій та громадян. Від якості, достовірності та оперативності інформації залежить велика кількість рішень, що приймаються на різних рівнях – від глав держав до громадян. З розвитком інформаційних технологій виникають нові виклики та загрози, тому потрібно до них адаптувати систему забезпечення інформаційної безпеки. Інформаційна безпека також пов'язана з національною безпекою. Україна знаходиться в стані війни, тому інші країни можуть використовувати кіберзасоби для реалізації своїх політичних цілей. Як, наприклад, сьогодні це робить росія: кількість щоденних інформаційно-психологічних атак на українців вимірюється десятками, а то і сотнями, тому необхідно оперативно реагувати на ці загрози, виявляти їх та знешкоджувати. Відповідно, потрібно переглянути та адаптувати наявну законодавчу базу під нові загрози та виклики. Крім того, інформаційні операції ворога сьогодні загрожують фізичному життю громадян: як-от намагання вивідати інформацію про переміщення та розміщення Сил оборони, важливих об'єктів критичної інфраструктури. Завдяки зібраній інформації з громадян ворог може наносити ракетно-дронові удари, від чого, відповідно, можуть страждати українці.

Також сьогодні російська дезінформація загрожує не лише внутрішній безпеці України, а й зовнішній, інформаційній безпеці багатьох країн світу. Тому потрібно розробляти та реалізовувати стратегічні підходи до боротьби з нею, активно співпрацювати у цій галузі та ділитися досвідом, проводити інформаційні кампанії, які будуть сприяти забезпеченню інформаційної безпеки.

Сучасні проблеми інформаційної безпеки України та напрями її удосконалення, зокрема, в умовах війни, все частіше стають предметом вивчення науковців, державних діячів та членів громадянського суспільства. Вагомий внесок у розвиток теоретичних та практичних засад проблем

управління інформаційною безпекою держави зробили такі вчені, як: Ю. О. Саричев, П. М. Сніцаренко, В. А. Ткаченко, В. М. Семененко, Я. І. Чмир, В. О. Демиденко, П. І. Гаранюк, А. П. Ряполов, Л. Р. Наливайко, О. І. Наливайко, З. М. Бржевська, Н. М. Довженко, Р. В. Киричок, Г. І. Гайдур, А. О. Аносов та інші. Але слід зазначити, що сьогодні через динамічний розвиток інформаційних технологій та наявність загроз з боку росії нові виклики виникають щодня, тому особливої уваги потребують питання розробки стратегічних підходів протидії дезінформації та захисту інформаційної безпеки в умовах воєнного стану, адаптації законодавства під вимоги часу, що обумовлює актуальність дослідження і вибір теми магістерської роботи.

Об’єкт дослідження – суспільні відносини у сфері публічного управління інформаційною безпекою України.

Предмет дослідження – процес удосконалення системи забезпечення інформаційної безпеки України.

Метою дослідження є визначення напрямів удосконалення системи забезпечення інформаційної безпеки України.

Відповідно до мети в роботі поставлено до вирішення *такі завдання*:

– визначити поняття та сутність інформації та інформаційної безпеки в цифрову еру;

– дослідити засади публічного управління у сфері забезпечення інформаційної безпеки України;

– розглянути передумови та особливості публічного управління у сфері захисту інформаційної безпеки України в умовах російської війни;

– з’ясувати підходи до боротьби з дезінформацією в ЄС та інших країнах світу як стратегічні вектори забезпечення інформаційної безпеки;

– окреслити вектори удосконалення стратегії забезпечення інформаційної безпеки України в умовах війни;

– визначити стратегічні підходи до протидії дезінформації та захисту інформаційної безпеки під час війни.

Виконання магістерської роботи базується на застосуванні фундаментальних, загальнонаукових та спеціальних методів наукових досліджень. Зокрема, у розділі 1 були застосовані такі методи: порівняння, узагальнення, класифікації інформації, логічний, системного аналізу і синтезу, що дало змогу узагальнити теоретичні засади публічного управління у сфері забезпечення інформаційної безпеки. У розділі 2 за допомогою застосування системно-функціонального, проблемно-логічного, статистичних методів і аналізу емпіричної інформації здійснено оцінювання стану вітчизняного та світового досвіду публічного управління у сфері забезпечення інформаційної безпеки, передумови та особливості публічного управління у сфері захисту інформаційної безпеки України в умовах війни. У розділі 3 використано методи узагальнення, синтезу й екстраполяції, які дали підстави обґрунтувати напрями удосконалення системи інформаційної безпеки України, а також – стратегічні підходи до протидії дезінформації.

Інформаційну базу дослідження склали закони та підзаконні нормативно-правові акти, що регулюють публічне управління у сфері захисту інформаційної безпеки, публікації провідних вітчизняних і зарубіжних вчених, монографічні дослідження фахівців щодо засад та напрямів удосконалення забезпечення інформаційної безпеки, зокрема, в умовах війни.

Практичне значення одержаних результатів полягає у тому, що теоретичні положення, висновки та рекомендації можуть бути використані органами публічного управління, експертним середовищем, міжнародними партнерами для підготовки та впровадження стратегічних підходів до протидії дезінформації та захисту інформаційної безпеки, адаптування законодавства до вимог часу.

Структура роботи визначена її метою і завданнями. Робота складається зі вступу, трьох розділів по два підрозділи, висновків, списку використаних джерел. Обсяг роботи: 66 стор., 3 рис., 70 джерел.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття та сутність інформації та інформаційної безпеки в цифрову еру

21 століття нерідко називають «століттям інформації» або «цифровим століттям», оскільки воно відзначається стрімким розвитком технологій інформації та зв'язку. Також часто використовується термін «постіндустріальне суспільство», щоб вказати на перехід від виробництва товарів до виробництва та обробки інформації як основного джерела економічного розвитку.

Сьогодні інформація є основним об’єктом інформаційного суспільства. Інформація, відображаючи реальний світ, проникає в усі сфери діяльності держави, суспільства та громадян. З появою нових інформаційних технологій, заснованих на впровадженні комп'ютерів, телекомунікацій та телекомунікаційних систем, інформація стає постійним і основоположним атрибутом діяльності держав, юридичних осіб, громадських організацій та громадян. Від якості, достовірності та оперативності інформації залежить велика кількість рішень, що приймаються на різних рівнях – від глав держав до громадян.

Сьогодні інформація має значний вплив на державу в різних аспектах. Наприклад, інформація є основою для прийняття рішень в різних органах влади. Доступ до правдивої, об'єктивної та актуальної інформації допомагає в ухваленні обґрунтованих рішень у сферах економіки, безпеки, соціальної політики тощо. Крім того, інформація грає ключову роль у взаємодії держави з громадськістю: прозорість і доступність інформації сприяють довірі до влади та створюють умови для активної громадянської участі в різних суспільно-політичних процесах. Інформацію можна використовувати для впливу на свідомість людей та формування суспільної свідомості та цінностей. Сьогодні

інформація та інформаційні технології стали зброєю, за допомогою якої можна вести інформаційні війни – як проти окремих груп людей, так і проти держави в цілому.

У цифрову еру поняття інформації набуває нових вимірів, оскільки цифрові технології змінюють способи збору, обробки, зберігання та передачі інформації. Інформацією в цьому контексті є не лише дані, а й цінність, яка впливає на рішення, знання та поведінку людей. Інформаційна безпека в цифрову еру, відповідно, стає ключовим аспектом для захисту цих даних від несанкціонованого доступу, зміни, розголошення та інших загроз. Вона охоплює широкий спектр практик та технологій, спрямованих на захист інформації від цифрових атак, забезпечуючи конфіденційність, цілісність та доступність інформації в умовах постійно зростаючих кіберзагроз [4].

Як сказано в статті 17 Конституції України, «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [24].

Щоб розуміти, як забезпечити інформаційну безпеку, насамперед, потрібно розглянути основні поняття, терміни та визначення.

Український термін «інформація» походить від латинського «informatio», що означає роз’яснення, виклад, обізнаність, тлумачення тощо. У науці це поняття з’явилося в середині XX століття та використовується в багатьох галузях. На сьогоднішній день існує дуже багато підходів до його розуміння.

Термін «інформація» вперше використав американський інженер Клод Шеннон у математичній теорії інформатики та передачі даних каналами зв'язку. Шеннон розумів «інформацію» як різноманітні повідомлення, які є корисними для одержувача. Пізніше творець основ кібернетики Норберт Вінер запропонував ще одне визначення. На його думку, під інформацією слід розуміти не будь-які дані, а лише ті, які були новими і корисними для одержувача [67]. На основі цих та інших робіт формувалися нові визначення поняття «інформації». Так в Енциклопедичному словнику з державного

управління наведено наступне визначення: «інформація – нові відомості, які прийняті, зрозумілі й оцінені її користувачем як корисні, нові знання, які отримує користувач (суб'єкт) у результаті сприйняття і переробки певних відомостей…Інформація – одне з найбільш загальних понять науки, що позначає деякі відомості, сукупність яких-небудь даних, знань тощо» [15, с. 301].

Організація Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО) під інформацією розглядає універсальну субстанцію, яка є у всіх сферах діяльності людей, є провідником знань та думок, інструментом спілкування, співробітництва тощо.

А згідно із Законом України «Про інформацію» «інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [37].

Серед основних властивостей інформації дослідники виокремлюють:

– об'єктивність (має бути неупередженою, незалежною від думок та бажань людини);

– достовірність (має відображати дійсний стан справ);

– повноту (дає чітке уявлення про те, про що повідомляється, до неї не виникають додаткові питання);

– точність (не викривлює реальність, а подає все так, як є);

– актуальність (важлива на даний момент, торкається нагальних питань, ситуацій тощо);

– корисність (несе користь одержувачу);

– зрозумілість (має доступну для розуміння подачу);

– доступність (має бути доступна у будь-який час) тощо.

В умовах війни ми б додали до цього переліку і захищеність.

Згідно із Законом України «Про інформацію» за змістом виокремлюють такі види інформації:

– про фізичну особу;

– довідково-енциклопедичного характеру;

– про стан довкілля (екологічна інформація);

– про товар (роботу, послугу);

– науково-технічна;

– податкова;

– правова;

– статистична;

– соціологічна;

– критична технологічна тощо [37].

Також у Законі виокремлено масову інформацію – це «інформація, що поширюється з метою її доведення до необмеженого кола осіб» [37]. Крім того, Закон України «Про інформацію» за порядком доступу поділяє інформацію на відкриту та інформацію з обмеженим доступом. Відповідно до Закону України «Про доступ до публічної інформації» виділяють такі види інформації з обмеженим доступом: конфіденційна, таємна та службова [34].

Інформація – це об'єкт інформаційних відносин, суб'єктами яких є фізичні особи, юридичні особи, об'єднання громадян, суб'єкти владних повноважень. Якщо говорити про основні принципи інформаційних відносин, то тут слід зазначити:

– гарантованість права на інформацію;

– відкритість, доступність інформації, свобода обміну інформацією;

– достовірність і повнота інформації;

– свобода вираження поглядів і переконань;

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

– захищеність особи від втручання в її особисте та сімейне життя [37].

У контексті війни та кіберзагроз інформація представляє собою будь-який вид даних, які можуть бути використані для досягнення стратегічних або тактичних цілей військових, політичних або геополітичних характеристик. Ця інформація може бути як фактичними даними, так і дезінформацією, яка

використовується для маніпулювання або збурювання суспільства та прийняття рішень.

Інформація у контексті війни та кіберзагроз може приймати різні форми, включаючи:

1. Фактичну інформацію: це може бути військова розвідка, геополітичні дані, звіти про події на полі бою, аналіз ситуації тощо. Ця інформація використовується для прийняття рішень на військовому та політичному рівнях.

2. Дезінформація: змішана з правдивою інформацією, дезінформація призначена для введення в оману громадськості, політичних лідерів або військового командування. Вона може приймати форму фейкових новин, підроблених звітів або маніпулятивних інтерпретацій подій.

3. Кібератаки – використання комп'ютерних систем для вторгнення в інформаційну інфраструктуру супротивника з метою викрадення конфіденційних даних, завдання шкоди інфраструктурі або розповсюдження дезінформації через Інтернет.

4. Психологічна війна, що включає в себе вплив на мислення та психологічний стан супротивника або населення через інформаційні засоби масової інформації, соціальні мережі, пропаганду та інші засоби.

Психологічну війну часто називають частиною гібридної війни через її комплексний та багатогранний характер, який включає в себе різні методи та стратегії, спрямовані на досягнення військових, політичних або соціальних цілей. Гібридна війна характеризується використанням поєднання традиційних військових методів (залучення збройних сил) та нетрадиційних методів (кібератаки, пропаганда, економічний та моральний тиск). Психологічна війна є ключовою частиною цієї нетрадиційної складової [5].

У гібридній війні, на відміну від традиційної війни, велика увага приділяється не тільки військовим цілям, а й цивільному населенню. Психологічна робота з ним спрямована на формування впливу на громадську думку, моральний дух та на створення розбіжностей і політичної полярності у суспільстві. Із цією метою застосовується широка палітра методів

маніпулювання інформацією, зокрема, дезінформаційні кампанії. Ці методи дозволяють впливати на сприйняття, установки та поведінку противника або цивільного населення. З цією ж метою гібридна війна часто ведеться у так званому «тумані невизначеності», де важко чітко розрізнити цілі, мотиви, провести розподільну лінію між військовими та цивільними діями, між фактами та дезінформацією. Яскравим прикладом тут є лінія «туманної поведінки» рф щодо тлумачення сенсу нападу на Україну. Переважна більшість даних приховується стороною-агресором, частина з них трансформується в «альтернативне пояснення» дійсності. Психологічна війна сприяє цьому, створюючи невизначеність та дезорієнтацію людей, які втомлюються від великої кількості інформації, яку вони не можуть перевірити і критично оцінити.

В інформаційному просторі війни багатьом споживачам інфопродуктів важко розрізняти правду від дезінформації, тому дії з боку супротивника можуть спрямовуватися на зміну думок, поглядів та рішень людей. У цьому контексті інформаційна безпека стає критично важливою для захисту суспільства та національних інтересів.

Загрози інформаційній безпеці значно посилюються в умовах російської війни з наступних причин, наведених на рис. 1.1.

Рис. 1.1. Основні загрози інформаційній безпеці в умовах війни [61; 62; 68]

Визначаючи зазначені причини, можна класифікувати їх наступним чином:

1. Цілеспрямовані кібератаки: військові конфлікти сьогодні часто супроводжуються кібератаками, спрямованими на урядові, військові та цивільні цілі. Це можуть бути атаки на критичну інфраструктуру, таку як енергетичні мережі, водопостачання, телекомунікації, що веде до серйозних наслідків.

2. Інформаційна війна: ворогом поширюється велика кількість дезінформації та пропаганди, спрямованої на маніпулювання громадською думкою та дестабілізацію ситуації. Це створює додаткові ризики для інформаційної безпеки, оскільки неправдива інформація може швидко поширюватися через цифрові канали.

3. Зростання шпигунства та контррозвідувальної діяльності: умови війни активізують шпигунську та контррозвідувальну діяльність, включаючи цифрове шпигунство, що загрожує безпеці конфіденційної інформації.

4. Фізичні загрози інфраструктурі: бойові дії призводять до фізичних пошкоджень інфраструктури, яка підтримує інформаційні системи, що робить дані вразливими до втрати або злому.

5. Зростання загроз внутрішньої безпеки: з активізацією ворожої активності в Інтернеті зростає ризик зради, внутрішньої дезінформації та інших внутрішніх загроз, які можуть підривати інформаційну безпеку зсередини країни.

6. Законодавчі та нормативні зміни: війна часто змушує до введення нових законодавчих актів, що можуть впливати на інформаційну безпеку, включаючи збір і обробку персональних даних, цензуру та інше.

Враховуючи ці фактори, забезпечення інформаційної безпеки в умовах війни вимагає посилення заходів захисту, активного моніторингу та адаптації до швидкозмінних умов протистояння загрозливій цифровій активності агресора.

1.2. Засади публічного управління у сфері забезпечення інформаційної безпеки України

Забезпечення інформаційної безпеки в Україні вимагає комплексного підходу в рамках публічного управління. Це означає розробку та впровадження національних стратегій, політик і законодавчих актів, які визначають рамки для захисту інформаційних ресурсів. Важливим аспектом є також взаємодія з міжнародними організаціями та партнерами для обміну досвідом, підвищення кіберзахисту та впровадження кращих світових практик. Управління інформаційною безпекою також передбачає створення та підтримку спеціалізованих інституцій, відділів та служб, які відповідають за моніторинг, аналіз та реагування на інформаційні загрози. Підвищення обізнаності серед населення та урядових структур щодо важливості інформаційної безпеки та методів її забезпечення також є критично важливим. В умовах сучасного цифрового світу, де інформація стає ключовим ресурсом, ефективне управління інформаційною безпекою є необхідністю для забезпечення стабільності та безпеки держави [8].

Забезпечення інформаційної безпеки в Україні як складова публічного управління вимагає комплексного та багатогранного підходу, оскільки ця задача охоплює не тільки технічні аспекти захисту інформації, але й стратегічне планування, правове регулювання, міжнародну співпрацю та освіту і просвітництво громадян [10].

По-перше, фундаментальним елементом є розробка та впровадження національної стратегії інформаційної безпеки, яка повинна враховувати сучасні кіберзагрози, геополітичну ситуацію та особливості інформаційного простору України. Ця стратегія вимагає чіткого визначення цілей, пріоритетів, відповідальності різних органів влади, а також механізмів реалізації та контролю.

По-друге, правове регулювання є ключовим для створення надійної основи інформаційної безпеки. Це включає в себе прийняття законів та

нормативно-правових актів, які регламентують діяльність у сфері захисту даних, реагування на кіберзлочини та визначення стандартів безпеки для урядових та комерційних інформаційних систем.

По-третє, важливою складовою є міжнародна співпраця, оскільки кіберзагрози не знають кордонів, а ефективна боротьба з ними вимагає обміну інформацією, досвідом та координації зусиль на міжнародному рівні. Україна може співпрацювати з іншими державами, міжнародними організаціями та експертними спільнотами у сфері кібербезпеки.

Нарешті, не менш важливим є питання освіти та підвищення обізнаності серед громадян та державних службовців. Програми освіти та тренінгів можуть сприяти кращому розумінню кіберзагроз, а також навчати навичкам ефективного захисту інформації.

Отже, комплексний підхід до інформаційної безпеки в Україні в рамках публічного управління включає стратегічне планування, правове регулювання, міжнародну співпрацю та освітні ініціативи, що разом формують стійку систему захисту інформації на національному рівні [10].

Стратегія інформаційної безпеки встановлює ключові проблеми та ризики для національної безпеки України у сфері інформації, окреслює головні цілі та завдання для відповіді на ці загрози, включаючи захист інформаційних прав індивідів та персональних даних [50]. Ця стратегія має на меті підсилення здатностей країни до забезпечення інформаційної безпеки, підтримки соціальної та політичної стабільності через інформаційні засоби, оборону країни, захист суверенітету і територіальної цілісності, а також підтримку демократичного устрою і прав громадян. Задля досягнення цієї мети планується впровадити ряд заходів, спрямованих на протидію інформаційним загрозам та зменшення впливу інформаційної агресії, в тому числі дій держави-агресора, що підривають державний суверенітет України. Також передбачається зміцнення інформаційної стійкості суспільства, вдосконалення взаємодії між державними структурами, місцевим самоврядуванням та громадськістю, а

також розвиток міжнародного співробітництва у цій сфері на основі партнерства і взаємопідтримки.

Концептуальні підходи до подальшого розвитку національної системи інформаційної безпеки включають у себе аналіз цифрового середовища, глобальних тенденцій у сфері кібербезпеки, при цьому враховуючи національні інтереси України; поліпшення законодавства в галузі кібербезпеки; чітке визначення ролей, потреб, обов'язків у вирішенні завдань кібербезпеки; впровадження механізмів публічно-приватного партнерства у сфері кібербезпеки; проактивний підхід, що включає профілактичні заходи; забезпечення демократичного громадянського контролю над функціонуванням національної системи кібербезпеки [51].

Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [50].

Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина.

Досягнення мети здійснюється шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.

Правовою основою Стратегії є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Стратегія інформаційної безпеки в Україні під час російської війни відіграє критичну роль, оскільки вона допомагає країні протистояти інформаційним викликам, що є ключовою частиною сучасних конфліктів. В умовах, коли росія активно використовує дезінформацію та пропаганду як засоби гібридної війни, здатність України виявляти та нейтралізувати такі спроби маніпуляції є важливою для забезпечення національної безпеки та стабільності. Також, у цей час, надзвичайно важливо мати змогу забезпечувати доступ до достовірної та перевіреної інформації для громадян та міжнародної спільноти. Це допомагає не тільки у відображенні реального стану справ, але й у підтримці морального духу населення та національної єдності. Крім того, ефективна стратегія інформаційної безпеки включає захист критичної інформаційної інфраструктури від кібератак, які можуть бути частиною ворожих дій. Отже, ця Стратегія є ключовим елементом у забезпеченні комплексної безпеки та стійкості України в умовах війни [17].

Крім національних законів, міжнародна взаємодія в контексті інформаційної безпеки має критичне значення для країни, що веде оборону. Однією з ключових переваг такої взаємодії є обмін інформацією та розвідувальними даними, що допомагає країні-жертві агресії краще розуміти загрози та планувати свою оборону. Крім того, міжнародна співпраця може включати навчання та підготовку фахівців з інформаційної безпеки, а також сприяння у розробці та впровадженні передових технологій та методик у цій сфері [57].

Ще одним важливим аспектом є політична підтримка на міжнародній арені у викритті та протидії інформаційним атакам агресора. Це може включати спільні заяви, дипломатичні ініціативи та активну роботу в міжнародних організаціях з метою засудження дезінформаційних кампаній та пропаганди.

Така міжнародна солідарність та підтримка важливі для підвищення довіри до інформації, що поширюється країною, яка захищається, і підсилюють її позиції на міжнародній інформаційній арені.

Проте основною є робота з населенням країни, яка зазнає цифрового насилля під тиском масованих дезінформаційних кампаній.

Для підготовки населення до загроз інформаційної війни та боротьби з дезінформацією, країни вживають різноманітні заходи:

1. Освітні програми: розвиток та оновлення освітніх програм, спрямованих на навчання громадян вмінню критично аналізувати інформацію. Це включає введення освітніх курсів у школах та закладах вищої освіти, а також публічних лекцій-роз’яснень та заходів неформальної освіти медіаграмотності, таких як тренінги, воркшопи та семінари. Навчання зосереджується на розпізнаванні фейкових новин, перевірці фактів та розумінні механізмів маніпулювання інформацією.

2. Інформаційні кампанії захисту та контратаки щодо дезінформації: розробка та проведення кампаній, спрямованих на підвищення обізнаності громадськості про загрози інформаційної війни. Це може включати рекламу в медіа, соціальних мережах, публічні заходи та освітні матеріали, які висвітлюють приклади дезінформації та методи її виявлення.

3. Співпраця з медіа: налагодження тісної співпраці з незалежними медіа-організаціями для забезпечення об'єктивного висвітлення подій та протидії дезінформації. Це включає підтримку вільних та незалежних ЗМІ, а також сприяння прозорості та відповідальності у журналістиці.

4. Широке використання технологій та штучного інтелекту: застосування програмного забезпечення та алгоритмів для виявлення та блокування дезінформації в Інтернеті, особливо в соціальних мережах. Це може включати розробку та використання інструментів для виявлення фейкових новин, аналізу сентиментів та виявлення ботів.

5. Міжнародне співробітництво щодо кібербезпеки громадян: участь у міжнародних ініціативах та співпраця з іншими країнами для обміну

інформацією, найкращими практиками та стратегіями боротьби з дезінформацією. Це також включає участь у міжнародних конференціях, семінарах та робочих групах, присвячених питанням інформаційної безпеки [33].

Розглянемо окремо деякі із груп зазначених заходів протидії.

Щодо першої групи освітніх компонентів підвищення обізнаності населення про загрози інформаційній безпеці, слід зазначити, що вони мають важливе значення у формуванні здатності громадян критично аналізувати інформацію. Ці програми охоплюють введення спеціалізованих освітніх курсів у школах та закладах вищої освіти, а також проведення публічних лекцій та семінарів. Основна мета такого навчання полягає у наданні навичок розпізнавання фейкових новин, вмінні перевіряти факти, а також у розумінні методів і механізмів маніпулювання інформацією. Це відіграє ключову роль у боротьбі з дезінформацією та підвищенні інформаційної грамотності населення.

Насамперед до заходів цієї групи слід віднести навчання критичного мислення, адже основа боротьби з фейками кремлівської пропаганди – це розвиток критичного мислення українців. З розгортанням війни та російських атак українці вчаться ставити під сумнів інформацію, аналізувати джерела та визначати їхню достовірність.

Програми медіаграмотності допомагають нам розуміти, як працює медіа, як створюється та розповсюджується контент, тим самим збільшуючи нашу здатність критично оцінювати інформацію. Розбори ситуацій в публічному просторі, як соціальні медіа, вчать розуміти, як емоції та психологічні механізми впливають на сприйняття інформації та як цим можуть маніпулювати. Для цього часто використовуються реальні приклади фейкових новин російських ЗМІ (як, зокрема, РІА новини), щоб продемонструвати, як вони створюються та поширюються. Це допомагає краще розуміти специфіку фейкових новин.

Не менш важливим є пізнання методів фактчекінгу: освітні кампанії включають тренінги та воркшопи з перевірки фактів, навчаючи, як користуватися фактчекінговими інструментами та базами даних.

Цифрова грамотність населення та інформаційна безпека держави мають глибокий і важливий зв'язок. Цифрова грамотність населення визначається здатністю людей ефективно користуватися цифровими технологіями та розуміти їхні можливості та обмеження. Інформаційна безпека держави стосується заходів, спрямованих на захист інформаційних систем, даних та інформаційних ресурсів від загроз, включаючи кіберзлочинців та дезінформацію [33]. Вони пов'язані наступним чином:

– вплив дезінформації на інформаційну безпеку є значним. Тому низька цифрова грамотність населення може сприяти поширенню дезінформації та фейкових новин. Люди з недостатньою цифровою грамотністю можуть вірити неправдивим повідомленням та легко стати жертвами кіберманіпуляцій. Це загрожує інформаційній безпеці держави. Насамперед підвищується ризик суспільного вибору кандидатів на політичні посади з прихованою антиукраїнською позицією, або кандидатів, які свідомо або несвідомо працюють на інтереси ворожої сторони;

– децентралізований захист персональних даних: цифрова грамотність населення включає усвідомлення важливості засобів захисту особистих даних в Інтернеті. Якщо люди не розуміють, як захищати свої дані, це може призвести до порушень інформаційної безпеки і витоку важливої інформації, яка може принести користь агресору;

– запобігання кіберзлочинам: люди з вищою цифровою грамотністю можуть бути більш обережними у використанні Інтернету та електронних послуг, що допомагає запобігти кіберзлочинам, таким як шахрайство та фішинг даних;

– реагування на кіберзагрози: інформовані та грамотні громадяни можуть допомогти виявляти та повідомляти про кіберзагрози та інциденти, що сприяє підвищенню інформаційної безпеки національного рівня;

– попередження розповсюдження дезінформації: інформовані громадяни можуть бути більш обізнаними у розпізнаванні та виявленні дезінформації та фейкових новин, що допомагає запобігти їхньому поширенню та впливу на суспільство.

Отже, цифрова грамотність населення визначає ступінь інформаційної безпеки держави, їх взаємодія є важливою для забезпечення стійкості та захищеності інформаційних систем та суспільства загалом.

Наступний стратегічно важливий компонент публічної політики – широка співпраця з медіа. Співпраця з медіа відіграє важливу роль у забезпеченні інформаційної безпеки для уряду та суспільства в цілому за рахунок наступного:

– поширення достовірної інформації: уряд України співпрацює з інформаційними джерелами та медіаорганізаціями, щоб забезпечити ефективну комунікацію та поширення достовірної інформації. Медіа допомагає уряду швидко та ефективно інформувати громадян про важливі події, кризи та заходи безпеки;

– публічні виступи та брифінги Президента В. Зеленського, головнокомандувача В. Залужного та офіційних представників влади всіх рівнів забезпечують прозорість та необхідну присутність органів влади в українському медіаполі. Це дозволяє пояснювати громадянам актуальну ситуацію, надавати відповіді на запитання, що сприяє уникненню паніки та непоширенню недостовірної інформації, яка активно розповсюджується ворогом в цілях внесення паніки та дестабілізації ситуації в Україні;

– засоби технічної та мануальної фільтрації дезінформації: медіа може виконувати важливу роль у виявленні та розкритті дезінформації та фейкових новин, зокрема, із використанням засобів штучного інтелекту. Журналісти власними силами та проєктами проводять розслідування, перевіряють факти та публікують достовірні матеріали, що допомагає розкрити маніпуляції та брехню;

– всебічна взаємодія з громадськістю: медіа виступає як посередник між урядом та громадськістю, допомагаючи залучати громадян до процесу прийняття рішень та інформування їх про ризики та заходи безпеки. Громадяни отримують можливість висловлювати свої погляди та питання через медійний простір. Також громадяни можуть збирати дані та передавати їх СБУ, використовуючи боти та інші технічні засоби;

– запобігання паніці та хаосу: медіа допомагають уряду контролювати інформаційне середовище та запобігати паніці та хаосу в кризових ситуаціях, таких як, зокрема, пошкодження фізичної інфраструктури під час російських атак. Сприйняття розуміння ситуації засобами медіа дозволяє громадянам залишатися спокійними та дізнаватися про рекомендації уряду;

– налагодження ефективної комунікація у критичних ситуаціях: урядові комунікаційні служби співпрацюють із журналістами для забезпечення швидкого, точного та обережного (уникнення розповсюдження фотографій з місць ураження російськими снарядами) розповсюдження інформації під час російських терористичних атак;

– моніторинг загроз: медіа слугує джерелом інформації для уряду щодо появи нових загроз та трендів у сфері кібербезпеки та інформаційної безпеки.

Загалом, співпраця з медіа допомагає уряду створювати інформаційне середовище, в якому громадяни отримують доступ до достовірної та важливої інформації, а також сприяє розкриттю, фільтрації та запобіганню дезінформації та інших загроз інформаційній безпеці.

Багатостороння співпраця в межах комплексної політики дозволяє розширювати можливості забезпечення інформаційної безпеки держави та її громадян, застосовувати новітні технології до протидії наявним і новим загрозам.

РОЗДІЛ 2
ВІТЧИЗНЯНИЙ ТА СВІТОВИЙ ДОСВІД ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Передумови та особливості публічного управління у сфері захисту інформаційної безпеки України в умовах російської війни

Захист інформаційної безпеки в Україні базується на нормативно-правових засадах, які визначають стратегію та правила у сфері кібербезпеки та захисту даних. Ці закони та норми є важливими для забезпечення безпеки інформації на національному рівні та впливають на діяльність публічних та приватних суб'єктів:

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» встановлює основні принципи та вимоги для захисту інформації в інформаційних системах. Він визначає обов'язки операторів інформаційних систем та регламентує порядок реагування на інциденти безпеки. Цей закон є ключовим для забезпечення технічної безпеки та конфіденційності інформації.

2. Закон України «Про захист персональних даних» регулює обробку та захист персональних даних громадян. Він визначає права суб'єктів персональних даних та обов'язки організацій, що обробляють ці дані. Захист приватності та персональних даних стає надзвичайно важливим у цифрову епоху.

3. Закон України «Про основні засади забезпечення кібербезпеки України» визначає стратегічні завдання та принципи державної політики у сфері кібербезпеки. Він встановлює органи влади, що відповідають за забезпечення кібербезпеки країни, та регулює важливі аспекти захисту від кіберзагроз.

4. Закон України «Про національну безпеку України» включає в себе аспекти захисту інформаційної безпеки як частину загальної національної

безпеки. Забезпечення національної безпеки включає в себе і захист важливої інформації та інфраструктури від можливих загроз.

5. Закон України «Про електронні комунікації» регулює діяльність у сфері електронних комунікацій та радіочастотного спектра, встановлює вимоги до захисту інформації та приватності користувачів електронних комунікаційних послуг. Забезпечення конфіденційності спілкування є важливим аспектом цього закону.

Ці нормативно-правові акти створюють важливий правовий фреймворк для забезпечення інформаційної безпеки в Україні. Вони регулюють важливі аспекти технічного та правового захисту інформації, встановлюють відповідальність за порушення цих норм та сприяють створенню безпечного інформаційного середовища для громадян та організацій.

Умови російської війни дещо трансформують формат інформаційної роботи, адже вона все більше потребує адаптації технік інформаційного захисту та контратак. У цьому контексті насамперед необхідно розглянути сутність кіберзагроз, що виникають в умовах російської війни. Російська федерація використовує різні кібертактики, включаючи кібершпигунство, кіберсаботаж, дезінформацію та інші, для досягнення своїх стратегічних цілей [25]. Це створює серйозні загрози для інформаційної безпеки України та інших країн, що стикаються з подібними викликами.

Також умови війни створюють надзвичайно складну та вимогливу ситуацію щодо інформаційної політики України, оскільки російські служби активно використовують кіберзагрози як частину своєї гібридної війни. Для розуміння сутності цих кіберзагроз та їхнього впливу на публічне управління, необхідно детально розглянути деякі з найважливіших аспектів.

По-перше, це кібершпигунство для отримання конфіденційної інформації, включаючи державні та військові секрети. Це створює загрозу для національної безпеки та ефективного публічного управління в цій сфері, оскільки супротивник може мати доступ до конфіденційних даних. Також це кіберсаботаж або здійснення кібератак на критичну інфраструктуру, таку як

енергосистеми та транспорт. Це може призвести до серйозних перебоїв у функціонуванні життєзабезпечуючих систем країни та вимагати негайних заходів від державних органів.

По-друге, дезінформація: росія використовує інформаційні кампанії для поширення дезінформації та впливу на громадську думку в Україні та ЄС. Це може призвести до недовір'я до офіційної інформації та підриву довіри до урядових інституцій. Подібного роду кіберзагрози можуть впливати на зовнішні відносини та міжнародну політику України. Вони можуть викликати реакцію інших держав та міжнародних організацій.

Тому для забезпечення інформаційної безпеки в умовах російської війни антикризові заходи публічного управління повинні бути спрямовані на:

– розробку та впровадження стратегічних планів кібербезпеки;
– створення механізмів виявлення та реагування на кіберзагрози;
– забезпечення кіберзахисту критичних об'єктів та інфраструктури;
– підвищення освіти та свідомості громадян щодо кібербезпеки;
– міжнародну співпрацю для обміну інформацією та спільного реагування на кіберзагрози [17].

Враховуючи всі ці аспекти, публічне управління у сфері захисту інформаційної безпеки в умовах російської війни стає надзвичайно важливим завданням для держави, оскільки воно впливає на національну безпеку та стабільність країни.

Медійна контрпропаганда України в умовах російської війни є важливим інструментом для протидії російській дезінформації та забезпечення інформаційної безпеки. Ця стратегія включає в себе різноманітні види та прийоми, що спрямовані на розповсюдження правдивої інформації та виявлення дезінформації. Зміст медійної контрпропаганди України полягає в наступному:

1. Розповсюдження правдивої інформації: основний компонент контрпропаганди полягає в поширенні об'єктивної та достовірної інформації про події, які відбуваються або відбувалися в Україні. Прикладом є виявлення і

повернення історичної правди про Голодомор українців, влаштований керівництвом СРСР, що довгий час приховувалось і викривлялося. У цілому таке розповсюджння правди включає в себе новини, репортажі, інтерв'ю та інші медійні матеріали, що дозволяють громадськості отримувати правдиву картину подій, реконструювати справедливу історичну дійсність.

2. Виявлення дезінформації і закриття чи блокування джерел її походження: Україна активно працює над виявленням та викриттям дезінформації, що надходить від російських джерел. Це включає в себе аналіз новин, соціальних мереж, інтернет-платформ та інших джерел інформації з метою ідентифікації фейкових новин та маніпуляційної інформації.

3. Інформаційні кампанії: Україна проводить інформаційні кампанії з метою розповсюдження ключових повідомлень та інформації про свої дії та позицію у війні. Ці кампанії орієнтовані на внутрішню аудиторію та міжнародне співтовариство.

Суб’єктами здійснення медійної контрпропаганди в Україні є:

– інформаційні агентства та канали: Україна має ряд державних та приватних інформаційних агентств і каналів, які відповідають за створення та розповсюдження новин та інформації;

– фактчекінгові організації: різні фактчекінгові організації в Україні працюють над перевіркою інформації та виявленням фейкових новин;

– професійні команди громадських організацій та незалежні експерти, які займаються аналізом та реагуванням на кіберзагрози та дезінформацію;

– кооперація з міжнародними організаціями: Україна співпрацює з міжнародними організаціями та партнерами у сфері медійної контрпропаганди та обміну інформацією щодо російської дезінформації, наприклад, Bellingcat [58].

Медійна контрпропаганда України є важливим інструментом для забезпечення інформаційної безпеки країни та протидії російській дезінформації в умовах російської війни. Вона допомагає розповсюджувати

правдиву інформацію та зменшувати вплив фейкових новин та маніпулятивних інформаційних кампаній.

Технології, зокрема штучний інтелект (ШІ), відіграють значну роль у підвищенні інформаційної безпеки та боротьбі з дезінформацією. Вони допомагають у наступних аспектах:

1. Аналіз тексту та детектори фейків: ШІ може використовуватися для аналізу тексту та виявлення фейкових новин. Програми, які використовують машинне навчання та нейронні мережі, можуть автоматично аналізувати структуру та зміст тексту, виявляти маніпулятивні заголовки, недостовірні джерела та несправжні факти.

2. Моніторинг соціальних мереж та Інтернету: ШІ-програми можуть автоматично відстежувати соціальні мережі та Інтернет для виявлення поширення фейкових новин та дезінформації. Вони можуть використовувати аналіз великих даних для виявлення трендів та попередження масового поширення дезінформації.

3. Робота з великими даними та аналіз публічних відгуків: ШІ може аналізувати великі обсяги даних та публічних відгуків для виявлення негативного впливу дезінформації та ідентифікації потенційних джерел.

4. Створення фільтрів та автоматизоване виявлення маніпуляцій: ШІ може розробляти фільтри та алгоритми для виявлення маніпуляцій та фейкових новин на веб-сайтах та платформах соціальних мереж. Вони можуть автоматично блокувати або позначати сумнівний контент.

5. Застосування голосових асистентів та перевірка фактів: голосові асистенти, як Siri та Google Assistant, можуть надавати доступ до перевірених джерел інформації та перевіряти факти. Деякі ШІ-програми також розробляють ботів, які можуть відповідати на запитання громадян та перевіряти факти. Співпраця з громадським сектором і медіа дозволяє широке використання таких можливостей.

6. Кібербезпека та захист інформаційних систем: ШІ використовується для захисту інформаційних систем та моніторингу кіберзагроз. Він може

автоматично виявляти та блокувати кібератаки, виявляти вразливості та допомагати відновити пошкоджені системи.

7. Персоналізовані рекомендації: ШІ може використовувати алгоритми машинного навчання для надання персоналізованих рекомендацій щодо джерел інформації та новин, що сприяє більш обізнаним виборам громадян.

Програми, що використовуються для цих цілей, включають в себе системи штучного інтелекту для аналізу тексту (наприклад, GPT-3/4), аналітику великих даних, системи моніторингу соціальних мереж та кіберзахисту. Наприклад, багато медійних організацій використовують аналітику для виявлення та відстеження фейкових новин, а також для вдосконалення процесу редакції та контролю якості інформації.

Уряд України активно співпрацює з фактчекінговими організаціями в рамках боротьби з дезінформацією та фейковими новинами [9]. Ця співпраця є надзвичайно важливою для забезпечення інформаційної безпеки країни та підвищення інформаційної грамотності громадян. Один із основних аспектів цієї співпраці – це надання фактчекінговим організаціям доступу до різних джерел інформації. Україна надає їм можливість отримувати доступ до публічної інформації, офіційних заяв, статистичних даних та інших джерел під час війни, що дозволяє проводити об'єктивний аналіз і перевірку інформації, співставляти її із заявами російської сторони та викривати недоброчесні заяви.

Фактчек, як тренд розслідувань і перевірки інформації, став надзвичайно важливим в умовах війни та інформаційної боротьби. Цей підхід до перевірки фактів і виявлення дезінформації став актуальним через розповсюдження антиукраїнської пропаганди, яка швидко і агресивно заполонила медіа та інформаційні платформи Інтернету. У цей найгостріший період, коли Україна зіштовхнулася з інформаційною війною, професійні журналісти взяли на озброєння інструменти фактчеку для контрпропагандистської «оборони». Інформаційна безпека стала пріоритетною, і фактчек став ефективним способом розкрити брехливі повідомлення та відверті маніпуляції. Після того, як фактчек набув популярності серед журналістів, він також вплинув на політичне та

державне середовище. Політичні лідери та чиновники виявилися звиклими до використання словесних маніпуляцій і неправдивих заяв для досягнення своїх цілей. Фактчек став інструментом, який розкривав неправдивість їхніх заяв та риторики. Багато політичних діячів використовували і продовжують робити популістські заяви. Фактчек став засобом розкриття пустих слів та недостовірних заяв. Це сприяло підвищенню інформованості громадян та скептичному ставленню до неправдивої інформації.

Важливою метою фактчеку стало збільшення обізнаності громадян та зменшення впливу маніпулятивних інформаційних кампаній. Уміння розрізняти факти від дезінформації стало критичним для збереження інформаційної безпеки в умовах війни [9].

Фінансова підтримка від уряду також відіграє важливу роль у розвитку фактчекінгових організацій. Ця фінансова підтримка дозволяє фактчекерам здійснювати свою діяльність та розвивати інфраструктуру для ефективного виявлення фейкових новин.

Спільні проєкти та інформаційні кампанії є ще однією складовою співпраці. Уряд України спільно з фактчекінговими організаціями проводить кампанії, спрямовані на підвищення інформаційної грамотності громадян та виявлення дезінформації. Такі проєкти сприяють поширенню правдивої інформації серед населення та викриттю маніпуляцій. Можна навести декілька прикладів таких спільних ініціатив:

– проєкт «Стоп Фейк», створений для виявлення та викриття фейкових новин та дезінформації. Фактчекінгові організації спільно з урядом виявляють найпоширеніші фейки та надають інформацію про їхню неправдивість;

– національні та місцеві інформаційні кампанії з підвищення інформаційної грамотності, які проводилися та проводяться органами управління спільно з громадськими організаціями для навчання громадян розпізнавати фейки та використовувати надійні джерела інформації;

– спільні з журналістами репортажі та матеріали, що розкривають дезінформацію та фейки. Це допомагає надавати об'єктивну інформацію

громадянам, на конкретних прикладах вчити розрізняти неправдиву інформацію;

– аналітичні звіти та дослідження за підсумками дослідницьких проєктів, що фінансуються іноземними фондами, такими як BST, USAID тощо. Ці матеріали надають об'єктивний аналіз ситуації з дезінформацією та допомагають приймати обґрунтовані рішення, керуючись фактами та точними цифрами;

– уряд України також вживає законодавчі заходи, які регулюють діяльність медіа та інтернет-платформ з метою запобігання поширенню дезінформації. Судові рішення і накладення обмежень можуть використовуватися для закриття проросійських, загрозливих чи недоброчесних ресурсів, які просувають російську політичну ідею поглинання України, поширюють дезінформацію або сіють ворожнечу серед українців.

Як приклад, Media Development Foundation (MDF) відіграє важливу роль у підтримці українських незалежних ЗМІ під час війни [66]. Заснований у 2013 році як відповідь на репресії щодо преси під час режиму Януковича, фонд активно працює над зміцненням інформаційної безпеки та розвитком медіа в Україні. Під час війни MDF виконав ряд важливих завдань. Вони створили Екстрений фонд порятунку українських регіональних медіа для збереження екосистеми місцевих ЗМІ та допомоги їм адаптуватися до умов війни. Крім того, фонд придбав та доставив захисне спорядження для журналістів, зокрема бронежилети, шоломи, бойові джгути, аптечки та інше. MDF також активно працює над розвитком медіаорганізацій, надаючи їм інструменти та тренінги для підвищення їхньої ефективності. Вони розробили програму для незалежних регіональних ЗМІ, надаючи консультації щодо контенту, розповсюдження та управління. Крім того, фонд допомагає вирішувати проблеми з людськими ресурсами, залучаючи випускників та фрилансерів до співпраці зі ЗМІ. У реалізації своїх завдань MDF використовує різноманітні методи, включаючи опитування, тренінги та іспити для покращення знань, а також консультації та підтримку у переїзді медіаорганізацій. Загалом, MDF є важливим гравцем у

підтримці незалежних ЗМІ в Україні під час війни, сприяючи зміцненню інформаційної безпеки та розвитку медіа в країні.

Загалом, співпраця між урядом України та фактчекінговими організаціями включає в себе різноманітні заходи та інструменти, спрямовані на боротьбу з дезінформацією та забезпечення інформаційної безпеки країни.

2.2. Боротьба з дезінформацією в ЄС та інших країнах світу як стратегічний вектор забезпечення інформаційної безпеки

Як зазначалося у попередньому розділі роботи, інформаційна ера принесла з собою безпрецедентні можливості для розвитку суспільства, але водночас породила нові загрози у вигляді дезінформації, зокрема і передусім, російського походження. Дезінформація, або поширення неправдивої чи прихованої інформації з метою впливу на громадську думку, стала серйозною загрозою інформаційній безпеці сучасних держав. Ця проблема відчувається не лише в Європейському Союзі (ЄС), але й у багатьох інших країнах світу. Основним завданням сьогодні є розгляд сутності дезінформації, її впливу на суспільство та способи боротьби з цією загрозою як стратегічним вектором забезпечення інформаційної безпеки.

Дезінформація, у всій своїй різноманітності форм і методів, є систематичним зловживанням інформаційними ресурсами для досягнення певних геостратегічних цілей. Вона може бути спрямована на вплив на політичні процеси, економіку, суспільний дискурс та навіть на здоров'я громадян [40]. Останнє було яскраво проілюстровано історією так званої кремлівської «вакцинної дипломатії» під час пандемії коронавірусу, коли російські ЗМІ розповсюджували завідомо некоректну і не підкріплену фактами інформацію про російську вакцину «Супутник», про її надзвичайну дієвість порівняно з європейськими вакцинами.

У цілому, головна мета дезінформації – створити неправдиву реальність або спотворити існуючу, щоб суттєво вплинути на прийняття рішень та

переконання людей [40]. Як бачимо на прикладі російського населення, масові наслідки дезінформації можуть бути серйозними, і ціла нація може вірити в неіснуючі факти. Також вона може поглибити поділ у суспільстві, сприяти розпалюванню конфліктів, порушувати громадську довіру до державних інституцій та ЗМІ. Також дезінформація може призвести до шкідливих дій, таких як відмова від вакцинації або від виїзду з територій, що опиняються в окупації, через поширення міфів та обману.

Європейський Союз та інші країни світу стали об'єктом активних кампаній дезінформації. Ця проблема особливо загострюється під час виборів та важливих політичних подій. Росія відома своєю діяльністю у поширенні дезінформації на міжнародному рівні, яка спрямована на дестабілізацію та підрив суспільної стабільності в інших країнах.

Засоби масової інформації, соціальні мережі та Інтернет стали основними платформами для поширення дезінформації. Зловживання соціальними мережами дозволило дезінформаторам та так званим ботофермам легко долучити до цього процесу велику кількість осіб, збільшуючи обсяг та вплив дезінформації.

Російські ботоферми – це організації або групи осіб, які займаються створенням та управлінням ботами в соціальних мережах та на інших онлайн-платформах з метою поширення дезінформації, маніпуляції громадською думкою та впливу на політичні процеси в інших країнах. Російські ботоферми здебільшого асоціюються із російським впливом на іноземні країни та спробами втрутитися у внутрішні справи інших країн, зокрема в Європейському Союзі та Сполучених Штатах Америки (США). Яскравими прикладами були кампанії на підтримку «пропутінської» кандидатки у президенти Франції Марін ле Пен у ЄС та такі ж кампанії на підтримку екс-президента США Дональда Трампа, який також просував проросійську пропаганду вирішення конфлікту у Східній Європі шляхом погодження на кремлівські умови і припинення озброєння України.

Принциповою ідеєю роботи російських ботоферм є створення великої кількості штучних облікових записів (ботів) в соціальних мережах, таких як Twitter, Facebook, Instagram тощо. Ці боти активно використовуються для розповсюдження дезінформації та публікації політично спрямованого контенту, який може бути спрямований на підтримку конкретних політичних поглядів, кандидатів або партій, а також на створення конфліктів та підрив стабільності в інших країнах.

Основні методи роботи російських ботоферм включають:

– створення штучних облікових записів: ботоферми створюють тисячі фальшивих облікових записів у соціальних мережах, які здаються реальними користувачами;

– автоматизовані дії: боти автоматизовано публікують, коментують та репостять контент, що сприяє поширенню дезінформації;

– масова розсилка повідомлень: боти можуть масово розсилати спам-повідомлення, посилання на фейкові новини або маніпулятивний контент;

– підтримка окремих політичних кампаній (таких як «пропутінські» політики М. Ле Пен та Д. Трамп): російські боти активно використовуються Кремлем для підтримки вигідних йому політичних кандидатів або партій (наприклад, ліві та праві радикальні партії Німеччини) під час виборів або політичних кампаній;

– ситуативні зміни громадської думки: ці боти намагаються впливати на громадську думку, створюючи враження підтримки або протистояння певним ідеям чи партіям за рахунок масовості голосів та повідомлень щодо їх підтримки.

Розуміючи рівень загрози, в останні роки уряди багатьох країн, зокрема в ЄС та США, приділяють увагу цій проблемі і вживають заходів для виявлення та придушення російських ботоферм. Це включає в себе спеціальні служби та агентства для моніторингу інформаційної безпеки, розробку алгоритмів виявлення ботів та співпрацю з соціальними мережами для видалення фейкового контенту. Також вживаються заходи для підвищення інформаційної

грамотності громадян та навчання їх розрізняти дезінформацію від правдивої інформації.

Щодо політики та ініціатив Європейського Союзу щодо протидії дезінформації в онлайн-середовищі, Європейська Комісія вживає заходів для запобігання поширенню дезінформації та невірної інформації з метою захисту європейських цінностей та демократичних систем. Поширення як дезінформації, так і невірної інформації вже має різного роду шкідливі наслідки, такі як загроза європейським демократіям, поляризація політичних дискурсів та нараження на небезпеку громадян ЄС [40].

Саме тому масштабні кампанії дезінформації є серйозним викликом для Європи та вимагають координації зусиль від країн ЄС, європейських інституцій, онлайн-платформ, новинних медіа та громадян ЄС.

Для вирішення цього питання Європейська Комісія прийняла Програму роботи «Цифрова Європа» на 2023-2024 роки [64].

Крім того, Комісія розробила низку ініціатив для протидії дезінформації:

– комюніке «Протидія онлайн-дезінформації: європейський підхід» є збіркою інструментів для боротьби з поширенням дезінформації та забезпечення захисту європейських цінностей;

– план дій щодо дезінформації: він спрямований на зміцнення спроможностей ЄС та співпраці в боротьбі з дезінформацією;

– план дій з демократії: встановлює правила, обов'язки та межі відповідальності онлайн-платформ у боротьбі з дезінформацією;

– Кодекс практик з дезінформації 2018 року, який був першим у світі документом, коли ця галузь погодилася, на добровільних засадах, встановити стандарти саморегулювання для боротьби з дезінформацією. Це спрямовано на досягнення цілей, визначених в комюніке Комісії, яке представили у квітні 2018 року;

– моніторинг дезінформації COVID-19, проведений учасниками Кодексу практик, діяв як заходи прозорості для забезпечення відповідальності онлайн-платформ у боротьбі з дезінформацією;

– EDMO – незалежна спостережна місія, яка об'єднує фактчекерів та вчених з експертизою у галузі онлайн-дезінформації, соціальних медіа, журналістських медіа та практиків медіаграмотності;

– підсилений Кодекс практики з дезінформації, підписаний 16 червня 2022 року, що об'єднує широкий спектр учасників для виконання широкого спектру добровільних зобов'язань у боротьбі з дезінформацією.

Кодекс відіграв важливу роль протягом минулих років та поточного року. У 2022 році провідні онлайн-платформи або найбільші гравці в індустрії реклами разом з дослідницькими та громадськими організаціями розробили набір практики та план дій щодо дезінформації відповідно до Директиви Європейської Комісії.

Кодекс спрямований на досягнення цілей, визначених у Директиві Комісії. Наприклад, він визначає, як залучити більше учасників – зацікавлені сторони можуть внести свій внесок в ресурсах чи експертному досвіді, приєднуючись до Кодексу. Ще однією важливою метою є позбавлення дезінформації фінансової підтримки, наприклад, шляхом обміну інформацією про відмовлення у розміщенні реклами однією з учасниць, покращенням прозорості та відповідальності щодо розміщення реклами та відмовлення в участі акторів, які публікують спростовану інформацію.

Кодекс також передбачає забезпечення цілісності послуг та надає користувачам можливість розуміти та сигналізувати про дезінформацію, надаючи їм доступні та ефективні інструменти та процедури для сигналізації про дезінформацію. Також він передбачає розширення покриття фактчекінгу та забезпечення збільшеного доступу до даних для дослідників. Нарешті, Кодекс включає моніторингову структуру на основі ключових показників ефективності (KPI), яка вимірює результати та вплив заходів, які приймають платформи. Платформи регулярно звітують про прийняті заходи та їхні KPI Комісії.

Звіти учасників ініціативи, які були подані в Центр прозорості в лютому 2023 року [60], розкривають вражаючі дані щодо боротьби з дезінформацією (рис. 2.1).

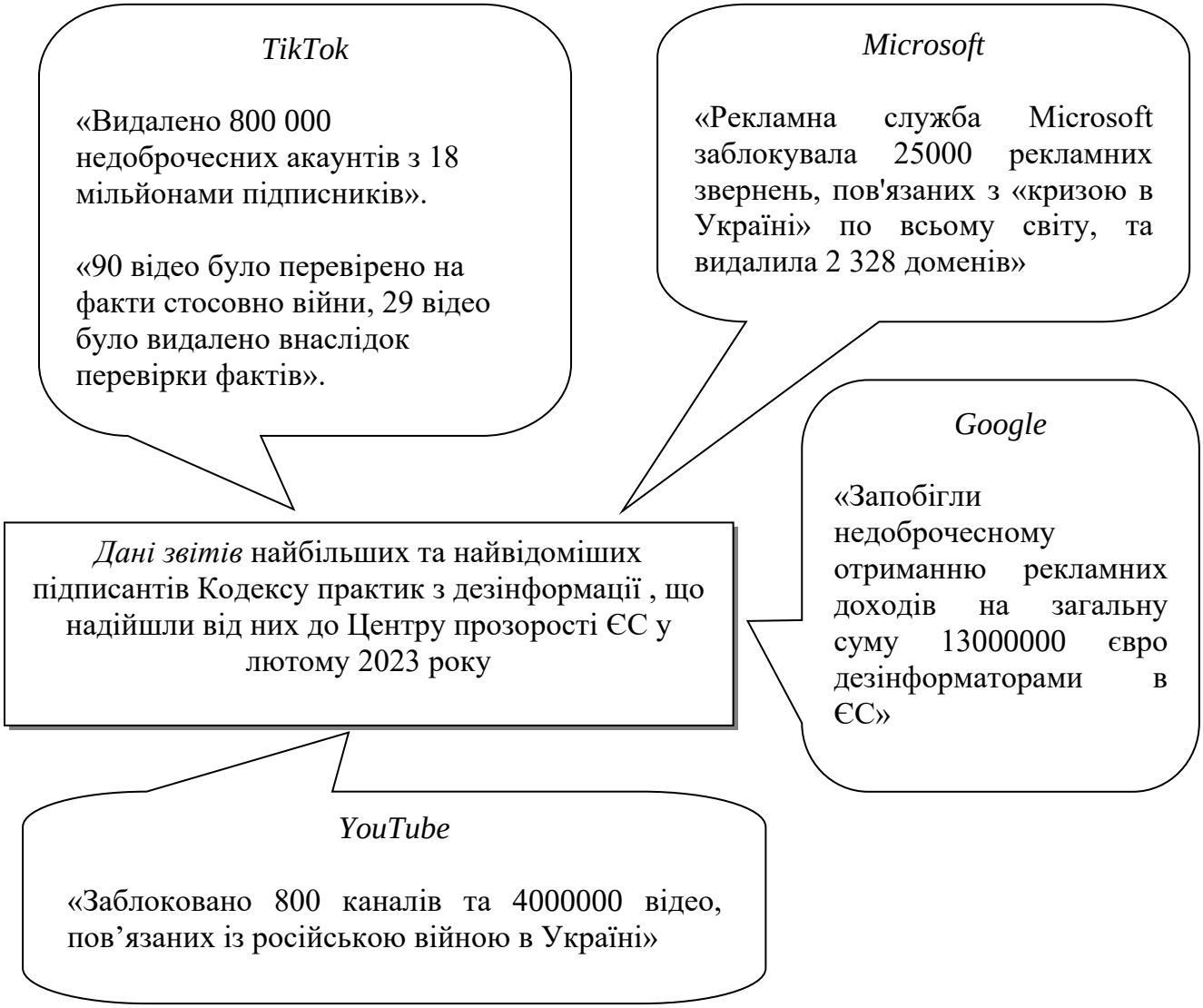

Рис. 2.1. Інформація зі звітів найбільших та найвідоміших підписантів Кодексу практик з дезінформації ЄС, лютий 2023 року [60]

Серед підписантів виділяється компанія TikTok, яка повідомила про успішне видалення 800 000 фейкових облікових записів, які мали аудиторію в 18 мільйонів фоловерів по всьому світу. Це свідчить про важливий крок у зменшенні поширення дезінформації на цій платформі. Додатково було проведено фактчекінг 90 вірусних відео, пов'язаних з російською війною в Україні, і внаслідок цього вилучено 29 відео. Цей процес фактчекінгу став важливим кроком у виявленні та припиненні поширення дезінформації на платформах відеоспільнот, що приєдналися до лідера.

Компанія Microsoft Advertising також внесла вагомий внесок, запобігаючи розміщенню 25 000 рекламних заявок, пов'язаних із українською кризою на світовому рівні, та видалила 2 328 доменів. Це сприяло обмеженню фінансової підтримки для акторів, які поширюють дезінформацію. Компанія Google взяла на себе відповідальність за запобігання витраті 13 мільйонів євро на рекламні доходи на користь акторів дезінформації в ЄС. Це показало важливість зупинки фінансування дезінформаційних джерел. Крім того, платформа YouTube заблокувала 800 каналів та 4 мільйони відео, пов'язаних із російською війною в Україні, що свідчило про важливість спрямованого та організованого припинення поширення дезінформації через відеоконтент.

Усі ці заходи і досягнення вказують на успішну боротьбу з дезінформацією та на важливість партнерства між різними сторонами у цій ініціативі для забезпечення інформаційної безпеки та збереження демократичних цінностей.

У боротьбі з російськими ботофермами важливо співпрацювати на міжнародному рівні, обмінюючись інформацією та координуючи дії для запобігання втручанню у внутрішні справи країн і поширенню дезінформації.

Боротьба з дезінформацією вимагає комплексного підходу та спільних зусиль на рівні держави, суспільства та медіа. Зростаюча інформаційна грамотність громадян допомагає їм розрізняти дійсність від дезінформації та маніпуляцій. Програми навчання інформаційної грамотності мають бути впроваджені у школах та доступні громадянам усіх вікових категорій. Соціальні мережі повинні приймати активні заходи для виявлення та видалення дезінформаційного контенту. Публікація інформації про алгоритми та правила модерації також сприяє прозорості. Державні інституції та компанії з інформаційних технологій повинні співпрацювати для виявлення та запобігання дезінформації. Це може включати обмін інформацією та ресурсами для виявлення та видалення фейкових новин. Журналісти повинні мати доступ до навчання та ресурсів для виявлення дезінформації. Професійна етика журналістики має бути високою. Якісний журналізм, який дотримується

високих стандартів фактчеку та документації, може зменшити вплив дезінформації. Підтримка незалежних ЗМІ та журналістів є важливою складовою боротьби з дезінформацією.

Оскільки наслідки поширення дезінформації можуть бути руйнівними для суспільства та демократії, боротьба з дезінформацією вимагає спільних зусиль держави, медіа та громадян. Інформаційна грамотність, прозорість соціальних мереж, співпраця між секторами та якісний журналізм є ключовими елементами стратегії боротьби з цією загрозою. Важливо надавати пріоритет цьому питанню для забезпечення інформаційної безпеки та збереження демократичних цінностей.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Вектори удосконалення стратегії забезпечення інформаційної безпеки України в умовах війни

Російська агресія проти України, що розпочалася у 2014 році з анексії Криму та подальшої війни на сході України, призвела до серйозних змін у глобальних та регіональних інформаційних ландшафтах. Ця війна не лише стала причиною геополітичних перетворень, але й активізувала інформаційні протистояння, збільшивши обсяг інформаційної експансії та агресії. Така динаміка створює серйозні загрози національній безпеці України, спонукаючи до введення спеціального правового режиму для забезпечення інформаційної безпеки.

У воєнний час особливого значення набуває питання забезпечення інформаційної безпеки. Сьогодні для України це не просто компонент національної безпеки, але й ключовий елемент захисту держави, суспільства та населення в інформаційній сфері. Визнаючи це, інформаційна безпека має бути інтегрована як невід'ємна частина державної політики у сфері національної безпеки та оборони. Україна стикається з унікальними викликами в інформаційній сфері, які включають пропаганду, дезінформацію, кібератаки та вплив зовнішніх медіа. Це вимагає комплексного підходу до інформаційної безпеки, який забезпечуватиме не лише захист від зовнішніх загроз, але й підтримку надійних та точних джерел інформації внутрішньо.

За словами експертів, український інформаційний простір залишається вразливим до негативних інформаційно-психологічних впливів та пропагандистських атак [59]. Тому розробка та впровадження ефективних стратегій протидії цим загрозам стає пріоритетним завданням для державних та недержавних інститутів [3; 30].

Серед ключових заходів у цій сфері – опрацювання та адаптація законодавства, що регулює державну інформаційну політику та може забезпечувати ефективну нейтралізацію загроз. Відносно контексту інформаційних відносин, це законодавство пропонуємо класифікувати наступним чином:

– засади державної інформаційної політики: закони та нормативні акти, що визначають основи політики, включаючи Стратегію інформаційної безпеки, Закони України «Про інформацію», «Про національну безпеку» та інші;

– забезпечення інформаційної безпеки в умовах війни: нормативні акти, які регулюють діяльність в умовах воєнного стану, включаючи рішення Ради національної безпеки і оборони, законодавчі зміни щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформації;

– регулювання статусу суб'єктів інформаційної безпеки: норми, які визначають повноваження та статус органів державної влади, правоохоронних органів, зайнятих у забезпеченні інформаційної безпеки.

Незважаючи на наявне законодавство, умови війни та існуючі загрози вимагають його постійного перегляду та адаптації, щоб забезпечити адекватний рівень нормативно-правового регулювання. Варто зазначити, що відсутність чіткого визначення інформаційної безпеки та інформаційної політики в українському законодавстві створює ряд значних викликів.

По-перше, це призводить до неконсистентності та розрізненості в підходах до розуміння та застосування цих концепцій у різних сферах державного управління. Ця неоднозначність може спричинити проблеми з інтерпретацією законодавства, особливо у випадках, коли потрібно зробити важливі рішення щодо інформаційної політики або безпеки на державному рівні.

По-друге, неясність у визначеннях ускладнює розробку ефективних механізмів для захисту інформаційного простору України. Це стосується як

боротьби з дезінформацією та зовнішніми інформаційними впливами, так і захисту державних інформаційних ресурсів та інфраструктури.

По-третє, нечіткість у законодавстві може призвести до суперечностей і конфліктів у практичному застосуванні законів, оскільки різні органи влади можуть інтерпретувати положення по-різному. Це може впливати на ефективність роботи державних інституцій та створювати правову невизначеність.

Окрім того, відсутність чітких визначень ускладнює міжнародну співпрацю у сфері інформаційної безпеки. Умови такої співпраці часто вимагають взаєморозуміння і сумісності законодавчих норм, що стає складнішим без уніфікованих та чітко визначених стандартів. Враховуючи ці аспекти, проблема відсутності чітких визначень інформаційної безпеки та інформаційної політики в українському законодавстві виявляється багатогранною та впливає на широкий спектр державних функцій і процесів.

Основною причиною «розмитості» державної інформаційної політики України, яка в свою чергу призводить до недосконалості національних механізмів забезпечення інформаційної безпеки, є неоднозначність та подекуди недостатньо адекватний понятійно-категорійний апарат цієї ключової галузі державної діяльності, закріплений у чинному законодавстві. Це відображається у таких фундаментальних документах, як Закони України «Про інформацію», «Про електронні комунікації», «Про основні засади забезпечення кібербезпеки України», Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки України, Воєнна доктрина України, Стратегічний оборонний бюлетень України.

Така неясність призводить до дезорієнтації як у теоретичній, так і у практичній діяльності, викликаючи довільне розуміння та застосування термінів, їх ситуативну модифікацію і навіть ігнорування у випадках, коли це є недоцільним. Ще однією значущою причиною нестабільності стану інформаційної безпеки в Україні є відсутність рамкового закону, який би конкретизував основні поняття та положення щодо інформаційної безпеки

держави, незважаючи на існуючу конституційну вимогу. Це серйозно гальмує процеси об'єднання та забезпечення їх адекватності як у теоретичному, так і у практичному аспектах.

Отже, з огляду на викладене, важливою є потреба уточнення та удосконалення чинної законодавчої бази, що регулює інформаційну сферу України, особливо її понятійно-категорійного апарату. Це стане основою для чіткого та однозначного розуміння та підходу до питань забезпечення інформаційної безпеки держави.

Ґрунтуючись на напрацюваннях дослідників Центру воєнно-стратегічних досліджень Національного університету оборони України ім. І. Черняховського Сніцаренка П. М., Саричева Ю. О., Семененка В. М. та Ткаченка В. А. [47], можливо запропонувати наступні зміни до чинного законодавства.

Так, до Закону України «Про інформацію» можна внести такі зміни: пункт 1 статті 1 викласти в редакції: «інформація – значення (сутність, змістовність) даних (відомостей), знання або висновки, отримані на їх основі»; у статті 1 необхідно ввести також низку нових понять у редакції: «факт – реальна (дійсна) подія, явище, випадок»; «відомості – зафіксовані у будь-якій формі подання певні факти про будь-кого, будь-що»; «дані – будь-які відомості, факти або показники, що подаються в умовній формі, зручній для інтерпретації, обробки, пересилання людиною чи технічними засобами, як основа для певних уявлень, висновків, рішень»; «інформаційна сфера – середовище та умови діяльності, пов’язані зі створенням, обробкою, використанням (поширенням) і захистом інформації (інформаційних ресурсів)»; «інформаційний ресурс – сукупність інформаційних продуктів, доступних користувачу (споживачу) для безпосереднього використання у разі потреби»; «інформаційний продукт – інформація або дані (відомості), які підготовлені у формі, зручній для користувача (споживача), і призначені для задоволення його потреб»; «інформаційна продукція – документовані інформаційні продукти». Можна додати, що інформація може бути в числовій, текстовій, звуковій, візуальній

або іншій формі. Це забезпечить більшу гнучкість у визначенні і допоможе адаптуватися до змін у способах зберігання та передачі інформації.

З урахуванням зростаючих викликів у сфері інформаційної безпеки, доцільно включити визначення, що стосуються захисту інформації, конфіденційності, цілісності даних та доступності. У контексті глобалізації та міжнародного обміну даними важливо також мати чітке визначення інформаційного суверенітету, що описує права та обов'язки держави у забезпеченні контролю над власними інформаційними ресурсами.

Доцільним є і розширення визначення «інформаційної продукції»: до нього можна додати, що інформаційна продукція може включати не лише документовані продукти, але й різноманітні форми медіаконтенту, програмне забезпечення, бази даних тощо.

У статтю 3 цього закону варто додати визначення: «державна інформаційна політика України – складова державної політики як сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових та організаційних завдань і заходів, спрямованих на забезпечення інформаційної безпеки України». Сюди можна додати, що державна інформаційна політика повинна враховувати та гармонізуватися з міжнародними стандартами та нормами, що дозволить Україні ефективно інтегруватися в глобальну інформаційну спільноту; включити аспекти, пов'язані з цифровізацією та інформаційними технологіями, визначаючи роль держави у розвитку цифрової інфраструктури, цифрової освіти та цифрової грамотності населення. Не менш важливим є акцент на захисті персональних даних громадян, включаючи правила збору, зберігання, обробки та передачі персональної інформації. З тих самих міркувань слід включити стратегії та заходи, спрямовані на протидію дезінформації та фейковим новинам, які є вагомим аспектом сучасної інформаційної безпеки України. Для підвищення ефективності діяльності в цій сфері варто включити положення про співпрацю держави з громадянським суспільством, недержавними організаціями,

академічними колами та приватним сектором для створення більш відкритої та прозорої інформаційної політики.

Щодо поводження з воєнною інформацією, у статтю 10 слід внести вид інформації «інформація воєнна», а через це внести до Закону нову статтю 20 в редакції [47]:

Стаття 20. Інформація воєнна.

1. Інформація воєнна – зміст, значення (сутність) даних воєнного характеру, незалежно від форми подання, що використовуються у практичній роботі органами військового управління, при управлінні військами та зброєю, а також органами воєнно-політичного керівництва держави при вирішенні питань оборони.

2. Джерелами інформації воєнної можуть бути органи військового управління, сили та засоби усіх видів розвідки, органи управління взаємодіючих військ (сил), перебіжчики, полонені, захоплені у противника бойові документи і зразки озброєння та військової техніки, місцеві жителі, а також спеціальна література, різні довідники, описи, топокарти тощо.

3. Правовий режим інформації воєнної визначається законодавством України, а також міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України.

Ці доповнення дозволять створити більш повне та ефективне законодавче поле для регулювання обігу воєнної інформації, забезпечуючи при цьому її захист та відповідність сучасним вимогам інформаційної безпеки.

Крім цього, пропонуються такі зміни до Закону України «Про основні засади забезпечення кібербезпеки України»:

Стаття 1, пункт 5:

Оновлене визначення поняття «кібербезпека»: частина інформаційної безпеки, яка забезпечує захист життєво важливих інтересів людини, суспільства і держави в кіберпросторі, включаючи запобігання шкоді через недостовірну, невчасну або неповну інформацію, негативний інформаційний вплив, неправомірне використання інформаційних технологій, порушення цілісності

та конфіденційності інформації, а також низький рівень медіакультури і недоліки державної політики у сфері соціальних медіа.

Стаття 1, пункт 6:

Визначення «кіберзагроза»: наміри, дії або процеси, які використовують можливості кіберпростору і можуть призвести до негативних наслідків, включаючи шкоду від недостовірної інформації, неправомірного використання інформаційних технологій, порушення цілісності та доступності інформаційних ресурсів, а також відсутності ефективної комунікативної політики і недостатнього рівня медіакультури.

Стаття 1, пункт 9:

«Комп'ютерна злочинність» – вчинення злочинів, пов'язаних з комп'ютерними системами та даними, згідно зі статтями 2-12 Конвенції про кіберзлочинність.

Стаття 1, пункт 10:

«Кібероборона» включає заходи держави у політичній, економічній, соціальній, військовій, науковій та інших сферах для захисту інформаційної інфраструктури та відбиття кіберагресії.

Стаття 1, пункт 11:

«Кіберпростір» – частина інформаційного простору, що включає електронні інформаційні ресурси та системи, функціонуючі на основі єдиних принципів та правил.

Стаття 1, пункт 19:

«Критичний об'єкт інформаційної інфраструктури» – елемент, чиє пошкодження може негативно вплинути на управління національною безпекою.

Для доповнення та розвитку пропонованих змін до Закону України «Про основні засади забезпечення кібербезпеки України» також рекомендуємо включити наступні аспекти (до статті 1):

– додати новий пункт щодо кібергігієни: ввести визначення «кібергігієна», яке описує комплекс заходів та практик, спрямованих на підтримку безпечного та відповідального використання інформаційних

технологій користувачами. Це включає навички безпечного використання Інтернету, захисту персональних даних та відповідального поводження з інформацією;

– розширити пункт щодо кіберзагроз: додати визначення кіберзагроз, що стосуються штучного інтелекту та машинного навчання, які можуть використовуватися для створення та розповсюдження дезінформації або втручання в автоматизовані системи;

– додати доповнення щодо кіберрозвідки: включити пункт про «кіберрозвідку», який визначає заходи збору, аналізу та використання інформації в кіберпросторі для захисту національних інтересів;

– уточнити визначення «комп'ютерна злочинність», включивши в нього тлумачення злочинів, пов'язаних із несанкціонованим доступом до інформаційних систем, шпигунським програмним забезпеченням, а також інші форми шкідливих дій у кіберпросторі;

– додати доповнення про кіберінциденти: визначити «кіберінцидент» як подію в кіберпросторі, яка може мати негативний вплив на інформаційну безпеку, та включити положення про процедури реагування та звітності щодо кіберінцидентів;

– розширити пункт про кібероборону: доповнити визначення «кібероборони» заходами, які стосуються розробки та застосування кіберзахисту критичної інфраструктури, включаючи енергетичні системи, транспорт, комунікації та фінансові послуги;

– додати доповнення щодо кіберосвіти: ввести пункт про «кіберосвіту», який визначає заходи з підвищення обізнаності громадян та навчання їх навичкам кібербезпеки, а також інтеграцію кібербезпеки в освітні програми.

На наше переконання, ці доповнення забезпечать більш глибоке та комплексне розуміння кібербезпеки, враховуючи швидкий розвиток технологій та зростаючі виклики у кіберпросторі.

Пропоновані зміни спрямовані на зміцнення законодавчої бази України у сфері кібербезпеки, адаптацію до сучасних викликів та ефективне реагування на існуючі та можливі кіберзагрози.

При цьому важливо відзначити, що для виконання вимог статті 17 Конституції України, інформаційне законодавство країни потребує розробки комплексу положень в межах існуючого законодавств, який би регулював інформаційні процеси як у цифровому середовищі, так і в традиційних формах (друк, усне спілкування, заходи захисту інформації тощо). Таким законом, перш за все, є закон про «Про інформаційну безпеку України». Він повинен включати оновлений комплекс базових визначень, які охоплюють наступне:

– «Інформаційна безпека України» – стан, при якому захищені життєво важливі інтереси людини, суспільства та держави від шкоди через ненадійну, невчасну або неповну інформацію, негативний інформаційний вплив, неправомірне використання інформаційних технологій, порушення конфіденційності інформації та інші подібні ризики;

– терміни, що визначають якість інформації, як «повнота», «вчасність», «вірогідність», «цілісність», «конфіденційність» та «доступність» інформації, включаючи їхнє визначення та значення;

– визначення, що описують різні аспекти інформаційних процесів, такі як «інформаційний вплив», «негативний інформаційний вплив», «цільова аудиторія», «інформаційна технологія», «створення та обробка інформації», «інформаційна інфраструктура держави» та інші;

– специфічні терміни, пов’язані з інформаційною безпекою, такі як «кіберзлочинність», «комп’ютерна система», «комп’ютерні дані», «протидія кіберзлочинності», «захист персональних даних» та інші.

Ці зміни, переважно термінологічного характеру, є логічним продовженням основного поняття «інформація» і не суперечать одне одному, створюючи системний взаємозв'язок. Вони допоможуть досягти відповідності вимогам Конституції України забезпечення інформаційної безпеки держави, а також забезпечать адекватність всіх подальших дій у цій сфері.

Як було зазначено, в умовах гібридної війни важливого значення набуває питання кібербезпеки. Кіберпростір часто використовується для підривних операцій, від крадіжки даних до кібертероризму [11, с. 18; 31]. Правове регулювання та впровадження заходів для нейтралізації кібератак та підвищення захищеності систем є сьогодні нагальним завданням [29].

Забезпечення інформаційної безпеки в Україні має бути комплексним, включаючи превентивні заходи, оперативне реагування на загрози, постійний захист інформаційного простору. Така система має ефективно протидіяти інформаційно-психологічним атакам та іншим викликам.

У практичній площині важливим напрямом також є посилення спроможності здійснювати захист інформаційних ресурсів та оборонного потенціалу. Це включає не тільки використання інформаційних технологій, але й розробку ефективних механізмів протидії загрозам у цій сфері.

Для забезпечення захисту інформації від витоку в руки агресора, особливо в умовах гібридної війни та потенційних загроз з боку росії, Україні необхідно активізувати роботу в органах управління на всіх рівнях, що працюють із інформацією, та вжити наступних заходів:

– посилення кіберзахисту: розвиток та впровадження передових кіберзахисних технологій. Це може включати в себе захист критичної інфраструктури, органів державної влади, фінансових установ та інших ключових секторів;

– навчання персоналу та розвиток культури кібербезпеки: регулярне навчання персоналу основам кібербезпеки, роз'яснення загроз та методів їх запобігання. Важливо створити серед співробітників усвідомлення необхідності захисту даних;

– використання шифрування та інших захисних технологій: важливо забезпечити шифрування важливої інформації, а також використовувати надійні методи аутентифікації та авторизації для доступу до даних;

– створення резервних копій інформації: регулярне створення резервних копій важливих даних та їх зберігання в безпечному місці, віддаленому від первинних джерел, може запобігти втраті інформації в разі кібератак;

– моніторинг та аналіз кіберпростору: використання спеціалізованого програмного забезпечення для моніторингу мережевого трафіку та виявлення ознак несанкціонованого доступу або аномальної поведінки в системі;

– взаємодія з міжнародними партнерами: обмін інформацією та досвідом з міжнародними партнерами для покращення стратегій кіберзахисту та реакції на кіберзагрози;

– регулярне оновлення програмного забезпечення: постійне оновлення програмного забезпечення, операційних систем та антивірусних програм, щоб запобігти вразливостям, через які може бути здійснений несанкціонований доступ;

– створення спеціалізованих відділів кібербезпеки: організація спеціалізованих підрозділів кібербезпеки в урядових та комерційних структурах для координації заходів з кіберзахисту;

– проведення кібербезпекових аудитів та вправ: регулярне проведення аудитів та тренувальних вправ для виявлення та виправлення вразливостей системи, а також для підготовки до можливих кібератак.

3.2. Стратегічні підходи до протидії дезінформації та захисту інформаційної безпеки під час війни

Стратегія протидії дезінформації під час війни є значущим інструментом в забезпеченні інформаційної безпеки держави. Це особливо актуально, враховуючи, що дезінформація вже багато років служить засобом психологічного впливу на українське населення, спрямованого на зниження морального духу та дестабілізацію ситуації в країні.

Кремлівська військова дезінформація представляє значну загрозу не тільки для України, але й для країн Європейського Союзу та інших держав, що

широко визнається на їх законодавчому рівні. Основні аспекти цієї загрози включають наступне:

1. Підрив довіри до правових і демократичних інституцій: дезінформаційні кампанії, які виходять за межі України, все частіше спрямовуються на зниження довіри громадян до власних урядів та міжнародних інституцій, що може призвести до політичної нестабільності та ерозії демократичних процесів [69]. Враховуючи, що ці кампанії часто виходять за межі окремих країн, вони стають глобальною проблемою, що впливає на стабільність та демократичні процеси в міжнародному масштабі. Вони спрямовані на зниження довіри громадян не лише до власних урядів, але й до міжнародних інституцій, створюючи атмосферу невпевненості та конфліктів. Одним із основних викликів у цьому контексті є ідентифікація та протидія дезінформації. Це вимагає зусиль з боку урядів, міжнародних організацій, а також громадянського суспільства. Важливо розробити ефективні механізми верифікації інформації та просвітницькі програми, спрямовані на підвищення критичного мислення та медіаграмотності серед населення. Залучення медіа та освітніх інституцій може сприяти формуванню більш критичного та обізнаного суспільства, здатного самостійно аналізувати та оцінювати інформацію. Крім того, важливо стимулювати відкритий та конструктивний діалог між різними соціальними групами, щоб уникнути поляризації суспільства.

Урядам та міжнародним організаціям необхідно активно співпрацювати для виявлення джерел дезінформації та протидії їм, а також для розробки спільних стратегій щодо захисту демократичних цінностей та інституцій. Це має включати в себе розвиток законодавчих ініціатив, що регулюють поширення інформації в Інтернеті, а також міжнародне співробітництво в області кібербезпеки. Це дозволить створити більш стійке суспільство, здатне протистояти викликам, які несе із собою російська інформаційна політика.

2. Вплив на громадську думку та локальні політичні рішення: через маніпуляції громадською думкою кремлівська дезінформація може впливати на політичні рішення у країнах ЄС, особливо у питаннях, що стосуються

зовнішньої політики, оборони та безпеки, а також військової та технічної допомоги Україні, включаючи політику санкцій щодо країни-агресора. Кремлівська дезінформація, зокрема, може мати великий вплив на політичні процеси у країнах Європейського Союзу, як це мало місце у Німеччині та Франції. Цей вплив особливо помітний у сферах, що стосуються зовнішньої політики, оборони та безпеки, а також у контексті військової та технічної підтримки України і політики санкцій проти країни-агресора. Дезінформаційні кампанії часто спрямовані на маніпуляцію громадською думкою шляхом поширення помилкової або викривленої інформації про українську політику та соціум, що може призвести до неправильного сприйняття подій або викликати сумніви щодо існуючих політичних позицій щодо підтримки України. Це може призвести до того, що громадяни в країнах ЄС можуть почати підтримувати інші політичні підходи, особливо у сферах, де інтереси України та росії є протилежними, такими як постачання техніки і зброї в Україну. Також маніпуляції громадською думкою можуть вплинути на загальну підтримку політики санкцій проти росії у ЄС, особливо якщо дезінформація спрямована на підкреслення економічних труднощів, які можуть виникнути в результаті такої політики. Так само вплив може бути спрямований на обмеження військової та технічної допомоги Україні, підігріваючи страхи щодо можливого загострення конфлікту та ескалації війни. Для протидії цьому впливу важливо розвивати критичне мислення серед громадян та забезпечувати доступ до перевіреної та незалежної інформації. Урядам країн ЄС потрібно також співпрацювати для розробки ефективних стратегій боротьби з дезінформацією та визначати її джерела, щоб мінімізувати її вплив на громадську думку та політичні рішення. Ключовим аспектом такої стратегії є також зміцнення міжнародної солідарності та підтримки України у її протистоянні з агресором, а також забезпечення дотримання міжнародних норм і принципів.

3. Сприяння розпалюванню конфліктів: поширення дезінформації може спонукати до міжетнічних, міжнаціональних та релігійних конфліктів, підігріваючи існуючі напруження в суспільстві. Так, підтримка терористичної

організації ХАМАС Кремлем та запуск глобальної інформаційної кампанії на підтримку Палестини мала на меті розхитування міжнаціональної єдності на основі порушення релігійних питань і відвернення уваги міжнародної спільноти від України. З метою протидії такому інформаційному впливу, уряди та міжнародні організації мають співпрацювати з платформами соціальних медіа для розробки алгоритмів, які виявляють і пригнічують розповсюдження дезінформації. Це може включати в себе розробку інструментів штучного інтелекту, здатних виявляти фальсифіковані зображення та відео.

Уряди країн ЄС та міжнародні організації вже активно співпрацюють із технічними командами TikTok, Facebook, Twitter та інших соціальних медіа для створення алгоритмів, які ефективно ідентифікують потенційно фальсифіковані новини або дезінформацію. Ці алгоритми можуть використовувати штучний інтелект для аналізу текстових патернів, зображень та відеоматеріалів, що часто використовуються у дезінформаційних кампаніях.

Після розробки ці алгоритми тестуються для забезпечення їхньої ефективності та точності. На нашу думку, потрібно ширше залучати громадянське суспільство до такого тестування, що заодно справляло би освітній вплив на учасників тестування. Залучення користувачів у процес верифікації передбачає створення механізмів, які дозволяють користувачам позначати підозрілий контент та сприяти його перевірці. Це може допомогти збирати дані для вдосконалення алгоритмів і залучити громадськість до боротьби з дезінформацією. Робочі групи для розробки таких алгоритмів повинні включати не тільки програмістів та спеціалістів у галузі штучного інтелекту, але й експертів з комунікацій, журналістики, політології та психології. Це дозволить враховувати різні аспекти дезінформації та її вплив на громадську думку.

Покращення алгоритмічних можливостей є надзвичайно важливим компонентом. Використання передових технологій машинного навчання та обробки природної мови для забезпечення більш точного виявлення дезінформації. Це може включати глибоке навчання для аналізу контексту,

стилістики та семантики контенту. Тестування та налаштування в реальному часі має передбачати регулярне тестування алгоритмів на різних вибірках даних для виявлення можливих вразливостей та помилок. Оперативне налаштування алгоритмів на основі зібраних даних сприятиме забезпеченню постійного підвищення їх точності.

Водночас, уряди та організації працюють над розробкою правил та рекомендацій для використання цих інструментів, гарантуючи, що вони не порушують права на свободу слова та не цензурують легітимний контент, і цю роботу треба продовжувати.

І нарешті, важливим є залучення впливових осіб і спільнот: співпраця з популярними блогерами, відомими особистостями та спільнотами в соціальних мережах для поширення точної інформації та освітніх матеріалів може змінювати суспільну думку в громадах, уражених впливом ворожих інформаційних кампаній. Це може допомогти досягти більшої аудиторії та зменшити вплив неправдивої інформації. Залучення ширшого кола учасників забезпечує міжкультурні обміни практиками та діалоги між громадами, щоб руйнувати стереотипи і упередження, які часто використовуються у дезінформаційних кампаніях. Ці підходи можуть допомогти не тільки в боротьбі з дезінформацією, але й у зміцненні соціальної згуртованості та розумінні, як важливо відстоювати правду та підтримувати міжнародну стабільність і мир.

4. Вплив на економічну стабільність: успішні дезінформаційні та місінформаційні кампанії викликають невпевненість на ринках, впливаючи на інвестиційний клімат та економічну стабільність в країні, на яку вони направлені. Уряд та компанії повинні активно публікувати точну та своєчасну інформацію про свої фінансові показники та економічні перспективи. Це може включати регулярні прес-релізи, звіти про доходи та стратегічні плани. Підтримка незалежних фактчекерів, аналітиків та їхніх ініціатив і проєктів має тут значний потенціал. Підтримка та фінансування індивідуальних ініціатив з перевірки фактів, що дозволяють швидко ідентифікувати та спростовувати

неправдиву інформацію, може включати фінансування або партнерства з організаціями, які займаються перевіркою фактів, підготовкою та розповсюдженням власної аналітики. Постійний моніторинг інформаційного простору для виявлення та аналізу трендів дезінформації також дозволяє швидко реагувати на нові виклики.

5. Порушення інформаційної безпеки та втручання у внутрішні справи: систематичне розповсюдження дезінформації є спробою кібератаки, яка спрямована на порушення інформаційної безпеки країни. Через дезінформацію можливе втручання у внутрішньополітичні процеси країн ЄС, що підриває суверенітет та стабільність цих держав. Такий вплив може продовжувати чинитися кібервійськами рф для впливу на країни та їхні системи. Це може включати в себе хакерські атаки на важливі інфраструктури, крадіжку конфіденційної інформації та інші дії, які можуть завдати значної шкоди національній безпеці. З метою втручання у внутрішньополітичні процеси дезінформація може бути використана для маніпулювання суспільною думкою та впливу на політичні процеси. Це може включати в себе фальшиву інформацію про вибори, політичних лідерів або суспільні події. Внаслідок цього, країни можуть стикатися зі значними соціальними та політичними проблемами, що загрожує стабільності.

Загалом вжиття заходів щодо протидії дезінформації є фундаментальним кроком у забезпеченні інформаційної безпеки України, відіграючи ключову роль у захисті суспільства від маніпулятивних інформаційних втручань та зміцненні демократичних цінностей та свобод.

Система протидії російській дезінформації має виходити за межі України. Схематично рівні її застосування можна представити на рис. 3.1.

Рис. 3.1. Рівні реагування на загрози російської дезінформації

На національному рівні Україна активно розробляє і втілює стратегії та заходи для протистояння інформаційно-психологічним операціям (ІПСО). Ці дії спрямовані на забезпечення захисту демократичних принципів та створення безпечного середовища для громадян. У зв’язку з повномасштабним вторгненням росії, українська громадськість активно підтримує заклики

держави до боротьби з пропагандою, дезінформацією та фальшивими повідомленнями. Це об’єднання нації та її рішуча відповідь на інформаційні виклики підтверджується зростанням рівня довіри у суспільстві. Зокрема, згідно з даними Київського міжнародного інституту соціології, рейтинг довіри до Президента збільшився з 27 % у 2021 році до 84 % у 2022 році. А станом на вересень 2023 року Гаранту держави довіряли 73 % українців. Аналогічні результати демонструє опитування Центру Разумкова у вересні 2023 року, де підтримка Президента склала 72 %. Продовження тактики прямої комунікації Президента та посадових осіб публічної влади через брифінги та соціальні мережі, включаючи Twitter, відіграє ключову роль у протистоянні цим викликам, особливо з точки зору інформування міжнародної спільноти, яка також є ціллю інформаційних атак рф.

Активне розповсюдження достовірної інформації серед внутрішніх та міжнародних глядачів є ключовим елементом у боротьбі проти інформаційно-психологічного впливу ворога. Цей процес включає не лише розповсюдження правдивих фактів, але й активне спростування дезінформації та неправдивих повідомлень, які поширює ворог, що в результаті підвищує рівень довіри до уряду. Крім того, важливо не тільки спростовувати помилкові наративи росії, а й активно надавати власні інформаційні повідомлення. Так, багато громадян, наприклад, у ЄС чи навіть у самій Україні, можуть не мати змоги чи бажання перевіряти новини з різних джерел і виявляти корінь дезінформації. Тому важливо забезпечувати постійну присутність теми України в світовому інфополі, інформувати про ситуацію в Україні через постійні оновлення в соціальних мережах, а також звернення з допомогою онлайн-платформ та через особисті зустрічі, шукаючи військової та дипломатичної підтримки.

Штучний інтелект відіграє вирішальну роль у боротьбі з розповсюдженням фейкових новин та дезінформації. Наприклад, в Україні вже існують численні проєкти, які інтегрують фахівців з ШІ для фактчекінгу та використання блокчейну. Одним із таких проєктів є Texty, що використовує передові технології для аналізу тисяч Telegram-каналів, де росія активно

проводить інформаційно-психологічні операції. Detector Media також застосовує машинне навчання та штучний інтелект для аналізу великих масивів даних, що допомагає розуміти та прогнозувати майбутні інформаційні кампанії Кремля. У співпраці з LetsData, українською компанією з ШІ, Detector Media веде моніторинг дискурсу і документує хроніки дезінформації в режимі реального часу у понад 30 країнах.

З огляду на це, для забезпечення інформаційної безпеки країни надзвичайно важливо розвивати власні інструменти на основі ШІ. Це допоможе автоматизувати та прискорити процес виявлення та спростовування дезінформації. Ключові напрямки удосконалення державної політики України мають включати:

– оперативне та швидке розповсюдження інформації про застосування рф інформаційно-психологічних операцій через заяви офіційних осіб та лідерів думок;

– комплексне вдосконалення правової бази інформаційної безпеки;

– розробка власних технологій аналізу даних для виявлення інформаційно-психологічних операцій, включаючи розвиток дистанційного зондування Землі, штучного інтелекту, нейромереж та супутникової навігаційної системи;

– створення надійної та своєчасної системи комунікації між урядом та громадянами;

– розробка Національної OSINT-стратегії для ефективного збору, аналізу та розповсюдження розвідданих з відкритих джерел;

– інвестування в освітні програми для підготовки висококваліфікованих фахівців, які зможуть ефективно протидіяти інформаційно-психологічним операціям рф.

У підсумку варто відзначити роль та важливість міжнародної роботи у площині посилення інформаційної безпеки.

Приєднання України у вересні 2022 року до програми «Цифрова Європа» стало значимим кроком у підвищенні цифрової компетентності країни. Ця

програма спрямована на підтримку цифрових технологій для підприємств, громадян і урядових структур, що є ключовим у покращенні відповіді на інформаційно-психологічні операції через використання новітніх технологій, включаючи штучний інтелект та інструменти кібербезпеки.

Фінансова підтримка від міжнародної спільноти також відіграє значну роль у протидії ІПСО рф, що спрямовані не лише на Україну чи окуповані території, але й на інформаційний простір інших країн. Потенційна проблема залишається у впливі росії на різні регіони, як-от Африка, Латинська Америка та пострадянські країни, де рф використовує культурні заходи для поширення політичної пропаганди.

У контексті удосконалення міжнародного співробітництва Україна має наступні перспективи:

– розвивати міжнародну співпрацю, обмінюючись досвідом з країнами, що ефективно протистоять ІПСО;

– залучати міжнародних партнерів, зокрема ЄС та НАТО, для підтримки та розвитку стійкості України;

– активно співпрацювати з аналітичними центрами та медіа за кордоном для протидії російській пропаганді;

– створювати або інтегрувати більше українських медіа-агенцій та видань за кордоном, забезпечуючи їм ефірний час;

– збільшувати присутність іноземних каналів та медіа в Україні;

– Міністерству закордонних справ та Міністерству культури та інформаційної політики встановити зв'язок з міжнародною аудиторією;

– обмежити канали для поширення ІПСО рф за кордоном і відсторонити росію від участі в міжнародних заходах;

– розвивати культурну дипломатію, покращуючи міжнародний імідж України та протидіючи інформаційному впливу росії через культурні ініціативи.

Підсумовуючи вищезазначене, слід констатувати, що для ефективної протидії російській дезінформації Україні необхідно застосовувати

комплексний підхід, який включає як технологічні, так і стратегічні заходи. Важливим аспектом є використання цифрових технологій, особливо штучного інтелекту, для виявлення та спростування фейкових новин і дезінформації. Приєднання до програми «Цифрова Європа» сприяє підвищенню цифрових можливостей країни в цій сфері.

Крім технологічних ініціатив, ключовим є розвиток міжнародного співробітництва та партнерства, зокрема з Європейським Союзом та НАТО, обмін досвідом з країнами, які вже мають успіх у боротьбі з ІПСО, та активна робота з аналітичними центрами та медіа за кордоном. Окрім того, важливо розвивати культурну дипломатію для покращення міжнародного іміджу України та протидії російському інформаційному впливу.

Такий комплексний підхід дозволить Україні ефективніше протистояти інформаційним викликам, збільшити стійкість перед дезінформацією та зміцнити свою позицію на міжнародній арені.

ВИСНОВКИ

У результаті проведеного дослідження сформульовано наступні висновки та надано рекомендації, що мають як теоретичне, так і практичне значення.

1. Визначено поняття та сутність інформації та інформаційної безпеки в цифрову еру. Поняття інформації в цифрову еру охоплює дані, знання, ідеї, факти, зображення, звуки та інші відомості, які можуть бути перетворені в цифровий формат і передані, збережені, оброблені або поширені за допомогою електронних пристроїв. В умовах російської війни інформація стала важливим ресурсом, ефективне використання якого може забезпечувати конкурентні переваги, інновації та знання для прийняття рішень в оборонній, соціальній та господарській діяльності. Інформаційна безпека в цифрову еру – це захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, зміни, перевірки або знищення з метою забезпечення конфіденційності, цілісності та доступності інформації. Сутність інформаційної безпеки полягає у створенні надійної захисної системи, яка включає технічні та організаційні заходи, політики безпеки, процедури та практики управління ризиками, а також освіту та тренінги користувачів. Важливість інформаційної безпеки зростає в умовах поширення технологій, які створюють нові можливості для збору та аналізу даних, але також породжують нові виклики для захисту даних. У цьому динамічному середовищі інформаційна безпека стає центральним елементом стратегічного управління.

2. Досліджено засади публічного управління у сфері забезпечення інформаційної безпеки України, в результаті чого підкреслено важливість застосування комплексного підходу. Ключ до ефективної інформаційної безпеки в Україні полягає у гармонійному поєднанні стратегічного планування, законодавчого регулювання, міжнародної кооперації, технологічного розвитку та освітніх ініціатив, що разом створюють міцну основу для захисту інформаційного простору держави. Основні напрями діяльності в цій сфері включають опрацювання національної стратегії інформаційної безпеки, яка

враховує сучасні виклики і геополітичну обстановку, а також вимагає чітко визначених механізмів реалізації та контролю. Значна увага приділяється правовому регулюванню через прийняття законів і нормативних актів для захисту даних та реагування на інфозагрози. Міжнародна співпраця виступає ключовою складовою, що дозволяє обмінюватися досвідом та координувати зусилля у боротьбі з кіберзагрозами. Міжнародна підтримка також відіграє критичну роль у контексті обміну розвідувальними даними та протидії дезінформаційним кампаніям агресора. Освітні ініціативи та підвищення обізнаності громадян і державних службовців є необхідними для формування здатності критично оцінювати інформацію та розпізнавати дезінформацію. Це включає освітні заходи, інформаційні кампанії, співпрацю з медіа та застосування технологій й засобів штучного інтелекту для виявлення та блокування дезінформації. В умовах війни з росією стратегія інформаційної безпеки в Україні набуває особливої актуальності – вона спрямована на протидію інформаційній агресії, підтримку національної безпеки, забезпечення доступу до достовірної інформації та захист критичної інфраструктури.

3. Розглянуто передумови та особливості публічного управління у сфері захисту інформаційної безпеки України в умовах російської війни. Захист інформаційної безпеки в Україні ґрунтується на нормативно-правових засадах, що визначають стратегію і правила у сфері інформаційної безпеки та захисту даних. Умови російської війни актуалізують потребу в адаптації інформаційного захисту до сучасних кіберзагроз, які включають кібершпигунство, кіберсаботаж, дезінформацію та інші тактики. Основні закони України у цій сфері встановлюють рамки для захисту інформації в інформаційно-комунікаційних системах, регулюють обробку персональних даних, визначають стратегічні завдання у сфері кібербезпеки та включають аспекти інформаційної безпеки в систему забезпечення загальної національної безпеки. Важливим елементом захисту в умовах війни є медійна контрпропаганда, яка включає розповсюдження правдивої інформації, виявлення та блокування джерел дезінформації, інформаційні кампанії, а також

співпрацю з міжнародними партнерами. Фактчекінгові організації, у тісній співпраці з урядом, грають ключову роль у перевірці інформації та розкритті фейкових новин. Штучний інтелект також використовується для аналізу текстів, моніторингу соціальних мереж, виявлення маніпуляцій та захисту інформаційних систем. Фінансова підтримка уряду, спільні проєкти, інформаційні кампанії та законодавчі заходи є важливими елементами цієї співпраці, що допомагають підвищити інформаційну грамотність громадян та зменшити вплив дезінформаційних кампаній. Отже, ефективний захист інформаційної безпеки в Україні вимагає цілісного підходу, що об'єднує законодавчу базу, медійну контрпропаганду, використання сучасних технологій і активну співпрацю між різними суб'єктами, включаючи уряд, медіа, фактчекінгові організації та міжнародних партнерів.

4. З’ясовано підходи до боротьби з дезінформацією в ЄС та інших країнах світу як стратегічні вектори забезпечення інформаційної безпеки. Дезінформація, особливо з російським корінням, стала серйозною загрозою інформаційній безпеці різних держав, впливаючи на політичні процеси, економіку, суспільний дискурс і здоров'я громадян. Російські ботоферми активно використовують соціальні мережі та Інтернет для маніпуляцій громадською думкою, зокрема, в ЄС та США, та впливу на політичні процеси, що викликає необхідність координованої міжнародної відповіді. Протидія таким активностям включає ідентифікацію та блокування ботів, а також співпрацю між урядами, міжнародними організаціями та ІТ-компаніями. Європейський Союз активно працює над протидією дезінформації, розробляючи ініціативи та програми, які включають моніторинг, підвищення інформаційної грамотності громадян та регулювання онлайн-платформ. Це включає Кодекс практик з дезінформації, фактчекінг та співпрацю з онлайн-платформами. Важливим аспектом боротьби з дезінформацією є також забезпечення якісного журналізму та підтримка незалежних ЗМІ. Підвищення інформаційної грамотності допомагає громадянам критично оцінювати інформацію та розрізняти дезінформацію від достовірних фактів. Загалом,

боротьба з дезінформацією вимагає комплексного підходу, включаючи координацію міжнародних зусиль, розвиток технологічних рішень, освіту та підтримку якісної журналістики, щоб забезпечити інформаційну безпеку та захист демократичних цінностей.

5. Окреслено вектори удосконалення стратегії забезпечення інформаційної безпеки України в умовах війни. У зв'язку з російською агресією інформаційна безпека України має стати ключовим елементом національної безпеки та оборони. Зміцнення інформаційної безпеки вимагає комплексного підходу, що охоплює як законодавчі зміни, так і практичні заходи. Законодавчі ініціативи повинні включати уточнення та розвиток понятійно-категорійного апарату, оновлення визначень інформації, кібербезпеки та інших ключових термінів. Це дозволить забезпечити чіткість і консистентність у розумінні і застосуванні цих концепцій у різних сферах. На практичному рівні Україна має зосередитися на посиленні кіберзахисту, розвитку системи кібербезпеки, використанні захисних технологій, моніторингу та аналізу кіберпростору, а також на взаємодії з міжнародними партнерами. Також важливо регулярно оновлювати та модернізувати програмне забезпечення, створювати спеціалізовані відділи кібербезпеки, проводити кібербезпекові аудити та тренування для виявлення та виправлення вразливостей. У сукупності ці заходи сприятимуть забезпеченню інформаційної безпеки України, ефективній протидії інформаційно-психологічним атакам та захисту національної інформаційної інфраструктури.

6. Визначено стратегічний підхід до протидії дезінформації та захисту інформаційної безпеки під час війни. Комплексна стратегія щодо протидії дезінформації в умовах війни є критичною для забезпечення інформаційної безпеки держави. Російська дезінформація, яка націлена на підрив довіри до демократичних інституцій та сприяння політичній нестабільності, представляє загрозу не тільки для України, але й для глобальної стабільності. Основні напрямки такої протидії включають:

– розробку ефективних механізмів ідентифікації та протидії дезінформації, зокрема через законодавчі ініціативи та міжнародне співробітництво;

– використання технологій, зокрема штучного інтелекту, для аналізу даних і виявлення інформаційно-психологічних операцій;

– посилення прямої комунікації з громадянами та міжнародною спільнотою, що включає активне спростування дезінформації та розповсюдження правдивої інформації;

– розвиток міжнародного співробітництва, обміну досвідом з іншими країнами та активна робота з міжнародними організаціями і аналітичними центрами;

– підтримку ініціатив з фактчекінгу та забезпечення доступу до перевіреної інформації.

Реалізація ініціатив і заходів в цих напрямках не лише допоможе боротися з дезінформацією, але й сприятиме зміцненню демократичних цінностей, захисту інформаційної безпеки та підвищенню рівня довіри до уряду та державних інституцій. Україна зможе продовжувати демонструвати рішучість і єдність у протистоянні інформаційним викликам, що є ключовим для її стійкості в умовах війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. *Державне управління: удосконалення та розвиток.* 2019. № 11. URL: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf (дата звернення: 15.11.2023).

2. Баран М. В. Захист інформації у контексті забезпечення інформаційної безпеки. *Аналітично-порівняльне правознавство*. 2022. № 3. С. 150-155.

3. Бржевська З. М., Довженко Н. М., Киричок Р. В., Гайдур Г. І., Аносов А.О. Інформаційні війни: проблеми, загроза та протидія. *Кібербезпека: освіта, наука, техніка.* № 3 (3). 2019. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/65/79 (дата звернення: 17.11.2023).

4. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

5. Власюк В.В., Карман Я.В. Деякі основи поняття «гібридна війна» в міжнародному праві. *Право і громадянське суспільство*. – 2015. – №1. – С. 226 – 234.

6. Воєнна доктрина України, затверджена Указом Президента України від 24.09.2015 р. № 555/2015. URL: https://www.president.gov.ua/documents/5552015-19443 (дата звернення: 01.11.2023).

7. Гапеєва О. Л. Деякі питання забезпечення інформаційної безпеки в Україні. *Військово-історичний вісник*. 2017. № 3. С. 31 – 39.

8. Гбур З. В. Основи інформаційної безпеки держави в умовах війни. Київ, С. 868 – 872.

9. Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи: практичний посібник. Дніпро: *ЛІРА*, 2017. 133 с.

10. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: *Дніпроп. держ. університет внутріш. справ*, 2020. 144 с.

11. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 4. С. 16–26.

12. Динаміка довіри соціальним інституціям у 2021 – 2022 роках. Київський міжнародний інститут соціології. 2023. URL: https://kiis.com.ua/?lang=ukr&cat=reports&id=1174&page=1 (дата звернення: 19.11.2023).

13. Доктрина інформаційної безпеки України, введена в дію Указом Президента України від 25.02.2017 р. № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 01.11.2023).

14. Дослідження громадської думки для консультативної місії Європейського Союзу в Україні. Київський міжнародний інститут соціології. Вересень 2023. URL: https://kiis.com.ua/materials/pr/20231026_r/AReport_Public Survey_EUAM_sept2023_ukr_public.pdf (дата звернення: 19.11.2023).

15. Енциклопедичний словник з державного управління / уклад. : Ю. П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін. ; за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. К. : НАДУ, 2010. 820 с.

16. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.

17. Залєвська І., Удренас Г. Інформаційна безпека України в умовах російської військової агресії. *Північноукраїнський правничий часопис*. 2022. № 1. С. 20 – 26.

18. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є. Забезпечення інформаційної безпеки держави Є.В. Іванченко [та ін.] ; за ред. проф. В.О. Хорошка ; *Вид-во Нац. авіац. ун-ту*, 2016. 254 с.

19. Інформаційна безпека держави: підручник / [В.М. Петрик. М.М. Присяжнюк., Д.С. Мельник та ін.]; в 2 т. Т. 1. / за заг. ред. В.В. Остроухова. К.: *ДНУ «Книжкова палата України»*. 2016. 264 с.

20. Інформаційна безпека: навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник і інші; за заг. ред. Ю. Я. Бобала та І. В. Горбатого. Львів: *Видавництво Львівської політехніки*, 2019. 580 с.

21. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: *Видавництво Ліра-К*, 2021. 412 с.

22. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / зазаг. ред. А. Баровської. Київ : НІСД, 2016. 109 с.

23. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека. Навчальний посібник. Ч. 2. Хар-ків: *Вид. ХНЕУ*, 2018. 196 с.

24. Конституція України: від 28.06.1996 р. № 254к/96-ВР: Дата оновлення: 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 27.10.2023).

25. Лахтадир С. Л. Кібербезпека як елемент інформаційної безпеки держави. *Юридичний науковий електронний журнал.* 2021. № 4. С. 236 – 239. URL: http://www.lsej.org.ua/4_2021/58.pdf (дата звернення: 27.10.2023).

26. Лизанчук В. В. Інформаційна безпека України: теорія і практика: підручник. *Львів: ЛНУ ім. Івана Франка*, 2017. 725 с.

27. Міністерство освіти і науки України: вебсайт. Проєкт «Стоп фейк». URL: https://mon.gov.ua/ua/tag/stop-feyk (дата звернення: 23.11.2023).

28. Мужанова Т. М. Інформаційна безпека держави : навчальний посібник. *К. : ДУТ.* 131 с.

29. Наливайко Л. П. Трансформація державної освітньої політики в Україні в умовах євроінтеграції. *Право і суспільство.* 2015. № 3. Ч. 3. С. 31-36.

30. Наливайко Л. Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. *Вісник Запорізького державного університету.* 2003. № 1. С. 60 – 65.

31. Наливайко О. І. Принципи правового захисту людини: підходи до класифікації. *Держава і право. Серія «Юридичні і політичні науки».* 2001. Вип. 13. С. 26 – 33.

32. Оцінка громадянами ситуації в країні. *Разумков центр.* Вересень 2023. URL: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-sytuatsii-v-kraini-dovira-do-sotsialnykh-instytutiv-politykiv-posadovtsiv-ta-gromadskykh-diiachiv-stavlennia-do-provedennia-zagalnonatsionalnykh-vyboriv-v-ukraini-do-zavershennia-viiny-veresen-2023 (дата звернення: 19.11.2023).

33. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129 – 138.

34. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 08.10.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 15.10.2023).

35. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. №80/94-ВР. Дата оновлення: 01.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 22.10.2023).

36. Про захист персональних даних: Закон України від 23.02.2012 р. № 2297-VI. Дата оновлення: 27.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 22.10.2023).

37. Про інформацію: Закон України від 02.10.1992 р. №2657-XII. Дата оновлення: 27.07.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.10.2023).

38. Про національну безпеку України: Закон України від 04.03.2020 р. № 2469-VIII. Дата оновлення: 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 22.10.2023).

39. Про основні засади забезпечення кібербезпеки України: Закон України від 21.06.2018 р. № 2163-VIII. Дата оновлення: 17.08.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 22.10.2023).

40. Протидія дезінформації: європейські підходи та стандарти. Київ, 2021. Офіс Ради Європи в Україні. URL: https://www.coe.int/uk/web/kyiv/-/responding-to-disinformationeuropean-practices-and-standards (дата звернення 22.11.2023).

41. Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : монографія / за ред. Бебика В.М. ; Відкр. міжнар. ун-т розвитку людини «Україна». Київ : *Університет «Україна»,* 2019. 177 с.

42. Рогова Є. І. Теоретичні основи правового забезпечення інформаційної безпеки. *Актуальні проблеми держави і права.* 2020. Вип. 86. С. 190-196.

43. Ряполов А. П. Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни. 2023. *Scientific Collection «InterConf».* URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/3169 (дата звернення: 24.11.2023).

44. Саричев Ю. О. Загальнотеоретичні передумови необхідності удосконалення чинного законодавства України з питань інформаційної безпеки держави/ Ю. О. Саричев, П. М. Сніцаренко, В. А. Ткаченко. *Збірник наукових праць ЦВСД НУОУ ім. І. Черняховського*. 2018. № 1 (62). С.62 – 67.

45. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія / О. В. Левченко. Житомир : *Видавець ПП «Євро-Волинь»,* 2021. 172 с.

46. Слінько Т. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання. *Український часопис конституційного права.* 2021. № 4. С. 77 – 84. URL: https://www.constjournal.com/pub/4-2021/suchasni-zahrozyinformatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia/ (дата звернення 22.10.2023).

47. Сніцаренко П. М., Саричев Ю. О., Семененко В. М., Ткаченко В. А. Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2018. № 2(63). С. 68 – 74.

48. Стратегічний оборонний бюлетень України, введений в дію Указом Президента України від 17.09.2021 року № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/n0063525-21#Text (дата звернення 22.10.2023).

49. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця : монографія / [В. Азарова та ін. ; за заг. ред. Л. Компанцевої]. Київ : НА СБУ, 2021. 500 с.

50. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. №685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення 18.10.2023).

51. Стратегія кібербезпеки України (2021-2025 роки): проєкт Ради національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 22.10.2023).

52. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави. Київ: *Видавництво НА СБ України*, 2014. 196 с.

53. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України / Т. Ю. Ткачук. *ДВНЗ «Ужгородський національний університет»*, Ужгород, 2019.

54. Торічний В. О. Основні функції та принципи інформаційного забезпечення держави. *Державно-управлінські студії.* 2018. № 8 (10). URL: http://studio.ipk.edu.ua/wp-content/uploads/2019/11/Torichnyy-O.V.-Inform.-zabezp..pdf (дата звернення 13.11.2023).

55. Торічний В. О. Проблема інформаційної безпеки в умовах розвитку інформаційного суспільства. *Теорія та практика державного управління*. 2019. № 2 (65). С. 256 – 262.

56. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики.* 2016. Вип. 58. С. 66 – 76. URL: http://dspace.onua.edu.ua (дата звернення 18.11.2023).

57. Фролова О. М. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету.* Серія міжнародні відносини, 2019 р., Випуск 46. С.123 – 136.

58. Bellingcat: вебсайт. URL: https://www.bellingcat.com (Last accessed: 21.11.2023).

59. Bryhinets O., Shapoval R., Bakhaieva A., Pchelin V. & Fomenko A. Problems of intellectual property in the national security system of the country. *Entrepreneurship and Sustainability*. 2021. № 8(3), 471-486. URL: https://doi.org/10.9770/jesi.2021.8.3(30) (Last accessed: 21.11.2023).

60. Code of Practice on Disinformation. European Commission. 2023. URL: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-transparency-centre-provides-insights-and-data-online (Last accessed: 27.11.2023).

61. Cybersecurity and cyber defence in the emerging democracies. (n.d.). Tandfonline.com. Retrieved November 27, 2023, from https://www.tandfonline.com.

62. Cyber Warfare Threats and Opportunities. (n.d.). ResearchGate. Retrieved November 27, 2023, from https://www.researchgate.net.

63. Detector Media: вебсайт. URL: https://detector.media (Last accessed: 24.11.2023).

64. Digital Europe Programme (DIGITAL). European Commission. 2023. URL: https://www.digitaleurope.org/resources/europe-2030-a-digital-powerhouse-digitaleuropes-manifesto-for-the-next-commission/ (Last accessed: 11.11.2023).

65. LetsData: вебсайт. URL: https://letsdata.net/ (Last accessed: 21.11.2023).

66. Media Development Foundation: вебсайт. URL: https://research.mediadevelopmentfoundation.org/ (Last accessed: 17.11.2023).

67. Norbert Wiener. Cybernetics or Control and Communication in the Animal and the Machine, Paris – *Cambridge, Mass.,* 1948. 194 p.

68. Qiu, X., Zhao, L., Li, Y., Chen, L., & Zhou, Q. (2021). A comprehensive review study of cyber-attacks and cyber security in Wide Area Measurement System (WAMS)-based Frequency Regulation Reserve (FFR) control. Sciencedirect.com. Retrieved November 27, 2023, from https://www.sciencedirect.com.

69. Svintsytskyi A. V., Semeniuk O. H., Ufimtseva O. S., Irkha Y. B., & Suslin, S. V. Countering fake information as a guarantee of state information security. *Security Journal*, 2023. 36(3), 427-442.

70. Texty: вебсайт. URL: https://texty.org.ua/ (Last accessed: 14.11.2023).