ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ
КАФЕДРА МІСЦЕВОГО САМОВРЯДУВАННЯ ТА РЕГІОНАЛЬНОГО РОЗВИТКУ

КВАЛІФІКАЦІЙНА РОБОТА
перший (бакалаврський) рівень вищої освіти
спеціальність 281 «Публічне управління та адміністрування
ОПП «Адміністративний менеджмент»
на тему: **«ДЕРЖАВНА ПОЛІТИКА ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ»**

Виконала: студентка 4 курсу 437 групи
галузь знань:
28 Публічне управління та адміністрування
спеціальності:
281 Публічне управління та адміністрування
Гула Вікторія Михайлівна

Науковий керівник: кандидат політичних наук, доцент
Бондар Ганна Леонідівна

Рецензент: кандидат наук з державного управління, доцент
Шульга Анастасія Алімівна

м. Миколаїв – 2023 р.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У 2014 році російська федерація здійснила військовий напад на Україну, а у 2022 році – повномасштабне військове вторгнення з жертвами серед мирного населення, масштабами і руйнаціями, небаченими з часів другої світової війни, яке супроводжувалось надзвичайно потужним пропагадистським впливом та кібернападами на державні об’єкти та об’єкти критичної інфраструктури, супутниковий зв’язок України. Відповідно постало нагальне питання захисту інформаційного середовища від пропаганди російської федерації, оскільки для кожної країни питання інформаційної безпеки є пріоритетним. Якщо держава не реалізує системно інформаційну політику та комплекс заходів щодо протидії агресивним інформаційним впливам, пропаганді, інформаційно-психологічним операціям (ІПСО) ворога, то національна безпека буде під загрозою, чим може скористатись країна-агресор.

Проблеми інформаційної безпеки досліджувались у працях вітчизняних та закордонних науковців. Зокрема, це такі фахівці, як: Т. Дай, Дж. Фредерік Ч. Фуллер, Ж. Озолія, І. Аустерс, Д. Ліепнієцє, Ю. Шкілтерс, С. Струєрга; вітчизняні науковці: Г. Почепцов, Г. Бондар, В. Горбулін, М. Гребенюк, М. Дмитренко, О. Додонов, М. Кияк, Б. Леонов, В. Негодченко та інші.

Метою роботи є дослідити особливості реалізації державної політики у сфері інформаційної безпеки України, інструменти протидії загрозам в інформаційній сфері та запропонувати механізми її вдосконалення.

Завдання дослідження:

- проаналізувати джерельну базу, основні поняття та категорії дослідження;
- проаналізувати законодавче та нормативно-правове забезпечення

державної політики щодо інформаційної безпеки;

- проаналізувати міжнародний досвід реалізації державної політики щодо інформаційної безпеки;
- проаналізувати особливості і проблеми реалізації державної політики України щодо інформаційної безпеки;
- розкрити механізми державної політики щодо протидії загрозам в інформаційній сфері;
- запропонувати шляхи покращення державної політики щодо інформаційної безпеки.

Об'єктом дослідження є державна інформаційна політика.

Предметом дослідження є особливості, проблеми, механізми та перспективи вдосконалення державної політики України щодо інформаційної безпеки.

Методи дослідження. Для досягнення поставленої мети в роботі було застосовано комплекс загальнонаукових та спеціальних методів пізнання. Зокрема, використовувались наступні методи: аналізу – для розкриття теоретичних засад державної політики щодо інформаційної безпеки; Метод порівняння – використано у роботі під час дослідження міжнародного досвіду реалізації державної політики у сфері інформаційної безпеки. Системний метод використано при аналізі перспективи оптимізації реалізації державної політики у сфері інформаційної безпеки. Для уточнення наукових понять використовувався метод теоретичного узагальнення. У роботі також використовувались такі загальнонаукові методи, як метод аналізу та синтезу, метод індукції та дедукції.

Наукова новизна одержаних результатів полягає в тому, що в даній роботі зроблена спроба комплексного дослідження особливостей, проблем та шляхів вдосконалення державної політики України щодо інформаційної безпеки, з урахуванням світового досвіду та наслідків російсько-української війни.

Практичне значення одержаних результатів. Положення і висновки

дослідження можуть бути використані в практичній діяльності органами державної влади та у навчальному процесі при підготовці студентів за спеціальністю 281 «Публічне управління та адміністрування».

Структура роботи. Робота складається зі вступу, трьох розділів, які об’єднують сім підрозділів, висновків та списку використаних джерел та двох додатків. Загальний обсяг роботи складає 79 сторінок, основного тексту – 68 сторінок. Список використаних джерел налічує 103 найменування. Робота містить 18 рисунків.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Джерельна база, основні поняття та категорії дослідження

Державна інформаційна політика – це фундамент існування будь-якої країни, тому що інформація для сучасного суспільства несе важливу роль в повсякденному житті, так само як для держави в цілому. Томас Р. Дай у своїй праці «Основи державної політики» наводить таке трактування поняття державної політики: «це органи державної влади вирішують, що їм робити або не робити. Органи державної влади мають регулювати конфлікти, збирати податки, мати монополію на насильство, організовувати безпеку суспільства. Отже, державна політика робить багато речей одночасно» [20].

Науковцями Е. Янгом і Л. Куінном (Young E. and Quinn L.) наведено такі тлумачення поняття державної політики: «Державна політика – це дії, що їх реалізує владний орган, який має законодавчі, політичні та фінансові повноваження це робити; державна політика – це реакція держави на реальні життєві потреби чи проблеми; державна політика здійснюється одним або групою акторів; державна політика передбачає обґрунтування дій, тобто, як правило, містить пояснення логіки, на якій вона ґрунтується; державна політика це рішення, що вже ухвалене; державна політика – це курс дій, ретельно розроблений підхід або стратегія» [124].

Державну політику визначено як «сукупність ціннісних цілей, державно-управлінських заходів, рішень і дій, порядок реалізації державно-політичних рішень (поставлених державною владою цілей) і системи державного управління розвитком країни» [22].

Говлет М., Рамеш М. (Howlett. M., Ramesh, M.) у своїй книзі

«Дослідження державної політики: цикли та підсистеми політики» аналізують підходи, засоби, процес політики, впровадження, оцінювання політики та зазначають, що «реалізація політики є складним та безперервним процесом» [16].

Науковці розмежовують поняття державна політика на politics та policy. «Politics це використання державної влади у співпраці певних соціальних груп або соціальних індивідів для реалізації своїх інтересів. Policy – це дія, план за яким рухається державна влада» [78].

Розглянемо Конституцію України, а саме це частину другу статті 50 Конституції України, яка гарантує «право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена» [39].

На думку, Г. Бондар «відсутність інформаційної відкритості, прозорості та підзвітності влади суспільству, необґрунтоване засекречування інформації й обмеження свободи інформаційного обміну є дуже небезпечним явищем для майбутнього будь-якої держави, особливо України. Інформаційна сфера є основою, на якій базуються політичні, адміністративні, економічні, будь-які рішення в царині галузей людської діяльності. Ці рішення будуть лише тоді обґрунтованими та ефективними, коли для їх прийняття буде використано якомога більше інформації»[6].

Стаття 9 Закону України «Про інформацію» [63] визначає такі види інформаційної діяльності, а саме (див. Рис. 1.1):

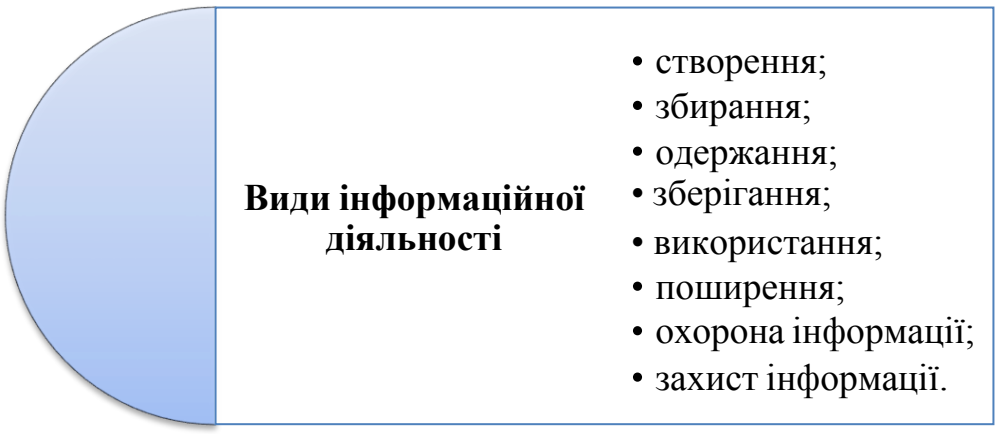

Рис. 1.1. Види інформаційної діяльності відповідно до Закону України «Про інформацію» [63]

Нині інформація не є допоміжною силою у боротьбі, а стає основною силою впливу на громадян та супротивника. Г. Почепцов дав дуже слушне визначення інформації, як інструменту боротьби із ворогом, а саме: «Інформація поступово припиняє бути додатковим до іншої сили інструментарієм. Вона стає самостійною силою. І саме це вимагає перегляду можливостей щодо її застосування» [58].

В українському законодавстві є визначення понять «інформації» та «державної інформаційної політики». Так, відповідно до Закону України «Про інформацію» [63], «інформація це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [63]. Також в статті 3 Закону України «Про інформацію» є визначення основних напрямів державної інформаційної політика, а саме це: «забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору» [63].

Також існує термін «інформаційні операції» про які пишуть в своїй монографії В. Горбулін, О. Додонов, Д. Ланде «Інформаційні операції та безпека суспільства: загрози, протидія, моделювання». Вони стверджують, що «інформаційні операції це заходи (акції) спрямовані на вплив на супротивника через інформацію та інформаційні системи, а також захисту власної інформації та систем» [17].

Категорія національної безпеки визначена в пункті 9 статті 1 Закону України «Про національну безпеку України», а саме: «національна безпека

України - це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [65].

Британський військовий історик Дж. Ф. Ч. Фуллер (J. F. C. Fuller) на початку 20 років XX століття першим почав вживати термін «психологічна війна» [106]. М. Дмитренко у статті «Проблемні питання інформаційної безпеки України» досліджує проблеми інформаційної безпеки України в контексті інформаційної війни, розглядає питання планування та проведення інформаційних впливів (інформаційних операцій, дій, акцій) у рамках реалізації завдань внутрішньої і зовнішньої політики держави, проводить аналіз інформаційних ризиків. «Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян»[24].

Важливі питання, що стосуються інформаційної політики в сфері національної безпеки, розглянули у своїй аналітичній доповіді науковці Національного інституту стратегічних досліджень. У праці наголошено, що «через збройну агресію рф Україна не може повноцінно забезпечити свою інформаційну присутність та повноцінно реалізовувати свою інформаційну політику на окупованих територіях. Найбільш актуальним питанням нині є реінтеграція у повному обсязі територій до інформаційного простору держави. Реалізація зазначеного завдання потребує скоординованої політики держави, зокрема, залучення органів державної влади, міжнародних партнерів, неурядових організацій та громадянського суспільства» [7].

Науковець В. Негодченко пропонує доповнити перелік основних напрямів державної інформаційної політики, закріплених у Законі України «Про інформацію» [48], такими: «сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій, засобів їх забезпечення; розвиток адміністративного законодавства у сфері інформаційних процесів (у тому числі приведення законодавчої бази у відповідність до міжнародних

стандартів у цій сфері), інформатизації і захисту інформації; правове регулювання функціонування в Україні міжнародних інформаційних систем (зокрема, мережі Інтернет); пропагування курсу держави на створення та розвиток відкритого інформаційного суспільства» [48].

Г. Почепцов, відомий фахівець у сфері інформаційних війн, у своїй праці «Сучасні інформаційні війни» пише, що «інформаційна політика працює з такими чутливими сферами, як а) контент (стабілізаційний чи дестабілізаційний); б) суспільні цінності (традиційні чи руйнівні); в) характер суспільства (демократичний, інноваційний)» [58]. Автор досліджує питання інформаційних технологій, інформаційно-комунікативних процесів в сучасних суспільствах, зокрема, проблеми, що виникають через надмірні покази на екранах розважальних програм, які стримують розвиток суспільного мислення [58].

Г. Почепцов наводить таке визначення психологічних війн, а саме: «психологічні війни є комунікативними технологіями, що спрямовані на внесення змін у поведінку індивіда за допомогою модифікації його моделі світу, що здійснюється шляхом внесення змін у інформаційні потоки. Тобто психологічні війни змінюють мислення людини на таке, яке необхідне супротивнику для вирішення поставлених тактичних та стратегічних цілей політики» [58].

«Коли розробляється психологічна операція важливо акцентувати увагу на тому через, які канали буде транслюватись або передаватись інформація або повідомлення. Також перед початком психологічної операції важливо зробити аналіз аудиторії на яку буде робитись вплив для каналів зв’язку та вибору відповідних меседжів для впливу на аудиторію [58].

Також він вказує на «Фактор соціального середовища» коли індивід на якого впливають психологічні операції спирається на своє соціальне середовище для прийняття відповідного рішення [58].

Вагомість інформаційної безпеки в системі національної безпеки України визначається активізацією ризиків в інформаційній сфері, зокрема, веденням

інформаційних війн. «Майбутні війни – війни без застосування безпосереднього насильства, засобами якого є не безпосередні дії, одним із методів яких є інформаційні війни» [43].

В. Панченко у своїй праці «Інформаційні операції в асиметричній війні росії проти України: підходи до моделювання» наводить чотири ознаки асиметричної війни:

1. «Межі бойових дій відсутні.
2. Ведення бойових дій малими групами.
3. Бойові підрозділи існують завдяки середовищу де знаходять.
4. Керований хаос» [55].

«Асиметрична війна – це війна із дисбалансом сил між ворогами, і які застосовують різні стратегії та тактику ведення бойових дій. Це можуть бути інформаційно-психологічні операції, спротив та диверсії, ведення партизанської війни, підтримка антиурядових громадських організацій та партій, а також проведення терористичних актів» [55].

Ризики, що пов’язані з інформаційною безпекою, пов’язані з впливом «негативних чинників або процесів, через які порушується їх функціонування, стримується розвиток об’єктів інформаційної безпеки» [19].

На основі звітів інститутів інформаційної безпеки, що «стосуються дотримання політики, виклики стосовно інформаційної безпеки були поділені на чотири групи: просування політики безпеки, невідповідність політиці безпеки, управління та оновлення політики безпеки, тіньова безпека. Чинники, що впливають на поведінку, були розділені на організаційні та людські. Висновок, який роблять автори, полягає у постійному навчанню працівників, підвищенню обізнаності та контролю за їх дотриманням політики інформаційної безпеки» [93].

Науковець S. Lutaaya у своєму дослідженні «Information Security Policy for Ronzag» зазначає, що уряди все більше використовують конфіденційну інформацію, отже питання належної інформаційної безпеки стоїть, критично. Важливо впровадити стандарти інформаційної безпеки. Метою інформаційної

безпеки для веб-служб є захист інформаційних активів компанії, незалежно від того, зберігаються вони в ручній або електронній формі. Це допоможе захистити репутацію компанії, оптимізувати управління ризиками та мінімізувати вплив інцидентів інформаційної безпеки. Будь-яка втрата інформації може мати серйозні наслідки для компанії та її споживачів. Порушення безпеки під час оброблення, зберігання, передачі даних може призвести також до фінансових втрат. Інформація про комп'ютерні системи має бути захищеною антивірусним програмним забезпеченням та регулярно оновлюватися. Повинні бути впроваджені визначені та затверджені політики та стандарти інформаційної безпеки» [107].

«В основі державної політики щодо забезпечення інформаційної безпеки має бути системна діяльність органів державного влади щодо надання гарантій інформаційної безпеки громадянам, соціальним групам, суспільству в цілому. Проблеми, що пов'язані з інформаційною безпекою держави варто розглядати у взаємозв'язку з іншими проблемами, які виникають у світовому просторі, національній економіці, соціальній, демографічній сфері тощо» [21].

Державна політика з інформаційної безпеки має бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки для всіх суб'єктів господарювання, державної влади, усіх громадян країни. До основних джерел внутрішніх ризиків у сфері інформаційної безпеки можна віднести такі: «недосконаліть законодавчої бази в галузі інформаційних відносин та інформаційної безпеки, протиправні дії окремих громадян в інформаційній сфері, виникнення непередбачуваних ситуацій в системах, які базуються на використанні інформаційних технологій, недосконаліть або відсутність засобів забезпечення інформаційної безпеки тощо» [56].

На думку О. Золотар «всі визначення інформаційної безпеки людини можна узагальнити в два основні підходи: технічний та гуманітарний. Перший підхід домінує в правових науках та ґрунтується на забезпечення людині здатності вільно і безперешкодно реалізовувати права та свободи в інформаційній сфері, зокрема право на інформацію – вільно збирати, зберігати,

використовувати і поширювати інформацію. Технічний аспект інформаційної безпеки полягає у здатності і вмінні людини передбачати та попереджувати загрози інформації, яка циркулює в технічних системах, і загрози самим системам» [34]. Другий підхід наголошує на «захищеності психіки та свідомості людини від небезпечних інформаційних впливів; маніпулювання, дезінформування, образ, спонукання до самогубства тощо» [32].

Розглянемо співвідношення понять: інформаційна безпека та кібербезпека. Кібербезпека – це безпека інформаційних систем (програм чи устаткування). Інформаційна безпека – це безпека інформації, у тому числі в інформаційних системах. «Кібербезпека є частиною інформаційної безпеки. Відповідно до пункту першого Окінавської хартії глобального інформаційного суспільства інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття» [50]. Пунктом п’ять Окінавська хартія закликає державний та приватний сектор ліквідувати розрив у сфері інформації та освіті. Також Окінавська хартія наголошує на тому, що «приватний сектор є важливою ланкою у створені та розробці комунікаційних та інформаційних мереж, але на уряді лежить створення політики та нормативно-правових актів» [50].

Відповідно до закону Г. Мура [27] (засновник корпорації Intel), кількість транзисторів в мікросхемах буде збільшуватись у два рази кожні два роки. Закон Мура пояснює це «особливостями створення та поширення різноманітних інформаційних технологій, таких як: соціальні мережі, відеохостинги» [9].

Чинний закон Україні «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» інформаційну безпеку визначає, як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності,

конфіденційності та доступності інформації» [66].

У свою чергу в підручнику «Інформаційна та кібербезпека: соціотехнічний аспект» В. Бурячок, В. Толубко, В. Хорошко, С. Толюпа, зазначають, що «інформаційна безпека це стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони» [9].

Також науковці В. Гур'єв, Д. Мехед, Ю. Ткач, І. Фірсова у навчальному підручнику «Інформаційна безпека держави» [33], наводять таке визначення: «інформаційна безпека – це захищеність (стан захищеності) основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі як повнота, об'єктивність, доступність і конфіденційність» [33].

Отже, державна політика з інформаційної безпеки має бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки для всіх суб'єктів господарювання, державної влади, усіх громадян країни. Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян. Проблеми, що пов'язані з інформаційною безпекою держави варто розглядати у взаємозв'язку з іншими проблемами, які виникають у світовому просторі, національній економіці, соціальній, демографічній сфері тощо. Вагомість інформаційної безпеки в системі національної безпеки України визначається й активізацією ризиків в інформаційній сфері, зокрема, веденням інформаційних війн. З різних визначень науковців та законодавства терміну «інформаційна безпека», є спільна риса – це запобігання нанесенню шкоди в будь-якій формі.

1.2. Законодавче та нормативно-правове забезпечення державної політики щодо інформаційної безпеки

Міжнародна інформаційна безпека реалізується в доктринах, стратегіях, законах держав і міжнародних організацій, зокрема, Організації Об'єднаних Націй, Європейського Союзу, Ради Європи, НАТО.

10 березня 1992 року Україна приєдналась до участі в Раді євроатлантичного партнерства [59]. 8 лютого 1994 року Україна приєдналась до Програми партнерство заради миру. Пунктом два цієї рамочної угоди щодо Програми партнерство заради миру наголошується на тому, що стабільність та безпека в регіоні має буди досягнута завдяки спільним діям та співробітництву.

Цілі цієї програми:

«1. сприяння відкритості у плануванні національної оборони та формуванні військового бюджету;

2. забезпечення демократичного контролю над збройними силами;

3. підтримання здатності та готовності брати участь в межах, дозволених конституцією, в операціях, здійснюваних під егідою ООН і/або в рамках відповідальності ОБСЄ;

4. розвиток відносин співробітництва з НАТО у військовій сфері з метою здійснення спільного планування, військової підготовки та учбових маневрів, покликаних підвищити їхню спроможність до виконання завдань, пов'язаних з миротворчою діяльністю, пошуковими і рятувальними операціями, операціями по наданню гуманітарної допомоги та іншими, про які згодом може бути домовлено.

5. формування у тривалій перспективі таких збройних сил, які зможуть краще взаємодіяти зі збройними силами держав-членів Північноатлантичного союзу» [59]. 8 липня 1997 року між Україною та Організацією Північноатлантичного договору і її країн-членів було підписано Хартію про особливе партнерство [84].

Питання міжнародної безпеки відображені в Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки», де заявлено про «створення нового міжнародно-правового режиму з поняттям інформаційна технологія» [113].

Відповідно до пункту першого Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки» Організація Об'єднаних Націй «закликає держави-члени сприяти розгляду на багатосторонньому рівні існуючих та потенційних загроз у сфері інформаційної безпеки» [113]. Також Резолюція Генеральної Асамблеї ООН A/RES/53/70 «Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки наголошує на тому, щоб зробити загальну оцінку проблем у інформаційній безпеці» [113].

Резолюції Генеральної Асамблеї ООН: A/RES/55/63 від 4.12.2000 р. і A/RES/56/121 від 19.12.2001 р., A/RES/57/239 від 20.12.2002 р., A/RES/58/199 від 23.12.2003 р., A/RES/64/211 від 21.12.2009 р., A/RES/62/17 від 5.12.2007 р. визначили напрями боротьби зі злочинним використанням інформаційних технологій, створенням глобальної культури кібербезпеки, захистом інформаційних інфраструктур, сприянням розгляду існуючих та потенційних загроз у сфері інформаційної безпеки тощо.

Варто підкреслити, що питання забезпечення інформаційної безпеки стає одним із пріоритетних напрямів діяльності й ЄС. У 2001 р. Комісією ЄС було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому була представлена концепція вирішення проблем щодо інформаційної безпеки. У документі сформульовано визначення «мережева та інформаційна безпека – здатність інформаційної системи чинити опір випадковим чи зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через мережі та системи» [112].

На початку 2000-х років органами ЄС було прийнято цілу низку

нормативно-правових актів, які передбачають різноманітні підходи забезпечення інформаційної безпеки в державах-членах ЄС. У повідомленні Комісії ЄС «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» від 22 травня 2007 року, пропонується визначення «кіберзлочинності» та основних напрямків політики ЄС щодо інформаційної безпеки [120].

У лютому 2013 року була прийнята Стратегія кібербезпеки ЄС «Відкритий, надійний та безпечний кіберпростір» в якій йде мова про міждержавне співробітництво та механізми протидії кіберзагрозам в ЄС [98]. У 2016 року Директивою Європейського парламенту та Ради ЄС було затверджено єдині правила та вимоги у сфері кібербезпеки для всіх держав-членів.

Для інформаційної безпеки в рамках ЄС у 2004 року було впроваджено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA). Завдання ENISA є: «удосконалення мережевої та інформаційної безпеки в ЄС, сприяння розвитку культури мережевої та інформаційної безпеки»[102].

У 2013 року в структурі Європейського поліцейського офісу (Європол) був утворений Європейський центр боротьби з кіберзлочинністю, основними напрямками діяльності якого є «розслідування шахрайства в мережі Інтернет, розслідування злочинів щодо критично важливої інфраструктури та інформаційних систем ЄС» [102]. Щороку Європейський центр боротьби з кіберзлочинністю оцінює загрози у сфері кіберзлочинності – загрози, що впливають на уряди, бізнес та громадян в ЄС та надає рекомендації для ефективного та узгодженого реагування на кіберзлочини.

В Україні на сьогоднішній день існує значна кількість законодавчих та нормативно-правових актів, які регулюють питання інформації та національної безпеки. В умовах російсько-української війни російські інформаційно-психологічні операції спрямовані на забезпечення домінування в українському інформаційному просторі. Через російські пропагандистські інформаційно-психологічні кампанії відбувається вплив не лише на суспільну свідомість

громадян України, а й на громадськість в усьому світі [12].

Відповідно до Стратегії національної безпеки України, яка затверджена Указом Президента України від 26 травня 2015 року № 287/2015, визначено наступні цілі:

– «мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно- визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави;

– утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО» [72].

Актуальною загрозою національній безпеці в Стратегії національної безпеки України визначено «інформаційно-психологічну війну, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу» [72].

Національні інтереси України та загрози в інформаційній сфері визначені в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [70]. «Національними інтересами України в інформаційній сфері є: життєво важливі інтереси особи та життєво важливі інтереси суспільства і держави, як то: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, забезпечення конституційних прав людини на захист приватного життя, захищеність від руйнівних інформаційно-психологічних впливів; захист українського суспільства від агресивного інформаційного впливу рф, розвиток та захист національної інформаційної інфраструктури, створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди тощо» [70].

«Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур; інформаційне домінування держави-агресора на тимчасово окупованих територіях; неефективність державної інформаційної політики тощо» [70].

У Стратегії національної безпеки України (2015 р.) вперше серед загроз національній безпеці визначаються загрози критичній інфраструктурі. А в підрозділі «Загрози кібербезпеці і безпеці інформаційних ресурсів», зазначається про вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак. Також уперше одними з «основних напрямів державної політики у сфері національної безпеки» названо забезпечення безпеки критичної інфраструктури та визначено пріоритети такого напряму» [29].

«Зелена книга» з питань захисту критичної інфраструктури в Україні. У «Зеленій книзі» є визначення «критичної інфраструктури», це – «об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих наслідків для соціальної й економічної сфер держави, негативно вплине на рівень її обороноздатності та національної безпеки. Функціонування критичної інфраструктури в мирний час пов'язується із підтримуванням життєво важливих функцій у суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки й захищеності» [29].

Процес удосконалення правового механізму державного управління захисту критичної інфраструктури в Україні в цілому відбувається з урахуванням передового досвіду країн ЄС та США та зберігається потреба

внесення змін і доповнення до чинного Закону України «Про національну безпеку України», та постійного моніторингу щодо актуальності у частині захисту об’єктів критичної інфраструктури нещодавно ухваленого закону «Про критичну інфраструктуру» [70].

У 2016 р. в Україні була прийнята Стратегія кібербезпеки України [69]. Цей документ визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики інформаційної безпеки, яка відповідатиме світовому рівню.

Указом Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», визначено, що окрім традиційних сфер ведення бойових дій таких, як «Земля», «Повітря», «Море», «Космос», діє Кіберпростір. Із широким застосуванням інформаційних технологій таких, як хакерські атаки та інформаційно-психологічні спеціальні операції країни агресора (ІПСО).

Відповідно до абзацу 5 розділу 2 Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016, передбачено що загрози у сфері кібербезпеки відбуваються через дію таких чинників:

- «невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
- безсистемність заходів кіберзахисту критичної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;
- недостатня ефективність суб’єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та

іншого характеру;

- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки» [69].

Воєнна доктрини України, яка затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» [68], визначає стратегічні комунікації, як «скоординоване і належне використання комунікативних можливостей держави, а саме інформаційно-психологічних операцій» [68].

Пункт 7 Воєнної доктрини України [68] визначає головні тенденції, військово-політичної обстановки довкола Україні:

- «проведення спеціальних операцій та дій провокаційного характеру для створення конфліктних ситуацій;

- інформаційна війна Російської Федерації проти України» [68].

Разом з тим пункт 9 Воєнної доктрини України [68] вказує на воєнні загрози:

- «проведення розвідувально-підривної діяльності в Україні для дестабілізації внутрішньої соціально-політичної обстановки в Україні, також підтримка незаконних збройних формувань у східних регіонах України;

- діяльність на території України не передбачених законом збройних формувань, спрямована на дестабілізацію внутрішньої соціально-політичної ситуації в Україні, залякування населення, позбавлення його волі до опору, порушення функціонування органів державної влади, місцевого самоврядування, важливих об'єктів промисловості та інфраструктури;

- інформаційно-психологічні операції з використанням сучасних інформаційних технологій» [68].

Доктриною інформаційної безпеки України, затвердженої Указом Президента від 25 лютого 2017 року № 47/2017 [68], передбачено, що технології гібридної війни, які застосовує російська федерація проти нашої країни перетворило інформаційну сферу на головну боротьбу за свідомість громадян.

Метою Доктрини інформаційної безпеки України є «формування та реалізація засад інформаційної безпеки щодо протидії Російській Федерації в умовах гібридної війни» [68].

Доктрина інформаційної безпеки [70] визначає сім загроз національній безпеці в сфері інформації, а саме:

- «проведення спеціальних операцій (підрив обороноздатності);
- проведення інформаційних спеціальних операцій;
- інформаційна інфраструктура РФ в Україні;
- домінування РФ в інформаційній сфері;
- нерозвиненість інформаційної інфраструктури;
- недосконалість законодавства у сфері інформації та неефективна державна інформаційна політика» [70].

У грудні 2017 р. було прийнято «Концепцію створення державної системи захисту критичної інфраструктури». «У документі визначаються основні напрямки, механізми та строки правового врегулювання даного питання, створення системи державного управління захисту» [40].

21 червня 2018 року Верховною Радою України було прийнято новий Закон України «Про національну безпеку України» [65]. В преамбулі цього закону сказано, що він «визначає засади державної політики у сфері національної безпеки і оборони» [65]. Також цей закон «визначає та розмежовує повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони» [65].

Отже, міжнародна інформаційна безпека реалізується в доктринах, стратегіях, законах держав і міжнародних організацій, зокрема, Організації Об'єднаних Націй, Європейського Союзу, Ради Європи, НАТО. Резолюції Генеральної Асамблеї ООН визначили напрями боротьби зі злочинним використанням інформаційних технологій, створенням глобальної культури кібербезпеки, захистом інформаційних інфраструктур, сприянням розгляду існуючих та потенційних загроз у сфері інформаційної безпеки. На початку 2000-х років органами ЄС було прийнято цілу низку нормативно-правових актів, які передбачають різноманітні підходи забезпечення інформаційної безпеки в державах-членах ЄС.

В Україні на сьогоднішній день існує значна кількість законодавчих та нормативно-правових актів, які регулюють питання інформації та національної безпеки. Зокрема, актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур; інформаційне домінування держави-агресора на тимчасово окупованих територіях; неефективність державної інформаційної політики.

1.3. Міжнародний досвід реалізації державної політики щодо інформаційної безпеки

У Сполучених Штатах Америки головним федеральним виконавчим органом у військовій сфері та питанні національної безпеки є Міністерство оборони США (англ. United States Department of Defense). «У складі Міністерства оборони США діє Агентство національної безпеки (англ. National Security Agency) повноваження якої є збір та аналіз закордонної розвідувальної інформації, захист інформаційних систем, комп'ютерних мереж уряду» [3].

Агентство національної безпеки (АНБ), (англ. National Security Agency (NSA) – агентство криптологічної розвідки Сполучених Штатів Америки. «АНБ є частиною Міністерства оборони США і відповідає за збір та аналіз іноземної розвідувальної інформації та за захист інформаційних систем і комп'ютерних мереж уряду США. Агентство було створено 4 листопада 1952 року указом президента США Г. Трумена. АНБ є складовою частиною системи безпеки країни разом з ЦРУ та іншими агентствами, однак на відміну від ЦРУ не займається використанням агентів в інших країнах. Згідно з федеральним законом, діяльність агентства обмежена збором та моніторингом іноземної розвідувальної інформації, однак з'являлися численні підозри у використанні агентства для збору інформації також і у США» [3].

Як пише в своїй статті Л. Буга, «досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах на даний час забезпечення інформаційної безпеки в Армії США є високим» [8].

Кіберкомандування Армії США та Управління програм з інформаційної Міністерства оборони забезпечують інформаційну безпеку в Армії США [8]. «Основні сфери відповідальності Кіберкомандування:

- захист інформаційних мереж Армії та Міністерства оборони;
- реагування на кібератаки;
- підтримка союзників США» [8].

«У 2015 році в Ізраїлі створено координаційний орган щодо посилення цифрового захисту Національне управління кібербезпеки» [18]. Як наголошує М. Гребенюк, Б. Леонов, у своїй статті «Досвід Ізраїлю у сфері забезпечення кібербезпеки», це управління було створене у зв'язку із загрозливими

тенденціями у кіберпросторі, і чимало державних та комерційних установ стали слабкими до кібератак» [18]. «Кібербезпека – це сфера майбутнього, яка потребує вкладення потужних державних та приватних інвестицій на перманентній основі. Розвиток цієї важливої складової світової національної безпеки є одним із головних чинників прискорення галузевої трансформації усієї світової економіки в найближчі десятиліття. У найближчій перспективі сфера кібербезпеки має стати ключовим параметром визначення рівня економічного розвитку будь-якої країни, її конкурентоспроможності на глобальному ринку» [18].

Для ефективної роботи системи кіберзахисту уряд Ізраїлю підтримує навчальні програми спеціалістів, і освітні програми для населення щодо цифрового захисту [18]. «Світовий досвід демонструє, що сьогодні сфера забезпечення кібербезпеки виходить за межі юрисдикції певних країн і має глобальний та міжнародний характер, що зумовлює потребу в розробці не тільки національної, а й відповідної міжнародної стратегії забезпечення безпеки у кіберпросторі» [18].

Серед країн-лідерів у сфері інформаційної безпеки – США, Китай, Південна Корея, Туреччина, Японія.

Активну політику у сфері забезпечення інформаційної безпеки реалізує ЄС. Інформаційна безпека Європейського Союзу ґрунтується на використанні численних рекомендацій, які викладені в міжнародних стандартах. «Країни Європейського Союзу активно впливають на міжнародні відносини, встановлюють норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах» [80].

У 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій» [97], де визначено завдання забезпечення інформаційної безпеки, зокрема:

- «захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;
- забезпечення цілісності інформаційних ресурсів шляхом їх захисту

від несанкціонованої модифікації або знищення;

- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні» [97].

Досліджуючи міжнародні критерії інформаційної безпеки держави, науковці визначають поняття інформаційної війни як «протиборство інформаційно-комунікаційних технологій та здатності державних і комерційних інформаційних систем забезпечити безпеку інфраструктури держави в цілому» [49].

Науковець Т. Ткачук, досліджуючи досвід країн Європи: Польщі, Угорщини, Швейцарії та інших, зазначає, що «європейські держави усвідомлюють та протидіють кіберзагрозам. Політика національної безпеки країн ЄС спрямована на захист інформації, критичної інформаційної інфраструктури, інформаційно-психологічної безпеки громадян» [79].

«З 2011 року в Німеччині безпекою інформації займається Національний центр кібербезпеки, на який покладені завдання реагування та попередження на загрози у кіберпросторі та захисту критичної інфраструктури» [79].

«В Польщі безпекою інформації в кіберпросторі займається Центр криптології при Міністерстві національної оборони, завдання якого – це захист інформації, кібернетична оборона та ін.» [79].

«Хорватія покладає свій захист інформації безпеки на Бюро з безпеки інформаційних систем, національний орган із питань суспільної інформації Республіки Хорватії, Управління Ради національної безпеки» [79].

«У Болгарії важливу роль у кіберзахисті покладено на Міністерство оборони, яке в межах повноваження повинно реагувати та попереджати атаки на критичну інфраструктуру, а також співпрацювати з НАТО» [79].

«Забезпечення захисту інформації в Румунії, шляхом припинення, попередження кібератак, захист критичної інфраструктури, покладено на Румунську службу інформації» [79].

У своїй праці «Cyber Security Policy and Strategy in the European Union and Nato» пан L. Kovács пише про те, що «кібербезпека в першу чергу залежить від

інформаційної освіти користувачів інформаційних ресурсів» [105].

З 2016 року в Європейському Союзі діє Директива 95/46/EC General Data Protection Regulation [99], яка уніфіковує законодавство держав-членів Європейського Союзу щодо захисту приватних та персональних даних. Санкції за порушення Директиви - 20 мільйонів євро, а також 2% та 4% від обороту компанії або організації [105].

Стаття 17 Директиви 95/46/EC General Data Protection Regulation встановлює поняття «Right to erasure («right to be forgotten»)», що означає «право на забуття» – зобов'язання до знищення даних із серверів та баз даних розробників на вимогу користувача [99].

Але в свою чергу стаття 18 Директиви 95/46/EC General Data Protection Regulation встановлює, що ця Директива не застосовується «до обробки персональних даних фізичною особою під час приватної діяльності і, отже, без зв'язку з професійною чи комерційною діяльністю. Приватна діяльність може включати листування, або соціальні мережі та діяльність в Інтернеті, що проводяться в контексті такої діяльності» [99].

2017 році Президент Європейської комісії у щорічному посланні заявив, що в Європейському Союзі буде створено Агенцію з кібербезпеки для допомоги у боротьби із кіберзлочинами членам Європейського Союзу [115]. «Агенція з кібербезпеки Європейського Союзу покращить реагування на кібератаки, а також будуть проводитись загальноєвропейські з протидії кібератак» [115]. Також головною задачею Агенції буде «запровадження сертифікації пристроїв «Інтернет речей» для їх безпечного використання на території Європейського Союзу» [115].

9 липня 2016 року НАТО на Варшавському саміті у своєму Комуніке засудило «дії російської федерації щодо анексії Криму, військових дій на сході України, а також агресивну ядерну діяльність. НАТО підтримує спеціальну моніторингову місію ОБСЄ на сході України» [122]. У комуніке Варшавського саміту наголошується на «незмінності прихильності НАТО до безпеки, прав людини, верховенства права ...» [122]. Зазначено, що «російська федерація

продовжує створювати загрозу НАТО на східних кордонах та є джерелом нестабільності в регіоні» [122].

Таким чином, аналіз позитивних здобутків країн світу має важливе значення при розбудові системи забезпечення інформаційної безпеки України. Більшість країн світу усвідомлюють безпосередню залежність свого добробуту від інформаційної сфери, відтак, питання забезпечення інформаційної безпеки закономірно посідає одне з чільних місць у безпекових стратегіях відповідних держав. Активну політику у сфері забезпечення інформаційної безпеки проводить не лише НАТО, ООН, але й ЄС, який сьогодні об'єднує розвинуті країни, які відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав, зокрема, в інформаційній сфері. Інформаційна безпека Європейського Союзу ґрунтується на використанні численних рекомендацій, які викладені в міжнародних стандартах. Визначившись із зовнішньополітичним курсом, Україна має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері.

Висновки до першого розділу

1. Державна політика з інформаційної безпеки має бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки для всіх суб'єктів господарювання, державної влади, усіх громадян країни. Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян. Проблеми, що пов'язані з інформаційною безпекою держави варто розглядати у взаємозв'язку з іншими проблемами, які виникають у світовому просторі, національній економіці,

соціальній, демографічній сфері тощо. Вагомість інформаційної безпеки в системі національної безпеки України визначається й активізацією ризиків в інформаційній сфері, зокрема, веденням інформаційних війн. З різних визначень науковців та законодавства терміну «інформаційна безпека», є спільна риса – це запобігання нанесенню шкоди в будь-якій формі.

2. Міжнародна інформаційна безпека реалізується в доктринах, стратегіях, законах держав і міжнародних організацій, зокрема, Організації Об'єднаних Націй, Європейського Союзу, Ради Європи, НАТО. Резолюції Генеральної Асамблеї ООН визначили напрями боротьби зі злочинним використанням інформаційних технологій, створенням глобальної культури кібербезпеки, захистом інформаційних інфраструктур, сприянням розгляду існуючих та потенційних загроз у сфері інформаційної безпеки. На початку 2000-х років органами ЄС було прийнято цілу низку нормативно-правових актів, які передбачають різноманітні підходи забезпечення інформаційної безпеки в державах-членах ЄС.

В Україні на сьогоднішній день існує значна кількість законодавчих та нормативно-правових актів, які регулюють питання інформації та національної безпеки. Зокрема, актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур; інформаційне домінування держави-агресора на тимчасово окупованих територіях; неефективність державної інформаційної політики.

3. Таким чином, аналіз позитивних здобутків країн світу має важливе значення при розбудові системи забезпечення інформаційної безпеки України.

Більшість країн світу усвідомлюють безпосередню залежність свого добробуту від інформаційної сфери, відтак, питання забезпечення інформаційної безпеки закономірно посідає одне з чільних місць у безпекових стратегіях відповідних держав. Активну політику у сфері забезпечення інформаційної безпеки проводить не лише НАТО, ООН, але й ЄС, який сьогодні об'єднує розвинуті країни, які відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав, зокрема, в інформаційній сфері. Інформаційна безпека Європейського Союзу ґрунтується на використанні численних рекомендацій, які викладені в міжнародних стандартах. Визначившись із зовнішньополітичним курсом, Україна має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері.

РОЗДІЛ 2
ОСОБЛИВОСТІ І ПРОБЛЕМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Інформаційні війни і технології, та їх вплив на Україну

У період інформаційних технологій критично важливо державним структурам системно проводити роботу з убезпечення всіх сфер діяльності держави від інформаційних атак. Інформаційна війна це новий вид введення бойових дій, який уражає населення, військовослужбовців, змінюючи їх світогляд та світосприйняття. Все більше об’єктів критичної інфраструктури переходить на інформаційні технології або у кіберпростір, де хакери можуть здійснити взлом та відключити атомний енергоблок, або вплинути на виборчий процес. Тому дуже важливо із боку державної влади планувати захист держави не тільки звичайними методами (армія, спецслужби), а також спеціальними методами у кіберпросторі.

Сучасні бойові дії ведуться не тільки традиційними засобами, а також із використанням інформаційних технологій, таких як:

- «хакерські атаки на критичну інфраструктуру;
- інформаційно-психологічні спецоперації;
- дезінформація у соціальних мережах» [77].

Інформаційна війна це новий вид введення бойових дій, який впливає на населення, військовослужбовців, змінюючи їх світогляд та світосприйняття.

На нашу думку, в інформаційній війні в Україні використовуються наступні засоби:

- соціальні мережі;
- блогери;
- фейкові новини;

- політики;
- 5 колона (Шарій);
- Українська православна церква московського патріархату (філія російської православної церкви);
- теорії змов.

Рис. 2.1. Динаміка користування топ-джерелами інформації [125]

За даними на лютий 2019 року, ГО «Детектор медіа» найбільша кількість респондентів 85,7% отримують інформацію із загальнонаціональних каналів цей показник дещо збільшився порівняно із аналогічним періодом 2018 року (див. Рис. 2.1). В той же час лише 27,5% із сайтів українського інтернет-середовища, а 23,5% із соціальних мереж, вітчизняним друкованим виданням довіряють надто мала кількість опитаних, всього 6,7% [51].

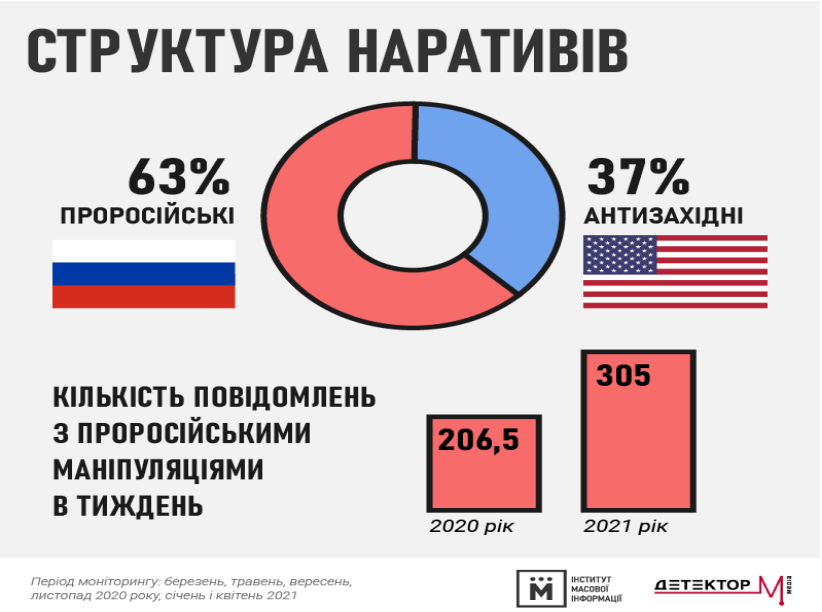

Рис 2.2. Структура наративів [126]

Як ми можемо побачити на Рис. 2.2 найбільша кількість наративів має російське походження (63%), і лише (37%) є антизахідними за походженням. У період з 2020 року (206, 5 повідомлень на тиждень) по 2021 рік дещо зросла кількість повідомлень (305 на тиждень) з проросійськими маніпуляціями на тиждень [51].

Рис. 2.3 Топ медіа з антизахідними та проросійськими наративами [127]

Низка ЗМІ протягом 2021 року активно ретранслювала різні антизахідні

наративи, та активно поширювала проросійські. Лідером став канал Страна майже 400 матеріалів, найменше спостерілаось у Подробности біля 30 (див. Рис. 2.3).

Ще один шкідливий російський пропагандистський наратив, який в останні місяці активно поширюють в інформаційному просторі тимчасово окупованого Криму, – про те, що «український народ став жертвою політики НАТО» [51] (див. Рис. 2.4).

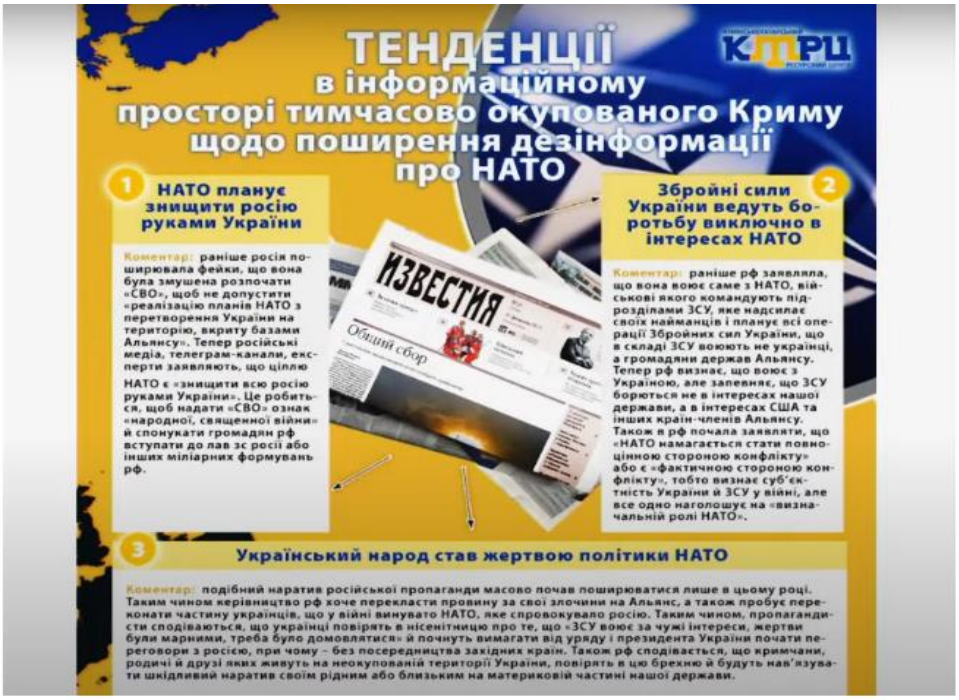

Рис. 2.4. Скрін з сайту «Детектор медіа» щодо дезінформації про НАТО[51]

«Таким чином керівництво росії хоче перекласти провини за свої злочини на Альянс, та намагається переконати частину українців, що у цій війні винувате НАТО, і що це Альянс спровокував Росію. Пропагандисти сподіваються, що українці повірять у нісенітницю про те, що ЗСУ воюють за чужі інтереси, жертви були марними, а треба було домовлятися» [51]. На прикладі рис. 2.5. подивимось на приклади гібридних тактик авторитарних країн.

Рис. 2.5. Перелік гібридних тактик рф, Китаю та Ірану за даними кризового медіацентру [52]

Інтернет-видання The New York Times створило документальний фільм Operation InfeKtion про поширення та створення дезінформації, яку створює російська федерація. У другому епізоді документального фільму розкриваються сім заповідей дезінформації:

1. Знайти суперечності в суспільстві.
2. Створити брехню, абсолютну маячню.
3. Брехня має бути з насінням правди.
4. Джерело інформації не повинно бути знайдено «Ховайте ваші руки».
5. Корисні ідіоти.
6. Все заперечувати.

7. Стратегічне планування або довга гра.

Біла книга. Модель серіалів для отримання знань про російські пропагандистські кампанії в медіа та мережі Інтернет. У Білій книзі спеціальних інформаційних операцій проти України, за 2014-2018 рр., що підготовлена колективом експертів Міністерства інформаційної політики України (зараз Міністерство культури та інформаційної політики України), було запропоновано модель серіалів для отримання знань про російські пропагандистські кампанії в медіа та мережі Інтернет «…російські наративи та дезінформаційні прийоми мають високий ступінь ефективності саме завдяки повторюваності в медіа. Іншими словами, об'єктам дезінформації постійно розповідають одні й ті самі історії, роблячи їх щоразу цікавішими та більш «екзотичними» [4]. Автори білої книги акцентують увагу на тому, що «частота згадування ключових слів в рф, пов'язаних із темою ЛГБТ чи педофілії в березні 2013 року збільшилась у 13-12 разів, якщо порівнювати з 2012 роком. «Ісламську державу» Кремль використовує у своїх наративах з 2013 року, «гаряча фаза» інформаційної війни розпочалась у жовтні 2013 року, коли відбувся переможний поєдинок В. Кличка (Україна) й А. Повєткіна (росія). Дослідження інформаційного простору показали, що саме в той день у тестовому режимі було запущено перший «бойовий» проект масованого «тролінгу». Приводом стала поразка російського боксера на ринзі» [4]. «Використовуючи наративи, російська федерація спрямовано тисла на цільові аудиторії та примушувала повірити в потрібні їй ідеї. Такий наратив російської пропаганди автори назвали Серіал. Серії в сезонах, які об'єднані навколо однієї проблематики, автори назвали Сезон» [4].

26 лютого 2013 року Начальник Генерального штабу збройних сил російської федерації генерал армії В. Герасимов публікує в газеті «Военно-Промышленный Курьер» статтю «Ценность науки в предвидении» [111], так звана «Доктрина Герасимова». В цій статті автор припускає співвідношення військових та невійськових дій 1:4. Це співвідношення дуже успішно реалізується в Україні з 2014 року, з початком анексії Автономної республіки

Крим в кінці лютого 2014 року, а після в Донецькій та Луганських областях. А з лютого 2022 року це охопило більшу частину території України.

Міфами про ІДІЛ в Україні рф прагнули заохотити європейських лідерів на співпрацю через боротьбу з тероризмом, у 2015 році було запущено інформаційну операцію під назвою «тренувальні табори ІДІЛ в Україні, для цього використовували іноземні засоби масової інформації та французьку сенаторку Н. Гуле, яка в інтерв'ю радіостанції «France Inter» повідомила, що в Україні діють табори ІДІЛ «на 1.28'40 хвилині, пані Гуле каже: «Ніхто мене не слухає зараз, але через півроку, згадаєте, що я про це говорила. Посеред України діє табір підготовки джихадистів. Адже, все ж таки, друга мова, якою говорять в Ісламській Державі – російська. Уявіть собі, табір підготовки просто біля нас! Який фінансується усією цією протизаконною торгівлею людьми, предметами мистецтва» [42]. 3 квітня 2016 р. Н. Гуле спростувала свою заяву. Трохи згодом кореспондент «Українського тижня» А. Лазарева в своїй статті від 4 квітня 2016 року показує свою переписку із сенаторкою, яка засвідчує, що Н. Гуле повідомляла фейкову новину» [42].

«Оскільки українська армія, добровольчі батальйони та волонтерські рухи фактично зупинили російську армію, то для російських спеціальних служб головною задачею стояла (та продовжує стояти) дискредитація цих рухів. З 2014 року українську армію та добровольчі батальйони починають прив'язувати до ІДІЛ, мета операції була зменшення європейської допомоги на фоні терористичних актів в Європейському союзі» [4].

На сайті американського видання «The Intercept» в лютому 2015 року виходить публікація польського журналіста М. Марцина «В розпал війни Україна стає воротами Джихада. Автор статті бере інтерв'ю у чоловіка на ім'я Халід керівника ІДІЛ в місті Стамбул. Халід розповідає про Різвана (Руслана), який воює в батальйоні Дж. Дудаєва. Різвана (Руслана) повідомляє Марцину про те, що в Україні можна отримати громадянство за 15 тисяч доларів США. Головно метою інформаційної операції був показ того, що джихадисти можуть безперешкодно отримати українське громадянство та добровольчий батальйон

імені Дж. Дудаєва наповнений бойовиками ІДІЛ» [4].

Наступним прикладом роботи спецслужб російської федерації було прив'язання міфу про ІДІЛ в Україні до Збройних Сил України, та їх дискредитація. Кінцева мета спецслужб – це удар по престижу української Армії. Інтернет видання Lenta.Ru у 28 вересня 2017 року посилаючись на Twitter видання Syria Today, повідомило, що в будинку де перебували бійці ІДІЛ знайшли прапор України, зброю, пачку цигарок російського виробництва журнал з кросвордами. Далі спецслужби російської федерації продовжують поширювати міф про ІДІЛ в Україні, вже як ідентичний стиль війни. Так 12 січня 2018 року на так званій гарячій лінії сепаратистів ДНР з'являється інформація пропагандиста С. Пегова про те, що в період конфлікту між ЗСУ і ДНР в «сірій зоні» на лінії зіткнення в районі населених пунктів Гладосове і Травневе, українською стороною з дрона було скинуто саморобний вибуховий пристрій з вражаючими елементами по розташуванню особового складу однієї з донецьких бригад під Горлівкою» [4].

«13 січня 2015 року під Волновахою Донецької області сталася трагедія із мирними жертвами. Відбувся обстріл БМ-21 «Град» блокпосту Збройних Сил України, одна із ракет потрапила в автобус загинуло 13 та 18 осіб дістали поранення. Відразу бойові угруповання опублікували новину про знищення українського блокпоста на виїзді з Волновахи. Як згодом повідомив начальник головного командного центру Генерального штабу генерал Б. Бондар: в місті Докучаєвськ знаходилися кореспонденти російських та місцевих телеканалів з метою зняти, як українські військові будуть наносити удари у відповідь, але натомість було вжито заходів щодо стабілізації ситуації. Обстріл блокпосту мав на меті звинуватити Збройні Сили України в обстрілі Докучаєвська, викликаючи вогонь у відповідь на себе, таким чином дискредитувати українську Армію [4].

У лютому 2020 року усі ЗМІ та соціальні мережі обговорювали новину про українських громадян, які прилітають з Китаю, що спричинило поширення фейків та протестів. Першим написав про пасажирів літака С. Чередніченко,

який є прихильником Шарія. 19 лютого 2020 в соціальній мережі він робить пост - «Завтра всіх українців, які прибули з Китаю привезуть у санаторій в Нові Санжари. Санаторій. Інфекційних лікарень не знайшли. Керівництво району вже отримало розпорядження» (див. Рис. 2.6) [87].

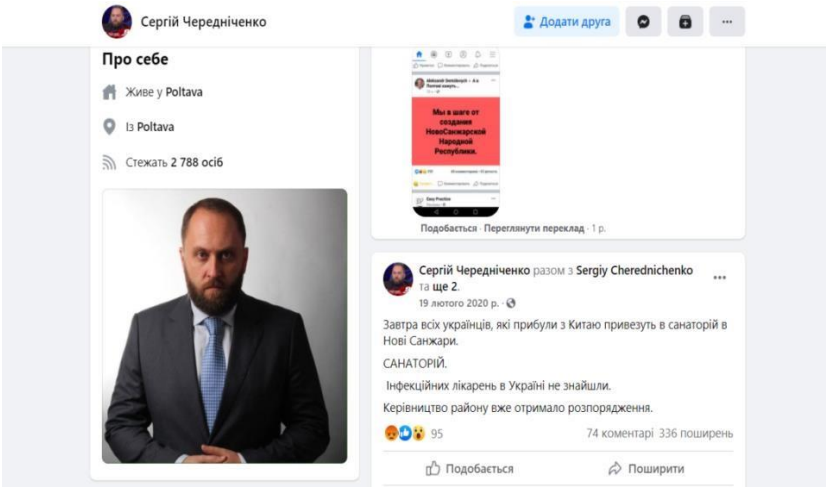

Рис. 2.6. Скріншот посту у соціальній мережі Facebook [87]

Пост пана Чередніченка мав 95 вподобайок та 336 поширень, що свідчить про штучну розгонку посту [87].

16 лютого 2021 року СБУ оголосило підозру за частиною першою статті 111 Кримінального кодексу України (державна зрада) [75]. «За даними СБУ Шарій з 2012 року, сприяв державним та неурядовим структурам російської федерації у проведенні спеціальних інформаційних операцій, використовуючи соціальні мережі, електронні засобі масової інформації, російські телевізійні канали» [75]. Наприклад, відео на Youtube каналі Шарія мав назву «День позора подошел к концу». Де з 7 хвилини 30 секунд починає обзивати громадян «животниє», а вкінці відео він називає 20 лютого 2020 року «днем позора», акцентуючи свою увагу на вшануванні загиблих у День Героїв Небесної Сотні, установлений Указом президента України № 69/2015 «Про вшанування подвигу учасників Революції гідності та увічнення пам'яті Героїв Небесної Сотні» [61].

Також Шарій дискредитує, маніпулює та поширює фейкову інформацію щодо діяльності Армії на Донбасі (див. Рис. 2.7, 2.8).

Рис. 2.7. Обґрунтування підозри СБУ [75]

Рис. 2.8. Обґрунтування підозри СБУ [75]

«18 липня 2019 року на сайті Український Мілітарний Портал виходить цикл статей російською мовою про Шарія, діяльність пропагандиста та роботу на користь спеціальних служб російської федерації. У першій частині цього циклу «Фейки Шарія – Шарий виправдовує вбивць українців. У першій частині досліджують та розвінчують його фейки щодо видавання російських військових та техніки за українську» [121].

«2 вересня 2014 року Шарій публікує відео у відеохостингу Youtube під

назвою «Как украинские СМИ над мертвым солдатом глумились». В цьому відео він розповідає про бій під Хрящуватим, а також показує підбитий танк та вбитого солдата, далі він показує інше відео із солдатами ворожої армії, які цей підбитий танк, оглядають. Шарій у своєму відео посилається на відео з відеохостингу Youtube «Хрящеватое Конец августа 2014 года». В цьому відео до підбитого танку підходить група військових, які танк називають «брошенной нацистской техникой», ця фраза є аргументом для Шарія. На відео «Хрящеватое 14 августа 2014г ВСУ», український командир танку розповідає, як він підбив ворожий танк, а інші військовослужбовці розглядають документи вбитих солдат, які виявились громадянами російської федерації. 55 секунда відео командир українського танку пробує прочитати напис на стволі танку, і не може прочитати бо напис згорів» [121].

26 липня 2014 року Шарій публікує відео «Про британскую журналистку», на захист британського громадянина Г. Філліпса (колишній позаштатний співробітник пропагандиських телевізійних каналів «Russia Today», «Звезда»). Пан Філліпс використовувався проти України в інформаційній війни, яку веде російська федерація. Дане відео із відеохостингу YouTube «Г. Филлипс. Донбасс. Канал рф «Звезда». Зима 2015, як приклад його участь в інформаційній війні проти України. На цьому відео Г. Филлипс сверджує, що «я не видел русские танки в Дебальцево», але на цьому відео «Грэм Филлипс. Дебальцево. Танки российской армии Т-72Б3 за 15 лютого 2015 року з 12 секунди пан Філліпс веде репортаж на фоні російських танків Т-72Б3 [121].

Таким чином, автором було досліджено питання інформаційних воєн, дезінформації, фейків, дискредитації Збройних Сил України, добровольчих батальйонів. Також було проаналізовано зразки інформаційних воєн, методи ведення інформаційної війни, які використовує російська федерація. На нашу думку, недовіра громадян України до державних інституцій, а також до самої держави в цілому, тільки підсилювала ворожу дезінформацію, фейки, манімупуляції. Російській Федерації це було легко зробити, оскільки України

сотні років перебувала у російськомовному інформаційному середовищі, яке паразитувало на питаннях «єдиного народу», «однієї країни» тощо. Автор робить висновок – якщо б держава починаючи з 1991 року займалася державною інформаційною політикою (патріотичне виховання, культурна пропаганда), освітою громадян, розвивала Збройні сили України, то можливо б такої катастрофи, яка сталась 2014 році та переросла у відкриту війну у 2022 року, не було. Відповідно нагально важливо для України проводити інформаційні кампанії щодо своєї культури, як всередині країни, так і на міжнародному рівні. Також державі варто «виховувати» своїх громадян, навчати їх бути громадянами своєї країни, починаючи із дошкільних навчальних закладів. За відсутністю державної інформаційної політики, інформаційне поле захоплює російська федерація яка формує інфопростір свідомо нав’язуючи свої наративи.

2.2 Інформаційна та національна безпека в добу пандемії COVID-19

На сайті Центру громадського здоров’я МОЗ України зазначено, що «вакцинація, це – безпечний, дієвий та простий захист населення від інфекційних захворювань» [23]. Після вакцинації імунна система вчиться створювати імунітет (антитіла) до інфекційних хвороб. Вакцини вводять ін’єкційно, і деякі через рот (перорально) та в ніс.

«Вакцинація необхідна для профілактики захворювань, зменшення смертності та контролю епідемій, пандемій. У 1796 році англійський вчений Е.Дженнер винайшов вакцину проти натуральної віспи та емпірично підтвердив, що вакцина формує імунітет від натуральної віспи. А вже у 1802 році з’являється карикатура намальована Дж. Гілрейем про те як люди бояться вакцинації, бо через вакцинацію проти натуральної віспи у них з’являться коровоподібні паростки» [103] (див. Рис. 2.9).

Рис. 2.9. Е. Дженнер вакцинує людей, які бояться, що через вакцинацію у них з’являться кровоподібні відростки. Дж. Гілрей 1802 р. [103]

Поширення вакцинонекерованих інфекційних хвороб є загрозою національній безпеці Україні, оскільки при не контрольованому поширенні інфекційних хвороб збільшується смертність населення, збільшується навантаження на систему охорони здоров’я, а також зменшується обороноздатність держави (як приклад хворіють військовослужбовці, як наслідок падає боєздатність підрозділу). Дуже активно поширювався антивакцинаторський рух в Україні та світі. Основними майданчиками для розповсюдження антивакцинальної інформації були соціальні мережі такі як Facebook, Twitter, Instagram та відеохостинг Youtube. 2 березня 2020 року відомий антивакцинатор З. Мілютін в соціальній мережі Facebook публікує пост про алюмінієвий вакцинальний ад’ювант, який спричиняє деякі захворювання, а також алюміній попадає в мозок та накопичується в м’язах. Аналітики в рамках партнерства з Facebook провели аналіз вищевказаного посту на ознаки неправдивої інформації та розмістили результати на сайті https://voxukraine.org/uk/» [81]. Мілютін вказує про шкідливість алюмінію та відсутність реакції імунної системи, хоча алюміній використовується у

вакцинах, як допоміжний засіб. Інформація про те, що імунна система не реагує є абсурдною, оскільки цей компонент дозволяє зменшити кількість доз вакцини [81].

«О. Ворожбит в статті «Інфлюенсери і «нульові пацієнти», який був опублікований 27 травня 2020 року на сайті tyzhden.ua пише про роль Кремля в розповсюдженні дезінформації стосовно вакцинації. Наприклад режисер Н. Міхалков розповсюджує інформацію на державному російському каналі про чипізацію населення планети Білом Ґейтсом, а «Первый канал» опублікував у 2020 році сюжет «Теорія змови чи таємна правда: чому Білла Ґейтса вважають архітектором COVID-19». Кремлівські пропагандисти формують свою теорію змови з уривку фільму «Event 21. The Global Pandemic Exercise». Фільм який створений для гри-симуляції пандемії. Але для російської пропаганди це фільм доказ «змови». Фонд Білла та Мелінди Ґейтс вкладають величезні кошти у розробку вакцин, лікування та попередження СНІДУ та туберкульозу та інші ініціативи. Фейк із чипом Білла Ґейтса з’явився вперше у США 18 березня 2020 року після питань-відповідей в соціальній мережі Reddit» [13] (див. Рис. 2.10).

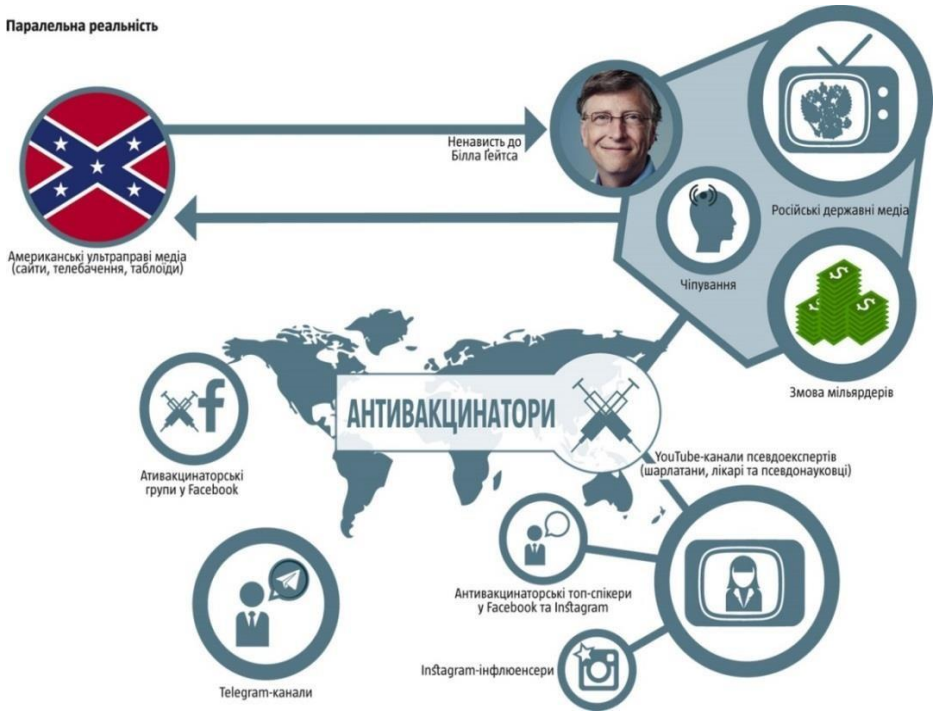

Рис. 2.10. Фейк про чип Білла Ґейтса [13]

У березні 2020 року ВООЗ оголосила пандемію у зв'язку з поширенням коронавірусної хвороби у світі. В Україні також було впроваджено карантин. Уряди країн Європейського Союзу вживали заходів для боротьби з глобальним поширенням COVID-19 та підтримки систем охорони здоров'я.

У Стратегії національної безпеки України-2020 визначено поширення COVID-19 як загрозу національній безпеці України [67]. Серед основних інформаційних загроз у сфері національної безпеки, пов'язаних із поширенням COVID-19, є зростання правопорушень в інформаційній сфері.

У Концепції розвитку сектору безпеки і оборони України серед нерозв'язаних проблем у секторі безпеки і оборони визначено «неефективність механізму запобігання та нейтралізації сучасних загроз національній безпеці України» [71]. «У Стратегії національної безпеки України 2020 р. проголошено, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека – найвища соціальна цінність в Україні, а також визначено, що однією із загроз національній безпеці України є поширення COVID-19. Крім того, поширення COVID-19 в Україні загострило та відкрило системні проблеми у сфері охорони здоров'я, біобезпеки й соціального захисту, недостатню готовність держави до дій у надзвичайних ситуаціях» [67].

Відповідно до Постанови Кабінету Міністрів України від 12 березня 2020 р. № 211, на території України запроваджено карантин [62], який пов'язаний із заходами запобігання поширенню COVID-19.

20 лютого 2020 року повернувся літак із евакуйованими з Уханю (Китай) громадянами України та іноземцями. Автобусами пасажирів літака повезли на обсервацію в Нові Санжари (Полтавська обл.). Автобуси із евакуйованими пасажирами місцеві мешканці зустріли протестом та сутичками із поліцією. Л. Величко у своїй статті «Майстри паніки. Як проросійська мережа в Україні організувала бунт в Нових Санжарах» [11] пише про організацію та підтримку паніки серед місцевих жителів в Нових Санжарах (див. Рис. 2.11, 2.12) [11].

Рис. 2.11. Зустріч мешканців евакуйованих з Уханю (Китай) на обсервацію в Нові Санжари (Полтавська обл.) [11]

Рис. 2.12. Скріншот із фейсбук- групи ГО «Голос Санжарщини» поширювався у вайбер-групах та в Інстаграмі ввечері 19 лютого [11]

В липні 2020 року Кримська правозахисна група опублікувала дослідження «Кримські медіа не надають людям вичерпної інформації про коронавірус (результати моніторингу), мета дослідження показати, як засоби масової інформації показуюсь ситуацію із пандемією в окупованому Криму.

Більшість публікацій у засобах масової інформації в період з квітня по червень 2020 року не мають критичної інформації щодо пандемії» [41].

У соціальній мережі Facebook 30 квітня 2021 року користувач під іменем Alexander Snesar поширив пост про інтерв'ю із доктором медичних наук А. Редьком, де пан Редько стверджує, що після щеплення проти COVID-19 «людина виділяє з себе вірус, вона захворіватиме у два рази частіше, ніж до щеплення, а хворіти – важче». Фактчекери із порталу StopFake досліди цю інформацію і становили, що це фейк, оскільки жодна вакцина, яка дозволена для застосування Всесвітньою організацією охорони здоров'я проти COVID-19, не має у складі живий вірус. Про те, що у вакцини проти COVID-19 має живого вірусу, також вказує Центр з контролю і профілактики захворювань США.

В соціальній мережі Facebook з'являлась інформація про те, що «в Ізраїлі вакцина від Pfizer «вбила» у 40 разів більше людей похилого віку, ніж коронавірус». Автори публікації наводять слова «інженера Хаїма Ятіва і доктора Ерве Селігмана», без жодних посилань на першоджерело [83]. 4 березня 2021 року цей фейк, що вакцинація викликає серйозну хворобу та приводить до смерті частіше, спростовує Міністерство охорони здоров'я Ізраїлю. «При визначенні ефективності вакцини вимірюється ризик зараження хворобою серед людей, вакцинованих двома дозами вакцини, в порівнянні з людьми, які не були вакциновані взагалі. Згідно з останніми даними було встановлено, що вакцина дуже ефективна щодо захворюваності, важкого перебігу захворювання, госпіталізацій і смертності». Висновки Міністерства охорони здоров'я Ізраїлю були зроблені на підставі звіту про ефективність щеплення проти COVID-19 відділу епідеміології Міністерства охорони здоров'я Ізраїлю .

«Глобальна мережа McAfee, що є одним з лідерів досліджень загроз у сфері кібербезпеки, зареєструвала зростання на 60,5% загальної кількості виявлених загроз в умовах COVID-19 за другий квартал 2020 р.» [109]. «У звіті за листопад 2020 р. розглядаються загрози та інциденти безпеки, які проявилися в умовах COVID-19 у другому кварталі 2020. Результати досліджень (третій

квартал до другого) показують: збільшення загроз, в середньому – 419 на хвилину, поява нових шкідливих програм для Office та їх зростання на 103%. Зловмисники атакували підприємства, уряди, школи і співробітників, які продовжували стикатися з проблемами, що пов'язані з обмеженнями COVID-19» [109]. «Найбільша кількість хмарних інцидентів сталася в Таїланді, менше – в США, Україна – за меншої їх кількості – на третьому місці після США і Гонконгу» [109].

«У другому кварталі 2020 року компанія McAfee зафіксувала близько 7,5 мільйона зовнішніх атак на хмарні облікові записи, збираючи дані про використання хмарних технологій від більш ніж 30 мільйонів користувачів по всьому світу. McAfee Labs нарахував 561 публічно розкритий випадок у другому кварталі 2020 р.». Розкриті випадки, були спрямовані на Північну Америку та становили 29% від загальної кількості інцидентів, зменшившись на 30% порівняно з попереднім кварталом. Розкриті інциденти, націлені на США в другому кварталі 2020 року, знизилися на 47%, у Великобританії – на 29%, а в Канаді – на 25% в порівнянні з попереднім кварталом [109]. Успішна інтеграція багатохмарного середовища створює реальні виклики для всіх секторів, зокрема для таких, як державний сектор. Керування безпекою в різних хмарах середовища можуть бути в переважній більшості ускладненими для IT-співробітники, тому їм потрібні інструменти, які можуть автоматизувати їх завдання та забезпечують постійний захист чутливої інформації, куди б вона не потрапляла всередину або поза хмарою.

«Відбувалося поширення злочинності в інформаційній сфері, спричиненої розповсюдженням COVID-19 у різних сферах життя людини та суспільства в цілому: зростання кількості шахрайств, які зумовлені продажем, а також придбанням медичних засобів або засобів індивідуального захисту та продуктів харчування, зокрема продажів у мережі «Інтернет» ліків для лікування COVID-19; поширення кіберзлочинності, зумовлене шахрайством у вигляді дзвінків чи смс-розсилок про фінансові компенсації державою витрачених на лікування коштів або інших виплат, які мають на меті поширення паніки серед населення

тощо» [34].

Ще однією загрозою, пов’язаною із застосуванням карантинних заходів COVID-19, є витік персональних даних громадян, які перебувають на лікуванні, карантині або самоізоляції. Держава зобов’язана забезпечувати достовірне інформування суспільства про COVID-19. Особливо важливим є недопущення поширення неправдивої чи некоректної інформації про COVID19. Однак, пандемія COVID-19 в інформаційному просторі України супроводжувалася поширенням фейків, які пов’язані із коронавірусом. З метою нівелювання цих процесів Кабінет Міністрів України та МОЗ публікували інформацію про COVID-19, окрім офіційних сайтів, на спеціально створених каналах та сайтах: Telegram, Viber, Facebook.

«Європейським Союзом прийнято низку документів з метою боротьби з дезінформацією про COVID-19: Action Plan against Disinformation (План дій проти дезінформації) та впроваджено Code of Practice on Disinformation (Кодекс практики проти дезінформації). Action Plan against Disinformation (План дій проти дезінформації) дезінформацію визначає, як оманливу, неправдиву інформацію, яка поширюється для введення суспільства в оману, що спричиняє шкоду суспільству» [92]. Code of Practice on Disinformation (Кодекс практики проти дезінформації) підписаний такими соціальними мережами як Facebook, Google, Twitter, Microsoft [96].

«Відповідно до закону про цифрові послуги, компанії, чиї онлайн-платформи мають відвідуваність на місяць у понад 10% населення ЄС, повинні здійснювати управління ризиками, проводити зовнішній і незалежний аудит, обмінюватися даними з органами влади і дослідниками та прийняти кодекс поведінки до серпня. 19 компаній мають стати орієнтиром у правилах ЄС щодо онлайн-контенту. До переліку компаній увійшли Google Maps, Google Play, Google Search, Google Shopping і YouTube від Alphabet, Facebook і Instagram від Meta, Marketplace від Amazon і App Store від Apple. Також у переліку підрозділи Microsoft Linkedin і Bing, Booking.com, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, Zalando та Alibaba від AliExpress. «Ми вважаємо, що ці 19

онлайн-платформ і пошукових систем стали систематично актуальними і несуть особливу відповідальність зробити інтернет безпечнішим», – заявив Т. Бретон, керівник Комісії з внутрішнього ринку ЄС. Компанії повинні будуть докласти більше зусиль для боротьби з дезінформацією, надати більше захисту та вибору користувачам і забезпечити сильніший захист для дітей, або ризикуватимуть штрафами до 6% від їхнього глобального обороту» [51].

Отже, автор проаналізував приклади інформаційних загроз в Україні та світі, пов’язаних з пандемією COVID-19. Серед основних інформаційних загроз у сфері національної безпеки, пов’язаних із поширенням COVID-19, є зростання правопорушень в інформаційній сфері. Зокрема, це стосується утворення конспірологічного руху Qanon та використання його під час інформаційних воєн. Було розглянуто питання кількості та масштабів поширення фейків та дезінформації під час обсервації в санаторії українських туристів з Китаю у Нових Санжарах Полтавської області. А також використання російською федерацією блогерів, іноземних громадян для поширення дезінформації та маніпуляцій проти Збройних сил України. Визначено, що антивакцинаторські рухи, які маніпулюючи інформацією спричиняють зменшення довіри громадян до вакцинації, що в свою чергу сприяє збільшенню захворюваності на інфекційні захворювання, збільшенню смертності населення та загрозу національної безпеки.

Висновки до другого розділу

1. Автором було досліджено питання інформаційних воєн, дезінформації, фейків, дискредитації Збройних Сил України, добровольчих батальйонів. Також було проаналізовано зразки інформаційних воєн, методи ведення інформаційної війни, які використовує російська федерація. На нашу думку, недовіра громадян України до державних інституцій, а також до самої держави в цілому,

тільки підсилювала ворожу дезінформацію, фейки, маніпуляції. Російській Федерації це було легко зробити, оскільки України сотні років перебувала у російськомовному інформаційному середовищі, яке паразитувало на питаннях «єдиного народу», «однієї країни» тощо. Автор робить висновок – якщо б держава починаючи з 1991 року займалася державною інформаційною політикою (патріотичне виховання, культурна пропаганда), освітою громадян, розвивала Збройні Сили України, то можливо б такої катастрофи, яка сталась 2014 році та переросла у відкриту війну у 2022 року, не було. Відповідно нагально важливо для України проводити інформаційні кампанії щодо своєї культури, як в середині країни, так і на міжнародному рівні. Також державі варто «виховувати» своїх громадян, навчати їх бути громадянами своєї країни, починаючи із дошкільних навчальних закладів. За відсутністю державної інформаційної політики, інформаційне поле захоплює російська федерація яка формує інфопростір свідомо нав’язуючи свої наративи.

2. Було проаналізовано особливості конспірологічного руху на прикладі Qanon та використання його під час інформаційних воєн, пропаганду, дезінформацію. Було розглянуто питання поширення фейків та дезінформації під час обсервації в санаторії українських туристів з Китаю у Нових Санжарах, Полтавської області. А також використання російською федерацією блогерів, іноземних громадян для поширення дезінформації та маніпуляцій проти Збройних сил України. Визначено, що антивакцинаторські рухи, які маніпулюючи інформацією спричиняють зменшення довіри громадян до вакцинації, що в свою чергу тягне за собою збільшення захворюваності на інфекційні захворювання, збільшення смертності населення та загрозу національній безпеці.

РОЗДІЛ 3
ШЛЯХИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Механізми державної політики щодо протидії загрозам в інформаційній сфері

В умовах «сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою і для України» [9].

В умовах російсько-українського конфлікту «захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави» [12].

До проблем гарантування інформаційної безпеки України «яка зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави»[24].

Коли з боку російської федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських

інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіазаходи відбувається вплив не лише на суспільну свідомість громадян України, а й на світову громадськість [12].

Авторка наукової статті «Кібервійна в Україні та виклики національній Безпеці: кібернапади на цифрову Інфраструктуру (державні установи, об'єкти критичної інфраструктури та організації третього сектору)» Г. Бондар зазначає що «кіберзлочинці використовують різноманітні методи отримання початкового доступу до своїх цілей, реалізуючи фішингові кампанії, використовуючи невиправлені вразливості локальних серверів Exchange і компрометацію постачальників IT-послуг. Цей початковий доступ дозволяє їм проводити операції зі знищення, вилучення даних, а також для довготривалого шпигунства та спостереження. Зловмисники часто змінюють своє шкідливе програмне забезпечення під час кожного застосування, щоб уникнути виявлення» [5].

Автори статті «Аналіз застосування існуючих технік розпізнавання фейкових новин для протидії інформаційній пропаганді» Є. Штефанюк, І. Опірський, О. Гарасимчук, опублікованої в електронному журналі «Безпека інформації» вказують на чотири особливості пропаганди російської федерації, а саме [87]:

1) «великий об'єм – це поширення великою кількістю користувачів та ЗМІ. Фактично створюючи ілюзію достовірності інформації;

2) неконсистентність це неузгодженість фейків із загальною пропагандою;

3) велика кількість каналів поширення – це ЗМІ, соціальні мережі, інформаційні портали;

4) фальсифікація та викривлення фактів» [87].

Критерії для ефективного виявлення фейків такі:

1) «знаходити фейки на ранній стадії;

2) коефіцієнт виявлення фейків має бути на високому рівні;

3) контент та реакцію користувачів на пости, повинні враховуватись;

4) враховувати, що у соціальних мережах можуть бути боти» [87].

Одним з головних прийомів кремлівських пропагандистів є «непослідовність, що має створити в свідомості аудиторії значний інформаційний хаос, наповнений великою кількістю «різноманітних правд». Незважаючи на зовнішню безсистемність, цей хаос створюється за добре відпрацьованим алгоритмом, на який працює вся машина дезінформації. Всі рівні пропаганди тут працюють разом: політики раз за разом проголошують нову «правду», яку моментально підхоплюють та розповсюджують провідні пропагандисти на телебаченні, в ЗМІ, соцмережах, месенджерах тощо (кожний канал точно відкалібрований відповідно до потреб одержувачів)» [82].

Одночасно прокремлівські тролі та боти в інтернеті намагаються максимально заповнити собою медіасередовище, створивши там відчуття масової підтримки війни в Україні, з одночасним тестуванням нових наративів, які, в залежності від ступеню успішності, або відкидаються, або стають готовими до застосування користувачами [82].

За задумом москви, інформаційна війна мала як підготувати ґрунт всередині українського суспільства напередодні збройної інтервенції, так і легітимізувати вторгнення на територію суверенної країни в очах росіян та міжнародної аудиторії, щоб отримати лояльність до дій російської влади.

В самому загальному вигляді алгоритм кремлівської брехні можна уявити як замкнутий цикл різноманітних, емоційно заряджених та суперечливих інформаційних версій, якими безперервно бомбардується аудиторія [82].

На яскравому та сучасному прикладі можемо побачити як російська пропаганда діє в Україні та як держава з цим бореться. Як запобігти та протидіяти загрозам в інформаційній сфері.

«Антизахідні наративи». Ця група наративів була переважно зосереджена на твердженні про те, що «війна в Україні була спровокована Заходом для власної вигоди, а Захід використовує Україну як пішака.

Рис. 3.1. Алгоритм російської пропаганди [82]

«Українці нападають на мирне населення та здійснюють інші військові злочини». Це повторюваний прокремлівський наратив, який намагається стверджувати, що Україна вчиняє військові злочини (див. Рис. 3.1). Провладні та ультраправі джерела поширили його на основі історії про те, що нібито українська ракета HIMARS убила 2 мирних жителів Донецької області» [82].

«Україна програє війну». Цей наратив припускає, що українська поразка неминуча, а Росія стабільно досягає успіху на полі бою, і тому нібито безглуздо намагатися вплинути на результат війни, підтримуючи Україну. За даними прокремлівських джерел, протягом 3 місяців щотижня Україна «втрачає Бахмут», а «український контрнаступ не вдасться». Це робиться, щоб підірвати життєво важливу військову підтримку України.

«Українські біженці». Ці наративи були переважно зосереджені на зображенні українських біженців як загрози безпеці Польщі, що польський уряд надає їм пріоритет над громадянами Польщі, а українські біженці у відповідь

невдячні країні, що її приймає. Українських біженців дезінформатори зображують як осіб, які переважно не тікають від війни, а прагнуть отримати прибуток за рахунок суспільства, яке їх приймає.

«Західні країни є русофобськими/російська культура піддається нападу». Теми, які піддавалися увазі в цьому контексті, здебільшого стосувалися Києво-Печерської лаври та домашнього арешту митрополита Павла. В цій напруженій ситуації, коли фейки, ІПСО стали майже щоденною практикою російських пропагандистів в українців зріс рівень недовіри до інформаційних джерел, що спричинило більш детальний аналіз (перевірку) матеріалів що публікуються у різних джерелах та месенджерах» [82].

За данним інтернет видання Детектор медіа, «кількість українців, які перевіряють інформацію на достовірність, за два роки (2020-2022) зросла майже вдвічі з 24% до 47%. 20% не стільки перевіряють, скільки шукають повнішу, деталізовану інформацію; не перевіряє медіаконтент менш як третина аудиторії (31%)» [51].

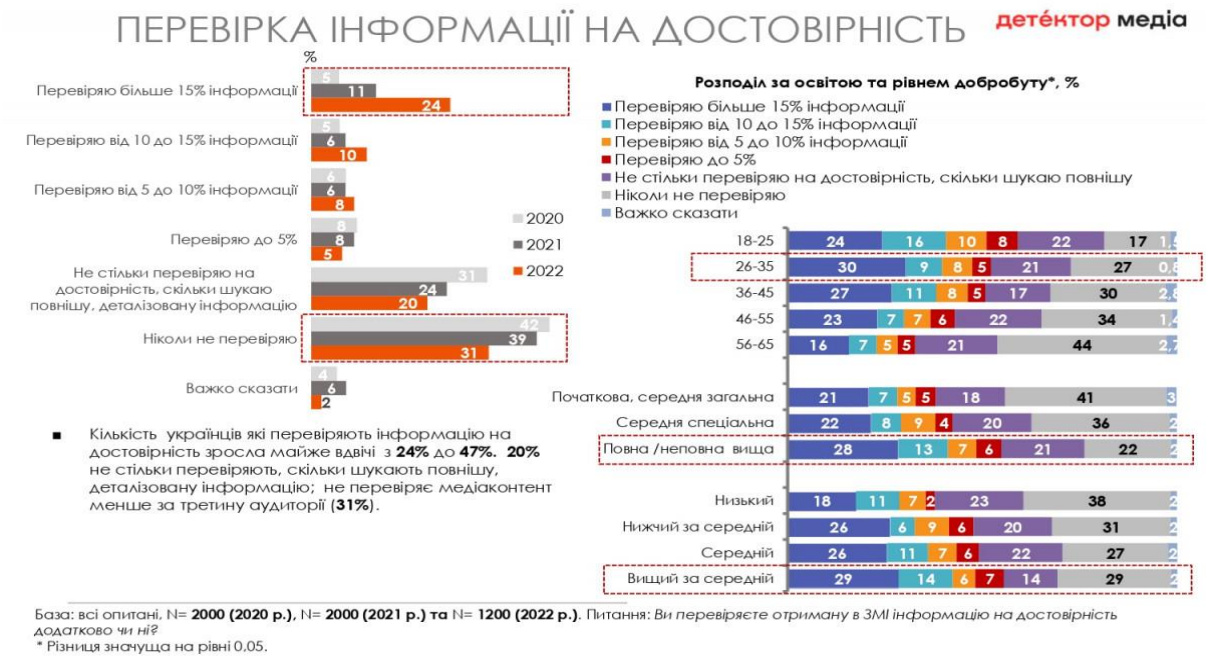

Рис. 3.2. Інфографіка «динаміка довіри до інформації» [51]

На Рис. 3.2 можна побачити,що більшість українців відмовилася і від

російської пропаганди, і від російських опозиційних ЗМІ – дослідження «Детектора медіа» [51].

В Україні в умовах війни існує величезна проблема захисту інформації, як персональних даних громадян, так і чутливої інформації (цілком таємної, інформація про персональні дані військовослужбовців тощо). Було багато випадків погроз у вигляді телефонних дзвінків та текстових повідомлень зі сторони Російської Федерації до ветеранів, діючих військовослужбовців, ветеранів та членам їх сімей. Були випадки витоку інформації із штабів про особовий склад батальйонів, рот, взводів тощо.

Рис. 3.3. П’ять основ російської дезінформації [52]

У звіті Державного департаменту США про дезінформацію описано «п’ять основ російської дезінформації» (див. Рис. 3.3**)** : «Офіційні комунікації уряду, Спонсоровані державою глобальні комунікації, Формування проксі-ресурсів, Соціальні медіа, як інфо-зброя, Підсилення дезинформації кібер-засобами. Інфографіка ідеально описує багатошарову суть російської дезінформації, а також класифікує кожну із п’яти основ відповідно до того, наскільки видимий чи заперечуваний зв’язок з РФ» [52].

Захист інформації про особовий склад Збройних Сил України. Важливим

джерелом про особливості захисту інформації про особовий склад Збройних Сил України є Аналітична записка «Як забезпечити захист штабної інформації, інформації про особовий склад ЗСУ» [35], де проаналізовано основні проблеми захисту інформації. Замовником визначено «Міністерство оборони України, Генеральний Штаб України. Мета вирішення проблеми визначена як захист інформації про особовий склад Збройних Сил України, впровадження кібербезпеки. Рекомендований варіант політики: Впровадження новітньої інформаційної системи на основі симетричного алгоритму блочного шифрування Advanced Encryption Standard (AES). Це дасть змогу підвищити обороноздатність, безпеку та захистити життя військовослужбовців та їх родин, оперативно прийняти рішення на полі бою, ефективно виконувати службу підрозділами Армії тощо» [56].

Також неодноразово витікала персональна інформація про пацієнтів. Так, 8 жовтня 2020 з'являється повідомленнями від Національного координаційного центру кібербезпеки при Раді безпеки і оборони України, який проводив моніторинг, про витік персональної інформації (медичні дані) найбільшої клініки Дніпра [3].

Таким чином, в Україні під час воєнного конфлікту виникла серйозна проблема щодо захисту інформації, як особистих даних громадян, так і конфіденційної інформації. Було багато випадків загроз, які здійснювалися шляхом телефонних дзвінків та повідомлень з боку Російської Федерації. Проаналізувавши різні технології маніпулюванням інформацією варто зазначити щоб ефективно протидіяти у сфері інформаційної безпеки України потрібна координація заходів, які здійснюються для забезпечення кібербезпеки суб'єктами забезпечення кібербезпеки відповідно до їх призначення (специфіки діяльності) та повноважень; взаємодія структур державного і приватного секторів на національному та міжнародному рівні з метою забезпечення адекватної відповіді кіберзагрозам; пріоритетність завдань і зосередження зусиль на забезпеченні захисту об'єктів критичної інформаційної інфраструктури; застосування новітніх технологій та передового досвіду для поліпшення

стану кіберзахисту об’єктів критичної інформаційної інфраструктури.

3.2. Інструменти та засоби формування політики у сфері інформаційної безпеки

Пріоритети державної політики в інформаційній сфері прописані у Доктрині інформаційної безпеки України [70] (див. Рис. 3.4).

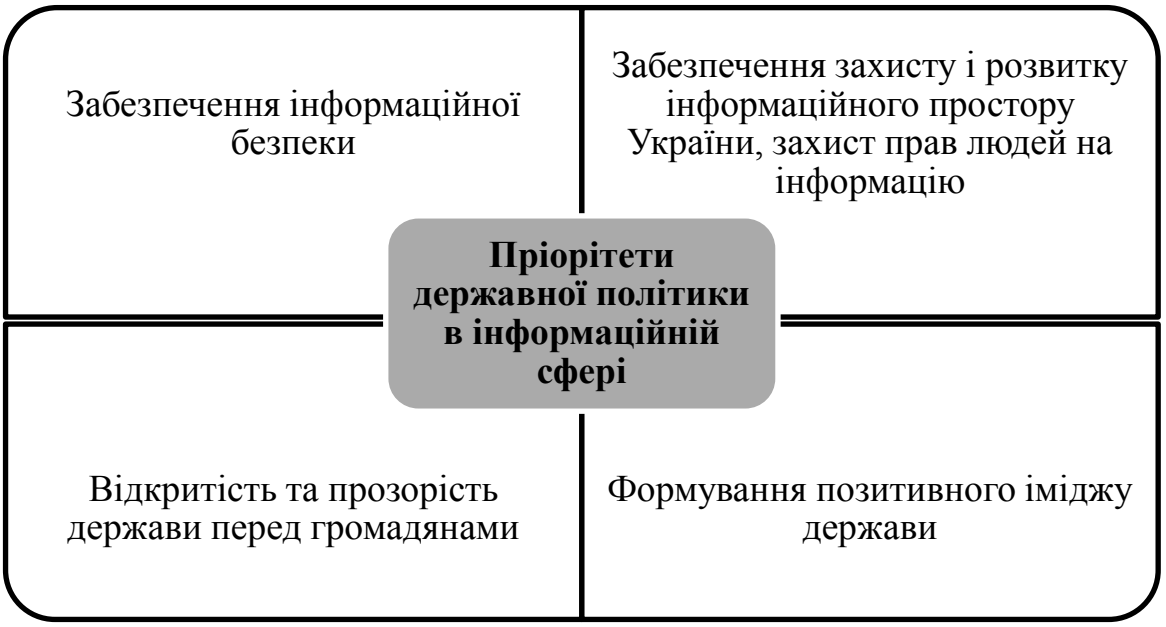

Рис. 3.4. Пріоритети державної політики в інформаційній сфері [70]

«Пріоритети державної політики в інформаційній сфері:

1) «щодо забезпечення інформаційної безпеки: створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет; забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій; розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України; боротьба з дезінформацією та деструктивною пропагандою з боку російської федерації; тощо» [70]

2) «щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію: стимулювання розвитку національного виробництва текстового і аудіовізуального контенту; розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист; удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці; пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз тощо» [70]

3) «щодо відкритості та прозорості держави перед громадянами: розвиток механізмів електронного урядування; проведення реформи урядових комунікацій; розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень; сприяння формуванню культури суспільної дискусії» Пріоритети державної політики в інформаційній сфері» [70];

4) «щодо формування позитивного міжнародного іміджу України: ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені; розвиток публічної дипломатії, у тому числі культурної та цифрової; сприяння поширенню та розвитку системи іномовлення України; створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства; участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності; запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини» [70].

Підходи до формування державної політики повинні випливати із того на, що саме ми будемо протидіяти та яку стратегічну ціль ми собі ставимо.

На даний час проти України ведеться новий тип військових дій, які

описані у так званій «Доктрині Герасимова» [111] і в першу чергу інформаційна війна ведеться проти цивільного населення. Тобто задача посіяти паніку, недовіру до політиків, а також до державних інституцій.

На думку аналітика з безпекових питань Ю. Костюченка «в інформаційній сфері вигоду від ведення бойових дій набувають не тільки держава агресор, а також окремі групи впливу у самій державі агресора. Тобто, головна задача держави агресора – це створення постійного конфлікту, всередині суспільства. Якщо громадяни вірять у фейки та ворожу пропаганду, то вона присутня в інформаційному середовищі держави» [90].

31 березня 2021 року при Міністерстві культури та інформаційної політики було створено Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ) з метою протидії дезінформації. ЦСКІБ об'єднав зусилля громадських організацій та влади у боротьбі із дезінформацією, швидкого реагування на фейки, а також для промоції українських наративів.

Основними напрямками діяльності ЦСКІБ передбачено такі (див. Рис. 3.5).

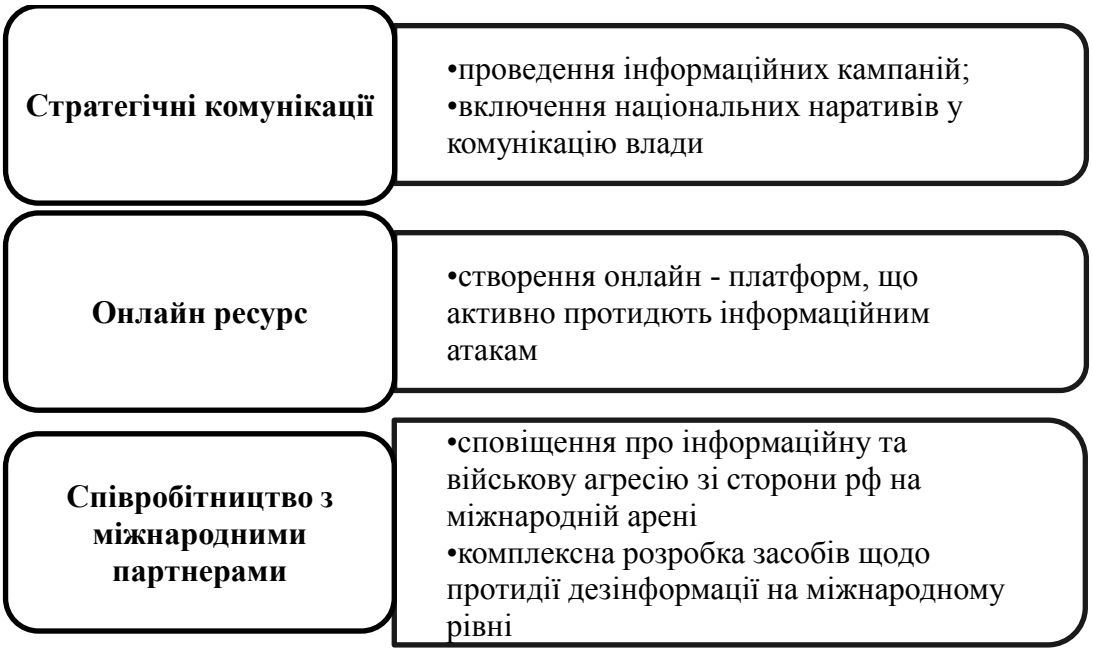

Рис. 3.5. Напрямки діяльності Центру стратегічних комунікацій та інформаційної безпеки

Наразі реалізується стратегія співробітництва у військовій сфері Україна

– НАТО, яке виконується відповідно до Річної національної програми під егідою Комісії Україна – НАТО в межах Робочого плану Військового комітету Україна – НАТО [76]. Завдання співробітництва у військовій сфері: «посилення обороноздатності та нарощення оперативних спроможностей Збройних Сил України у сучасних безпекових умовах; досягнення взаємосумісності Збройних Сил України зі збройними силами країн Альянсу; сприяння реформуванню та професіоналізації Збройних Сил України, впровадження у їх діяльність кращих військових стандартів; забезпечення участі Збройних Сил України у операціях з підтримання миру та безпеки під проводом Альянсу, залучення до Сил реагування НАТО. Починаючи з 2015 року збільшується військове співробітництво у сферах системи управління та зв'язку, кібербезпека, медичне забезпечення, логістика, стандартизація, стратегічні комунікації» [76].

Отже, технічні заходи в рамках державної політики забезпечення інформаційної безпеки мають бути спрямовані на: створення технологічної складової національної системи інформаційної безпеки, зокрема формування конкурентного середовища у сфері електронних комунікацій; розвиток технологій кіберзахисту, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку; удосконалення технічного захисту інформації, забезпечення регламентації процедури підтвердження відповідності засобів технічного захисту інформації; створення вітчизняних програмних продуктів для захисту державних інформаційних ресурсів, зокрема національної операційної системи, національного антивірусного програмного забезпечення.

Фінансово-економічні заходи мають бути спрямовані на створення економічних передумов для розвитку і забезпечення безпеки критичної інформаційної інфраструктури держави та її ресурсів, активізації інвестиційної діяльності держави у сферу високих технологій, збільшення державного бюджетного фінансування на потреби реалізації заходів щодо забезпечення інформаційної безпеки, збільшення обсягів на фінансування сектору безпеки і оборони України; створення конкурентоспроможної національної системи виробництва. Заходи державної політики у сфері забезпечення інформаційної

безпеки виховного та наукового спрямування мають передбачати: налагодження процесу підготовки кадрів у сфері кібербезпеки, забезпечення внесення змін до навчальних планів і програм середньої та вищої школи, підготовки наукових та науково-педагогічних кадрів; розробку загальнодержавних програм підвищення рівня обізнаності населення щодо кібервикліків. Потребують державної підтримки вітчизняні фундаментальні та прикладні дослідження, розробки у сфері інформатизації, телекомунікацій і зв'язку, необхідні активні загальнодержавні зусилля, спрямовані на підтримку та формування кадрового потенціалу у сфері забезпечення інформаційної безпеки.

Висновки до третього розділу

1. В Україні існує величезна проблема захисту інформації, як персональних даних громадян, так і чутливої інформації (цілком таємної, інформація про персональні дані військовослужбовців тощо). Технічні заходи в рамках державної політики забезпечення інформаційної безпеки мають бути спрямовані на: створення технологічної складової національної системи інформаційної безпеки, зокрема формування конкурентного середовища у сфері електронних комунікацій; розвиток технологій кіберзахисту, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку; удосконалення технічного захисту інформації.

2. Технічні заходи в рамках державної політики забезпечення інформаційної безпеки мають бути спрямовані на: створення технологічної складової національної системи інформаційної безпеки, зокрема формування конкурентного середовища у сфері електронних комунікацій; розвиток технологій кіберзахисту, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку; удосконалення технічного захисту інформації,

забезпечення регламентації процедури підтвердження відповідності засобів технічного захисту інформації; створення вітчизняних програмних продуктів для захисту державних інформаційних ресурсів, зокрема національної операційної системи, національного антивірусного програмного забезпечення. Фінансово-економічні заходи мають бути спрямовані на створення економічних передумов для розвитку і забезпечення безпеки критичної інформаційної інфраструктури держави та її ресурсів, активізації інвестиційної діяльності держави у сферу високих технологій, збільшення державного бюджетного фінансування на потреби реалізації заходів щодо забезпечення інформаційної безпеки, збільшення обсягів на фінансування сектору безпеки і оборони України; створення конкурентоспроможної національної системи виробництва.

ВИСНОВКИ

1. Державна політика з інформаційної безпеки має бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки для всіх суб'єктів господарювання, державної влади, усіх громадян країни. Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян. Проблеми, що пов'язані з інформаційною безпекою держави варто розглядати у взаємозв'язку з іншими проблемами, які виникають у світовому просторі, національній економіці, соціальній, демографічній сфері тощо. Вагомість інформаційної безпеки в системі національної безпеки України визначається й активізацією ризиків в інформаційній сфері, зокрема, веденням інформаційних війн. З різних визначень науковців та законодавства терміну «інформаційна безпека», є спільна риса – це запобігання нанесенню шкоди в будь-якій формі.

2. Міжнародна інформаційна безпека реалізується в доктринах, стратегіях, законах держав і міжнародних організацій, зокрема, Організації Об'єднаних Націй, Європейського Союзу, Ради Європи, НАТО. Резолюції Генеральної Асамблеї ООН визначили напрями боротьби зі злочинним використанням інформаційних технологій, створенням глобальної культури кібербезпеки, захистом інформаційних інфраструктур, сприянням розгляду існуючих та потенційних загроз у сфері інформаційної безпеки. На початку 2000-х років органами ЄС було прийнято цілу низку нормативно-правових актів, які передбачають різноманітні підходи забезпечення інформаційної безпеки в державах-членах ЄС.

В Україні на сьогоднішній день існує значна кількість законодавчих та нормативно-правових актів, які регулюють питання інформації та національної безпеки. Зокрема, актуальними загрозами національним інтересам та

національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур; інформаційне домінування держави-агресора на тимчасово окупованих територіях; неефективність державної інформаційної політики.

3. Таким чином, аналіз позитивних здобутків країн світу має важливе значення при розбудові системи забезпечення інформаційної безпеки України. Більшість країн світу усвідомлюють безпосередню залежність свого добробуту від інформаційної сфери, відтак, питання забезпечення інформаційної безпеки закономірно посідає одне з чільних місць у безпекових стратегіях відповідних держав. Активну політику у сфері забезпечення інформаційної безпеки проводить не лише НАТО, ООН, але й ЄС, який сьогодні об’єднує розвинуті країни, які відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав, зокрема, в інформаційній сфері. Інформаційна безпека Європейського Союзу ґрунтується на використанні численних рекомендацій, які викладені в міжнародних стандартах. Визначившись із зовнішньополітичним курсом, Україна має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері.

4. Автором було досліджено питання інформаційних воєн, дезінформації, фейків, дискредитації Збройних Сил України, добровольчих батальйонів. Також було проаналізовано зразки інформаційних воєн, методи ведення інформаційної війни, які використовує російська федерація. На нашу думку, недовіра громадян України до державних інституцій, а також до самої держави в цілому, тільки підсилювала ворожу дезінформацію, фейки, маніпуляції. Російській

Федерації це було легко зробити, оскільки України сотні років перебувала у російськомовному інформаційному середовищі, яке паразитувало на питаннях «єдиного народу», «однієї країни» тощо. Автор робить висновок – якщо б держава починаючи з 1991 року займалася державною інформаційною політикою (патріотичне виховання, культурна пропаганда), освітою громадян, розвивала Збройні сили України, то можливо б такої катастрофи, яка сталась 2014 році та переросла у відкриту війну у 2022 року, не було. Відповідно нагально важливо для України проводити інформаційні кампанії щодо своєї культури, як в середині країни, так і на міжнародному рівні. Також державі варто «виховувати» своїх громадян, навчати їх бути громадянами своєї країни, починаючи із дошкільних навчальних закладів. За відсутністю державної інформаційної політики, інформаційне поле захоплює російська федерація яка формує інфопростір свідомо нав’язуючи свої наративи.

Було проаналізовано особливості конспірологічного руху на прикладі Qanon та використання його під час інформаційних воєн, пропаганду, дезінформацію. Було розглянуто питання поширення фейків та дезінформації під час обсервації в санаторії українських туристів з Китаю у Нових Санжарах, Полтавської області. А також використання російською федерацією блогерів, іноземних громадян для поширення дезінформації та маніпуляцій проти Збройних сил України. Визначено, що антивакцинаторські рухи, які маніпулюючи інформацією спричиняють зменшення довіри громадян до вакцинації, що в свою чергу тягне за собою збільшення захворюваності на інфекційні захворювання, збільшення смертності населення та загрозу національній безпеці.

5. В Україні існує величезна проблема захисту інформації, як персональних даних громадян, так і чутливої інформації (цілком таємної, інформація про персональні дані військовослужбовців тощо). Технічні заходи в рамках державної політики забезпечення інформаційної безпеки мають бути спрямовані на: створення технологічної складової національної системи інформаційної безпеки, зокрема формування конкурентного середовища у сфері

електронних комунікацій; розвиток технологій кіберзахисту, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв’язку; удосконалення технічного захисту інформації,

6. Технічні заходи в рамках державної політики забезпечення інформаційної безпеки мають бути спрямовані на: створення технологічної складової національної системи інформаційної безпеки, зокрема формування конкурентного середовища у сфері електронних комунікацій; розвиток технологій кіберзахисту, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв’язку; удосконалення технічного захисту інформації, забезпечення регламентації процедури підтвердження відповідності засобів технічного захисту інформації; створення вітчизняних програмних продуктів для захисту державних інформаційних ресурсів, зокрема національної операційної системи, національного антивірусного програмного забезпечення. Фінансово-економічні заходи мають бути спрямовані на створення економічних передумов для розвитку і забезпечення безпеки критичної інформаційної інфраструктури держави та її ресурсів, активізації інвестиційної діяльності держави у сферу високих технологій, збільшення державного бюджетного фінансування на потреби реалізації заходів щодо забезпечення інформаційної безпеки, збільшення обсягів на фінансування сектору безпеки і оборони України; створення конкурентоспроможної національної системи виробництва.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. 100+ відповідей на запитання про вакцинацію проти COVID-19 для медичних працівників та пацієнтів URL: https://drive.google.com/file/d/1L0r19z2S8IW19aNp4jCE_ob4YzcDM4rx/view?fbclid=IwAR3RxZE8Fgy4

2. Автобус з цивільними під Волновахою розстріляли задля російських журналістів. Espreso від 13 січня 2015 URL: https://espreso.tv/news/2015/01/13/avtobus_z_cyvilnymy_pid_volnovakhoyu_rozstrilyaly_zadlya_rosiyskykh_zhurnalistiv

3. Агентство національної безпеки (англ. National Security Agency), URL: https://cutt.ly/VysoEXZ

4. Бійці «Азова» у жартівливому відео підняли американський прапор над Широкіним. Unian. URL: https://www.unian.ua/society/1063441-biytsi-azova-u- jartivlivomu-video-pidnyali-amerikanskiy-prapor-nad-shirokinim.html

5. Бондар Г. (2022). Кібервійна в Україні та виклики національній безпеці: кібернапади на цифрову інфраструктуру (державні установи, об’єкти критичної інфраструктури та організації третього сектору. Публічне управління та регіональний розвиток, (15), 30-67. URL: https://doi.org/10.34132/pard2022.15.02

6. Бондар Г., Гаркуша А. (2019). Інформаційна політика та етика в добу діджиталізації. Публічне управління та митне адміністрування, № 4 (23). Режим доступу: https://doi.org/10.32836/2310-9653-2019-4-27-33

7. Боровська А., Гнатюк С. та інші. Стан та проблеми забезпечення державної інформаційної політики: зона проведення АТО та окуповані території. Аналітична доповідь. [Авт. кол]. К. : НІСД, 2016. URL: https://niss.gov.ua/sites/default/files/2016-12/AD_InfoStrat-8505e.pdf

8. Буга Л.В. Досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах. Наукові записки Львівського

університету бізнесу та права. Том 19 (2018). – С. 174-178. URL: https://nzlubp.org.ua/index.php/journal/article/download/68/66/

9. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. с. 7. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

10. В Україні день жалоби за загиблими під час пожежі в Одесі. Укрінформ, 08.12.2019 URL: https://www.ukrinform.ua/rubric-society/2833516-v-ukraini-den-zalobi-za-zagiblimi-pid-cas-pozezi-v-odesi.html

11. Величко Л. Майстри паніки. Як проросійська мережа в Україні організувала бунт в Нових Санжарах. Texty.org.ua. URL: https://texty.org.ua/articles/100356/specoperaciya-imeni-portnova-ta-shariya-yak-rozhanyaly-paniku-v-novyh-sanzharah-i-hto-za-cym-stoyit/

12. Войціховський А. (2020). Інформаційна безпека як складова системи національної безпеки. Вісник Харківського національного університету імені В.Н.Каразіна. Серія «Право», (29), 281-288. URL: https://periodicals.karazin.ua/law/article/view/15648

13. Ворожбит О. Інфлюенсери і «нульові пацієнти». Український тиждень. 27.05.2020. URL: https://tyzhden.ua/Pandemic/243855

14. Всеукраїнський форум «Україна 30. Безпека країни». 11.05.2021. URL: https://ukraine30.com/national_security/

15. Всеукраїнський форум «Україна 30». URL: https://ukraine30.com/#task- forum-home

16. Говлет М., Рамеш М. Дослідження державної політики: цикли та підсистеми політики; [пер. з англ. О. Рябова]. Львів : Кальварія, 2004. 264 с. URL: https://issuu.com/irf_ua/docs/govlet_studying_public_policy-2004

17. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія [Авт. кол]. – К.: Інтертехнологія, 2009.

18. Гребенюк М.В., Леонов Б.Д., Досвід Ізраїлю у сфері забезпечення кібербезпеки. Інформація і право, 2018, № 2(25). – С. 45-50. URL:

http://ippi.org.ua/sites/default/files/6_9.pdf

19. Гуцалюк М. В. Організація захисту інформації : [навч. посібн.]. К. : Альтерпрес, 2012. 224 с.

20. Дай Томас Р. «Основи державної політики». Р. 1. Аналіз політики. Р. Модель політики: підр. для ВНЗ. Одеса: АО БАХВА, 2005. 468 с. URL: https://books.google.com.ua/books?hl=uk&lr=&id=gYwzprJAEDAC&oi

21. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Х. : Фоліо, 2002. 285 с.

22. Державна політика : підручник / Нац. акад. держ. упр. при Президентові України ; ред. кол. : Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови) [та ін.]. К. : НАДУ, 2014. 448 с. URL: http://academy.gov.ua/NMKD/library_nadu/Pidruchnuiky_NADU/9fa81bc0-991f-47e7-817d-a853b8627f97.pdf

23. Державна установа «Центр громадського здоров'я Міністерства охорони здоров'я України». Вакцинація. URL: https://www.phc.org.ua/news/vse-scho-varto-znati-pro-vakcinaciyu

24. Дмитренко М. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія «Політичні науки». 2017, №17. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3318

25. Ємельянов В., Бондар Г. (2019). Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. Публічне управління та регіональний розвиток, (5), 493-523. URL: https://doi.org/10.34132/pard2019.05.02

26. Загибель дітей на окупованих територіях: як Росія ескалує ситуацію в інформаційному полі. URL: https://www.ukrinform.ua/zagibel-ditej-na-okupovanih-teritoriah-ak-rosia-eskalue-situaciu-v-informacijnomu- poli.html

27. Закон Мура : URL: https://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf

28. ЗеДжокер і президентський стендап. Джеркало Тижня, 25.10.2019, URL: https://zn.ua/ukr/internal/zedzhoker-i-prezidentskiy-stendap-327411_.html

Біла книга спеціальних інформаційних операцій проти України, 2014 2018: наук.-популярне вид. [Колектив експертів Міністерства інформаційної політики України під заг. ред. Золотухіна Д.Ю.]. К., 2018. 384 с. URL: https://mip.gov.ua/files/pdf/white_book_2018_mip.pdf

29. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ : НІСД, 2015. 176 с.

30. Знайдіть корисного ідіота. 7 заповідей російської дезінформації. Texty.org.ua. 2018-12-03 URL: https://texty.org.ua/articles/89724/Znajdit_korysnogo_idiota_7_zapovidej_rosijskoji_dezinformaciji

31. Золотар О. Загрози інформаційній безпеці людини. Журнал «Правова інформатика». №2(42)/2014. URL: http://ippi.org.ua/sites/default/files/14zooibl.pdf

32. Інформаційна безпека (соціально-правові аспекти) : підручник / [В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк та ін.] ; за ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с.

33. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» / В. І. Гур'єв, Д. Б. Мехед, Ю. М. Ткач, І. В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%D0BD%D1%84

34. Калініна А.В. Вплив світової пандемії коронавірусу на стан злочинності. Держава і злочинність. Нові виклики в епоху постмодерну : збірник тез доп. наук.-практ. конф. / МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНАДУ 2020. С. 36–38.

35. Командування Сил спеціальних операцій ЗС України, 12 лютого 2021 URL: https://www.facebook.com/usofcom/posts/2934505563447735

36. Коментар Посольства щодо заяви сенаторки Н.Гуле у ефірі France Inter URL: https://france.mfa.gov.ua/news/5518-komentar-posolystva-shhodo-zajavi-senatorki-ngule-u-jefiri-france-inter

37. Кондратюк Т.В. Концептуальні моделі як відображення різних аспектів державної управлінської політики. Науковий вісник Академії муніципального управління. Серія : Управління. – 2012. – Вип. 1. С. 133. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cg_64. Nvamu_upravl_2012_1.pdf

38. Конспірологи з QAnon разом з іншими штурмували Капітолій. Розробник ігор аналізує, як функціонує цей рух. texty.org.ua. 2021-01-26 URL: https://texty.org.ua/articles/102817/

39. Конституція України (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141). URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

40. Концепція створення державної системи захисту критичної інфраструктури. URL: https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi- stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi

41. Кримські медіа не надають людям вичерпної інформації про корона вірус (результати моніторингу), Колектив авторів, 15.07.2020 URL: https://crimeahrg.org/uk/krimski-media-ne-nadayut-lyudyam-vicherpno%d1%97-informaczi%d1%97-pro-koronavirus-rezultati-monitoringu/

42. Лазарева А. Чи є табори джихадистів під Дніпропетровськом? Про розмови з Наталі Гулею. Тиждень. ua. 4.04.2016 URL: http://tyzhden.ua/World/162250

43. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України. К.: Текст, 2003. 600 с.

44. Міністерство культури та інформаційної політики. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: https://mkip.gov.ua/news/5234.html

45. Місія ОБСЄ з’ясувала подробиці загибелі хлопчика в ОРДЛО URL: https://www.ukrinform.ua/rubric-ato/3222669-misia-obse-zasuvala-podrobici-zagibeli-hlopcika-v-ordlo.html

46. Мороз О. Коли підгорає. 10 пасток в Facebook, які змушують вас поширювати брехню. Texty.org.ua від 18.02.2020. URL: https://texty.org.ua/articles/99962/Koly_pidgoraje_10_pastok_v_facebook_jaki-

99962/

47. «М’яка сила» Кремля в дії: як Росія експортує свій «культурний продукт» в Україну». Укрінформ, 28 квітня 2021 URL: https://www.ukrinform.ua/-maka-sila-kremla-v-dii-ak-rosia-eksportue-svij-kulturnij-produkt-v-ukrainu.html

48. Негодченко В. Основні напрями державної інформаційної політики в Україні. Інформаційне право, 2016, №4. URL: http://pgp-journal.kiev.ua/archive/2016/04/15.pdf

49. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40-45. URL: http://visnyk.academy.gov.ua/wp-content/uploads/2014/02/2013-3-8.pdf

50. Окінавська хартія глобального інформаційного суспільства. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text

51. Офіційний сайт громадської платформи Детектор Медіа: Режим доступу: https://go.detector.media/

52. Офіційний сайт Українського кризового медиа центру: URL: https://uacriss.org/uk/

53. Павлов Д. М., Микитюк М. А. Правові та організаційні засади забезпечення захисту критичної інфраструктури у контексті формування нової безпекової парадигми України. Науковий журнал «Честь і закон». Том 4 № 75 (2020). URL: http://www.drs.gov.ua/wp-content/uploads/2020/07/5854-ob.pdf

54. Пал Л.А. Аналіз державної політики. Основи, 1999. – 424 с. URL: http://kyiv-heritage.com/sites/default/files/%D0%9F%D0%90%D0%9B%20-%B5%D1%80%D0%B6%20%D0%BF%D0%%201999%20424%D1%81.pdf

55. Панченко В.М. у своїй праці «Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання». Інформація і право, № 3(12) / 2014, с. 13-14. URL: http://ippi.org.ua/sites/default/files/14pvmupm.pdf

56. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. Серія: державне управління. № 3 (2019). URL:

http://periodica.nadpsu.edu.ua/index.php/governance/article/view/296

57. Партнерство заради миру, Рамковий документ. URL: https://zakon.rada.gov.ua/laws/show/950_001#Text

58. Почепцов Г. Сучасні інформаційні війни. К.: Видавничий дім «Києво-Могилянська академія», 2015. 497 с.

59. Правові засади співробітництва Україна – НАТО Режим доступу: https://nato.mfa.gov.ua/dokumenti/pravovi-zasadi-spivrobitnictva-ukrayina-nato

60. Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору): Закон України від 7 лютого 2019 р. URL: https://zakon.rada.gov.ua/laws/show/2680-19#n2

61. Про вшанування подвигу учасників Революції гідності та увічнення пам'яті Героїв Небесної Сотні, Указ Президента України № 69/2015 URL: https://www.president.gov.ua/documents/692015-18468

62. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARSCoV-2: Постанова КМУ України від 11.03.2020 № 211. URL: https://zakon.rada.gov.ua/laws/show/211- 2020-п

63. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

64. Про критичну інфраструктуру: Закон України, від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

65. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII URL: https://cutt.ly/Ct5Fcca

66. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 року № 537-V URL: https://zakon.rada.gov.ua/laws/show/537-16#top

67. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року Указ Президента України «Про Стратегію національної безпеки України» від 14 вересня 2020 року № 392/2020. URL:

https://www.president.gov.ua/documents/3922020-35037

68. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України», Указ Президента України Офіційний вісник Президента України від 09.10.2015 р., № 78, стор. 38, стаття 2592, URL: https://cutt.ly/nt5Vhe0;

69. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», Указ Президента України Офіційний вісник Президента України від 05.04.2016 р., № 10, стор. 39, стаття 198, URL: https://cutt.ly/Zt5GfpO

70. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року Указ Президента України «Про Доктрину інформаційної безпеки України» поточна редакція від 25.02.2017, URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

71. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України», № 92/2016. Указ Президента України. URL: https://zakon.rada.gov.ua/laws/show/92/2016#n2

72. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року Указ Президента України, «Про Стратегію національної безпеки України», Офіційний вісник Президента України від 03.06.2015 р., № 13, стор. 50, стаття 874, URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text;

73. Російський артист Morgenshtern під час виступу в Одесі… від 09 грудня 2019 року. URL: https://afisha.24tv.ua/rosiyskiy_artist_morgenshtern_pid_chas_vistupu_v_odesi

74. Савченко Гліб. Коротка історія QAnon. Що це за теорія змови. 12 січня 2021. URL: https://www.bbc.com/ukrainian/features-55629653

75. СБУ оголосила про підозру відомому проросійському пропагандисту Шарію, URL: https://ssu.gov.ua/novyny/sbu-oholosyla-pro-pidozru-vidomomu-prorosiiskomu-propahandystu-shariiu

76. Співробітництво Україна – НАТО у військовій сфері. URL:

https://nato.mfa.gov.ua/ukrayina-ta-nato/spivrobitnictvo-ukrayina-nato-u-vijskovij-

77. Тарасюк А. В. Співвідношення інформаційної та кібернетичної безпеки. Інформація і право. № 4(31) / 2019. – с. 73. Режим доступу: http://ippi.org.ua/sites/default/files/11_13.pdf

78. Тертичка В. Аналіз державної політики і політологія. Політичний менеджмент. №6, 2004. URL: http://dspace.nbuv.gov.ua/bitstream/handle/1/11578/01- Tartuchka.pdf?sequence=1

79. Ткачук Т.Ю. Забезпечення інформаційної безпеки в країнах Центральної Європи. Юридичний науковий журнал. №5/2017. С. 104-110. URL: http://lsej.org.ua/5_2017/30.pdf

80. Ткачук Т.Ю., Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. Інформація і право, 2017. № 4(23). С. 62-72. URL: http://ippi.org.ua/sites/default/files/8_6.pdf

81. Токсичний алюміній у вакцинах викликає аутоімунні захворювання та невропатології. Vox Ukraine. Аналітична платформа, 14 липня 2020. URL: https://voxukraine.org/uk/fejk-toksichnij-alyuminij-u-vaktsinah-viklikaye-autoimunni-zahvoryuvannya-ta-nevropatologiyi/

82. Тренди дезінформації та пропаганди в соціальних медіа Півдня України за 5 місяців війни. URL: https://intent.press/publications/medialiteracy/2022/trendi-dezinformaciyi-ta-propagandi-v-socialnih-media-pivdnya-ukrayini-za-5-misyaciv-vijni/

83. Фейк: В Ізраїлі вакцина від Pfizer «вбила» у 40 разів більше людей похилого віку, ніж коронавірус. URL: https://www.stopfake.org/uk/fejk-v-izrayili-vaktsina-vid-pfizer-vbila-u-40-raziv-bilshe-lyudej-pohilogo-viku-nizh-koronavirus/

84. Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору. Дата підписання та набуття чинності: 09.07.1997. URL: https://zakon.rada.gov.ua/laws/show/994_002#Text

85. Центр Стратегічних Комунікацій та Інформбезпеки. URL: https://www.facebook.com/StratcomCenterUA

86. Цибульська назвала цинічними російські заяви про «Сребреницю» на

Сході України. URL: https://www.ukrinform.ua/rubric-polytics/3226041-cibulska-nazvala-cinicnimi-rosijski-zaavi-pro-srebrenicu-na-shodi-ukraini.html

87. Чередніченко С. facebook.com від 19 лютого 2020 року. URL: https://www.facebook.com/permalink.php?story_fbid=2517384035203212&id=1000

88. Шевчук О.М. Covid-19 як загроза національній безпеці України. Юридичний науковий електронний журнал Запорізького національного університету № 1/2021. URL: http://www.lsej.org.ua/1_2021/53.pdf

89. Штефанюк Є. Ф., Опірський І. Р., Гарасимчук О. І. Аналіз застосування існуючих технік розпізнавання фейкових новин для протидії інформаційній пропаганді. Безпека інформації, том 26, № 3 (2020). – С. 139-144. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/14942

90. Шторгін І. Якою має бути інформаційна політика України в умовах війни? Radio svoboda. URL: https://www.radiosvoboda.org/a/28338927.html

91. A Game Designer’s Analysis Of QAnon. Medium. URL: https://medium.com/curiouserinstitute/

92. Action Plan against Disinformation. Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions. URL: https://ec.europa.eu/newsroom/dae/document.cfm?docid=56166

93. Code of Practice on Disinformation. European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

94. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, 2012. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf

95. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: https://ec.europa.eu/digital-single- market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

96. Directive 95/46/EC (General Data Protection Regulation) URL: https://eur- lex.europa.eu/eli/reg/2016/679/oj

97. European Cybercrime Centre (EC3) URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

98. European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa

99. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

100. Resolution Adopted by the General Assembly. 04.12.1998. A/RES/53/70 Developments in the field of information and telecommunications in the context of international security». URL: https://undocs.org/en/A/RES/53/70

101. Динаміка користування топ-джерелами інформації. URL: https://detector.media/infospace/article/164308/2019-03-21-dzherela-informatsii-mediagramotnist-i-rosiyska-propaganda-rezultaty-vseukrainskogo-opytuvannya-gromadskoi-dumky/

102. Структура наративів. URL: https://imi.org.ua/monitorings/dyskredytatsiya-bajdena-ta-ukrayina-vynna-u-vijni-antyzahidni-ta-prorosijski-naratyvy-v-ukrayinskyh-i39592

103. Топ медіа з антизахідними та проросійськими наративами. URL: https://imi.org.ua/infographics/prorosijski-ta-antyzahidni-naratyvy-v-ukrayinskyh-media-i39889