

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ  
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН  
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ  
ТА РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач випускової кафедри

\_\_\_\_\_ Ніна РЖЕВСЬКА

« \_\_\_\_\_ » \_\_\_\_\_ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА  
ЗДОБУВАЧКИ ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР  
ЗА СПЕЦІАЛЬНІСТЮ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ  
КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»  
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ  
«МІЖНАРОДНА ІНФОРМАЦІЯ»

**Тема: «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В  
СОЦІАЛЬНИХ МЕРЕЖАХ В УМОВАХ ПОВНОМАСШТАБНОЇ ВОЄННОЇ  
АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ»**

Виконавець: здобувачка вищої освіти 4 курсу, 409Б групи, Калниболотська  
Єлизавета Володимирівна

Керівник: кандидат політичних наук, доцент кафедри міжнародних відносин,  
інформації та регіональних студій Мороз Андрій Сергійович

Нормоконтролер:

Валентина ЄМЕЦЬ

КИЇВ 2022

## ЗМІСТ

ВСТУП .....	3
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ФЕНОМЕНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІАЛЬНИХ МЕРЕЖАХ.....	6
1.1 Поняття та історія виникнення соціальних мереж .....	6
1.2 Вплив соціальних мереж на інформаційну безпеку країни .....	11
1.3 Проблеми захисту національних інтересів України в соціальних мережах .....	15
РОЗДІЛ 2. ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В СОЦІАЛЬНИХ МЕРЕЖАХ ЯК ВАЖЛИВИЙ ФАКТОР НАЦІОНАЛЬНОЇ БЕЗПЕКИ .....	21
2.1 «Фейкові новини» в соціальних мережах як загроза інформаційній безпеці України .....	21
2.2 Діяльність блогерів щодо розповсюдження дезінформації в соціальних мережах .....	25
2.3 Пропаганда як фактор впливу на громадську думку в соціальних мережах .....	31
РОЗДІЛ 3. ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В СОЦІАЛЬНИХ МЕРЕЖАХ В КОНТЕКСТІ ВОЄННОЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ.....	37
3.1 Державна інформаційна політика України щодо забезпечення інформаційної безпеки в соціальних мережах .....	37
3.2 Контрпропаганда та офіційні сторінки вищих посадових осіб держави, як джерело об'єктивного інформування суспільства .....	42
3.3 Роль кібервійськ у виявленні, нейтралізації та протидії інформаційним загрозам в процесі воєнної агресії Російської Федерації проти України.....	45
ВИСНОВКИ .....	50
СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ .....	53
ДОДАТКИ .....	62

## ВСТУП

**Актуальність** теми дослідження. Глобальна всесвітня комп'ютерна мережа Інтернет з'явилась ще наприкінці ХХ століття, а сьогодні бізнес, суспільство, політики і громадяни не уявляють життя без користування цією технологією. Окрім великих масивів інформації стосовно різних сфер людського життя і діяльності, Інтернет забезпечив можливість різних видів спілкування на відстані: листування через електронну пошту, дзвінки і відеодзвінки через месенджери, можливість спостерігати за життям своїх родичів і друзів в соціальних мережах через фото і відео. Соціальні мережі – це те чим ми користуємося кожного дня: ділимося власними фотографіями, слідкуємо за друзями і родичами, слухаємо музику, читаємо новини. Це без перебільшень невід'ємна частина нашого життя і також поширений спосіб маніпуляції масами людей. До того ж з появою карантину в нашому житті в кінці 2019-го року (пандемія COVID-19), стрімко зріс час, який люди щоденно проводять в соціальних мережах, як, власне, і вплив соціальних мереж на людей. Соціальні мережі виконують багато функцій: для когось це спосіб заробітку, для когось – можливість поспілкуватись з друзями на відстані, а для когось – привід відволіктись від рутини.

Але для українського суспільства дата 24-го лютого 2022 року стала переломною, вона змінила більшість поглядів та стереотипів, оскільки Російська Федерація після 8 років так званої «гібридної війни» розв'язала повномасштабну воєнну агресію на території України. У нових обставинах роль соціальних мереж також змінилась. Соціальні медіа тепер не просто виконують функцію джерела хорошого настрою і відпочинку після роботи, але в деяких ситуаціях стають основним джерелом інформації про воєнні дії. З початком повномасштабної війни Росії проти України соціальні медіа в особливий спосіб проявляють дуалізм свого призначення, адже з одного боку вони виступають джерелом поширення правдивої інформації, а з іншого боку – використовуються як засіб ведення інформаційної війни.

Сьогодні роль такого засобу масової комунікації як соціальні мережі – це одночасно велика сила, що дає змогу поширити всьому світові правду про цілеспрямоване знищення українського народу і культури Російської Федерацією, але поза тим – це і величезний масив «фейків» і недостовірної інформації. Це спосіб ведення інформаційної війни і в той же час джерело для боротьби з нею. Такі соціальні мережі як Instagram, Facebook, TikTok, Twitter, Youtube стали осередками ведення інформаційного протистояння України і Російської Федерації.

Актуальність теми дослідження, а саме забезпечення інформаційної безпеки в соціальних мережах з початком повномасштабної воєнної агресії Російської Федерації проти України не те що зросла, а стала пріоритетним напрямком в інформаційному полі України. Оскільки соціальні мережі в наш час користуються високим попитом в усьому світі, вони є рушійною силою ведення інформаційної війни і поширення пропаганди, і Російська Федерація користується цією зброєю на повну потужність. Саме тому забезпечення інформаційної безпеки в соціальних мережах є пріоритетним національним інтересом України.

**Мета дослідження** – розкрити вплив соціальних мереж на перебіг війни Російської Федерації проти України, показати способи забезпечення інформаційної безпеки і роль кібервійськ в протистоянні інформаційній війні розв'язаний Російською Федерацією проти України.

**Основні завдання**, для досягнення поставленої мети дослідження:

- дослідити історію виникнення соціальних мереж;
- розкрити вплив соціальних мереж на інформаційну безпеку України;
- виявити головні проблеми захисту національних інтересів України в соціальних мережах;
- показати способи пропаганди і маніпулювання громадською думкою як українців, так і росіян;
- дослідити внесок блогерів в створення і поширення дезінформації;
- розкрити сутність «фейкових новин» і показати в чому полягає їх загроза інформаційній безпеці;

—розглянути державну інформаційну політику України і засоби боротьби з дезінформацією;

—виявити значення контрпропаганди в веденні інформаційної війни;

—дослідити роль кібервійськ у виявленні, нейтралізації та протидії інформаційним загрозам в процесі воєнної агресії Російської Федерації проти України.

**Об'єкт дослідження** – інформаційна безпека України

**Предмет дослідження** – інформаційна безпека України в соціальних мережах, в умовах повномасштабної воєнної агресії Російської Федерації проти України.

**Методологічна основа роботи** – це збір і порівняння новин з різних пабліків і на різних каналах в соціальних мережах, аналіз і синтез отриманої інформації, зокрема аналіз маніпулятивного впливу дописів публічних осіб та громадських діячів, щодо їх політичної позиції з приводу війни в Україні в 2022-му році, для подальшого узагальнення способів маніпуляцій масовою свідомістю людей, а також дослідження механізмів протистояння таким маніпуляціям.

**Джерельна база дослідження** – соціальні мережі, такі як: Instagram, Facebook, TikTok, Telegram, YouTube, і зібрана в них інформація, а також офіційні сайти Міністерства культури і інформаційної політики України і Ради національної безпеки і оборони України і офіційний сайт Федеральної служби з нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій Російської Федерації. Також в підготовці наукової роботи були використані матеріали наукових статей, зокрема Національної академії державного управління при Президентові України, матеріали III Всеукраїнської науково практичної конференції та ін..

**Структура роботи** визначена метою і головними завданнями кваліфікаційної роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і з додатків. Загальний обсяг даної роботи – 69 сторінок, з них основний матеріал складає 50 сторінок.

# РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ФЕНОМЕНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІАЛЬНИХ МЕРЕЖАХ

## 1.1 Поняття та історія виникнення соціальних мереж

Соціальна мережа – це сайт в мережі інтернет, що є автоматизованим і складає соціальне середовище, яке дозволяє групі людей (користувачів) контактувати один з одним дистанційно. На такому Інтернет-ресурсі кожен користувач має власний акаунт з якого і веде спілкування.

Історія появи соціальних медіа ресурсів бере свій початок з 1950-их років, коли науковець-інформатик Рей Соломоноф, почав досліджувати штучний інтелект у розрізі створення і розповсюдження інформації [83] і американський математичний психолог Анатоль Рапопорт розробив аналіз соціальних мереж в якому показав швидкість розповсюдження інформації в соціумі [81].

Пізніше, в 1960 роках, Пол Ердос разом з Альфредом Реньї створили близько восьми наукових статей про головні принципи створення і функціонування соціальних мереж, де також дослідили їх відмінність від засобів масової інформації, пояснюючи відмінність у зацікавленості учасників соціальних медіа бути частиною поширення інформації і при цьому залишатись анонімними.

Вперше сам термін «соціальна мережа» виник у 1954 р. Він був започаткований британським соціологом, а також представником Манчестерської школи – Джеймсом Барнсом і тлумачився як взаємовідносини між двома або більшою кількістю людей. Використовувалось дане словосполучення для позначення соціальних зв'язків, що різнились від вже прийнятих і звичних для багатьох соціологів понять, таких як наприклад «категорія» чи «обмежена група»[28].

Сьогодні під терміном «соціальна мережа» ми розуміємо віртуальний майданчик для ведення спілкування і підтримки комунікацій з друзями родичами, обміну даними між користувачами засобом створення власного облікового запису.

У даній роботі «соціальна мережа» розглядається як інтернет-сервіс, тобто платформа, яка допомагає людям здійснювати зв'язок між собою, ділитися інформацією та новинами, і завдання якої полягає в забезпеченні користувачів різноманітними шляхами для комунікації один з одним, такими як чати, фото- та відео- матеріали, музика, блоги, історії.

Глобальна соціальна мережа – це соцмережа, що об'єднує велику масу людей в незалежності від їх індивідуальних особливостей, місця проживання і уподобань[27].

Перші попередники соціальних мереж, з'явилися в 90-их роках ХХ століття, ними стали сайти з наступними інтернет-адресами: [classmates.com](http://classmates.com), що з'явився в 1995 р. та менш відомий [SixDegrees.com](http://SixDegrees.com), рік його появи 1997-ий. А вже у 2001 році відкрились перші сайти, що використовували технологію «коло друзів» (це можливість об'єднання свого акаунту з певною кількістю людей у соціальних мережах, взаємна підписка). Дана технологія дозволяла користувачам обирати за власним бажанням з ким спілкуватися в Інтернеті, відшукувати акаунти друзів і родичів і в подальшому слідкувати за їх сторінками в соціальних мережах, знаходити нових друзів зі схожими хобі та інтересами, поширювати інформацію не для всіх, а тільки для обмеженої кількості обраних людей.

І такі сайти швидко здобули високу популярність, вже в 2003 р. їх було більше 15, а на даний момент їх існує понад 250. Вони і складають основну частину сучасних соціальних мереж.

І ось буквально через 3 роки після появи даної технології «коло друзів», Марк Цукерберг запустив одну з відомих широкому загалу людей і наймасштабніших на сьогоднішній день соціальну мережу «TheFacebook» на просторах Інтернету даний соціальний медіаресурс з'явився 4 лютого 2004 року і працював за посиланням «[thefacebook.com](http://thefacebook.com)». Це була закрита соцмережа, доступ до якої мали лише студенти Гарвардського коледжу, вони мусили пройти спеціальний етап автентифікації, щоб підтвердити, що вони є студентами Гарвардського коледжу і тільки після цього отримували допуск до соціальної мережі, здебільш її використовували для навчання і позастудентської діяльності: поширювали новини, відкриті лекції і додатковий

науковий матеріал, запрошення на різні події та ін.. І лише за місяць існування, на даній платформі зареєструвалась більша половина студентів Гарварду.

Побачивши такий попит на сайт Марк Цукерберг почав його розширювати вже не як сайт студентів окремого коледжу, а саме як соціальну мережу для спілкування студентів різних навчальних закладів, а допомогли йому в цьому його знайомі: бізнес-менеджер – Едуардо Саверін, програміст – Дастін Московіц, графічні дизайнери – Ендрю Мак-Коллум та Кріс Хьюз. І вже через 2 місяці, в березні 2004 р. соцмережею Facebook користувалися в Єльському університеті, університетах Колумбії і також в університетах Стенфорда [28].

Згодом до даного соціального медіаресурсу змогли долучитися й студенти інших шкіл Ліги Плюща, Нью-Йоркського і Бостонського університетів, Массачусетського технологічного інституту, а також студенти різних університетів США і Канади. Технологічну компанію Facebook – як розробників масштабної соціальної мережі було створено вже влітку того ж року.

Очолив компанію Facebook інтернет-підприємець з США Шон Паркер. А на початку осені 2006 р. Facebook став відкритим і доступним ресурсом для всіх бажаючих користувачів віком від 13 років в усьому світі, що мали власну електронну пошту і бажання зареєструватись на даному сервісі інтернет-комунікації. В даний час, станом на весну 2022-го року, сайтом користується майже третина населення планети і Facebook є однією з найбільших соціальних мереж в світі [27].

Зацікавленість користувачів у розвитку соціальних мереж стала зрозуміла ще в 2005 р., коли переглядів сторінок сайту MySpace (соціальна мережа) стало більше ніж у сайту Google. Хоча Google теж запропонував Web-сайт з можливістю роботи із соціальними мережами Orkut у 2004 році. Тим не менш людей цікавила саме можливість дистанційного спілкування в Інтернеті, а також можливість показувати фрагменти свого власного життя і розказувати про нього. Тобто MySpace на той час надав людям можливість відчувати себе потрібними і навіть стати наставниками для своїх підписників. Зіграв психологічний фактор – соціальна мережа стала місцем, де кожен користувач міг підняти свою самооцінку і відчувати, що він робить свій внесок



для всього світу, що він існує не просто так, оскільки інші люди (підписники) зацікавлені в його житті і самореалізації. В цьому і полягає феномен соціальних мереж, вони дають ковток життя людям, що втратили віру і не розуміють навіщо існують; вони вселяють віру в себе, відволікають від рутини. І бачучи такий високий попит на соціальні мережі з боку користувачів, в цей час соціальні мережі і почали розглядатися в розрізі інтернет-стратегії.

У березні 2005 р. Yahoo запустила Yahoo 360 °, а в липні 2005 р. News Corporation запустила всім відомо платформу MySpace. Популярну в країнах СНД деякий час соціальну мережу «Вконтакте» було створено 1 жовтня 2006 р. А найбільша українська соціальна мережа connect.ua була запущена у 2007 р.

Саме початок 2000-х років став етапом найфорсованішого розвитку соціальних мереж. Тоді здебільш створювали соціальні мережі загального вжитку, нові ж соціальні мережі все більше концентруються на певних сферах, таких як мистецтво, музика, розваги, спорт та ін[28].

На сьогодні соціальні мережі стали важливою частиною спілкування в суспільстві і способом комунікації на відстані, а також сервісом для листування окремих осіб і розповсюдження інформації.

#### Класифікація соціальних мереж

Як вже було описано вище, головною метою користування соціальними мережами є соціалізація і прагнення до спілкування з іншими користувачами, а головні функції соціальних мереж – комунікаційна і інформаційна. У всесвітній мережі Інтернет існує безліч соціальних мереж і класифікувати їх можна за різними ознаками, такими як доступність, спрямування, обсяг.

Станом на 2022 р., виходячи з даних платформи Social media states[32] найпопулярнішою соціальною мережею залишається Facebook (ним користується 65.75 % користувачів Інтернет), на 2-му місці Pinterest – 15.06 %, 3-й 4-е місце розділяють YouTube і Twitter – 7.5 %, на 5-му місці Instagram – 1,64 %, на 6-му – Tumblr – 0,93 % користувачів. Це шестірка світових лідерів соціальних медіа ресурсів (див. Додаток А).

Цільова аудиторія всіх цих платформ доволі широка, це люди з різними інтересами у віці від 13 до 65 років.

Кожна третя людина в світі користується хоч якоюсь соціальною мережею.

За доступністю виділяють:

—Закриті (для певного кола людей);

—Відкриті (доступні для всіх);

—Змішані (наприклад Clubhouse до якого можна приєднатись лише за посиланням-запрошенням від вже існуючого користувача).

За спрямуванням:

—загально тематичні, тобто спрямовані на підтримання та налагодження уже існуючих знайомств та пошук нових;

—соціальні мережі ділового спрямування, тобто для ведення бізнесу;

—спеціалізовані соцмережі, тобто соціальні мережі за вузьким профілем: музика, хобі, спорт і тому подібне.

За обсягом:

—глобальні;

—локальні.

В цілому ж соціальні мережі можна розділити за таким чином:

—Соціальні мережі для спілкування, такі як Instagram, Facebook. На даних платформах кожен користувач створює свій персональний міні сайт, відомий як профіль і спілкується з іншими користувачами які мають свої власні акаунти;

—Соціальні мережі для обміну медіа контентом, до них відносять YouTube та Instagram. Це соцмережі де люди можуть ділитися відео- і фотоматеріалами, поширювати власні світлини і друкувати дописи, вести блог чи відеоблог про своє життя чи хобі, створювати власні онлайн магазини і новинні сторінки;

—Соціальні мережі для авторського запису, найвідоміша платформа Twitter, на даних платформах користувач публікує текстово-медійний контент найрізноманітнішого спрямування, але цей контент може бути обмежений у своїх розмірах;

—Сервіси соціальних закладок, це додатки, де користувач може зберегти знайдений контент у власну онлайн-бібліотеку, наприклад Pinterest – соцмережа для поширення власних і зберігання чужих відео- і фото- матеріалів, для подальшого їх об'єднання у медіа збірник[29].

Отже це умовна класифікація, яка дає можливість розділити соціальні мережі на види і типи.

Оскільки в наш час нові соціальні мережі створюються і з'являються все нові категорії соціальних мереж - ця класифікація також буде розширюватись.

Якщо узагальнювати, то створення мережевої спільноти – це своєрідна історична відповідь на необхідність високого рівня комунікації між людьми.

Саме соціальні мережі в наш час відіграють комунікативну роль у суспільстві.

Пряма комунікація відходить на другий план, її заміняє невербальна: повідомлення, фото-, відео- матеріали, дописи, історії.

Доцільним є порівняння сучасних соціальних мереж з засобами масової комунікації, оскільки і ті і ті служать для виконання функцій комунікації мас. І в період повної комп'ютеризації, коли інформаційні технології вийшли на перший план в усіх галузях функціонування людини, соціальні мережі стали головним осередком спілкування між індивідами заміни котрим поки що немає.

## **1.2 Вплив соціальних мереж на інформаційну безпеку країни**

Сфера інформації є важливим системоутворюючим елементом суспільного життя, що активно впливає на політичну, оборонну, економічну і багато інших пріоритетних сфер розвитку держави. В сучасному світі Інтернет виконує провідну роль у поширенні інформації, оскільки дана мережа зберігає в собі великі масиви даних з приводу будь-чого. Саме в Інтернеті можна знайти всі необхідні матеріали: енциклопедичні дані, наукові статті, розважальний контент, світові новини, музику, відео контент, будь-які товари, різного роду послуги. Все це і складає інформацію, тож таким чином Інтернет є місцем поширення всієї необхідної інформації.

Однак користуючись будь-якою інформацією слід бути впевненим у її достовірності, правдивості, а також пересвідчитись чи не була вона спотворена чи урізана у процесі її передачі. Це головна причина чому інформаційна безпека є головним елементом системи національної безпеки країни, оскільки неправдива і недостовірні інформація несе в собі пряму загрозу для безпеки життя людей і держави.

Одним з факторів, що може спричинити загострення загроз інформаційній безпеці є інформація поширена в соціальних мережах. Неправдива і недостовірні, перекручена новина поширена в соціальній мережі, може спровокувати розв'язання як внутрішньополітичного так і зовнішньополітичного конфлікту. Ось чому таке важливе ведення вдалої інформаційної політики країни.

Важливим елементом гібридної війни виділяють вторгнення в інформаційно-комунікаційний простір певної країни. Дана маніпуляція робиться задля придушення будь-якого опору громадян і насамперед щоб сформувати світовий політичний стандарт, яким керується країна-агресор.

Основними методами такої провокації, що може поширюватись в інформаційному полі є:

- вторгнення в функціонування інформаційно-телекомунікаційних мереж та систем;
- розвиток рівня кіберзлочинності;
- тиск впливу на засоби масової комунікації;
- маніпулювання суспільною громадською думкою[22].

Безпека соціальних мережах – це дуже важливий аспект безпеки громадян країни, оскільки люди хочуть, користуючись соціальними мережами, знаходитись в безпечному середовищі, і не перейматися через свою конфіденційність. Тому підтримання, а також безпека користувачів соціальних мереж прямопропорційне популярності соціальної мережі. Також важливим елементом ведення політики інформаційної безпеки в соціальних мережах є політика несення відповідальності за діяльність на платформі. Тобто кожна неправомірні дія чи вороже висловлювання,

поширення будь-якої забороненої в соціальних мережах інформації має бути покаране (користувача має бути заблоковано на час чи назавжди). Гарним прикладом ведення такої політики є соціальна мережа TikTok, яка розробила спеціальні правила платформи, де вказано що вважається порушенням правил публікації контенту і які заходи покарання будуть прийняті у разі недотримання правил.

Конфіденційність користувачів стосується як їх профілів, так і з'єднання і спілкування в додатку. Наприклад на даний момент Telegram вважається найбільш конфіденційним ресурсом для спілкування, оскільки розробник обіцяє повний захист переписок за допомогою їх шифрування. А Instagram наприклад дає можливість користувачам створювати приватні закриті акаунти, доступ до яких мають лише вибрані користувачем особи.

Безпека персональних даних користувачів важлива не лише для них самих а й для держави. Оскільки витік баз даних громадян певної держави може мати безповоротні негативні наслідки, такі як шантаж, використання даних в корисливих цілях, і безпосередня загроза життю.

Якщо ми говоримо про інформаційну безпеку країни, то саме соціальні мережі несуть в собі велику загрозу, таку як місце розгортання і ведення інформаційної війни, оскільки через глобалізацію інформаційного простору такий ресурс може забезпечувати цей вид воєнного протистояння.

Соціальні мережі можуть виступати не тільки загрозою для інформаційної безпеки, а й впливати на рішення влади, а отже нести в собі загрозу і національній безпеці в цілому[19].

Вперше така загроза впливу на владу відбулася в Молдові в 2009 р., коли студенти протестували проти результатів парламентських виборів, дані соціальних опитувань сильно різняться від офіційних результатів виборів. Це і було першопричиною масових протестів.

Заклики виходити на мітинг з'являлися у Facebook і Twitter, був навіть створений спеціальний гештег «#rman» (Пяца Марій Адунерь Націонале – головна площа Кишинева).

Про хід протестів також багато студентів публікувало пости у Twitter. Тобто соціальні мережі використовувалися як засоби інтернет-координації дій протестувальників. В постах соціальних мережах часто говорили про заклик до об'єднання опозицій, про кількість постраждалих і арештованих у сутичках з поліцією, тобто про хід подій на мітингах. А для розповсюдження інформації на широкий загал, пости друкувалися англійською мовою, щоб іноземним засобам масової інформації було легше освітлювати це питання.

Паралельно з «твіттами» на платформу YouTube викладались і відеозаписи подій. Згодом саме ці події стали відомою нам «Твіттер революцією».

Саме ця подія суттєво підняла вплив соціальних мереж на політику багатьох країн.

Оскільки на мітингах люди чинили погроми і підпалювали будівлі державних установ в Тегерані, то владою було прийняте рішення про введення жорстокої інформаційної блокади.

Ця інформаційна блокада включала блокування стільникового зв'язку, заборона соціальних мереж, вимкнення іноземних радіостанцій, а на державних телеканалах висвітлювались включно безлади і неконтрольовані акти вандалізму мітингуючими на вулицях.

Для комунікації між собою протестувальники користувалися мобільним інтернетом, а також поширювали інформацію в Twitter: викладали фото і відео ходу протестів, інформацію про дати нових пікетів, дані про переміщення поліцейських, а також списки заарештованих мітингувальників.

Очільники ж влади Ірану з метою протидії інформації наданої народом, опублікували свій недостовірний контент на платформі. Тобто велась інформаційна війна. Проте мітингувальниками вдалося перемогти в цій Інтернет-битві. А результатом даного інформаційного протистояння стали повна зміна уряду і відставка президента.

Соціальні мережі стали своєрідними незалежними засобами масової інформації де почали публікуватися новини і висвітлювалися всі інциденти на мітингах в усьому світі[34].

Виходячи з цього стає зрозуміло що за останні 13 років світ занепокоївся інформаційною небезпекою, що несуть в собі соціальні мереж.

Завдяки всім правилам політики конфіденційності, гештег-революціям на Twitter та Instagram, питанням безпеки конфіденційної інформації в Facebook, вплив соціальних мереж на інформаційну безпеку в цілому стрімко зріс.

Отже для того аби забезпечити інформаційну безпеку країни, необхідно стрімко і своєчасно розвивати інформаційну сферу держави, виявляти всі загрози інформаційній безпеці держави в соціальних мережах, слідкувати за загрозами інформаційній безпеці не тільки власної держави, але й сусідніх країн.

Поширеною практикою для забезпечення інформаційної безпеки держави в соціальних мережах, є створення спеціальних державних ботів для формування суспільної думки з актуальних питань і обговорення важливих новин, проведення анкетувань з боку держави, а також блокування акаунтів окремих медійних осіб в соціальних мережах, які несуть загрозу для інформаційної безпеки держави.

Оскільки саме соціальні мережі є доволі дієвим інструментом впливу на різні політичні, а також суспільні процеси в країні, то забезпечення інформаційної безпеки держави в соціальних інтернет-ресурсах в умовах глобалізації інформаційного простору і в умовах ведення гібридних інформаційних воєн є ключовим питанням забезпечення національної безпеки.

### **1.3 Проблеми захисту національних інтересів України в соціальних мережах**

Інформаційна безпека України – це сукупність усіх діючих законів і заходів уповноважених державних органів, що стосуються насамперед інформаційної сфери і які спрямовані на забезпечення захисту національної безпеки і оборони України. Тобто інформаційна безпека України – це постійне забезпечення стану повної захищеності інформаційного поля держави, при якому інформаційний вплив

проведення спеціальних інформаційних операцій не завдає суттєвої шкоди національним інтересам України[49].

Згідно з чинним на 2022-й рік законодавством України поняття "інформаційна безпека" має таке тлумачення:

*«стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації. [30]»* – Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»[30].

Зазвичай виділяють наступні три головні рівні забезпечення інформаційної безпеки України:

—рівень особи (до нього відносять формування раціонального і критичного мислень, що базуються на принципах свободи вибоору);

—суспільний рівень (це формування якісного інформаційного аналітичного простору, де задіяні незалежні засоби масової інформації, що належать українським власникам);

—державний рівень (забезпечення інформаційної і аналітичної діяльності в державних органах, а також інформаційне забезпечення внутрішньої політики і зовнішньої політики, а також система захищеності інформації із обмеженим доступом і відповідно, протидія будь-яким правопорушенням в сфері інформації, кіберзлочинності)

Головною загрозою інформаційній безпеці України у Доктрині інформаційної безпеки України [31] визначено маніпуляції суспільною свідомістю, в тому числі способом поширення неперевіреної, неповної і недостовірної або упередженої інформації. Іншими не менш важливими загрозами є:

—обмеження свободи слова і доступу громадян України до інформації;

—кібертероризм і кіберзлочинність;



—поширення жорстокості, порнографії засобами масової інформації;

—розповсюдження інформації, що є державною таємницею, або ж іншої конфіденційної інформації, що перебуває у власності держави чи спрямована на забезпечення національних потреб інтересів.

У липні 2009 р. президентом України була підписана «Доктрина інформаційної безпеки України» [37]. В ній виділялись такі загрози інформаційній безпеці України:

—розповсюдження в глобальному інформаційному просторі недостовірної й упередженої інформації, що може завдавати шкоди і нести загрозу національним інтересам України;

—будь-які способи впливу на свідомість суспільства засобами масової інформації, а також через мережу Інтернет;

—інформація, що несе в собі посил до підриву конституційного ладу країни, суверенітету і територіальної цілісності та недоторканності України;

—будь-які прояви сепаратизму у державних і недержавних засобах масової інформації, які діють на території України, у мережі Інтернет і соціальних медіа платформах, за принципом етнічності, а також будь-яка дискримінація на основі мови, релігії, раси та ін.

Розробка нової Доктрини інформаційної безпеки України, що б відповідала вимогам часу почалася одразу після відсторонення Віктора Януковича з посади президента держави після перемоги Євромайдану в 2014 році. У той час найвагомішою загрозою національній і зокрема інформаційній безпеці України було здійснення іноземними державами негативного інформаційно-психологічного тиску на свідомість суспільства в цілому і громадян України в частості через інформаційний простір (засоби масової інформації і соціальні медіа ресурси).

Все це відбувалося засобом проведення інформаційних акцій та компаній, а також спеціальних інформаційних операцій, тобто іноземні держави регулярно поширювали неповну або упереджену інформацію з приводу України в цілому, зокрема про політичні процеси, що відбуваються в державі.

Все це нанесло суттєвий вплив на внутрішню політику нашої держави і на зовнішню політику також[34].

Таким чином міжнародний імідж України падав на фоні висвітленого політичного та економічного факторів. Метою проведення цих інформаційних операцій було забезпечення власних національних інтересів держав якими ця політика проводилась.

Взагалі можна виділити три основні напрями розвитку національних інтересів України, це:

- Забезпечення економічного добробуту всіх верств населення України;
- Задоволення культурних потреб громадян;
- Дотримання воєнно-політичного суверенітету.

Отже ці три фактори і є основними складовими національних інтересів України. І дані елементи є досить вразливими до навколишніх обставин, а їх запровадження і розвиток залежать від політики сусідніх держав, внутрішньополітичної ситуації всередині країни, геополітичного і ідеологічного факторів[38].

Іншими словами, всі ці умови і можуть виступати основними проблемами захисту національних інтересів. А проблеми інформаційного характеру загроз найбільш поширені саме в соціальних мережах, оскільки дані інтернет-ресурси виступають осередком поширення і обговорення будь-яких новин, як достовірних, так і неправдивих і неперевірених, а також місцем розповсюдження пропаганди, оскільки інформацію подану в соціальних мережах не завжди можливо перевірити на достовірність.

Якщо згадати події 2014 року в Україні, то саме в соціальних мережах люди збирались на мітинги проти діючого на той час президента держави (Революція гідності), поширювали там інформацію про хід протестів. А згодом події анексії Криму і початок збройної воєнної агресії Російської Федерації на сході України, показали нам можливість застосування соціальних інтернет-ресурсів у розрізі засобу пропаганди з боку Російської Федерації.

Американське військове видавництво RealClearDefense провело розслідування і виявило інформацію про витрату 19.000.000 \$, вони були направлені на фінансування діяльності 600 спеціально залучених акторів в Вконтакте, Facebook, Однокласники. Ці актори публікували на своїх сторінках в соцмережах статті про нібито «підтримку» місцевим населенням анексії Криму, Донецької і Луганської областей, в коментарях поширювали чутки про звірства проти народу з боку України, розпалювали ворожнечу, посилювали почуття ненависті до України.

Паралельно з цим російські засоби масової інформації публікували в соціальних мережах дезінформацію з приводу утисків російськомовних в Україні і як підтвердження поширювали пости даних акторів. Це була така своєрідна технологія маніпулювання суспільною думкою, що стала серйозною загрозою для інформаційної безпеки України, оскільки саме дані дії в той час суттєво вплинули на хід подій[39].

Також у цей час Російська Федерація використала соціальні мережі для легітимізації результатів псевдореферендуму про статус Республіки Крим.

Тоді ж у Криму війська Російської Федерації створювали інформаційний вакуум за рахунок блокування офіційних урядових сайтів України, наносячи кібернетичні атаки на сайти офіційних українських засобів масової інформації та офіційні аканти посадових осіб України.

Таким чином Російська Федерація отримала ряд суттєвих переваг в інформаційному просторі, це і спростило анексію півострова, бо на той час Україна не могла чинити суттєвий опір у інформаційній війні, оскільки такий вид ведення протистояння був цілком непередбачуваним.

Тобто тоді даний перелік подій і спричинив масову загрозу інформаційній безпеці України, що призвело не просто до загрози національній безпеці, а до її руйнування і зокрема до початку загарбницької гібридної війни Російської Федерації проти України.

Також дана ситуація показала, що соціальні мережі є ефективним інструментом управління суспільством в цілому і окрім небезпеки для

інформаційного простору країни, вони можуть слугувати і засобом боротьби з нею, використовувались для чинення опору чи для поширення контрпропаганди[36].

У даний час, в 2022 році в умовах повномасштабної воєнної агресії Російської Федерації проти України і в час ведення інформаційної війни Російської Федерації проти України, національне інформаційне поле України є не повністю захищеним від зовнішніх негативних інформаційно-психологічних факторів і пропагандистських впливів і загроз, тож забезпечення інформаційної безпеки і створення потужної ефективної системи інформаційної безпеки України є ключовими завданнями органів державної влади України і недержавних інституцій в Україні також.

## РОЗДІЛ 2. ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В СОЦІАЛЬНИХ МЕРЕЖАХ ЯК ВАЖЛИВИЙ ФАКТОР НАЦІОНАЛЬНОЇ БЕЗПЕКИ

### 2.1 «Фейкові новини» в соціальних мережах як загроза інформаційній безпеці України

Сфера медійних комунікації не стоїть на місці і постійно розвивається, відкриваючи для нас все нові можливості, вона несе в собі й нові загрози. Великою проблемою нашого часу стало масове поширення «фейкової» інформації.

«Фейкові» новини – це розповсюджена неперевірена інформація, що може бути не цілком достовірною, вигаданою і не відповідати дійсності. Головна проблема розповсюдження «фейкової» інформації – поява панічних настроїв у споживачів цієї інформації, розкол суспільства. Зазвичай такі недостовірні новини стають масовими і популярними в періоди зростання напруги у суспільстві. Зазвичай це проплачені акції, які несуть у собі завдання спричинити чи то масове обурення, чи то придавити опір.

Тобто, «фейкові» новини – це спосіб маніпуляції масами людей[52].

Перша в історії згадка про «фейкові новини» з'явилась у XVII ст., тоді таку неперевірену і неправдиву інформацію називали «газетною качкою», така назва пішла від анекдоту одного бельгійського журналіста Корнеліса, який одного разу опублікував жарт під видом наукової статті, де цілковито серйозно розповідалось про ненажерливість качок, нібито певний вчений порубав на дрібнесенькі шмати качура і годував ними щоранку інших 19 качок, а вони все не наїдається. А автори місцевих газет, незважаючи на абсурдність історії, розповсюдили її в своїх роботах як чисту правду.

Згодом, коли правда прояснилась – журналісти почали використовувати термін «качка», він означав вигадану історію, яка набула широкого загалу.

Якщо розбирати етимологію фейкових новин, то можна пройти до наступного висновку: слово «fake» у перекладі з англійської означає «копія або підробка будь-чого задля введення в оману когось», тобто слово «fake» використовують коли хочуть видати за оригінальну річ чи достовірну інформацію якийсь фальсифікат, щось несправжнє.

Тобто слово «fake» має суто негативне забарвлення. Відповідно «fake news» - оперативне інформаційне повідомлення, що базується на неправдивій, недостовірній інформації, а суть такого повідомлення - маніпуляція і обман[51].

Варіантів «фейкових новин» існує безліч, до них відносяться:

—фото- та відео- підробки (фото оброблені в фотошопі, змонтовані відео, дипфейки);

—підроблені сторінки в соціальних мережах (коли ведуть акаунт державних осіб чи новинних пабліків і розповсюджують неперевірену інформацію від імені іншої особи);

—новинні статті, що не відповідають дійсності і публікуються в неперевірених джерелах;

—підроблені аудіозаписи (вирвані з контексту матеріали телефонних розмов чи підкастів, накладені на відео аудіодоріжки);

—спродюсовані для ведення спеціального замовного блогу медіаособи.

Науковці А.Б. Качинський та А.В. Ткаченко вважають розповсюдження «фейкових новин» основою проведення «інформаційних операцій» і виділяють такі властивості характерні для них:

—високу схожість текстів, поширених в соціальних мережах;

—приблизно схожий час публікації текстів (один часовий відрізок);

—маловідоме чи щойно створене новинне агентство, регіональні чи спеціалізовані джерела і місця публікації текстів[52].

Також доречно додати до цього списку властивостей, таку особливість фейкових новин, як «скандальність і провокаційність заголовку», тобто назви

характерні для таких неправдивих новин зазвичай викликають яскраві емоції (паніку, обурення, злість; тобто здебільш негативні реакції).

Також «фейкові новини» можна класифікувати і наступним чином:

—за відсотковим співвідношенням інформації, що відповідає і не відповідає дійсності (процент правдивості новини);

—залежно від актуальності опублікованої новини (інформація може бути правдива, але дата зробленої заяви, звернення чи розповсюдження повідомлення – змінена; Поширення інформації про подію чи явище, що дійсно відбулися, але в тексті змінено місце проведення чи локацію);

—за метою публікації (розважальний контент; політичні цілі; спосіб маніпуляції масами; новини направлені на збільшення популярності джерела, де була опублікована інформація; шахрайство і засіб наживи на читачах; дезінформація стосовно конкурента).

Що стосується впливу «фейкових новин» на інформаційну безпеку країни в цілому, то він доволі суттєвий, оскільки даний спосіб маніпуляції населенням несе в собі ряд загроз:

—поява соціальної напруги серед населення;

—дестабілізація суспільно-політичної ситуації в державі чи окремому регіоні;

—висока вірогідність зміни світогляду та переконань громадян певної країни;

—формування національної ідеї у вигідному для замовника «фейкових новин» напрямку[50].

У розрізі саме впливу «фейкових новин» на інформаційну безпеку України, можна виділити, що в 2022 році, в період повномасштабного воєнного вторгнення Російської Федерації на територію України, коли кожен українець щогодини переглядає новинні пабліки в соціальних мережах – «фейкові новини» стали дуже поширеними. Ворог атакує Україну і в Інтернеті, Російська Федерація веде відкриту інформаційну війну.

Ціль розповсюдження «фейкових нових» з приводу війни Російської Федерації проти України – дестабілізація ситуації всередині нашої держави і зміна громадської думки населення Російської Федерації.

Як було описано в розділі 1, країна-агресор розпочала інтернет-війну проти України, ще в 2014 році під час анексії Автономної Республіки Крим, і саме завдяки масштабному поширенню «фейкових новин» - заручилася підтримкою свого народу щодо незаконної анексії півострова, окупації Донецької і Луганської областей, а згодом і повномасштабного наступу на територію незалежної України.

Головне чим апелювали росіяни – це утиски «російськомовних українців», це і стало так би мовити причиною «визволення» українців.

Дана інформаційна атака «фейковими новинами» з боку Російської Федерації як на просторах засобів масової інформації України, так і на російському телебаченні і у світових соціальних мережах, що триває вже 9-й рік виявилась доволі дієвою для агресора і принесла наступні наслідки:

—за результати соціологічного дослідження компанії Active Group приблизно 80% росіян підтримують режим Путіна і повномасштабне воєнне вторгнення Російської Федерації на територію України;

—близько 75% опитаних росіян впевнені, що в Україні панує «нациський режим» і тут заборонена російська мова, тож українців треба рятувати від української влади засобом війни;

—формування в певного відсотка українців анти національної позиції і позитивне ставлення до війни розпочатої Росією;

—поява колаборантів;

—сприяння діяльності терористичних організацій з боку колаборантів;

—викривлення наявної громадської думки щодо сучасних подій в Україні;

—масові напади паніки в населення України після масового розповсюдження кожної окремої «фейкової новини».



Також додаткова небезпека «фейкових новин» полягає в неможливості їх швидкого спростування, оскільки доволі складно притягти до відповідальності окремих осіб, які створили недостовірну новину.

Дуже позитивною новиною є те, що з початком повномасштабної воєнної агресії з боку Російської Федерації проти України, Центр протидії дезінформації при РНБО (Рада національної безпеки і оборони України) працює доволі ефективно і часто попереджає громадян про «фейкові новини», ще до моменту їх появи в мережі. Наприклад, як було з своєчасним попередженням про поширення Росією дипфейку з президентом України Володимиром Зеленським, де він нібито здає Київ.

Університети Нью-Йорка і Принстона провели наукове дослідження і виявили, що найбільш вразливими до «фейкової» інформації є люди похилого віку. У більшості випадків це пов'язано з низьким рівнем вміння розпізнавання недостовірних новин в Інтернеті, зокрема в соціальних мережах[52].

Тим не менш вражаюча більшість громадян України, що займаються розповсюдженням прочитаних «фейкових новин», не є особами похилого віку. Це вказує на низький рівень медіаграмотності українців в цілому. В цьому і є головна загроза інформаційній безпеці України, те що громадяни держави сильно піддаються паніці і не перевіряють інформацію в офіційних джерелах.

Єдиний спосіб вберегти себе від недостовірної інформації – читати лише перевірену інформацію на офіційних новинних ресурсах і порівнювати її розповсюдженими новинами (хоча враховуючи воєнний стан і важливість швидкої подачі і публікації актуальних подій, навіть в перевірених джерелах іноді можна натрапити на «фейк») і не довіряти чуткам.

## **2.2 Діяльність блогерів щодо розповсюдження дезінформації в соціальних мережах**

Блогер – це людина яка веде власний веб-сайт чи сторінку в соціальній мережі про своє життя чи діяльність, головний зміст такого веб-сайту – це дописи, фото та

відео публікації, що регулярно оновлюються. Тобто основа роботи блогера – створення і поширення контенту в Інтернеті.

Термін «блог» вперше з'явився наприкінці 90-х років ХХ століття і був запроваджений редактором американського журналу «Robot Wisdom» і в подальшому блогером – Йорном Баргером і тлумачився як «ведення журналу в Інтернеті».

У подальшому один із основоположників компанії зі створення і розвитку інформаційних технологій Pyra Labs Еван Віліамс створив і саме поняття «блогер», що позначало автора блогу[53].

УВ наш час блогери – це рушійна сила прогресу. Вони є трансетерами для своїх підписників, які прислухаються їх порад. Тому дуже важливо фільтрувати інформацію яка надходить нам від блогерів. Враховуючи їх сильний вплив на аудиторію.

З боку державної влади і спецслужб дуже важливо тримати під контролем інформацію яку розповсюджують медіа особи, особливо що стосується політики, бо за великим рахунком блогери мають достатньо ресурсів аби за ними пішли люди.

Відповідно, блогери є чудовим засобом впливу на людей, А отже їх може використовувати влада в своїх інтересах. Для більшості блогерів-мільйонників їх акаунти в соціальних мережах, це не лише місце розповсюдження інформації щодо їх життя, а й спосіб заробітку.

На своїх сторінках вони рекламують товари і послуги, сторінки і блоги інших користувачів, а іноді вдаються до незаконного бізнесу: рекламують ставки на спорт, казино і політичну пропаганду, таким чином нав'язуючи глядачам свою думку.

З боку держави, блогери – це чудовий засіб ведення пропагандистської політики і маніпуляції масами людей.

У рамках війни Російської Федерації проти України, як вже зазначалося раніше, Росія веде й інформаційну війну, використовуючи і медійних осіб задля досягнення своїх цілей.

Влада сама пише пости для розповсюдження блогерами, створює політичні пропагандистські тренди і таким чином заручається підтримкою народу, бо люди йдуть за своїми кумирами і переймають їх позицію.

На просторі соціальних мереж є безліч прикладів використання діяльності блогів для розповсюдження дезінформації, розберемо декілька з них:

Приклад 1. Тіна Канделаки.

Діюча російська телеведуча і журналістка родом з Грузії. Медіа особа, яка підтримує режим Путіна і воєнну агресію Російської Федерації проти України. На даний момент вже зарахована в базу «Миротворець».

Почала свою кар'єру Тінатін Гівіївна Канделаки (це повне ім'я) в 2002 р. як інтерв'юер відомих діячів шоу-бізнесу Росії. Надалі ідучи по кар'єрним сходам швидко набрала популярність як на телебаченні, так і в соціальних мережах таких як Instagram і Facebook[54].

У лютому 2022 р. після повномасштабного воєнного вторгнення Росії на території України відкрито підтримала даний акт воєнної агресії.

Підтримка путінського режиму почалася з посту в Instagram з гештегом «#ДавайЗаМир». Не дивлячись на здавалося б позитивний зміст і намір даного тегу, в доданому тексті посту йшлося про те, що будь-які опубліковані відео з бомбардуваннями населених пунктів і риданнями й криками мирних жителів України - це постанови, всі українські засоби масової інформації доносять недостовірну інформацію, війна на Донбасі – це справа рук українців, які і бомбардували мирних жителів, а інформація і фото з відео з російськими полоненими — це смішно і неправда (див. Додаток 2).

Саме така заява була зроблена відомою телеведучою 25-го лютого, на другий день ведення повномасштабної воєнної агресії Російської Федерації в Україні. В час коли ракети ворога потрапляли в будинки мирних жителів по всій Україні, в час коли російські війська на танках давили мирних людей, в час коли вже весь світ говорив про розпочату росіянами війну.

У цей час Росія і почала створювати інформаційний залізний занавіс всередині країни, щоб громадяни не знали правди стосовно того, що відбувається насправді.

У коментарях до даного посту Тіну Канделакі підтримали як блогери так і прості росіяни, насправді це і не дивно, оскільки російське телебачення займалося пропагандою проти України більше ніж 8 років і готувало росіян до цього (детальніше в підрозділі 2.3).

На цьому підтримка дій російської влади Тіною Канделакі не закінчилась.

18 березня 2022 р., в річницю анексії Криму Російською Федерацією, на стадіоні Лужники у Москві відбувся мітинг у формі концерту «Кримська весна»[56]. Дана подія несла в собі мету звеличити воєнну агресію проти України і виправдати свої дії країни-агресорки[54].

На даному концерті виступила і Тіна Канделакі. Вона звернулася до росіян з закликом не соромитись свого походження. Розповіла про русофобію яка набирає обертів у світі, але яка робить росіян тільки сильнішими. Нагадала, що росіян ненавидять за російську мову, таким чином притягнувши за вуха те, що Росія рятує «російськомовних українців» в Україні. І нагадала, що «Росія ніколи не стане на коліна»[55].

Також телеведучою були використані такі недоречні формулювання:

—«Это мы (росіяни) изобрели лекарство от сибирской язвы и коронавируса», ремарка – ліки від сибірської виразки винайшов Луї Пастер – уродженець Доль Жура, Франш-Конте, Королівство Франція (нічого спільного з Росією не мав)[57];

—«Это мы открыли гиперзвуковые технологии», ремарка – вперше про створення гіперзвукових технологій, вчасності зброї, дійсно заявив президент Російської Федерації Володимир Путін у 2018р. Але згодом дана інформація була уточнена, Путін говорив про бойову частину з планетарними бойовими елементами «Авангард», але даний проєкт був майже реалізований ще в СРСР під шифром «4202» і у 1990 р. навіть були проведені його випробувальні запуски. Тобто інженери Росії після розпаду СРСР просто зайнялась допрацюванням вже майже готового проєкту. Як висновок, Російська Федерація це лише складова частина СРСР яка забрала собі технологію виготовлену в Радянському Союзі[58];

—«Это мы открыли Антарктиду», ремарка – У 1820 році До Антарктики наблизилися кораблі 3 капітанів: капітан російського імператорського флоту - Фабіан Готліб фон Беллінсгаузен, Капітан військово-морських сил Великої Британії – Едвард Брансфілд, І мисливець на тюленів зі штату Коннектикут - Натаніель Палмер. За історію радянського союзу, першими підпливли до континенту саме учасники експедиції російського імператорського флоту, однак дослідження і дані експедиції британців ставлять під сумнів це твердження. Як зафіксував капітан Едвард Брансфілд у звіті складеному ним про експедицію - Російський імператорський флот Олександра 1-го тоді не підплив до Антарктиди, лише до окремих островів, про це йдеться і у звіті міністра морського флоту Олександра 1-го Траверсе[59]. Тому дане твердження Тіни Канделаки не цілком однозначне.

—Як ми бачимо з вище поданого матеріалу, дана російська телеведуча апелювала не достовірними фактами спростованими історією. Її трактування мали возвеличити російський народ, але лише показали його неграмотність.

—Враховуючи всі дії щодо пропаганди і підтримку путінського режиму з боку телеведучої Тіни Канделаки, її оголошено в міжнародний розшук як одну з головних пропагандистов Російської Федерації і розповсюджувачів закликів до підтримки кремлівської військової машини і війни в Україні з боку Російської Федерації.

Приклад 2. Микола Басков.

Російський співак і з 2001 р. заслужений артист Російської Федерації. У 2004 р. удостоєний звання Народний артист України, але незважаючи на антиукраїнську позицію і підтримку режиму Путіна й війни в Україні станом на 30 березня 2022 р. не позбавлений даного звання. Тим не менш даний артист входить в список бази «Миротворець»[61].

У мережі Instagram Микола Басков є інфлюенсером для 5.000.000 людей.

25 лютого 2022 р., на 2-й день розпочатої Росією воєнної агресії проти України співак і блогер Микола Басков поширив допис в Instagram з текстом «Россия войны не начинает. Россия их заканчивает.» [62].

У дописі йшлося, що Росія розпочала не війну, а миротворчу операцію задля закінчення геноциду і запобігання нападу на Росію з боку України. Співак написав що неможливо і надалі терпіти вбивства російськомовних громадян України й нарощування воєнної сили і заявленої ядерної інфраструктури. Він сказав що захід не хоче признавати права росіян і громадян і настав час все називати своїми іменами, Басков заявив що США їх союзники хочуть знищити Російську Федерацію[62].

Логічно що українських підписників співака обурило даний пост, тим не менш він знайшов і велику підтримку серед багатьох росіян (див. Додаток 3).

Однак менш ніж через місяць мережа Instagram визнала даний пост дезінформацією (див. Додаток 4).

Це був не єдиний акт підтримки російської агресії проти України. Пізніше Басков публікував ще кілька дописів в яких виступав проти русофобії і вже висував свою позицію нібито він за мир (див. Додаток 5).

Окрім вищезгаданих заяву в Instagram Басков веде відкриту політику підтримки воєнної агресії і в соцмережі Telegram, де регулярно публікує пости про те що «Російська Федерація звільняє Братський народ».

Таким чином Басков відкрито підтримує політику знищення українського народу.

До того ж Микола Басков зробив одну некоректну заяву в мас медіа, в якій прибіг до неумісного використання Статуту ООН: «Решение о проведении специальной военной операции принято в соответствии со ст. 51 части 7 Устава ООН, которая предусматривает неотъемлемое право на индивидуальную или коллективную самооборону. Она распространяется не только на России как члена ООН, но и на ее союзников – признанных Россией независимыми республиками ДНР и ЛНР. Россия имеет полное право взять на себя защиту этих республик [63]», – заявив Микола Басков.

Приклад 3. Анатолій Шарій.

Проросійський пропагандист, в минулому журналіст українського походження, також політик і відомий відеоблогер. Має власний блог на платформі YouTube, частий гість антиукраїнських ток-шоу [64].

У своєму відеоблозі займається російською антиукраїнською пропагандою, дискредитує українську мову, прапор, гімн, герб, публікує неправдиві дані щодо української армії та уряду, а також про Україну в цілому.

У 2021 р. блогеру оголошена підозра у державній зраді з боку Служби Безпеки України.

Де-факто Шарій є керівником опозиційної партії «Партія Шарія», що займалася поширенням агітаційних матеріалів використовуючи карту України без Автономної Республіки Крим. Анатолій Шарій відкрито підтримує режим Путіна і воєнну агресію Росії.

25 квітня 2022 р. був оприлюднений документ Департаменту державної безпеки Литви, в якому йшлося про пряму співпрацю Анатолія Шарія з адміністрацією президента Російської Федерації Володимира Путіна [65]. В документі було вказано що відео блогер Анатолій Шарій є публічною особою, яку Російська Федерація використовує як засіб політичного, а також інформаційного впливу за кордоном, також зазначалося, що діяльність даного пропагандиста є виконанням завдань країни агресора, а не його власною політичною позицією (див. *Додаток б*).

Отже Російська Федерація активно використовує проплачених пропагандистів на теренах соціальних мереж і дана маніпуляція несе високу ефективність для зміни політичної позиції їх фоловерів на вигідну для Росії.

### **2.3 Пропаганда як фактор впливу на громадську думку в соціальних мережах**

Пропаганда – це спосіб цілеспрямованого впливу і засіб змінення переконань, основна мета якого – вплинути на ставлення цільової аудиторії до певного явища чи

події способом розповсюдження спеціально підготовлених повідомлень через інформаційні канали [66].

Ми живемо в період переформатування структури сучасного світу, отож часто стикаємося з пропагандою у політичній, економічній, культурній, суспільній і інших сферах. Цей засіб впливу на думку окремого індивіда чи групи людей призначений для досягнення поставленої мети суб'єкта, який цю пропаганду і продуктує.

Тобто дієвим засобом спрямованим на поширення в суспільстві певного світогляду і засобом впливу на суспільну думку і є пропаганда. В широкому розумінні – це спектор знань з метою їх втілення в суспільну свідомість, а в більш вузькому ж – це спеціально спрямована ідеологічна діяльність політичної партії призначена для створення у конкретних об'єднань чи верств населення вигідних поглядів і уявлень.

Особливість пропаганди на відміну від об'єктивної правдивої інформації, це часткова подача матеріалу і уникнення певної інформації задля того аби створити вигідне для замовника емоційне забарвлення повідомлення.

Головним результатом пропаганди є зміна позиції що відношенню до певного суб'єкта. Зазвичай пропаганду використовують для політичної боротьби.

Термін «пропаганда» бере свій початок від назви католицької організації *Congregatio de Propaganda Fide* (що проводила політику відмови від реформації церкви і активно поширювала цю думку у Ватикані), і був створений Папою Римським Григорієм 15-м у 1622-ому році [68].

Таким чином пропаганда є некінетичним методом ведення війни у формі інформаційної атаки.

У стародавні часи пропаганда була усною, її розповсюджували оратори-агітатори на площах міст в усьому світі, проповідники у церквах. А в період появи друкарства, даний інструмент впливу на маси набрав ще більшої популярності й поширення, з часом його роль тільки зростала оскільки з'являлись і інші канали передачі інформації: спочатку радіо, потім телебачення, а згодом і Інтернет. Але подавати пропаганду просто на окремих сайтах в пошукових браузерах було



неефективно, тому з появою соціальних мереж, основним місцем ретрансляції даного способу маніпулятивного впливу встали саме вони.

Такий метод є набагато більш затратним і важчим у веденні ніж пряма фізична війна. Але і вплив пропаганди є більш дієвим.

Зараз пропаганда знаходиться повсюду, вона не обмежується агітаційними заголовками в газетах, вона зосереджена в новинах, в літературі і мистецтві, в кінематографі, в науці, освіті і звісно в релігії. Іноді вона хитро замаскована, а іноді подана прямим текстом. Щодо соціальних мереж, то її можна зустріти в будь-якій з них[67].

До прикладу розберемо пропаганду щодо повномасштабної воєнної агресії Російської Федерації проти України в різних соціальних мережах:

—Instagram, Соціальна мережа в якій зосереджується найбільший відсоток російської пропаганди спрямованої проти української влади і народу. Російський режим застосовує медійних осіб зареєстрованих в Instagram, на яких підписана велика кількість людей, як засіб поширення цієї пропаганди. Тобто влада Росії платить блогером гроші аби ті підтримували загарбницьку політику Російської Федерації в дописах. Окрім того на теренах Instagram зареєстровані акаунти новинних служб Росії, які займаються ретрансляцією поширеної на телебаченні пропаганди. Однак з середини березня 2022 р. Instagram почав попереджувати своїх користувачів про публікації, які містять російську пропаганду. Тобто коли гортаєш стрічку оновлень в цій соціальній мережі і натрапляєш на допис з прямою підтримкою режиму Путіна і вбивств Україні – на екрані висвітлюється інформаційний банер Instagram, в якому вказується, що даний пост містить недостовірну інформацію, або розпалює ворожнечу[70]. Тим не менш поки що Instagram не блокує такі пости. А ось кадри жорстокості російських військ в Україні, соцмережа доволі часто видаляє, бо вони «порушують правила спільноти».

—Facebook, 2-а за популярністю поширення пропаганди проти України соцмережа. На даній же платформі здебільш поширенням пропаганди займаються прості росіяни. Вони репостять посилання на новинні відео російських телеканалів і

фейки. Розпалюють ворожнечу в коментарях під постами в підтримку України і створюють групи в підтримку путінського режиму.

—YouTube, повністю відмінна від Instagram платформа, яка використовує дуже схожі способи впровадження пропаганди. Аналогічно до Instagram, проросійські блогери створюють в соцмережі відео в підтримку путінського режиму і необхідності воєнного вторгнення Російської Федерації в Україну. Паралельно з цим на акаунти новинних ресурсів Росії в YouTube заливаються відео трансляцій новин з російського телебачення.

—TikTok, соціальна платформа яка була створена для публікації розважальних відео для підлітків, стала місцем розпалення ворожнечі між представниками цієї вікової категорії. Станом на 2022 р. платформа TikTok є розважальною соціальною мережею для широкої цільової аудиторії від 13 до 35 років. Однак більшість користувачів – підлітки. Ось як ця мережа пов'язана з пропагандою: проросійське керівництво не обмежиться створенням маніпуляцій для заручення підтримкою дорослого населення Росії і притягнуло ще й дітей. Основна ціль TikTok – постинг коротких розважальних відео і створення відео трендів. Російська Федерація і використала цей ресурс: було створено низку спеціальних проросійських трендів з використанням символіки «Z» і «V» (символ невинуватості російської воєнної агресії) і різних пісень на тему війни на підтримку російської агресії і підняття бойового духу російських солдат, а також для просування ідеї про «братський народ». Почалось запровадження цих трендів з розсилки з пропозицією знати такі відео тітокерам з великою аудиторією (100 000+ підписників) за грошову винагороду. А розповсюджувати вже ці тренди почали за допомогою підписників тітокерів, що погодились на дану пропозицію і знали такі відео. Їх підписники почали знімати аналогічні відео на свої акаунти. Як наслідок ці TikTok аудиторія України і Росії поділилася на людей, що підтримують путінський режим і людей, що виступають за незалежність України і вважають, що Російська Федерація поступила неправомірно. Ці два TikTok фронти почали відкривати суперечки в коментарях під будь-якими популярними відео в Тік ток, незважаючи на те пов'язані вони з війною

чи це просто розважальний контент, таким чином TikTok став місцем розпалення ворожнечі між молоддю.

Незважаючи на поширеність і популярність використання, пропаганда є дуже вразливим засобом ведення боротьби, оскільки в будь-який момент її подача може перерватися. Наприклад коли відбувається блокування російських соціальних мереж і телеканалів на території України (тобто засобів впровадження і поширення пропаганди), то відповідно і зв'язок між замовником (Російською Федерацією) і кінцевим отримувачем (українським народом) - безповоротно руйнується.

Суттєвим мінусом даного методу переривання зв'язку є його неефективність в сучасному цифровому світі, в час коли існує безліч альтернативних каналів передання цієї інформації такі як неофіційні українські засоби масової інформації, що передають пропагандистські меседжі Росії або ж проросійські блогери, що живуть в Україні і ретранслюють позицію Путінського режиму[67].

Блокування джерел пропагандистської інформації також ускладнюються свободою вираження думок і свободою слова в Україні, тобто в окремих ситуаціях блокування джерела пропаганди може розцінюватися як заборона свободи слова.

Однак «Роскомнадзор» (Федеральна служба Росії з нагляду в сфері інформаційних технологій, масових комунікацій і зв'язку) це не зупинило. 11 березня 2022 р. рішенням суду Російської Федерації спільноту Meta (Об'єднання таких соціальних мереж як Facebook і Instagram) було визнано екстремістською організацією і заблоковано для використання на території Росії. Таке рішення було прийнято для захисту російського населення від недостовірної і «фейкової» інформації стосовно війни. Аналогічна ситуація відбулася і з соціальною мережею TikTok. Причини ті самі.

Отже таким чином Росія поступово створює інформаційну ізоляцію від зовнішніх джерел для придушення можливих бунтів і створення у населення Російської Федерації однобокого бачення ситуації, що відбувається. Таким чином російська пропаганда будується на принципі підтримки політики президента Російської Федерації.

Але для об'єктивності також варто додати, що Україна також використовує пропаганду. Здебільш це конструктивна пропаганда – такий вид пропаганди не є способом маніпуляції громадською думкою, а скоріш сприяє об'єднанню народу для вирішення спільної проблеми і не нав'язує певні переконання, а лише поширює загальноприйняті цінності.

Тому пропаганда – це важливий інструмент ведення інформаційної війни, який може нести в собі і позитивні, і негативні наслідки.

## РОЗДІЛ 3. ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В СОЦІАЛЬНИХ МЕРЕЖАХ В КОНТЕКСТІ ВОЄННОЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

### 3.1 Державна інформаційна політика України щодо забезпечення інформаційної безпеки в соціальних мережах

Пріоритетним напрямом державної інформаційної політики України є прагнення до створення інформаційного суспільства відкритого для всіх людей, де б кожен зміг створювати і зберігати інформацію та знання, мати вільний доступ до них, користуватись і обмінюватись даними. Щоб кожен громадянин України міг повною мірою реалізовувати свій потенціал в інформаційному полі, спираючись на особистий досвід і суспільний розвиток, а також покращувати якість власного життя.

Головною задачею державної інформаційної політики України насамперед є:

- забезпечення доступу всіх громадян до інформації;
- запровадження спеціальних національних систем та мереж поширення інформації;
- покращення рівня забезпечення матеріально-технічної, наукової, економічної, організаційної, правової баз інформаційної діяльності держави;
- гарантування ефективного використання інформації в суспільстві;
- підтримка постійного оновлення, збагачення і зберігання національних ресурсів інформації;
- запровадження загальної системи охорони інформації;
- сприяння інтернаціональній співпраці в сфері інформації та гарантування інформаційного суверенітету України;
- сприяння задовільненню інформаційних потреб українців, які знаходяться за кордоном [73].

Щодо інформаційної безпеки в соціальних мережах, то держава постійно працює і розвиває правове регулювання змістовного наповнення новин і забезпечення поширення правдивої інформації без цензури, тобто розширюючи межі свободи слова, а також розробляє правове регулювання щодо доцільності поширення різного роду контенту на теренах соціальних медіа ресурсів.

На нашу думку, запорука забезпечення інформаційної безпеки держави – це насамперед повна довіра громадян держави до уряду і державної влади. На сьогодні в Україні рівень такого роду довіри значно зріс у співвідношенні з попередніми роками, але досі є недостатнім.

Головним актуальним питанням інформаційної політики нашого часу, я вважаю все ж таки включення розвитку сфери інформаційних технологій України в рейтинг головних пріоритетних напрямків державної інформаційної політики. Оскільки на 2022-ий рік саме сфера інформаційних технологій становить основу розвитку держави, це не просто засіб отримання потрібної інформації і спосіб спілкування, це базис будь-якої сфери діяльності людини.

Однак паралельно з вирішенням даного питання, влада України, вводячи нові технології прозорості, сприяє підвищенню і забезпеченню високого рівня довіри населення, ці технології спрямовані на змогу суспільством контролювати владу. Запровадження даної технології є лиш початком для усвідомлення державою того рівня відповідальності, що вона несе перед народом України.

Тому варто зазначити, що важливим аспектом забезпечення державної інформаційної політики є її правове регулювання[8].

На сьогодні ще й досі засобом соціальних мереж здійснюється сильний вплив на громадськість шляхом маніпулювання суспільною свідомістю, такого роду агітація негативно впливає на інформаційну безпеку країни.

Відбувається наступна ситуація: коли якась певна особа заходить у соціальні мережі і отримує лише негативні відомості про події та явища, які відбуваються в країні чи суспільстві, людиною починають керувати негативні настрої. Наступним кроком вона несе цей негатив у маси, поширюючи таким чином почуті чи прочитані

новини. З часом починається масова паніка, а це вже пряма загроза національній безпеці держави.

Отож моральний стан суспільства відіграє ключову роль у безпосередньому впливі на подолання економічної кризи і розбудову сильної держави з високим рівнем національної свідомості.

Об'єктивно, висвітлення лише негативної або лише позитивної інформації — це 50 відсотків від реальності, де у матеріалі робиться акцент або на безнадійності і відчаї, або на гордості і радості.

Сьогодні ж в період фінансової кризи і війни в Україні, тільки завдяки адекватному стабільному емоційному стану населення наша країна буде здатна вийти з кризи і перемогти у війні. Тому країні необхідно публікувати лише достовірну інформацію, яка звісно може викликати і хороші і погані емоції, але буде описувати реально ситуацію що відбувається. В цей же час необхідне і регулювання психоемоційного стану населення, аби воно й не падало у відчай і було оптимістично налаштоване.

Гарним прикладом позитивного впливу необхідної маніпуляції населенням в період війни є регулярні виступи представника офісу президента Олексія Арестовича.

Брифінги Олексія Арестовича спрямовані саме на населення. І ось в чому полягає його особливість:

Спокійний тон розмови, неформальна манера ведення брифінгу, що заключається у розгляді подій під позитивним кутом, словах що підбадьорюють і навіть гіпнотичній інтонації спікера, все це впливає на сприйняття і діє як порція заспокійливих новин для українців. Олексій Арестович дійсно висококваліфікована і освічена людина, що добре виконує свою роботу, роботу психолога і аналітика. Звісно що підготовкою будь-якого його брифінгу він займається не один, а скоріш за все разом з командою. І різна реакція на його виступи, як позитивна, так і негативна - також цілком логічна. Оскільки багато людей правильно трактують роль його виступів. А основна мета цих виступів – це підтримати бойовий дух і нагадати

українцям наскільки ми сильна нація і що все в нас вийде. З цим даний представник офісу президента України справляється на 100 відсотків [72].

Таким чином даний приклад показує, що інформаційна політика, спрямована на забезпечення інформаційної безпеки українців і заключається не лише в протидії дезінформації, а й в налагодженні зв'язків комунікації.

А основа безпеки інформаційного поля – це відкритий доступ до достовірної інформації і забезпечення стабільного психоемоційного стану населення.

Великий внесок в забезпечення інформаційної безпеки України в соціальних мережах робить Міністерство та Комітет цифрової трансформації України (Мінцифра). Вони дуже ефективно вирішують проблеми з навмисним блокуванням сторінок в соціальних мережах українських блогерів (дуже часто масові скарги з боку росіян поступають на акаунти блогерів, які виступають за підтримку України і як наслідок соціальні спільноти спочатку їх блокують, але Мінцифра вирішує це питання шукаючи чи правомірно відбулось закриття профілю) [77].

Також важливий вклад Міністерство цифрової трансформації робить поширюючи в маси інформацію щодо того яку інформацію можна публікувати в соціальних мережах, а яку ні.

Був навіть створений спеціальний список з повним розбором інформації яку не варто поширювати у месенджерах:

— Не варто показувати свою геолокацією і місце перебування, розташування українських військових, їх переміщення і місцезнаходження складів зберігання боєприпасів ЗСУ.

— Всю інформацію, яку ворог, прочитавши може використати проти Вас.

— Не слід також пересилати в месенджерах та соціальних мережах паролі від свої банківських і кредитних карток, соцмереж і гаджетів навіть використовувати спеціальні програми зашифрованих миттєвих повідомлень.

— З метою безпеки теж доречно не надсилати в месенджери інформацію про пересування і ворожої техніки. Краще таку інформацію повідомляти у ЗСУ через чатбот «Ворог», після чого слід одразу видалити переписку [75].



Ще одним доцільним нововведенням Міністерства цифрової трансформації України було створення спеціальних чатботів, що можуть допомогти подолати окупанта, в яких містяться поради, як вберегти себе та близьких під час війни у різних ситуаціях.

Ось їх перелік і функціонал:

—Чатбот Готовий до всього – містить актуальну інформацію про те, як вступити в територіальну оборону і поради як вижити цивільному під час бойових дій, як діяти в кризовій ситуації.

—Джгут 2.0. – навчить першій домедичній і медичній допомозі. В чат боті містяться підказки з приводу того, що робити, якщо ви не знаєте або ж не пам'ятаєте алгоритмів дій першомедичної допомоги при інфаркті, інсульті, зупинці серця, а також ряд інших поради першої медичної допомоги.

—SaveUA – це чат бот, що допоможе знайти у своїй області чи регіоні волонтерів, і місце де ви можете запропонувати власну допомогу, а також знайти чи віддати продукти харчування, транспорт, паливо та навіть надати прихисток.

—STOP Russian War. Чатбот створений для надання інформації щодо пересування ворожої техніки.

—StopRussia. Чатбот, що допомагає заблокувати Telegram- та YouTube-канали, Facebook-групи, Instagram-профілі, що займаються поширенням дезінформації, а також розповсюджують інформацію щодо місць перебування Збройних Сил України.

—Народний месник - спеціально створений чатбот, куди українці можуть надсилати інформацію про ворожі мітки знайдені у містах і на дорогах країни та про пересування загарбницьких сил Російської Федерації.

—Нам по дорозі. Чатбот, який допомагає українцям з автомобілями та українцям, яким немає чим їхати, знайти одне одного з зкомунікувати.

—Прихисти українців. Чатбот для комунікації тих, хто потребує притулку, і тих людей, які хочуть його надати, знайти одне одного.

—Турботник. Чатбот, який допомагає українським біженцям і переселенцям отримати тимчасовий прихисток та необхідні речі у ЦНАПах, які тимчасово працюють як пункти турботи [76].

Таким чином держава запобігає небезпеці інформаційних атак, попереджає про них в протидії інформаційній війні з боку Російської Федерації.

### **3.2 Контрпропаганда та офіційні сторінки вищих посадових осіб держави, як джерело об'єктивного інформування суспільства**

Організація засобів протидії негативному інформаційному впливу, пов'язаних з користуванням соціальними мережами, сприяє розвитку інформаційної діяльності держави в сфері створення загальнодержавної системи духовних цінностей і є необхідністю сьогодення.

У часи ведення війни боротьба з пропагандою є дуже важливим елементом захисту суверенітету держави, оскільки зараз країна-агресор приділяє велику увагу веденню саме інформаційної війни і розповсюджуючи пропаганду в соціальних мережах.

У цілому масова інформація є способом актуалізації пропаганди спрямованим на формування змінених соціальних процесів. Контрпропаганда ж — це підвид інформаційного впливу, що спрямований на знецінення і руйнацію пропагандованих ідеологій [1].

Контрпропаганда – це здебільш протидія пропаганді, тобто дескрипція дій і ідей поширених ворогом. Головна ціль контрпропаганди це руйнування об'єднань громадян, що виникли в результаті дії пропаганди і насамперед витиснення ідеї, яку в собі несе пропаганда.

Контрпропаганда як і пропаганда націлені в будь-якому випадку на формування певного стилю мислення масової аудиторії і зміну її подальшої поведінки.

Тим не менш контрпропаганда апелює нейтралізацією відкритої пропаганди політичних противників і попереджає негативні наслідки щодо пропагандивної активності.

І таким чином контрпропаганда стає джерелом об'єктивного інформування суспільства.

Тому політична контрпропаганда є дуже важливим елементом попередження протидії пропаганді агресора, однак не єдиним.

Також виділяють наступні контрпропагандистські технології:

—превентивні (попередження про можливий акт пропаганди ще до моменту її появи в медійному полі);

—протидіючі (нейтралізують пропаганду, яка вже поширилась, спростовують некоректну інформацію і недостовірні новини, апелюючи перевіреними даними);

—наступальні (створюють власний акт активної пропаганди в інформаційному полі агресора для протидії можливій пропаганді з його сторони, як у власному інформаційному полі, так і у інфополі країни, що веде даний акт контрпропаганди).

Такі технології працюють на випередження реакції опонента і спрямовані на зменшення поширення пропаганди агресора в майбутньому [67].

У період повномасштабної воєнної агресії Російської Федерації проти України і в час ведення інформаційної війни контрпропаганда з боку України є доволі дієвим засобом забезпечення інформаційної безпеки для держави.

Саме центр протидії дезінформації при Раді національної безпеки і оборони України є головною державною організацією, що активно бореться з російською пропагандою.

Проаналізуємо його роботу на прикладі добірки маніпуляцій і дезінформаційних дописів поширених ворогом 25 го квітня 2022-го року в соціальних мережах і на російському телебаченні.

### Маніпуляція 1.

Російські засоби масової інформації поширили інформацію що «Київська влада зірвала гуманітарну операцію» цивільного населення, що ховаються на території «Азовсталі». Хоча зранку цього ж дня віце-прем'єр-міністр з питань реінтеграції тимчасово окупованих територій України повідомила, що ніяких домовленостей про гуманітарні коридори з «Азовсталі» не було [-1827405823].

### Маніпуляція 2.

Російські пропагандисти заявили, що російське селище Нехотівка, Білгородської області «обстріляли з боку України» і що «пошкоджено житлові будівлі та особистий транспорт».

### Маніпуляція 3.

Кілька російських Telegram-каналів поширили інформацію, що в Курській області Російської Федерації було збито ударний безпілотною «Байрактар», що перебуває на озброєнні Збройних Сил України.

Таким чином, за один день Центр протидії дезінформації при Раді національної безпеки і оборони України спростував, щонайменше три акти пропаганди з боку Росії, що дуже позитивно впливає на забезпечення інформаційної безпеки України.

Окрім Центру протидії дезінформації при Раді національної безпеки і оборони України, вищі посадові особи держави ведуть офіційні сторінки, де також активно займаються сприянням протидії і виявленням недостовірних інформаційних «фейків».

Візьмемо до прикладу офіційну сторінку радника голови офісу президента України Михайла Подоляка у Twitter [79]. У своєму Twitter-акаунті Михайло Подоляк активно освітлює перебіг подій воєнного часу в Україні і поширює пости з спростуванням недостовірної інформації (див. Додаток 7).

Чи Ірина Верещук, віце-прем'єр-міністр з питань реінтеграції тимчасово окупованих територій України, дана представниця влади активно веде сторінку у Facebook [78], доволі часто спростовує дезінформацію яку поширює Росія з приводу гуманітарних коридорів з окупованих Російською Федерацією територій України (див. Додаток 8).

Також дуже часто можна побачити пости зі спростуванням дезінформації і актуальну інформацію щодо війни на сторінці президента України Володимира Зеленського в Instagram [80]. Він як президент України кожного дня з початку війни звертається до народу, розповідає про проведену роботу, про маніпуляції з боку росіян і про перебіг подій в цілому (див. Додаток 8).

Таким чином офіційні представники влади в Україні підтримують бойовий дух народу, показують нашу незламність і доносять до нашого відома тільки перевірену і достовірну інформацію.

А основними джерелами об'єктивного інформування населення України щодо війни є офіційні новинні ресурси і їх пабліки і канали в соціальних мережах, офіційні сторінки вищих посадових осіб держави, сайти міністерств України.

### **3.3 Роль кібервійськ у виявленні, нейтралізації та протидії інформаційним загрозам в процесі воєнної агресії Російської Федерації проти України**

Інформаційна війна займає вагому частину агресії Російської Федерації проти України. І часом не такі видимі як фізичний опір, але тим не менш дієві, наступ і оборона забезпечуються українським кібернетичним фронтом, що інформаційно протистоїть окупантам.

З 24 лютого 2022 р., після початку повномасштабного вторгнення Росії на територію України представники різних приватних ІТ компаній, професіонали, аматори та активісти об'єднались у потужну силу – Кібервійська. На сьогоднішній день відомі такі їх угруповання:

—Кваліфіковані міжнародні професіонали з досвідом роботи з інформаційними технологіями в галузі кібербезпеки.

—Висококваліфіковані фахівці з України в галузі кібербезпеки.

—Українські професіонали, що працювали в інших сферах ІТ і які вирішили долучились до кібернетичного фронту у якості волонтерів.

—Існуючі групи спеціалістів, що сформувалися ще з початку гібридної війни в Україні з боку Російської Федерації що почалась у 2014у році, і вже показали себе у боротьбі із ворогом на ІТ фронті.

—Мотивовані кібер активісти, що не мають спеціальних фахових навичок і досвіду в галузі ІТ, які долучилися до кібервійська і зараз займаються поширенням правди щодо воєнних подій в Україні, беруть участь у контр пропагандистських кампаніях, в пропагандистських актах спрямованих на населення країни-агресора [81].

Саме такі кібернетичні війська охороняють критичну інфраструктуру та мережі в Україні, відбивають хакерські атаки ворога, наносять власні хакерські атаки на мережу країни-агресора і їх центри даних, займаються кібернетичним шпіонажем, проводять інформаційні кампанії щодо захисту України, а також протидіють розповсюдженню дезінформації і «фейків» ворогом.

Сфера інформаційних технологій в Україні останніми роками розвивалася швидкими темпами, але не дивлячись на це все одно важливі інформаційні системи, сайти міністерств України, державні бази даних не були достатньо захищені. Та буквально за перший тиждень повномасштабної війни Російської Федерації проти України ситуація суттєво покращилася. Оскільки всі зрозуміли наскільки важливо мати захищене від ворога інформаційне поле. Тим паче від Росії.

У Російській Федерації завжди зосереджувалась еліта сфери інформаційних технологій і їхні ІТ спеціалісти завжди вважалися дуже висококваліфікованими, до того ж російські кібервійська Головного управління Генерального штабу Збройних Сил Російської Федерації давно були в бойовій готовності до завдання вирішальних ударів по найважливішим цифровим системам і сайтам України. Була навіть спеціально підготовлена програма шкідник «wiper malware», яка була націлена на стирання даних і при її використанні паралізувала б переважну кількість систем критичної інфраструктури України.

І в перші дні повномасштабної війни дійсно відбулись масштабні кібернетичні атаки з боку Росії на українську інфраструктуру: вони заблокували сайти, копіювали бази даних, стирали цілі інформаційні ресурси, вторгались на сайти і розміщували

там свою інформацію, взламували банківські системи і мережі провайдерів телефонного зв'язку. Але український кібернетичний фронт достойно оборонявся.

Тож наші кібервійська швидко все відновлювали. Це було неочікуваним поворотом подій для Росії, оскільки саме на кібератаки вона і робила величезні ставки [82].

Російська Федерація хотіла повністю відключити Україну від Інтернету і зруйнувати мобільний зв'язок, щоб впровадити свої інформаційні засоби комунікації і своїх операторів телефонного зв'язку. Таким чином Росія збиралась заручитись підтримкою українців способом пропаганди через ці джерела.

Та злагоджена дія українських ІТ професіоналів не дала планам ворога відбутись.

Звісно наш кібернетичний фронт працює не без допомоги інших країн і представників кібервійськ з усього світу. Наприклад організація хакерів з усього світу Anonymous. Це неурядова міжнародна організація кібернетичних активістів, що відома всім після численних атак на урядові системи і корпорації. Дане об'єднання виникло у 2003 році на закритому вебфорумі 4chan.

Починаючи з 26 лютого 2022 року вони активно допомагають Україні в веденні інформаційної війни з Росією. Вже на третій день повномасштабної війни дана організація виклала в мережу, з доступом для всіх, сотні гігабайтів конфіденційних даних різних російських державних органів і сприяли припиненню функціонування десятків урядових сайтів та пропагандистських новинних ресурсів. Їм навіть вдалося зламати російське телебачення, а якщо бути точнішими, потокові сервіси Російської Федерації.

Саме організація Anonymous оголосила Росії кібервійну в перші дні повномасштабного вторгнення Російської Федерації в Україну. І їхні дії не забарились. Протягом цієї кібервійни команда Anonymous вже зробила величезний внесок в ослаблення Росії.

7 березня об'єднання Anonymous засобом злому російського телебачення, показало на російських каналах реальні кадри війни з України і руйнування життя мирних українців, таким чином вони намагалися відкрити очі росіянам, також вони

вивели з ладу такі російські потокові сервіси як Ivi I Wink (Сайти для перегляду фільмів і серіалів).

Цікаву акцію провели Anonymouse зробивши заяву, що вони збираються зламати сайти понад п'ятиста компаній які або не вийшли з ринку Росії або не повністю призупинили свій бізнес або залишились на ринку. А поширення закритих даних таких компаній спонукає до величезних матеріальних втрат, оскільки даною інформацією можуть скористатись конкуренти компаній і це принесе за собою великі грошові витрати.

І вже на наступний день 2 великі іноземні компанії повністю закрили свій бізнес в Росії. Однак далеко не всі, але тим не менш допомога організації Anonymouse на кібер фронті дійсно вартісна для України.

Таким чином зламуючи сайти і зливаючи дані банківських служб, державних органів і реєстрів, дана хакерська організація допомагає Росії наблизитись до дефолту і повної недовіри населення до влади.

Отже спочатку повномасштабної воєнної агресії Російської Федерації на території України хакерська організація Anonymouse провели наступні кібератаки станом на 5 квітня 2022 року:

—масове розповсюдження закритих даних російських держорганів ( починаючи з 24 го березня 2022-го року);

—злам сайту «Роскомнагляду» (10 березня 2022-го року);

—злам сайту російської державної корпорації «Росатом» (15 березня);

—публікація 28 гігабайтів інформації користувачів, отриманої після зламу сайту Центробанку РФ (26 березня 2022-го року);

—оприлюднення таємного наказу виконуючого обов'язки міністра оборони російської федерації Дмитра Булгакова про підготовку фейкових відео, на яких нібито український військові мали знущатись над російськими військовополоненими (28 березня 2022-го року) ;

—злам Всеросійської державної телевізійної і радіомовної компанії медіа пропаганди Кремля (28 березня 2022-го року);



—злам інвестиційної компанії, що належить зам міністру закордонних справ Російської Федерації (31 березня 2022-го року);

—поширення 15-ти гігабайт злитих даних викрадених у благодійного крила російської православної церкви (02 квітня 2022-го року);

—злам інформаційних ресурсів російського «Липецького механічного заводу», що випускає компоненти для виготовлення зенітно-ракетних установок (02 квітня 2022 року).

Йде інформаційна війна і не без допомоги західних спецслужб. В перших числах квітня 2022 року спеціалісти американського Федерального Бюро Розслідувань забрали під свій контроль, а згодом і зовсім відключили пристрої і мережу, які використовували російські хакери що працюють на державу, таким чином перекривши їм кисень [31].

У цей же час німецька спецслужба успішно провела інформаційну кібер операцію проти кримінального крила російський хакерських угруповань, відомої мережі Hydra і «поклала» її.

Отже, таким чином кібернетичні війська роблять величезний вклад в приближення перемоги України. Бо головним засобом ведення війни Російська Федерація ще з 2014-го року виділяла саме інформаційну війну. Але завдяки українським і світовим ІТ спеціалістам і хакерам, Росія вперше перетворилася з кібернетичного агресора, в жертву масштабних хакерських атак. Саме інформаційний фронт допомагає нам пришвидшити падіння Росії у цій війні і саме він перевернув хід гри.

## ВИСНОВКИ

У кінці ХХ - на початку ХХІ століття були створені перші соціальні мережі і протягом останніх 20 років вони ставали все більш популярними і широко використовуваними серед людей в усьому світі. Зараз вони відіграють провідну роль у дистанційному спілкуванні між людьми і поширенні інформації.

У період повномасштабної воєнної агресії Російської Федерації проти України в 2022 р., інформаційна війна стала невід'ємним елементом протистояння. А основним засобом і місцем ведення інформаційної війни стали саме соціальні мережі. Оскільки саме пересічні громадяни України і Росії є рушійною силою у веденні даного протистояння, то і масштаби Інтернет-війни значні.

Все це є прямою загрозою інформаційній безпеці України. Тому необхідно своєчасно розвивати інформаційну сферу держави і шукати й розвивати нові способи забезпечення інформаційної безпеки в соціальних мережах, такі як створення державних ботів для формування суспільної думки з актуальних питань і обговорення важливих новин, блокування акаунтів окремих медійних осіб, що несуть загрози інформаційній безпеці держави, створення спеціальних державних Інтернет-ресурсів щодо протидії дезінформації.

Щодо головних проблем захисту національних інтересів України в соціальних мережах, то на даний момент це:

- кібертероризм з боку Російської Федерації і держав, що підтримують її політику;
- поширення конфіденційної інформації здобутої внаслідок кібератак на українські Інтернет-ресурси;
- розповсюдження в глобальному інтернет-просторі недостовірної й упередженої інформації;
- російська пропаганда, що поширюється в соціальних мережах.

В умовах протистояння повномасштабній воєнній агресії Російської Федерації, національне інформаційне поле України не є повністю захищеним від

негативних пропагандистських впливів і загроз, тому саме створення потужної ефективної системи інформаційної безпеки України є основним завданням органів державної влади і недержавних інституцій в Україні.

Основною складовою ведення війни в інформаційному полі є пропаганда. Це важливий інструмент, який несе в собі і позитивні і негативні наслідки. Російська Федерація у війні з Україною використовує саме негативну пропаганду, таким чином створюючи інформаційну ізоляцію від зовнішніх джерел для придушення можливих бунтів і для створення вузького бачення ситуації, що відбувається у росіян. Такого роду пропаганда подає тільки певну інформацію, вигідну для створення певної громадської думки у людей, при цьому приховуючи невігідну інформацію.

Нами досліджено, що величезний вклад в поширення пропаганди і дезінформації з боку Росії роблять блогери. Оскільки вони є інфлюенсерами для своїх підписників, то до них прислухаються. І переважно блогери з Росії чи проросійські блогери з України за гроші поширюють заготовлений для них текст у соціальних мережах у підтримку політики президента Російської Федерації і підтримку «спецоперації в Україні» або створюють цілі тренди в підтримку російського режиму. Таким чином блогери є основними розповсюджувачами дезінформації і відповідно Інтернет-злочинцями.

Важливою складовою у веденні інформаційної війни, зокрема в пропаганді є «фейкові новини». Така розповсюджена неперевірена інформація викликає появу панічних настроїв у читачів і викликає напругу у суспільстві, таким чином дестабілізуючи ситуацію у суспільстві. Російська Федерація користується таким введенням війни в інформаційному полі ще з початку 2014 р., коли почалась гібридна війна на Сході України. Така загроза інформаційній безпеці України є суттєвою оскільки діє на масову свідомість людей, тому дуже важливо проводити заходи з спростування таких недостовірних новин аби не наводити паніку у суспільстві.

Основою державної політики України на даний момент є насамперед боротьба з дезінформацією. У державі працює спеціальний Центр при Раді національної

безпеки і оборони України з протидії дезінформації, що спростовує неправдиві новини і заяви. Переважно вся державна інформаційна політика України в період повномасштабної воєнної агресії Російської Федерації проти України спрямована на захист інформаційного простору України.

Створення засобів протидії негативному інформаційному впливу, пов'язаних з користуванням соціальними мережами, сприяє розвитку інформаційної діяльності держави в сфері створення загальнодержавної системи духовних цінностей і є необхідністю сьогодення.

З'ясовано важливий акцент у веденні інформаційної війни: Росія першопочатково робила на хакерські атаки українських Інтернет-ресурсів, але українські кібервійська дали російським хакерам відсіч і показали свій професіоналізм у захисті українського інфопростору, а також перетворили саму Російську Федерацію в жертву масштабних хакерських атак. Отож кібернетичні війська роблять великий вклад у приближення перемоги України.

Таким чином, не дивлячись на загрози інформаційній безпеці України в соціальних мережах з боку Російської Федерації, Україна тримає оборону інформаційного простору і навіть здійснює контратаку. А державна політика в сфері інформаційної безпеки приймає виклики часу і захищає національні інтереси держави.

## СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Баровська А.В. Стратегічні комунікації vs пропаганда та контрпропаганда. Інформаційне суспільство в Україні: стан, проблеми, перспективи. / Упоряд.: М. Маюга; за заг. ред. д. держ. упр., проф. Н.В. Грицяк. Навч.-метод.посіб.-К: «Видавництво «Тезис», 2015. С. 60–63.
2. Бебик В.М. Менеджмент виборчої кампанії: ресурси; технології; маркетинг: Навч.-метод.посіб.-К.:МАУП, 2001.-216с.
3. Брижко В.М.,Цимбалюк В.С., Орехов А.А. Е-будущее и информационное право/Под ред. Р.А. Калужного, М.Я. Швеца.-К.: «Интеграл», 2002.-264 с.
4. Висоцький О. Ю. Стратегії фокусування та дефокусування уваги як інструменти пропаганди / О. Ю. Висоцький // Філософія, теорія та практика випереджаючої освіти для сталого розвитку : матеріали III Всеукраїнської науковопрактичної конференції. 14 грудня 2017 р., м. Дніпро, ДОШПО. Частина I. – Дніпро, 2018. – С. 110–113.
5. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентіві України. 2015. № 1. С. 136–141.
6. Гришук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Гришук, Ю. Г. Даник; під заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.
7. Дарморіз О.В. Війна як концепт соціальної міфології. Актуальні проблеми філософії та соціології. 2017. Вип. 18. С. 33–35.
8. Дубов Д.В. Державна інформаційна політика України в умовах гібридного миру та війни. Стратегічні пріоритети. 2016. № 3(40). С. 86–93
9. Золотар О. О. Класифікація загроз інформаційної безпеки .О. О. Золотар, І. О. Трубін. Інформація і право. – 2013. – № 3(9). – С. 105–112.
10. Остапенко Г. А., Парінова Л. В. Информационные риски в социальных сетях // Под ред. член-корр. РАН Д.А. Новикова. 2013. 161с.
11. Толубка В. Б.. Інформаційна безпека держави у контексті протидій інформаційними війнами: Навчальний посібник: НАОУ, 2004. – 315 с.

12. Шамрай В.О. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії та практики. Монографія/ За ред.Р.А.Калужног– Київ,2002.-296 с.
13. Шемшученко Ю.С. Інформаційне законодавство: Збірник законодавчих актів: У 6 т. Навч. посібник.:ТОВ "Видавництво "Юридична думка", 2005.-328 с.
14. Конах В. К. Національний інформаційний простір України: проблеми формування та державного регулювання : аналіт. доп. / В. К. Конах. – К. : НІСД, 2014. – 76 с.
15. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України [Текст]: монографія / Б. А. Кормич.– Одеса : Юридична література, 2007. – 471 с.
16. Красноступ Г.М. Організаційно-правові аспекти необхідності реформування сучасного інформаційного законодавства // Бизнес и безопасность.- 2005.-№ 6.- С.15-16.
17. Куц Г.М. Пріоритетні стратегії інформаційної політики у контексті національних інтересів України: ліберальний ракурс. політичне життя. 2017. № 3. С. 52–58.
18. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії : монографія. Київ : Сатсанга, 2000. 222 с.
19. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.
20. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Текст] : Навч. посібник: КНТ, 2006.
21. Лукашенко А.І. Ментальні структури агресора в інформаційній війні на прикладі російської федерації: погляд із минулого в сучасність, виклики західному суспільству. Збірник наукових праць «Гілея». 2019. Вип. 144. С. 72–75.
22. Молодецька К. В. Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави / К. В. Молодецька // Information technology and security. – 2016. – Vol. 4, Iss. 1(6). – С. 13–20.

23. Грищук Р.В. Наукова стаття: «Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах» Навч. посібник: КНТ, 2019– с. 6–10.

24. Корченко О. Г. Ознаковий принцип формування класифікацій кібератак / О. Г Корченко, С. В. Казмірчук, Є. В. Паціра, С. О. Гнатюк, В. М. Кінзерявий Ознаковий принцип формування класифікацій кібератак// Вісник СНУ ім. В. Даля. – 2010. – №4, т. 1. – С. 184–193.

25. Почепцов Г. Сучасні відомості війни / Г. Почепцов. – К. : Вид.дім «Києво-Могилянська академія» 2015. – 497 с.

26. Проблеми суспільної безпеки в процесі розвитку соціальних мереж : [монографія] / [В. Попик (кер. проекту), В. Горовий, О. Онищенко та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – Київ, 2015. – 202 с.

27. Расторгуев С.П. Информационная война. – М.: Радио и связь, 1998.

28. Свобода інформації та право на приватність в Україні. Том 2. Право на приватність: *conditio sine qua non*/Харківська правозахисна група, Харків: Фоліо, 2004.-200 с.

29. Соціальні мережі як чинник розвитку громадянського суспільства : [монографія] / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. – 220 с.

30. Юдін О. К. Інформаційна безпека держави : навч. посіб. / О. К. Юдін , В. М. Богущ. – Харків: Консум, 2004. – 508 с.

Електронні джерела:

31. Анатоль Рапопорт Аналітика соціальних мереж [Електронний ресурс]. – Режим доступу: [https://wikiukuk.top/wiki/Anatol\\_Rapoport#Social\\_network\\_analysis](https://wikiukuk.top/wiki/Anatol_Rapoport#Social_network_analysis) (дата звернення 22.04.2022)

32. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко. – Режим доступу: <http://www.crime-research.iatp.org.ua/library/strateg.htm> (дата звернення 16.04.2022)

33. Відео фрагменту виступу Тіни Канделаки на концерті в Лужниках [Електронний ресурс]. – Режим доступу: <https://www.youtube.com/watch?v=iRYxNDzJwew> (дата звернення 22.04.2022)
34. Вікіпедія Анатолій Шарій [Електронний ресурс]. – Режим доступу: <https://cutt.ly/4JkOe96> (дата звернення 22.04.2022)
35. Вікіпедія Історія Антарктики [Електронний ресурс]. – Режим доступу: <https://cutt.ly/5JkOahB> (дата звернення 30.04.2022)
36. Вікіпедія Луї Пастер [Електронний ресурс]. – Режим доступу: <https://cutt.ly/dJkOdif> (дата звернення 16.04.2022)
37. Вікіпедія Микола Басков [Електронний ресурс]. – Режим доступу: <https://cutt.ly/YJkOoqf> (дата звернення 10.04.2022)
38. Вікіпедія Пропаганда <https://cutt.ly/PJkOq3E>
39. «Вітер із Холодного Яру»: як працює кібернетичний опір російській агресії [Електронний ресурс]. – Режим доступу: <https://cutt.ly/dJkIGeI> (дата звернення 30.04.2022)
40. Вплив та значення фейків у світовій історії | Наукові журнали та конференції [Електронний ресурс]. – Режим доступу: <https://science.lpnu.ua/uk/sjs/vsi-vypusky/vypusk-4-nomer-2020/vplyv-ta-znachennya-feykiv-u-svitoviy-istoriyi> (дата звернення 22.04.2022)
41. Втрати окупантів на кіберфронті [Електронний ресурс]. – Режим доступу: <https://www.epravda.com.ua/publications/2022/04/7/685362/> (дата звернення 10.04.2022)
42. Гіперзвукова зброя: про її можливості та нові світові виклики [Електронний ресурс]. – Режим доступу: <https://mind.ua/openmind/20207704-giperzvukova-zbroya-pro-yiyi-mozhливosti-ta-novi-svitovi-vikliki> (дата звернення 10.05.2022)
43. Горбань Ю.О. Інформація про проти України та засоби її ведення [Електронний ресурс] / Ю. О. Горбань. [Електронний ресурс]. – Режим доступу: <http://www.visnyk.academy.gov.ua/wp-content/uploads/2015/04/20.pdf> (дата звернення 20.04.2022)



44. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В. Гусаров. [Електронний ресурс]. – Режим доступу: <http://www.osvita.mediasapiens.ua/material/34281> (дата звернення 30.04.2022)
45. Дивовижні Статистики в Інтернеті і соціальних медіа в 2022 році – [Електронний ресурс]. – Режим доступу: <https://cutt.ly/yGkY5Kv> (дата звернення 29.04.2022)
46. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: <http://www.zakon3.rada.gov.ua/laws/show/514/2009> (дата звернення 06.04.2022)
47. Захист інформаційної безпеки як функції держави [Електронний ресурс]. – Режим доступу: <http://www.mego.info/material/23-zakhystinformatsiinoi-bezpeky-ia-k-funktsiia-derzhavy> (дата звернення 12.04.2022)
48. Інстаграм пропаганда <https://cutt.ly/BJkI5GG>
49. Історія ведення блогів [Електронний ресурс]. – Режим доступу: [https://uk.upwiki.one/wiki/History\\_of\\_blogging](https://uk.upwiki.one/wiki/History_of_blogging) (дата звернення 22.04.2022)
50. Концепція національної безпеки України [Електронний ресурс]. – Режим доступу: [http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1](http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1) (дата звернення 12.04.2022)
51. Литва заявила про пряму співпрацю Шарія з Кремлем [Електронний ресурс]. – Режим доступу: [https://novyny.online.ua/shariy-napryamu-spivpratsyue-z-kremlem-departament-derzhbezpeki-litvi\\_n844436/](https://novyny.online.ua/shariy-napryamu-spivpratsyue-z-kremlem-departament-derzhbezpeki-litvi_n844436/) (дата звернення 12.04.2022)
52. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу: <https://cutt.ly/HJkPrS5> (дата звернення 30.04.2022)
53. Медвідь Ф. Інформаційна безпека України: виклики та загрози [Електронний ресурс] / Ф. Медвідь. – Режим доступу: <http://www.nato.ru.if.ua/journal/2009-2-28.pdf> (дата звернення 06.04.2022)
54. Методи впливу пропаганди та протидія їм [Електронний ресурс]. – Режим доступу: <https://imi.org.ua/monitorings/metody-vplyvu-propagandy-ta-protydiya-nym-i30638> (дата звернення 06.04.2022)

55. Методи інформаційного захисту простору. Інформаційна безпека України [Електронний ресурс]. – Режим доступу: <http://www.ua.textreferat.com/referat-7471.html> (дата звернення 02.04.2022)
56. Микола Басков захищатиме батьківщину від колег [Електронний ресурс]. – Режим доступу: <https://cutt.ly/SJkOy1w> (дата звернення 30.04.2022)
57. МІП : «Інформаційні війська України» стають самостійним проектом. [Електронний ресурс]. – Режим доступу: <http://mip.gov.ua/news/1931.html> (дата звернення 30.04.2022)
58. Офіційна сторінка Ірини Верещук в Facebook [Електронний ресурс]. – Режим доступу: <https://ru-ru.facebook.com/vereshchuk.ukraine> (дата звернення 30.04.2022)
59. Офіційна сторінка Михайла Подоляка у Twitter [Електронний ресурс]. – Режим доступу: <https://cutt.ly/AJkIOuj> (дата звернення 30.04.2022)
60. Офіційний акаунт президента України Володимира Зеленського в Instagram [Електронний ресурс]. – Режим доступу: [https://www.instagram.com/zelenskiy\\_official/](https://www.instagram.com/zelenskiy_official/) (дата звернення 30.04.2022)
61. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: <http://www.justinian.com.ua/article.php?id=3222> (дата звернення 10.04.2022)
62. Правове забезпечення державної інформаційної політики [Електронний ресурс]. – Режим доступу: [https://minjust.gov.ua/m/str\\_22116](https://minjust.gov.ua/m/str_22116) (дата звернення 16.04.2022)
63. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/n0004525-14#Text> (дата звернення 02.04.2022)
64. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351. Із зміни, внесеними згідно із Законом № 3200-IV [1/3] ЕПІДЕМІЯ ДЕЗІНФОРМАЦІЇ: ЧОМУ ФЕЙКИ СТАЛИ

ЧАСТИНОЮ НАШОГО ЖИТТЯ І ЯК “ВАКЦИНУВАТИСЯ” [Електронний ресурс]. – Режим доступу: <https://cedem.org.ua/analytics/epidemiya-dezinformatsiyi/> (дата звернення 22.04.2022)

65. Про що не слід писати у соцмережах під час війни: пояснює Мінцифри <https://cutt.ly/9JkI0rR> (дата звернення 21.04.2022)

66. Проект Концепції інформаційної безпеки України : Офіційний сайт Міністерства інформаційної політики України. [Електронний ресурс]. – Режим доступу: <https://mkip.gov.ua/cr/documents/30.html> (дата звернення 10.04.2022)

67. Пропаганда: історія питання [Електронний ресурс]. – Режим доступу: <https://uchoose.info/propaganda-istoriya-pytannya/> (дата звернення 05.04.2022)

68. Рей Соломоноф [Електронний ресурс]. – Режим доступу: [https://www.no-regime.com/ru-ru/wiki/Ray\\_Solomonoff#Life\\_history\\_through\\_1964](https://www.no-regime.com/ru-ru/wiki/Ray_Solomonoff#Life_history_through_1964) (дата звернення 03.04.2022)

69. Соціальна мережа. [Електронний ресурс]. – Режим доступу: <https://igroup.com.ua/seo-articles/sotsialna-merezha/> (дата звернення 26.04.2022)

70. Соціальні мережі: поняття, історія виникнення. [Електронний ресурс]. – Режим доступу: <http://old.zounb.zp.ua/Sotsial%CA%B9ni%20merezhi%3A%20ponyattya%2C%20istoriya%20vynyknennya> (дата звернення 06.04.2022)

71. Стаття «Поняття і класифікація рейкових новин» [http://journals.iir.kiev.ua/index.php/pol\\_n/article/viewFile/3936/3589](http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3936/3589) (дата звернення 10.04.2022)

72. Сторінка Мінцифри у Instagram [Електронний ресурс]. – Режим доступу: <https://www.instagram.com/mintsyfra.official/> (дата звернення 10.04.2022)

73. Сторінка співака Миколи Баскова в Instagram [Електронний ресурс]. – Режим доступу: <https://instagram.com/nikolaibaskov?igshid=YmMyMTA2M2Y=> (дата звернення 16.03.2022)

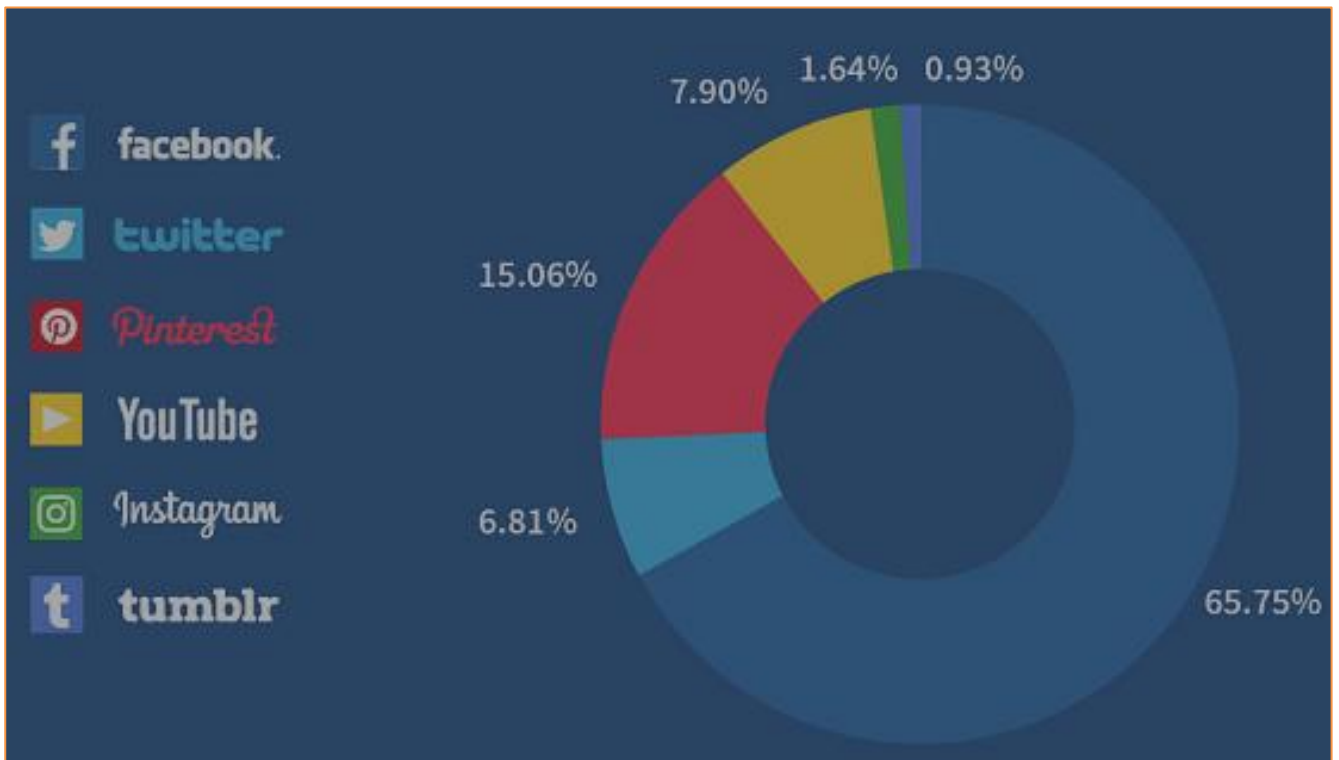
74. Сторінка телеведучої Тіни Канделакі в Instagram [Електронний ресурс]. – Режим доступу: [https://instagram.com/tina\\_kandelaki?igshid=YmMyMTA2M2Y=](https://instagram.com/tina_kandelaki?igshid=YmMyMTA2M2Y=) (дата звернення 30.04.2022)

75. Танці на своїх же кістках. Чому над «кримським» концертом Путіна в Лужниках глузують всупереч старанням пропагандистів [Електронний ресурс]. – Режим доступу: <https://nv.ua/ukr/world/countries/u-moskvi-vidbuvsya-propagandistskiy-koncert-miting-yakiy-ospivuvav-vtorgnennya-rf-v-ukrajinu-50226376.html> (дата звернення 16.04.2022)
76. У Росії заблокували Інстаграм [Електронний ресурс]. – Режим доступу: <https://www.epravda.com.ua/news/2022/03/11/683798/> (дата звернення 30.04.2022)
77. Україна назвала Тіну Канделаки одним із головних рупорів пропаганди Кремля: ведучу оголосять у міжнародний розшук [Електронний ресурс]. – Режим доступу: <https://news.obozrevatel.com/ukr/show/people/ukraina-nazvala-tinu-kandelaki-odnim-iz-golovnih-ruporiv-propagandi-kremlya-veduchu-ogolosyat-u-mizhnarodnij-rozshuk.htm> (дата звернення 16.04.2022)
78. Фейкові новини та дезінформація: що таке інформаційна гігієна та як її дотримуватися [Електронний ресурс]. – Режим доступу: <https://thepage.ua/ua/experts/fejkovi-novini-ta-dezinformaciya-sho-take-informacijna-gigiyena-ta-yak-yiyi-dotrimuvatis> (дата звернення 28.04.2022)
79. Феномен Арестовича <https://cutt.ly/jJkI3WI> (дата звернення 02.05.2022)
80. Чатботи, які допоможуть українцям під час війни [Електронний ресурс]. – Режим доступу: <https://cutt.ly/lJkIUpW> (дата звернення 01.05.2022)
81. Що таке соціальні мережі (види, класифікація, безпека...) [Електронний ресурс]. – Режим доступу: <https://futurenow.com.ua/shho-take-sotsialni-merezhi-vydy-klasyfikatsiya-bezpeka/> (дата звернення 10.04.2022)
82. Instagram попереджатиме про російську пропаганду та захищатиме користувачів з України [Електронний ресурс]. – Режим доступу: <https://cutt.ly/eJkI4B8> (дата звернення 17.04.2022)
83. Social Media Stats Worldwide [Електронний ресурс]. – Режим доступу: <https://gs.statcounter.com/social-media-stats> (дата звернення 25.04.2022)

## ДОДАТКИ

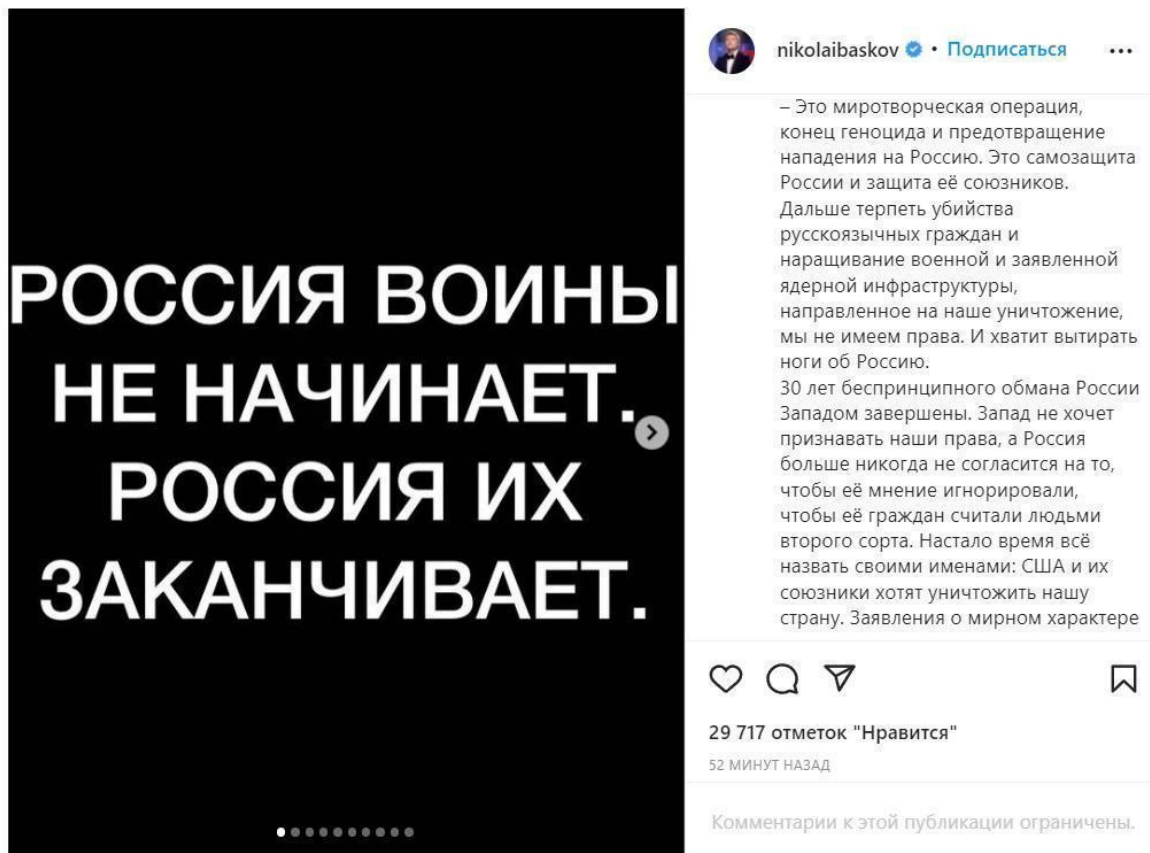
Додаток А

Діаграма світових лідерів соціальних медіа ресурсів





## Публікація Миколи Баскова на сторінці в Instagram



**РОССИЯ ВОИНЫ  
НЕ НАЧИНАЕТ.  
РОССИЯ ИХ  
ЗАКАНЧИВАЕТ.**

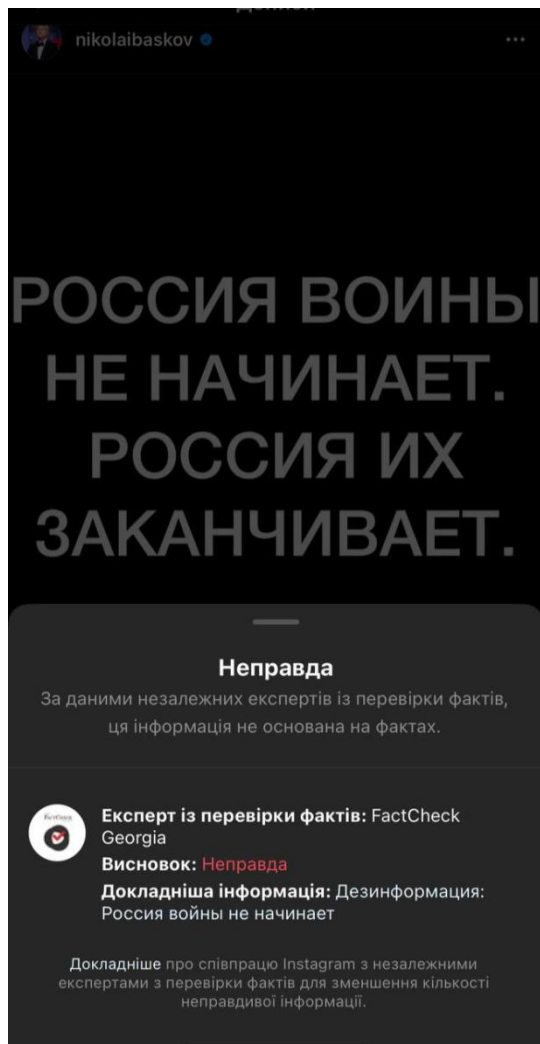
nikolaibaskov • Подписаться

– Это миротворческая операция, конец геноцида и предотвращение нападения на Россию. Это самозащита России и защита её союзников. Дальше терпеть убийства русскоязычных граждан и наращивание военной и заявленной ядерной инфраструктуры, направленное на наше уничтожение, мы не имеем права. И хватит вытирать ноги об Россию. 30 лет беспринципного обмана России Западом завершены. Запад не хочет признавать наши права, а Россия больше никогда не согласится на то, чтобы её мнение игнорировали, чтобы её граждан считали людьми второго сорта. Настало время всё назвать своими именами: США и их союзники хотят уничтожить нашу страну. Заявления о мирном характере

29 717 отметок "Нравится"  
52 МИНУТ НАЗАД

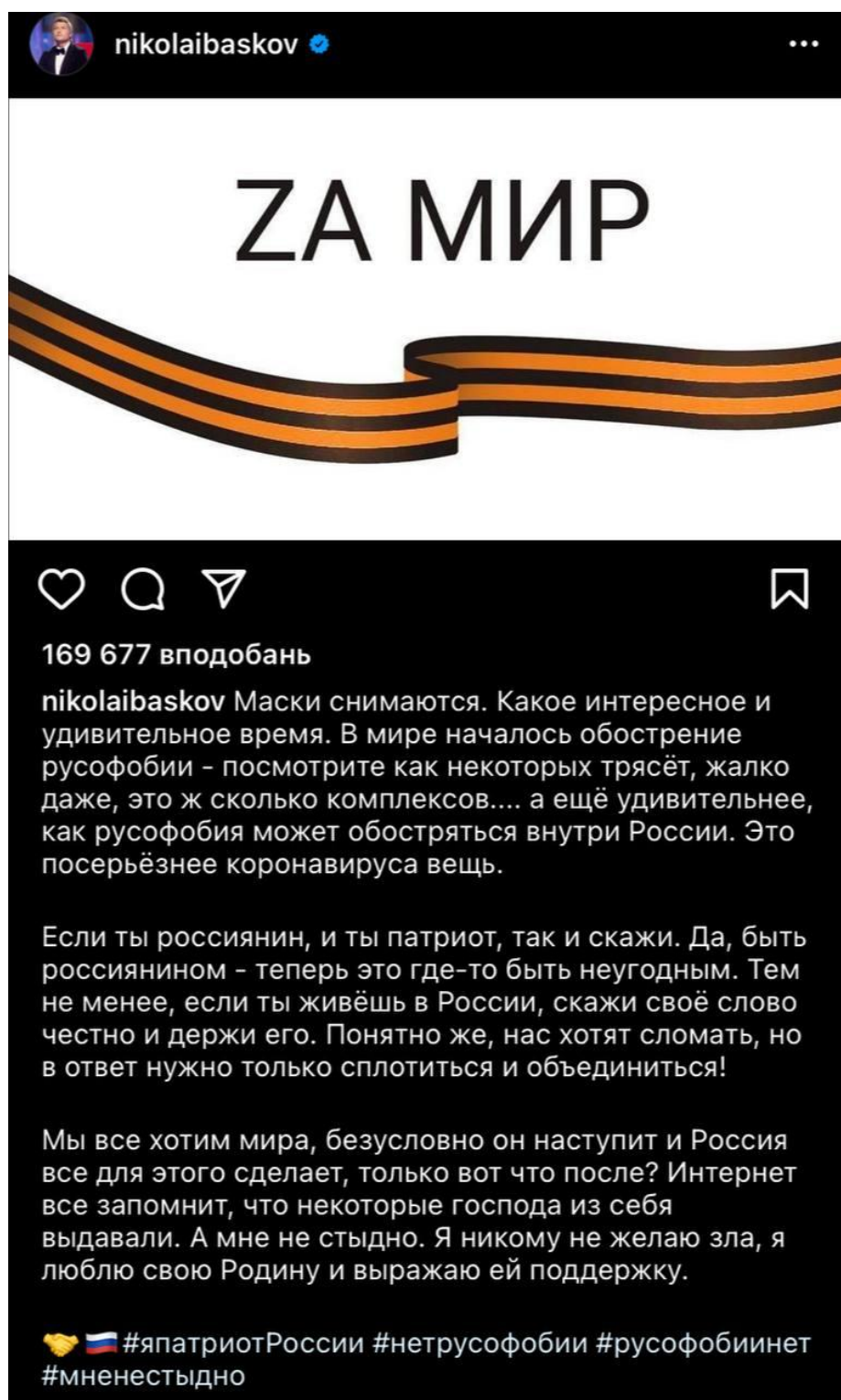
Комментарии к этой публикации ограничены.

Попередження від Instagram з приводу того, що публікація Миколи Баскова є неправдивою





## Публікація Миколи Баскова на сторінці в Instagram



Документ Департаменту державної безпеки Литви, в якому йдеться про пряму співпрацю Анатолія Шарія з адміністрацією президента Російської Федерації

Володимира Путіна

LIETUVOS RESPUBLIKOS VALSTYBĖS SAUGUMO DEPARTAMENTAS

Vilniaus miesto apylinkės teismui  
Laisvės pr. 79A  
LT-05274 Vilnius

2022-04-14 Nr. 18-3364  
[ 2022-03-24 Nr. e2-86-937/2022

DĖL PATIKSLINTOS IŠVADOS PATEIKIMO

Vilniaus miesto apylinkės teismas (toliau – Teismas) pagal ieškovo Anatolii Sharii ieškinį nagrinėjamoje civilinėje byloje Nr. e2-86-937/2022 2022 m. kovo 16 d. protokoline nutartimi Lietuvos Respublikos valstybės saugumo departamentą (toliau – VSD) įpareigojo pateikti patikslintą išvadą.

Atsižvelgdamas į tai, VSD teikia turimą žvalgybos informaciją ir patikslintą išvadą dėl ieškovo Anatolii Sharii keliamos grėsmės valstybės saugumui.

Kaip buvo paminėta ir 2020 m. spalio 30 d. raštu Nr. 18-10236 teiktoje VSD išvadoje (toliau – Išvada), VSD neturi informacijos apie tai, ar Anatolii Sharii iš Ukrainos pabėgo dėl 2013 m. Ukrainoje kilusios vadinamosios Maidano revoliucijos. VSD vertinimu, Anatolii Sharii viešai skelbiama informacija apie Ukrainos vidaus politinius ir socialinius procesus, karą Rytų Ukrainoje, pasisakymus Krymo okupacijos klausimu Rusijos žiniasklaida naudojo savo propagandiniams tikslais, siekdama destabilizuoti Ukrainos vidaus politinę ir socialinę padėtį, demoralizuoti ir skatinti visuomenės nepasitikėjimą Ukrainos valdžios ir teisėsaugos institucijomis, diskredituoti Maidano revoliuciją. Taip pat Anatolii Sharii šiais klausimais dalyvaudavo Rusijos televizijos propagandinėse laidose ar duodamas interviu interneto portalams.

Papildomai (jau po Išvados pateikimo Teismui) gautais VSD žvalgybos duomenimis, Ukrainos Respublikos pilietis Anatolii Sharii bendradarbiauja su priešišką veiklą prieš Lietuvos Respubliką ir kitas užsienio valstybes vykdančia Rusijos Federacijos (toliau – RF) valstybės institucija – RF prezidento administracija. VSD, remdamasis turimais žvalgybos duomenimis, vertina, kad A. Sharii yra asmuo, kurį RF išnaudoja siekdama politinės ir informacinės įtakos užsienio valstybėse, o jo veikla yra ne jo politinių įsitikinimų išraiška, o Lietuvos Respublikai priešiško subjekto užduočių vykdymas.

Remdamasis surinkta žvalgybos informacija, VSD vertina, kad A. Sharii buvimas Lietuvos Respublikoje kelia grėsmę valstybės saugumui. Pastebėtina, kad šis VSD vertinimas atsispindi administracinėje byloje Nr. e13-3636-595/2021, kuri Teismui atsiųsta 2022 m. balandžio 4 d. įdėdžiu Nr. e13-3636-595/2021.

Direktoriaus pavaduotojas,  
einantis direktoriaus pareigas

Vaidotas Mažeika

## Публікації Михайла Подоляка зі спростуванням дезінформації в Twitter

**!** Радник керівника Офісу президента Михайло Подоляк спростував твердження голови МЗС Росії Сергія Лаврова про нібито перемовини України з РФ про скасування санкцій, "денацифікацію" та "демлітаризацію".

Зокрема, Подоляк наголосив, що жодного разу не бачив Лаврова за столом переговорів між українською та російською делегаціями.

*"Не вперше доводиться говорити, що між фактами і фантазіями у представників РФ занадто велика дистанція", - зазначив Подоляк.*

**Михайло Подоляк** @Podolyak\_M · 7 год  
#Lavrov's direct anti-Semitic statements, accusations of Jews of the WWII and the Holocaust are the evidence of Russia being a successor to Nazi ideology. By trying to rewrite history, Moscow is simply looking for arguments to justify the mass murders of Ukrainians. (1/2)

94 1 112 4 315



**Михайло Подоляк** @Podolyak\_M · 6 год  
Відверті антисемітські заяви #Лаврова, звинувачення євреїв у WWII й Голокості – ще одне свідчення, що саме Росія є правонаступником нацистської ідеології. Намагаючись переписати історію, Москва просто шукає аргументи для виправдання масових убивств українців. (1/2)

37 504 2 629

**Михайло Подо...** @Podolyak... · 30 квіт.  
«Звільнити світ від Заходу» – Росія знову озвучила нову мету руйнівної «спецоперації» Україні. «Звільнення» по-російськи – це лише масові знищення. Втім, наступні цілі спецоперації РФ можуть стосуватися «звільнення» Марса від впливу марсіан. Чекаємо.

59 332 2 804

**Михайло Подол...** @Podolyak... · 22 год  
Дивлячись на склад Ради безпеки РФ та на окремих пропагандистів, маю одне питання: цікаво, хто як поводитиметься на Нюрнберзькому трибуналі 2.0? Хто даватиме свідчення та активно співпрацюватиме зі слідством, а хто просто не зможе пережити поразку? Ваші припущення?

127 326 3 623

# Сторінка Ірини Верещук у Facebook


facebook

Електронний адрес ил  Пароль

 Ірина Верещук




 [minre.gov.ua](http://minre.gov.ua)

 **Всегда открыто** ▾

## Фото

[Все фото](#)



 Ірина Верещук

25 апрель в 14:32 · 🌐

! Сьогодні російська сторона вчергове заявила про існування коридору для виходу цивільних осіб з Азовсталі.

Цьому можна було б вірити, якби росіяни багато разів до того не зривали гуманітарні коридори. Я знаю, що говорю, бо за дорученням Президента особисто веду такі переговори та займаюся організацію гуманітарних коридорів.

Важливо розуміти, що гуманітарний коридор відкривається за домовленості двох сторін. Коридор, анонсований в односторонньому порядку, не забезпечує б... **Ещё**

   275

Комментарии: 26 Поделились: 17

 Нравится  Комментировать  Поделиться

# Офіційна сторінка президента України Володимира Зеленського в Instagram

Instagram

Пошук

Увійти

Зареєструватися



zelenskiy\_official

Стежити

1 826 дописів

Читачі: 16,9млн

Стежить: 194

Володимир Зеленський  
Президент України

ДОПИСИ

ВІДЕО

ПОЗНАЧЕНО

