Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра «Києво-Могилянська школа врядування»

Магістерська робота

освітній ступінь – магістр

на тему: **«Державна політика у сфері інформаційної безпеки України»**

Виконав студент 2-го року навчання, спеціальність 281 Публічне управління та адміністрування

Роман Вікторович Антюхов

Керівник: Малиш Н.А.,
доктор наук з державного управління, професор.

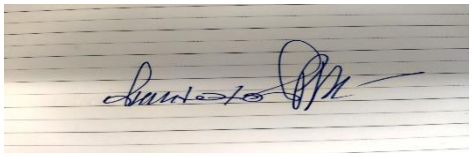
Рецензент: Кияк М.Т., експерт Ради зовнішньої політики “Українська призма”, кандидат філософських наук

Магістерська робота захищена

З оцінкою _____

Секретар _____

«____»_____ 2021 р.



Київ-2021

Декларація
академічної доброчесності

Я, Антюхов Роман Вікторович, студент магістерської програми за спеціальністю «Право» / «Публічне управління та адміністрування» НаУКМА, адреса електронної пошти roman.antiukhov@ukma.edu.ua, підтверджую таке:

- написана мною кваліфікаційна робота на тему «Державна політика у сфері інформаційної безпеки України» відповідає вимогам академічної доброчесності та не містить порушень, передбачених п. 3.1. Положення про академічну доброчесність здобувачів освіти у НаУКМА, зі змістом якого я ознайомлений/ознайомлена;

- надана мною електронна версія роботи є ідентичною її друкованій версії.

12.05.2021 Р.В. АНТЮХОВ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NSA	National Security Agency
AES	Advanced Encryption Standard
АНБ	Агентство національної безпеки (США)
ІДІЛ	Ісламська держава Іраку та Леванту
ЗСУ	Збройні сили України
МВФ	Міжнародний валютний фонд
НАБУ	Національне антикорупційне бюро України
НАЗК	Національне агентство з питань запобігання корупції
НАТО	Організації Північноатлантичного договору
ОЕСР	Організація економічного співробітництва та розвитку
ООН	Організація Об’єднаних націй
РНБО	Рада національної безпеки і оборони України
СБУ	Служба безпеки України
ЦОВВ	Центральні органи виконавчої влади
ЦРУ	Центральне розвідувальне управління
ЦСКІБ	Центр стратегічних комунікацій та інформаційної безпеки
StratCom	Strategic Communications Centre of Excellence NATO
ЄС	Європейський Союз

ВСТУП

Актуальність теми. З початком військової інтервенції Російської Федерації, яка активна фаза розпочалась 2014 року, постало нагальне питання захисту інформаційного середовища від пропаганди Російської Федерації. Для кожної держави питання інформаційної безпеки (захист інформації, інформаційна безпека), є пріоритетом. Оскільки якщо держава не займається системно інформаційної політикою, то національна безпека буде хиткою, і цим може скористатись країна агресор.

Досліджували проблеми інформаційної безпеки зарубіжні науковці Томас Р. Дай, Джон Фредерік Чарльз Фуллер (J.F.C.Fuller) Жанет Озолія, Іварс Аустерс, Солвіта Деніса-Лієпнієцє, Юргіс Шкілтерс, Сігіта Струьерга; українські науковці: В. Горбулін, М. Гребенюк, М. Дмитренко, О. Додонов, М.Кияк, Б. Леонов, Ланде, В. Негодченко, Г. Почепцов та інші.

Мета дослідження – проаналізувати технології ведення інформаційних війн, інструменти протидії загрозам в інформаційній сфері та запропонувати механізми формування та реалізації державної політики у сфері інформаційної безпеки України.

Завдання дослідження:

– проаналізувати нормативно-правове забезпечення державної політики у сфері інформаційної безпеки;

– дослідити міжнародний досвід реалізації державної політики у сфері інформаційної безпеки;

– визначити проблеми реалізації державної політики у сфері інформаційної безпеки, що виникли через поширення COVID-19;

– обґрунтувати механізми та інструменти формування та реалізації державної політики у сфері інформаційної безпеки.

Об'єкт дослідження: інформаційна безпека України.

Предмет дослідження: державна політика України у сфері інформаційної безпеки.

Під час написання магістерської роботи були використані загальнонаукові та спеціальні методи, а саме: аналіз, історичний метод, спостереження, порівняння, синтез, діалектичний, структурний та метод узагальнення.

Інформаційною базою дослідження стали Закони України, нормативно-правові акти Верховної Ради України, Кабінету Міністрів України та Президента України, інших органів виконавчої влади України, закордонні нормативно-правові акти, публікації засобів масової інформації щодо інформаційної політики України у сфері національної безпеки тощо.

Структура роботи обумовлена її метою та завданнями. Магістерська робота складається зі вступу, трьох розділів, висновків, списку 146 використаних джерел та 5 додатків.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ПІДХОДИ ДОСЛІДЖЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття державної політики у сфері інформаційної безпеки

Томас Р. Дай у своїй праці «Основи державної політики» [1] наводить таке трактування поняття *державної політики* – це органи державної влади вирішують, що їм робити або не робити. Органи держаної влади мають регулювати конфлікти, збирати податки, мати монополію на насильство, організовувати безпеку суспільства. Отже, державна політика робить багато речей одночасно [1, с. 19].

Автор розглядає моделі державної політики [1, с. 31-32]: модель публічного вибору, модель еліт, процесуальну, інкрементальну (ітеративну) раціональну, групову, інституційну моделі, модель на основі теорії ігор.

Модель публічного вибору державної політики, на думку автора, полягає у тому, що управлінець під час ухвалення політичного рішення та розробки державної політики, використовує процедури економічного аналізу [1, с. 49-52].

Модель еліт – це визначення державної політики особистими поглядами політичних або інших еліт держави [2, с. 133].

Процесуальна модель державного управління [3] ґрунтується на ідентифікації суспільної проблеми та її подальшому аналізу. Формулюється декілька варіантів політики, з яких визначається найкращий за певними критеріями.

«Розвиток процедур та особливих стилів вироблення державної політики допомагає створити стабільну базу переговорів і, отже, забезпечити безперервність вироблення політики» [3] .

Ітеративна модель державної політики [4] виникла на противагу раціональної моделі, яка базувалась на ідеалізації. Варто застосовувати елементи практики, наголошували прихильники ітеративної моделі державної політики.

У раціональній моделі державної політики порівнюються нерівнозначні альтернативи та ухвалюється оптимальне управлінське рішення [5].

Групова модель державної політики розглядається як результат збалансування позицій у результаті боротьби між різними групами стейкхолдерів [2, с. 133].

Інституційна модель державної політики визначає розподіл повноважень владних інституцій як систему противаг та стримувань між різними гілками влади [6]. Початком цьому підходу стали публікації науковців Дж.Марч (March) та Й.Ольсен (Olsen).

Bechtel M., Tosun J. розглядають модель на основі теорії ігор, яка полягає у прийнятті управлінських рішень на основі вибору варіанту політики, який можна реалізувати, та який залежить від вибору всі зацікавлених сторін державної політики. Використання методів теорії ігор підвищило ефективність формування державної політики в різних сферах життя [7].

Леслі А. Пал у книжці «Аналіз державної політики» вказує, що державна політика, це «дії або утримання від неї, обрані державними органами для розв'язання певної чи сукупності взаємно пов'язаних проблем» [8, с. 22].

Науковцями Е. Янгом і Л. Куінном (Young E. and Quinn L.) наведено такі тлумачення поняття державної політики: «Державна політика – це дії, що їх реалізує владний орган, який має законодавчі, політичні та фінансові повноваження це робити; державна політика – це реакція держави на реальні життєві потреби чи проблеми, …; державна політика здійснюється одним або групою акторів,…; державна політика передбачає обґрунтування дій, тобто, як правило, містить пояснення логіки, на якій вона ґрунтується; державна політика – це рішення, що вже ухвалене, …; державна політика – це курс дій, … ретельно розроблений підхід або стратегія» [9, с. 15-16].

Державну політику визначено як сукупність ціннісних цілей, державно-управлінських заходів, рішень і дій, порядок реалізації державно-політичних рішень (поставлених державною владою цілей) і системи державного управління розвитком країни [10, с. 8].

Говлет М., Рамеш М. (Howlett. M., Ramesh, M.) у своїй книзі «Дослідження державної політики: цикли та підсистеми політики» аналізують підходи, засоби, процес політики, впровадження, оцінювання політики та зазначають, що реалізація політики є складним та безперервним процесом [11].

Політики керують бюрократичним апаратом, тому важливо сильні інституції – парламент, уряд, бюрократичний апарат, суди та ін. Інституції надають державному управлінню легітимності, універсальності та застосування сили. Легітимність це нормативно-правові акти або правові норми, які обов'язкові для виконання [1, с. 32-33]. Універсальність – тільки політика уряду поширюється на всіх груп суспільства та їх членів. Застосування сили – це тільки держава є монополістом на позбавлення волі та застосування насилля по відношенню до громадян [1, с. 33].

Науковці розмежовують поняття державна політика на politics та policy. Politics це використання державної влади у співпраці певних соціальних груп або соціальних індивідів для реалізації своїх інтересів. Policy – це дія, план за яким рухається державна влада [12, с. 5].

У першу чергу розглянемо Конституцію України, а саме це частина друга статті 50 Конституції України, яка гарантує право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена [13].

Також стаття 9 Закону України «Про інформацію» [14, ст. 9] Закон про інформацію] визначає такі види інформаційної діяльності, а саме (рис. 1.1):

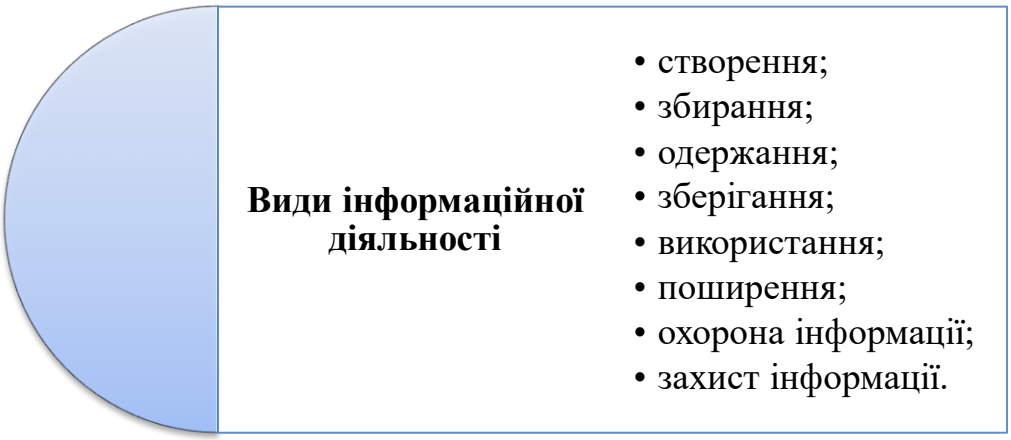


Рис. 1. 1. Види інформаційної діяльності відповідно до Закону України «Про інформацію» [14]

Нині інформація не є допоміжною силою у боротьбі, а стає основною силою впливу на громадян та супротивника. Георгій Почепцов дав дуже слушне визначення *інформації*, як інструмент боротьби із супротивником, а саме: «Інформація поступово припиняє бути додатковим до іншої сили інструментарієм. Вона стає самостійною силою. І саме це вимагає перегляду можливостей щодо її застосування» Г. Почепцов [15].

Державна інформаційна політика – це фундамент існування будь-якої країни, тому що інформація для сучасного суспільства несе важливу роль в повсякденному житті, так само як для держави в цілому.

В Українському законодавстві є визначення, що таке інформація та державна інформаційна політика. Так, відповідно до Закону України «Про інформацію» [14] інформація це «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді». Також звертаю увагу, що в статті 3 Закону України «Про інформацію» є визначення щодо основних напрямів державної інформаційна політика, а саме це: «забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості

діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору» [14].

Також існує термін «інформаційні операції» про які пишуть в своїй монографії В.П. Горбулін, О.Г. Додонов, Д.В. Ланде «Інформаційні операції та безпека суспільства: загрози, протидія, моделювання». Вони стверджують що інформаційні операції це заходи (акції) спрямовані на вплив на супротивника через інформацію та інформаційні системи, а також захисту власної інформації та систем [16].

Категорія *національної безпеки* визначена в пункті 9 статті 1 Закону України «Про національну безпеку України», а саме: «національна безпека України це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [17].

Британський військовий історик Джон Фредерік Чарльз Фуллер (J. F. C. Fuller) на початку 20 років XX століття першим почав вживати термін «психологічна війна» [18].

Дмитренко М. у статті «Проблемні питання інформаційної безпеки України» [19] досліджує проблеми *інформаційної безпеки* України в контексті інформаційної війни, розглядає питання планування та проведення інформаційних впливів (інформаційних операцій, дій, акцій) у рамках реалізації завдань внутрішньої і зовнішньої політики держави, проводить аналіз інформаційних ризиків. «Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян», – зазначає автор [19].

Важливі питання, що стосуються інформаційної політики в сфері національної безпеки, розглянули у своїй аналітичній доповіді науковці Національного інституту стратегічних досліджень. У праці наголошено, що через збройну агресії РФ Україна не може повноцінно забезпечити свою інформаційну присутність та повноцінно реалізовувати свою інформаційну політику на окупованих територіях [20]. Найбільш актуальним питанням нині є реінтеграція у повному обсязі територій до інформаційного простору держави.

Реалізація зазначеного завдання потребує скоординованої політики держави, зокрема, залучення органів державної влади, міжнародних партнерів, неурядових організацій та громадянського суспільства [20].

Науковець Негодченко В. пропонує доповнити перелік основних напрямів держаної інформаційної політики, закріплених у Законі України «Про інформацію», такими [21]: «сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій, засобів їх забезпечення; розвиток адміністративного законодавства у сфері інформаційних процесів (у тому числі приведення законодавчої бази у відповідність до міжнародних стандартів у цій сфері), інформатизації і захисту інформації; правове регулювання функціонування в Україні міжнародних інформаційних систем (зокрема, мережі Інтернет); пропагування курсу держави на створення та розвиток відкритого інформаційного суспільства» тощо [21].

Почепцов Г., відомий фахівець у сфері інформаційних війн, у своїй праці «Сучасні інформаційні війни» пише: «Інформаційна політика працює з такими чутливими сферами, як а) контент (стабілізаційний чи дестабілізаційний); б) суспільні цінності (традиційні чи руйнівні); в) характер суспільства (демократичний, інноваційний)». Автор досліджує питання інформаційних технологій, інформаційно-комунікативних процесів в сучасних суспільствах, зокрема, проблеми, що виникають через надмірні покази на екранах розважальних програм, які стримують розвиток суспільного мислення [15].

Георгій Почепцов наводить таке визначення психологічних війн, а саме «психологічні війни є комунікативними технологіями, що спрямовані на

внесення змін у поведінку індивіда за допомогою модифікації його моделі світу, що здійснюється шляхом внесення змін у інформаційні потоки». Тобто психологічні війни змінюють мислення людини таке, яке необхідне супротивнику для вирішення поставлених тактичних та стратегічних цілей політики [15].

Коли розробляється психологічна операція важливо акцентувати увагу на тому через, які канали буде транслюватись або передаватись інформація або повідомлення [15, с.198]. Також перед початком психологічної операції важливо зробити аналіз аудиторії на яку буде робитись вплив для каналів зв'язку та вибору відповідних меседжів для впливу на аудиторію [15, с.201].

Георгій Почепцов вказує на «Фактор соціального середовища» коли індивід на якого впливає психологічні операції, він спирається на своє соціальне середовище для прийняття відповідного рішення [15, с.203]

Вагомість інформаційної безпеки в системі національної безпеки України визначається активізацією ризиків в інформаційній сфері, зокрема, веденням інформаційних війн. «Майбутні війни – війни без застосування безпосереднього насильства, засобами якого є не безпосередні дії, одним із методів яких є інформаційні війни» [22, с. 160].

Ризики, що пов'язані з інформаційною безпекою, пов'язані з впливом негативних чинників або процесів, через які порушується їх функціонування, стримується розвиток об'єктів інформаційної безпеки [23, с.16].

Науковці University of Plymouth Mutlaq Alotaibi та інші у своїй праці «Information security policies: A review of challenges and influencing factors» досліджують питання інформаційної безпеки, зокрема, наголошують на впливі людського чинника на порушення інформаційної безпеки на підприємствах та в організаціях. Вони наводять думку, що проблеми в успішному впровадженні інформаційної безпеки залежить від менеджерських якостей керівників та обізнаності робітників. Порушення інформаційної безпеки це в першу чергу стосується технічної сторони проблеми, однак це є і проблемою, що пов'язана з людським чинником. Насамперед, можна виокремити: не бажання робити

складні паролі; записувати паролі на ліпкий папір та приклеїти його на монітор [24].

На основі звітів інститутів інформаційної безпеки, що стосуються дотримання політики, виклики стосовно інформаційної безпеки були поділені на чотири групи: просування політики безпеки, невідповідність політиці безпеки, управління та оновлення політики безпеки, тіньова безпека. Чинники, що впливають на поведінку, були розділені на організаційні та людські. Висновок, який роблять автори, полягає у постійному навчанню працівників, підвищенню обізнаності та контролю за їх дотриманням політики інформаційної безпеки [24].

Науковець Shafiq Lutaaya у своєму дослідженні «Information Security Policy for Ronzag» зазначає, що уряди все більше використовують конфіденційну інформацію, отже питання належної інформаційної безпеки стоїть, критично [25]. На думку автора важливо впровадити стандарти інформаційної безпеки. Метою інформаційної безпеки для веб-служб є захист інформаційних активів компанії, незалежно від того, зберігаються вони в ручній або електронній формі. «Це допоможе захистити репутацію компанії, оптимізувати управління ризиками та мінімізувати вплив інцидентів інформаційної безпеки», наголошує автор публікації. Будь-яка втрата інформації може мати серйозні наслідки для компанії та її споживачів. Порушення безпеки під час оброблення, зберігання, передачі даних може призвести також до фінансових втрат. Інформація про комп’ютерні системи має бути захищеною антивірусним програмним забезпеченням та регулярно оновлюватися. Повинні бути впроваджені визначені та затверджені політики та стандарти інформаційної безпеки [25].

В основі державної політики щодо забезпечення інформаційної безпеки має бути системна діяльність органів державного влади щодо надання гарантій інформаційної безпеки громадянам, соціальним групам, суспільству в цілому. Проблеми, що пов’язані з інформаційною безпекою держави варто розглядати у взаємозв'язку з іншими проблемами, які виникають у світовому просторі, національній економіці, соціальній, демографічній сфері тощо [26, с. 158].

Політика інформаційної безпеки має бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки для всіх суб'єктів господарювання, державної влади, усіх громадян країни. До основних джерел внутрішніх ризиків у сфері інформаційної безпеки можна віднести такі: недосконаліть законодавчої бази в галузі інформаційних відносин та інформаційної безпеки, протиправні дії окремих громадян в інформаційній сфері, виникнення непередбачуваних ситуацій в системах, які базуються на використанні інформаційних технологій, недосконаліть або відсутність засобів забезпечення інформаційної безпеки тощо [27].

На думку Золотар О. всі визначення інформаційної безпеки людини можна узагальнити в два основні підходи: технічний та гуманітарний. Перший підхід домінує в правових науках та ґрунтується на забезпечення людині здатності вільно і безперешкодно реалізовувати права та свободи в інформаційній сфері, зокрема право на інформацію – вільно збирати, зберігати, використовувати і поширювати інформацію. Технічний аспект інформаційної безпеки полягає у здатності і вмінні людини передбачати та попереджувати загрози інформації, яка циркулює в технічних системах, і загрози самим системам [28]. Другий підхід наголошує на захищеності психіки та свідомості людини від небезпечних інформаційних впливів; маніпулювання, дезінформування, образ, спонукання до самогубства тощо [29].

Співвідношення понять: інформаційна безпека та кібербезпека

Кібербезпека – це безпека інформаційних систем (програм чи устаткування). Інформаційна безпека – це безпека інформації, у тому числі в інформаційних системах. Кібербезпека є частиною інформаційної безпеки.

Відповідно до пункту першого Окінавської хартії глобального інформаційного суспільства інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття [30].

Пунктом п’ять Окінавської хартії призиває державний та приватний сектор ліквідувати розрив у сфері інформації та освіті [30].

Також Окінавська хартія наголошує на тому, що приватний сектор є важливою ланкою у створені та розробці комунікаційних та інформаційних мереж, але на уряді лежить створення політики та нормативно-правових актів [30].

Відповідно до закону Мура [31], який сформував Гордон Мур (засновник корпорації Intel), кількість транзисторів в мікросхемах буде збільшуватись у два рази кожні два роки. Закон Мура пояснює створенню та поширенню різноманітною інформаційних технологій, такі як: соціальні мережі, відеохостинги [32].

Українське законодавство в Законі Україні «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» інформаційну безпеку визначає, як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [33].

У свою чергу в підручнику «Іінформаційна та кібербезпека: соціотехнічний аспект» В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа, «інформаційна безпека це стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об’єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони» [32].

Також науковці В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова у навчальному підручнику «Інформаційна безпека держави» [34], наводять таке визначення «інформаційна безпека – це «захищеність (стан захищеності) основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі як повнота, об’єктивність, доступність і конфіденційність» [34].

З різних визначень науковців та законодавства терміну «інформаційна безпека», є одна спільна риса – це запобігання нанесенню шкоди в будь-якій формі.

1.2. Нормативно-правове забезпечення державної політики у сфері інформаційної безпеки

Міжнародна інформаційна безпека

Міжнародна інформаційна безпека знаходить своє відображення в доктринах, стратегіях, законах держав і міжнародних організацій: Організація Об‘єднаних Націй, Європейський Союз, Рада Європи, НАТО.

10 березня 1992 року Україна приєднується до участі в Раді євроатлантичного партнерства [35].

08 лютого 1994 року Україна приєднується до Програми партнерство заради миру [36].

Пунктом два цієї рамочної угоди щодо Програми партнерство заради миру наголошується на тому, що стабільність та безпека в регіоні буде досягнута завдяки спільним діям та співробітництву [36].

Цілі цієї програми такі:

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

2. забезпечення демократичного контролю над збройними силами;

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

4. розвиток відносин співробітництва з НАТО у військовій сфері з метою здійснення спільного планування, військової підготовки та учбових маневрів, покликаних підвищити їхню спроможність до виконання завдань, пов'язаних з миротворчою діяльністю, пошуковими і рятувальними операціями,

операціями по наданню гуманітарної допомоги та іншими, про які згодом може бути домовлено.

5. формування у тривалій перспективі таких збройних сил, які зможуть краще взаємодіяти із збройними силами держав-членів Північноатлантичного союзу.» [36].

09 липня 1997 року Між Україною та Організації Північноатлантичного договору і її країн-членів підписано Хартію про особливе партнерство між Україною та Організації Північноатлантичного договору [37].

Так, питання міжнародної безпеки відображені в Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки», де заявлено про створення нового міжнародно-правового режиму з поняттям інформаційна технологія [38].

Відповідно до пункту першого Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки» Організація Об'єднаних Націй «закликає держави-члени сприяти розгляду на багатосторонньому рівні існуючих та потенційних загроз у сфері інформаційної безпеки» [38].

Також Резолюція Генеральної Асамблеї ООН A/RES/53/70 «Розвиток у галузі інформації та телекомунікацій в контексті міжнародної безпеки» наголошує на тому, щоб зробити загальну оцінку проблем у інформаційній безпеці [38].

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

Питання забезпечення інформаційної безпеки стає одним із пріоритетних напрямів діяльності ЄС. У 2001 р. Комісією ЄС було представлено перший

документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому була представлена концепція вирішення проблем щодо інформаційної безпеки. У документі сформульовано визначення «мережева та інформаційна безпека» – як здатність інформаційної системи чинити опір випадковим чи зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через мережі та системи [39].

На початку 2000-х років органами ЄС було прийнято цілу низку нормативно-правових актів, які передбачають різноманітні підходи забезпечення інформаційної безпеки в державах – членах ЄС. У повідомленні Комісії ЄС «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» від 22 травня 2007 року, пропонується визначення «кіберзлочинність» та основні напрями політики ЄС щодо інформаційної безпеки [40];

У лютому 2013 року була прийнята Стратегія кібербезпеки ЄС «Відкритий, надійний та безпечний кіберпростір» в якій йде мова про міждержавне співробітництво та механізми протидії кіберзагрозам в ЄС [41].

У 2016 року Директивою Європейського парламенту та Ради ЄС було затверджено єдині правила та вимоги у сфері кібербезпеки для всіх держав-членів.

Для інформаційної безпеки в рамках ЄС у 2004 року було створено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA). Завданнями ENISA є: удосконалення мережевої та інформаційної безпеки в ЄС, сприяння розвитку культури мережевої та інформаційної безпеки тощо [42].

У 2013 року в структурі Європейського поліцейського офісу (Європол) [43] був утворений Європейський центр боротьби з кіберзлочинністю, основними напрямками діяльності якого є розслідування шахрайства в мережі Інтернет, розслідування злочинів щодо критично важливої інфраструктури та

інформаційних систем ЄС [44]. Щороку Європейський центр боротьби з кіберзлочинності оцінює загрози у сфері кіберзлочинності – загрози, що впливають на уряди, бізнес та громадян в ЄС та надає рекомендації для ефективного та узгодженого реагування на кіберзлочини.

Україна. В Україні на сьогоднішній день існує чимала кількість нормативно-правових актів які регулюють питання інформації та національної безпеки.

В умовах російсько-української війни російські інформаційно-психологічні операції спрямовані на забезпечення домінування в українському інформаційному просторі. Через російські пропагандистські інформаційно-психологічні кампанії відбувається вплив не лише на суспільну свідомість громадян України, а й на громадськість в усьому світі [45].

Відповідно до Стратегії національної безпеки України, яка затверджена Указом Президента України від 26 травня 2015 року № 287/2015 [46], визначено наступні цілі:

- мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави;
- утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО.

Актуальною загрозою національної безпеки в Стратегії національної безпеки України визначено інформаційно-психологічну війну, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу [46].

Національні інтереси України та загрози в інформаційній сфері визначені в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [47]. «Національними інтересами України в інформаційній сфері є: життєво важливі інтереси особи та життєво важливі інтереси суспільства і держави, як то: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, забезпечення конституційних прав людини на захист приватного життя, захищеність від руйнівних інформаційно-психологічних впливів; захист українського суспільства від агресивного інформаційного впливу РФ,…, розвиток та захист національної інформаційної інфраструктури, … створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди,…тощо» [47].

Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері [47] прописані у Доктрині інформаційної безпеки України: «Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, … загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, … проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур …; інформаційне домінування держави-агресора на тимчасово окупованих територіях; … неефективність державної інформаційної політики тощо» [47].

У Стратегії національної безпеки України (2015 р.) вперше серед загроз національній безпеці визначаються загрози критичній інфраструктурі. А в підрозділі «Загрози кібербезпеці і безпеці інформаційних ресурсів» зазначається про вразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак. Також уперше одними з «основних напрямів державної

політики у сфері національної безпеки» названо забезпечення безпеки критичної інфраструктури та визначено пріоритети такого напряму» [48].

«Зелена книга» з питань захисту критичної інфраструктури в Україні. У «Зеленій книзі» є таке визначення «критичної інфраструктури», це – «об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих наслідків для соціальної й економічної сфер держави, негативно вплине на рівень її обороноздатності та національної безпеки». Функціонування критичної інфраструктури в мирний час пов'язується із підтримуванням життєво важливих функцій у суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки й захищеності [48].

Процес удосконалення правового механізму державного управління захисту критичної інфраструктури в Україні в цілому відбувається з урахуванням передового досвіду країн ЄС та США та зберігається потреба внесення змін і доповнення до чинного Закону України «Про національну безпеку України», прийняття законопроєкту «Про критичну інфраструктуру та її захист» у частині захисту об'єктів критичної інфраструктури [49].

У 2016 р. в Україні була прийнята Стратегія кібербезпеки України [50]. Цей документ визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики інформаційної безпеки, яка відповідатиме світовому рівню.

Указом Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», визначено, що окрім традиційних сфер ведення бойових дій таких, як «Земля», «Повітря», «Море», «Космос», діє Кіберпростір. Із широким застосуванням інформаційних технологій таких, як гакерські атаки та інформаційно-психологічні спеціальні операції країни агресора (фейкові новини тощо) [50].

Відповідно до абзацу 5 розділу 2 Стратегії кібербезпеки України [50 Стратегія кібербезпеки], затвердженої Указом Президента України від 15

березня 2016 року № 96/2016, передбачено що загрози у сфері кібербезпеки відбуваються через дію таких чинників:

– «невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;

– недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

– недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки». [50],

Воєнна доктрини України, яка затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» [51], визначає стратегічні комунікації, як скоординоване і належне використання комунікативних можливостей держави, а саме інформаційно-психологічних операцій.

Пункт 7 Воєнної доктрини України [51] визначає головні тенденції, військово-політичної обстановки в довкола України:

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

– інформаційна війна Російської Федерації проти України.

Разом з тим пунктом 9 Воєнної доктрини України [51] вказує на воєнні загрози такими:

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

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

– інформаційно-психологічні операції з використанням сучасних інформаційних технологій. [51]

Доктриною інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № 47/2017 [51], передбачено, що технології гібридної війни, які застосовує Російська Федерація проти нашої країни перетворило інформаційну сферу на головну боротьбу за свідомість громадян.

Метою Доктрини інформаційної безпеки України [47] це формування та реалізація засад інформаційної безпеки щодо протидії Російській Федерації в умовах гібридної війни.

Доктрина інформаційної безпеки [47] визначає сім загроз національній безпеці в сфері інформації, а саме:

– «проведення спеціальних операцій (підрив обороноздатності)
– проведення інформаційних спеціальних операцій
– інформаційна інфраструктура РФ в Україні
– домінування РФ в інформаційній сфері
– нерозвиненість інформаційної інфраструктури
– недосконалість законодавства у сфері інформації та неефективна державна інформаційна політика»[47].

У грудні 2017 р. була прийнята Концепція створення державної системи захисту критичної інфраструктури [52]. У документі визначаються основні

напрямки, механізми та строки правового врегулювання даного питання, створення системи державного управління захисту.

21 червня 2018 року Верховною Радою України було прийнято новий Закон України «Про національну безпеку України» [53]. В преамбулі цього закону сказано, що він визначає засади державної політики у сфері національної безпеки і оборони [53]. Також цей закон «визначає та розмежовує повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони» [53].

1.3. Міжнародний досвід реалізації державної політики у сфері інформаційної безпеки: огляд джерел

Перш за все, вивчаючи міжнародний досвід, я звернув увагу на досвід Сполучених Штатів Америки.

У Сполучених Штатах Америки головним федеральним виконавчим органом у військовій сфері та питанні національної безпеки є Міністерство оборони США (англ. United States Department of Defense) [54]. У складі Міністерства оборони США діє Агентство національної безпеки (англ. National Security Agency) повноваження якої є збір та аналіз закордонної розвідувальної інформації, захист інформаційних систем, комп’ютерних мереж уряду [55].

Агентство національної безпеки (АНБ), (англ. National Security Agency (NSA)) – агентство криптологічної розвідки Сполучених Штатів Америки. АНБ є частиною Міністерства оборони США і відповідає за збір та аналіз іноземної розвідувальної інформації та за захист інформаційних систем і комп'ютерних

мереж уряду США. Агентство було створено 4 листопада 1952 року указом президента США Гаррі Трумена. АНБ є складовою частиною системи безпеки країни разом з ЦРУ та іншими агентствами, однак на відміну від ЦРУ не займається використанням агентів в інших країнах. Згідно з федеральним законом, діяльність агентства обмежена збором та моніторингом іноземної розвідувальної інформації, однак з'являлися численні підозри у використанні агентства для збору інформації також і у США [55].

Як пише в своїй статті Буга Л.В. «Досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах» на даний час забезпечення інформаційної безпеки в Армії США є високим [56].

Кіберкомандування Армії США та Управління програм з інформаційної Міністерства оборони забезпечують інформаційну безпеку в Армії США [56]. Основні сфері відповідальності Кіберкомандування:

- захист інформаційних мереж Армії та Міністерства оборони;
- реагування на кібер-атаки;
- підтримка союзників США [56].

У 2015 році в Ізраїлі створено координаційний орган щодо посилення цифрового захисту Національне управління кібербезпеки [57]. Як наголошує Гребенюк М.В., Леонов Б.Д., у своїй статті «Досвід Ізраїлю у сфері забезпечення кібербезпеки» це управління було створене у зв’язку із загрозливими тенденціями у сфері кіберпросторі, і чимало державних та комерційних установ стали слабкими до кібератак [57, С. 45-50]. «Кібербезпека – це сфера майбутнього, яка потребує вкладення потужних державних та приватних інвестицій на перманентній основі. Розвиток цієї важливої складової світової національної безпеки є одним із головних чинників прискорення галузевої трансформації усієї світової економіки в найближчі десятиліття. У найближчій перспективі сфера кібербезпеки має стати ключовим параметром визначення рівня економічного розвитку будь-якої країни, її конкурентоспроможності на глобальному ринку», – наголошують автори [57, с. 48].

Для ефективної роботи системи кіберзахисту Уряд Ізраїлю підтримує навчальні програми спеціалістів, і освітні програми для населення щодо цифрового захисту [57]. «Світовий досвід демонструє, що сьогодні сфера забезпечення кібербезпеки виходить за межі юрисдикції певних країн і має глобальний та міжнародний характер, що зумовлює потребу в розробці не тільки національної, а й відповідної міжнародної стратегії забезпечення безпеки у кіберпросторі» [57, с. 47].

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

Активну політику у сфері забезпечення інформаційної безпеки проводить ЄС. Країни Європейського Союзу активно впливають на міжнародні відносини, встановлюють норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах [58, с. 104].

У 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій» [59], де визначено завдання забезпечення інформаційної безпеки, зокрема:

– захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;

– забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;

– забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні [59].

Досліджуючи міжнародні критерії інформаційної безпеки держави, науковці визначають поняття інформаційної війни як «протиборство інформаційно-комунікаційних технологій та здатності державних і комерційних інформаційних систем забезпечити безпеку інфраструктури держави в цілому» [60, с. 44].

Науковець Т.Ткачук, досліджуючи досвід країн Європи: Польщі, Угорщини, Швейцарії та інших, зазначає, що європейські держави усвідомлюють та протидіють кіберзагрозам. Політика національної безпеки країн ЄС спрямована

на захист інформації, критичної інформаційної інфраструктури, інформаційно-психологічної безпеки громадян [58, с. 104-110], [61, с. 62].

З 2011 року в Німеччині безпекою інформації займається Національний центр кібербезпеки, на якого покладені завдання реагування та попередження на загрози у кіберпросторі та захисту критичної інфраструктури [58, с. 106].

В Польщі безпекою інформації в кіберпросторі займається Центр криптології при Міністерстві національної оборони, завдання якого це захисту інформації, кібернетична оборони та ін. [58, с. 107].

Хорватія покладає свій захист інформації безпеки на Бюро з безпеки інформаційних систем, національний орган із питань суспільної інформації Республіки Хорватії, Управління Ради національної безпеки [58, с. 108].

У Болгарії важливу роль у кіберзахисті покладено на Міністерство оборони, яке в межах повноваження повинно реагувати та попереджати атаки на критичну інфраструктуру, а також співпраця із НАТО [61, с. 66].

Забезпечення захисту інформації в Румунії, шляхом припинення, попередження кібератаки, захист критичної інфраструктури, покладено на Румунську службу інформації [61, с. 64-65].

У своїй праці «Cyber Security Policy and Strategy in the European Union and Nato» пан László Kovács пише про те, що кібербезпека в першу чергу залежить від інформаційної освіти користувачів інформаційних ресурсів [62].

З 2016 року в Європейському Союзі діє Директива 95/46/EC General Data Protection Regulation [63], яка уніфіковує законодавство держав-членів Європейського Союзу щодо захисту приватних та персональних даних. Санції за порушення Директиви передбачені, це 20 мільйонів євро, а також 2% та 4% від обороту компанії або організації. [62, с. 20].

Стаття 17 Директиви 95/46/EC General Data Protection Regulation встановлює поняття «Right to erasure («right to be forgotten»)», що означає «право на стирання» тобто наприклад соціальна мережа зобов’язана стерти Ваші дані із серверів та баз даних [63].

Але в свою чергу стаття 18 Директиви 95/46/EC General Data Protection Regulation встановлює, що ця Деректива не застосовується «до обробки персональних даних фізичною особою під час приватної діяльності і, отже, без зв'язку з професійною чи комерційною діяльністю. Приватна діяльність може включати листування та ведення адрес, або соціальні мережі та діяльність в Інтернеті, що проводяться в контексті такої діяльності.» [63].

2017 році Президент Європейської комісії у щорічному посланні заявив, що в Європейському Союзі буде створено Агенцію з кібербезпеки для допомоги у боротьби із кіберзлочинами членам Європейського Союзу [64].

Агенція з кібербезпеки Європейського Союзу покращить реагування на кібератаки, а також будуть проводитись загальноєвропейські з протидії кібератак [64]. Також головною задачею Агенції буде запровадження сертифікація пристроїв із «Інтернет речей» безпечного використання на території Європейського Союзу [64].

09 липня 2016 року НАТО на Варшавському саміті у своєму комуніке засудило дії Російської Федерації по анексії Криму, військових дій на сході України, а також агресивна ядерна діяльність. НАТО підтримує спеціальну моніторингову місію ОБСЄ на сході України [65].

У комуніке Варшавського саміту наголошується на незмінності прихильності НАТО до безпеки, прав людини, верховенства права та ін. [65].

Також наголошується, що Російська Федерація продовжує створювати загрозу НАТО на східних кордонах та є джерелом нестабільності в регіоні [65].

Панченко В.М. у своїй праці «Інформаційні операції в асиметричній війні росії проти України: підходи до моделювання» наводить чотири ознаки асиметричної війни [66]:

1. Межі бойових дій відсутні.
2. Ведення бойових дій малими групами.
3. Бойові підрозділи існують завдяки середовищу де знаходять.
4. Керований хаос [66].

Асиметрична війна – це війна із дисбалансом сил між ворогами, і які застосовують різні стратегії та тактику ведення бойових дій [66]. Це може бути інформаційно-психологічні операції, спротив та диверсії, ведення партизанської війни, підтримка антиурядових громадських організацій та партій, а також проведення терористичних актів [66].

Висновки до розділу 1

Інформація для сучасного суспільства несе важливу роль в повсякденному житті, так само як для держави в цілому. Інформацію можна віднести до їжі – яку інформацію будеш споживати таким ти і сформуєшся як особистість та громадянин.

Щодо правового регулювання державної інформаційної політики у сфері національної безпеки то на моє переконання воно дуже зарегульовано, але багато з того не виконується.

З міжнародного досвіду то США та Ізраїль технологічно дуже розвинуті. В обох країнах працюють відповідні інституції щодо захисту інформації. Що важливо, обидві країни покладаються не тільки на підготовку спеціальних фахівців, а на освіту населення, також.

Обравши євроінтеграційний курс, Україна має орієнтуватися також на стратегію розвитку провідних європейських країн в інформаційній сфері.

Державна інформаційна політика є критично важливою для розвитку будь-якою держави, оскільки теперішні війни в першу чергу мають впливати на цивільне населення. Головне завдання вплинути на громадян іншої країни, посіяти сумніви, не довіру до своєї влади, тоді легше проводити інформаційні війни.

Відповідні інституції держави, які відповідають за формування державної інформаційної політики мають також навчитись попереджувати, передбачати можливі загрози. Критично важливо це системна робота та стала політики цих органів щодо державної інформаційної політики. Цей напрям політики не має розвертатись на 360 градусів при кожній зміні Уряду, парламенту, президента, тобто має бути сталість політики.

РОЗДІЛ 2. АНАЛІЗ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Інформаційні війни та технології

Технології інформаційної війни

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

- Хакерські атаки на критичну інфраструктуру.
- Інформаційно-психологічні спецоперації.
- Дезінформація у соціальних мережах [67, с. 73].

У період інформаційних технологій критично важливо державним структурам системно проводити роботу з убезпечення всіх сфер діяльності держави від інформаційних атак. Оскільки все більше критичної інфраструктури переходить на інформаційні технології або у кіберпростір, де хакери можуть здійснити взлом та відключити атомний енерго блок або вплинути на виборчий процес. Тому дуже важливо із боку державної влади планувати захист держави не тільки звичайними методами (Армія, спецслужби), а також спеціальними методами у кіберпросторі (інформаційна безпека).

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

26 лютого 2013 року Начальник Генерального штабу збройних сил Російської Федерації генерал армії В.Герасимов публікує в газеті «Военно-Промышленный Курьер» статтю «Ценность науки в предвидении» [68], так звана «Доктрина Герасимова». В цій статті автор припускає співвідношення військових та невійськових дій 1:4. Це співвідношення дуже успішно реалізується в Україні з 2014 року, з початком анексії Автономної республіки Крим в кінці лютого 2014 року, а після в Донецькій та Луганських областях.

В інформаційній війні використовується:

- соціальні мережі;

- блогери;
- фейкові новини;
- політики;
- шарій;
- російська православна церква;
- теорії змов.

У 2017 році в США постає конспірологічний рух Qanon [69], який стверджує про існування міжнародної схеми сексуальної експлуатації дітей. Вони звинувачують лідерів Демократичної партії США, акцентуючи увагу на Гіларі Клінтон, а також звинувачують їх у поклоніні Сатані. 28 жовтня 2017 року на форумі https://www.4chan.org/ від анонімa під ніком Q з'являється наступне повідомлення, яке дає початок створення руху Qanon «Наказ про екстрадицію Гілларі Клінтон починаючи з вчора діє у декількох країнах на випадок спроби втечі через кордон. Паспорт на особливому контролі з 12:01 ночі 30 жовтня. Очікуються масові заворушення противників і інші спроби втечі з США. Операцію проведуть Озброєні сили США, Національна гвардія США приведена у бойову готовність. Доказ: 30 жовтня знайдіть бійця НГ у будь-якому з великих міст і запитайте, чи перебуває він на бойовому чергуванні».

Як пише сайт https://texty.org.ua/ у статті «Конспірологи з QAnon разом з іншими штурмували Капітолій. Розробник ігор аналізує, як функціонує цей рух» [70], який є переказом статті Ріда Берковітца (розробник ігор), опублікованої на сайті Medium [71]. У цій статті він пробує пояснити популярність теорії змови, яка каже про те, що весь світ хочуть захопити педофіли.

Творці теорії змови QAnon використовують Апофенію [72] – «це бачення бачення образів, тенденцій або зв'язків у випадкових або беззмістовних даних». (рис. 2.1.). Mishara Aaron L. описує це поняття у своїй публікації про Klaus Conrad – автора, який вперше ввів поняття Апофенія у 1958 році.

Рис. 2.1. «Картинка від QAnon: «Їхня потреба в символіці буде їхнім падінням... Вони цього не приховують. Ви вівці для них. Вони не бояться тебе. Ти для них годівниця» [70]

Інтернет-видання The New York Times створило документальний фільм Operation InfeKtion [73] про поширення та створення дезінформації, яку створює Російська Федерація. У другому епізоді документального фільму розкривається суть про сім заповідей дезінформації [74]:

1. Знайти суперечності в суспільстві.
2. Створити брехню, абсолютною маячнею.
3. Брехня має бути із зерном правди.
4. Джерело інформації не повинно бути знайдено «Ховайте ваші руки».
5. Корисні ідіоти.
6. Все заперечувати.
7. Стратегічне планування або довга гра.

Максим Кияк у статті «ЗеДжокер і президентський стендап» [75] звертає увагу на серіал від студії «Квартал 95» «Слуга народу» де тодішній керівник студії Володимир Зеленський, зіграв роль президента України. Головний меседж серіалу: говорити те чого хочуть люди. Головний герой, якого зіграв Зеленський, відповідав суспільним настроям громадян України на простого хлопця – такі як

усі «з народу» [75]. В серіалі зображено хорошого Зеленського «простого хлопця з народу», а політиків, олігархів – корумпованими, морально низькими, що в свою чергу програмує глядачів на те, що Зеленський – рятівник народу [75].

Серіал «Слуга народу» – це фактично прихована передвиборча агітація, яка заздалегідь формує у виборців відповідну точку зору [75].

Біла книга. Модель серіалів для отримання знань про російські пропагандистські кампанії в медіа та мережі Інтернет.

У Білій книзі спеціальних інформаційних операцій проти України, 2014 – 2018, що підготовлена колективом експертів Міністерства інформаційної політики України (зараз Міністерство культури та інформаційної політики України), запропоновано модель серіалів для отримання знань про російські пропагандистські кампанії в медіа та мережі Інтернет «…російські наративи та дезінформаційні прийоми мають високий ступінь ефективності саме завдяки повторюваності в медіа. Іншими словами, об'єктам дезінформації постійно розповідають одні й ті самі історії, роблячи їх щоразу цікавішими та більш «екзотичними» [76].

Автори акцентують увагу про те, що «частота згадування ключових слів, пов'язаних із темою ЛГБТ чи педофілії в березні 2013 року збільшилась у 13-12 разів», якщо порівнювати з 2012 роком. «Ісламську державу» Кремль використовує у своїх наративах з 2013 року, «гаряча фаза» інформаційної війни розпочалась у жовтні 2013 року, коли відбувся переможний поєдинок Володимира Кличка (Україна) й Алєксандра Повєткіна (Росія). «Дослідження інформаційного простору показали, що саме в той день у тестовому режимі було запущено перший «бойовий» проект масованого «тролінгу». Приводом стала поразка російського боксера на ринзі» [76].

Використовуючи наративи, Російська Федерація спрямовано тисне на цільові аудиторії та примушує повірити в потрібні їй ідеї. Такий наратив російської пропаганди автори назвали СЕРІАЛ. Серії в сезонах, які об'єднані навколо однієї проблематики, автори назвали СЕЗОН (Додаток Г). [76].

Міфи про ІДІЛ в Україні

Російська Федерація прагнучі заохотити європейських лідерів на співпрацю через боротьбу з тероризмом, 2015 року запускається інформаційна операція під назвою «тренувальні табори ІДІЛ в Україні» [76] для цього використовують іноземні засоби масової інформації та французьку сенаторку Наталі Гуле [77], яка в інтерв'ю радіостанції «France Inter» [78] повідомила, що в Україні діють табори ІДІЛ «на 1.28'40 хвилині, пані Гуле каже : «Ніхто мене не слухає зараз, але через півроку, згадаєте, що я про це говорила. Посеред України діє табір підготовки джихадистів. Адже, все ж таки, друга мова, якою говорять в Ісламській Державі – російська. Уявіть собі, табір підготовки просто біля нас! Який фінансується усією цією протизаконною торгівлею людьми, предметами мистецтва» [79]. 03.04.2016 пані Наталі Гуле через звернення до голови Служби безпеки України пана Василя Грицака, яка спростовує свою заяву. Трохи згодом кореспондент «Українського тижня» Алла Лазарева в своїй статті від 4 квітня 2016 року показує свою переписку із сенаторкою, яка засвідчує, що Наталі Гуле повідомляла фейкову новину [79]. Також цей фейк неодноразово спростовував сайт StopFake [80, 81].

Оскільки українська армія, добровольчі батальйони та волонтерські рухи фактично зупинили російську армію, то для російських спеціальних служб головною задачею стояла (та продовжує стояти) дискредитація цих рухів [76]. З 2014 року українську армію та добровольчі батальйони починають прив'язувати до ІДІЛ, мета операції була зменшення європейської допомоги на фоні терористичних актів в Європейському союзі [76].

На сайті американського видання «The Intercept» [82] в лютому 2015 року виходить публікація польського журналіста Mamon Marcin «IN MIDST OF WAR, UKRAINE BECOMES GATEWAY FOR JIHAD» (В розпал війни. Україна стає воротами Джихада») [76]. Автор статті бере інтерв'ю у чоловіка на ім'я Халід керівника ІДІЛ в місті Стамбул. Халід розповідає про Різвана (Руслана), який воює в батальйоні Джохара Дудаєва. Різвана (Руслана) повідомляє Mamon Marcin про те що в Україні можна отримати громадянство за 15 тисяч доларів

США [76]. Як ми бачимо встановити, що це за особа не можливо, оскільки він сидить в куртці та балаклаві.

Головно метою інформаційної операції було показати що джихадисти можуть безперешкодно отримати українське громадянство та добровольчий батальйон імені Джохара Дудаєва наповнений бойовиками ІДІЛ [76].

Наступною жертвою дискредитації спецслужб Російської Федерації та прив'язання міфу про ІДІЛ в Україні до Збройних Сил України. Кінцева мета спецслужб це престиж української Армії [76].

Інтернет видання Lenta.Ru у 28 вересня 2017 року посилаючись на Twitter видання Syria Today, яке повідомило, що в будинку де перебували бійці ІДІЛ знайшли «прапор України, зброю, пачку цигарок російського виробництва журнал з кросвордами» [76].

Далі спецслужби Російської Федерації продовжують розвивати міф про ІДІЛ в Україні, вже як «ідентичний стиль війни» [76]. Так 12 січня 2018 року на так званій гарячій лінії сепаратистів ДНР з'являється інформація пропагандиста Семена Пегова про таке «Місяць тому в період конфлікту між ЗСУ і ДНР в «сірій зоні» на лінії зіткнення в районі населених пунктів Гладосове і Травневе, українською стороною з дрона було скинуто саморобний вибуховий пристрій з вражаючими елементами по розташуванню особового складу однієї з донецьких бригад під Горлівкою» [76].

13 січня 2015 року під Волновахою Донецької області сталася трагедія із мирними жертвами. Відбувся обстріл БМ-21 «Град» блокпосту Збройних Сил України, одна із ракет потрапила в автобус загинуло 13 та 18 осіб дістали поранення [76]. Відразу бойові угруповання опублікували новину про знищення блокпоста на виїзді з Волновахи [83]. Як згодом повідомив начальник головного командного центру Генерального штабу генерал Богдан Бондар «В місті Докучаєвськ знаходилися кореспонденти російських та місцевих телеканалів з метою зняти, як українські військові будуть наносити удари у відповідь, але натомість були прийняті міри щодо стабілізації ситуації» [84]. Обстріл блокпосту мав на меті звинуватити Збройні Сили України в обстрілі Докучаєвська,

викликаючи вогонь у відповідь на себе, таким чином дискредитувати українську Армію [76].

2.2. Політика боротьби з антиукраїнською пропагандою в соціальних мережах.

Поширення пандемії спричинило чималу кількість фейків та протестів. У лютому 2020 року усі ЗМІ та соціальні мережі обговорювали новину про громадян, що прилітають з Китаю. Першим написав про пасажирів літака Сергій Чередніченко, який є прихильником Шарія. 19 лютого 2020 в соціальній мережі робить пост «Завтра всіх українців, які прибули з Китаю привезуть в санаторій в Нові Санжари. САНАТОРІЙ. Інфекційних лікарень не знайшли. Керівництво району вже отримало розпорядження». (Рис. 2.2) [85].

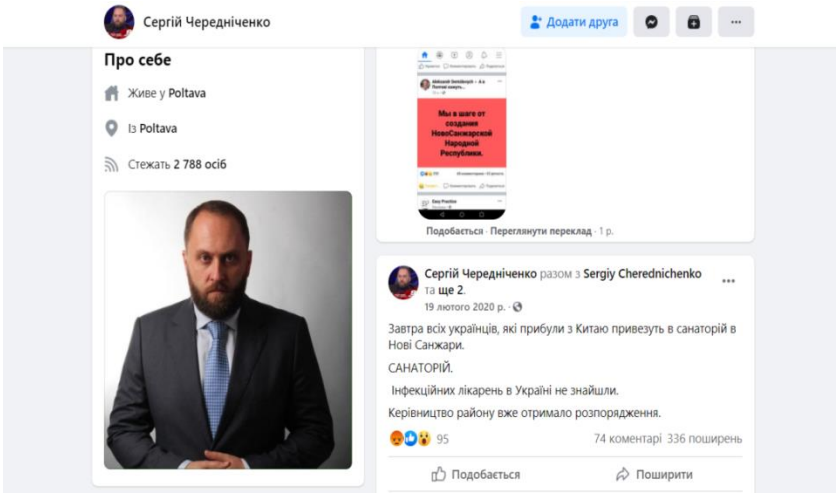


Рис. 2.2. Скріншот посту у соціальній мережі Facebook [85]

Пост пана Чередніченка має (станом на 10 травня 2021 року) 95 вподобайок та 336 поширень, що свідчить про штучну розгонку посту [86].

16 лютого 2021 року СБУ оголосило підозру за частиною першою статті 111 Кримінального кодексу України (державна зрада) [87]. За даними СБУ Шарій з 2012 року, сприяв державним та неурядовим структурам Російської Федерації у

проведенні спеціальних інформаційних операцій, використовуючи соціальні мережі, електронні засобі масової інформації, російські телевізійні канали [87].

Наприклад, відео на Youtube каналі Шарія відео, яке має назву «День позора подошел к концу». Де з 7 хвилини 30 секунд починає обзивати громадян «животниє», а вкінці відео він називає 20 лютого 2020 року «днем позора», акцентуючи свою увагу на День Героїв Небесної Сотні, установлений Указом президента України № 69/2015 «Про вшанування подвигу учасників Революції гідності та увічнення пам'яті Героїв Небесної Сотні» [88].

Також Шарій дискредитує, маніпулює та поширює фейкову інформацію щодо діяльності Армії на Донбасі. (Рис. 2.3, 2.4).

Рис. 2.3. Обґрунтування підозри СБУ [87]

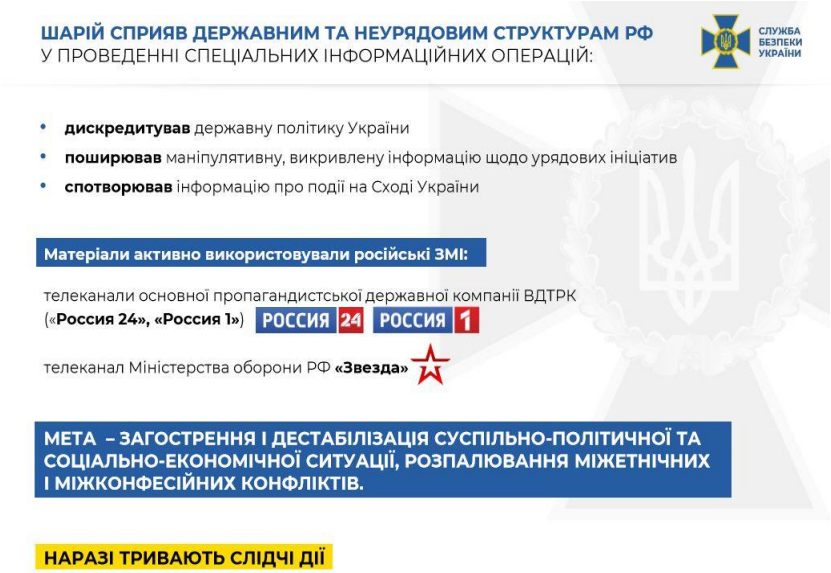


Рис. 2.4. Обґрунтування підозри СБУ [87]

18 липня 2019 року на сайті Український Мілітарний Портал виходить цикл статей російською мовою про Шарія його діяльність пропагандиста та роботу на користь спеціальних служб Російської Федерації [89].

У першій частині цього циклу «ФЕЙКИ ШАРИЯ. Как Шарий покрывает убийц украинцев. Часть 1» досліджують та розвінчують його фейки щодо видавання російських військових та техніки за українську [89].

02 вересня 2014 року Шарій публікує відео у відеохостингу Youtube під назвою «Как украинские СМИ над мертвым солдатом глумились». В цьому відео він розповідає про бій під Хрящуватим, а також показує підбитий танк та вбитого солдата, далі він показує інше відео із солдатами ворожої армії, які цей підбитий танк, оглядають [89].

Шарій у своєму відео посилається на відео з відеохостингу Youtube «Хрящеватое Конец августа 2014 года». В цьому відео до підбитого танку підходить група військових, які танк називають «брошенной нацистской техникой», ця фраза є аргументом для Шарія [89].

На відео «Хрящеватое 14 августа 2014г ВСУ», український командир танку розповідає, які він підбив ворожий танк, а інші військовослужбовці розглядають документи вбитих солдат, які виявились громадянами Російської Федерації. 55

секунда відео командир українського танку пробує прочитати напис на стволу танку, яку не може прочитати бо напис згорів [89].

26 липня 2014 року Шарій публікує відео «По британскому журналисту» [90], в захист британського громадянина Грема Вільяма Філліпса (колишній позаштатний співробітник пропагандиських телевізійних каналів «Russia Today», «Звезда»). Пан Філліпс використовувався проти України в інформаційній війни, яку веде Російська Федерація. Дане відео із відеохостингу YouTube «Грэм Филлипс. Донбасс. Канал РФ «Звезда». Зима 2015» [91], як приклад його участь в інформаційній війні проти України. На цьому відео «Грэм Филлипс «Я не видел русские танки в Дебальцево» пан Філліпс стверджує, що не бачив російські танки в Дебальцево, але на цьому відео «Грэм Филлипс. Дебальцево. Танки российской армии Т-72Б3 [15.02.2015]» [91] за 15 лютого 2015 року з 12 секунди пан Філліпс веде репортаж на фоні російських танків Т-72Б3.

2.3. Вакцинація, інформація та національна безпека

На сайті Центру громадського здоров'я МОЗ України зазначено, що вакцинація, це – безпечний, дієвий та простий захист населення від інфекційних захворювань [92]. Після вакцинації імунна система вчиться створювати імунітет (антитіла) до інфекційних хвороб. Вакцини вводять ін'єкційно, і деякі через рот (перорально) та в ніс [93].

Вакцинація необхідна для профілактики захворювань, зменшення смертності та контролю епідемій, пандемій.

Є два види вакцин «інактивована» та «атенуйована». Інактивована вакцина містить знешкоджений або ослаблений вірус. Необхідно декілька доз вакцин щоб інактивована вакцина дала імунну відповідь організму. Щоб інактивовану вакцина зробити спочатку вірус піддається високим температурам, радіацією або хімічним опроміненням [94].

Атенуйована вакцина має у складі живий ослаблений вірус. Така вакцина добре стимулює імунну систему. Приклади вакцин: проти кору, паротиту, краснухи, а також вітряної віспи [94].

1796 році англійський вчений Едвард Дженнер винайшов вакцину проти натуральної віспи та емпірично підтвердив, що вакцина формує імунітет від натуральної віспи [95].

А вже у 1802 році з’являється карикатура намальована Джеймсом Гілрейем про те як люди бояться вакцинації, бо через вакцинацію проти натуральної віспи у них з’являться коровоподібні паростки. (Рис. 2.5).

Рис. 2.5. Едвард Дженнер вакцинує людей, які бояться, що через вакцинацію у них з'являться коровоподібні відростки. Джеймс Гілрей 1802 року [95]

Поширення вакцинокерованих інфекційних хвороб є загрозою національній безпеці Україні, оскільки при не контрольованому поширенні інфекційних хвороб збільшується смертність населення, збільшується навантаження на систему охорони здоров’я, а також зменшується обороноздатність держави (як приклад хворіють військовослужбовці, як наслідок падає боєздатність підрозділу).

Останнім часом дуже активно поширюється антивакцинаторський рух в Україні та світі. У наш час цифрових технологій та соціальних мереж інформація поширюється миттєво для будь-якої аудиторії. Тому основні майданчики для розповсюдження антивакцинальної інформації є соціальні мережі такі як Facebook, Twitter, Instagram та відеохостинг Youtube.

02 березня 2020 року відомий антивакцинатор Захар Мілютін в соціальній мережі Facebook публікує пост [96] про алюмінієвий вакцинальний ад'ювант, який спричиняє деякі захворювання, а також алюміній попадає в мозок та накопичується в м'язах.

Аналітики в рамках партнерства з Facebook провели аналіз вище вказаного посту на ознаки неправдивої інформації та розмістили результати на сайті https://voxukraine.org/uk/ [97]. Пан Мілютін вказує про шкідливість алюмінієвого та відсутність реакції імунної системи, хоча алюміній використовується у вакцинах, як допоміжний засіб. Інформація про те, що імунна система не реагує є абсурдною, оскільки цей компонент дозволяє зменшити кількість доз вакцини [98].

Ольга Ворожбит в статті «Інфлюенсери і «нульові пацієнти» [99], який був опублікований 27 травня 2020 року на сайті tyzhden.ua пише роль Кремля в розповсюдженні дезінформації стосовно вакцинації. Наприклад режисер Нікіта Міхалков розповсюджує інформацію на державному каналі про чипізацію населення планети Білом Ґейтсом, а «Первый канал» опублікував у 2020 році сюжет «Теорія змови чи таємна правда: чому Білла Ґейтса вважають архітектором COVID-19». Кремлівські пропагандисти формують свою теорію змови з уривку фільму «Event 21. The Global Pandemic Exercise». Фільм який створений для гри-симуляції пандемії. Але для російської пропаганди це фільм доказ «змови» [99].

Також слід наголосити, що Фонд Білла та Мелінди Ґейтс вкладають величезні кошти у розробку вакцин, лікування та попередження СНІДУ та туберкульозу та інші ініціативи [100].

Як стверджує у своїй статті пані Ворожбит, що фейк із чипом Білла Ґейтса з’явився вперше у США 18 березня після питань-відповідей в соціальній мережі Reddit. (Рис. 2.6). [99].

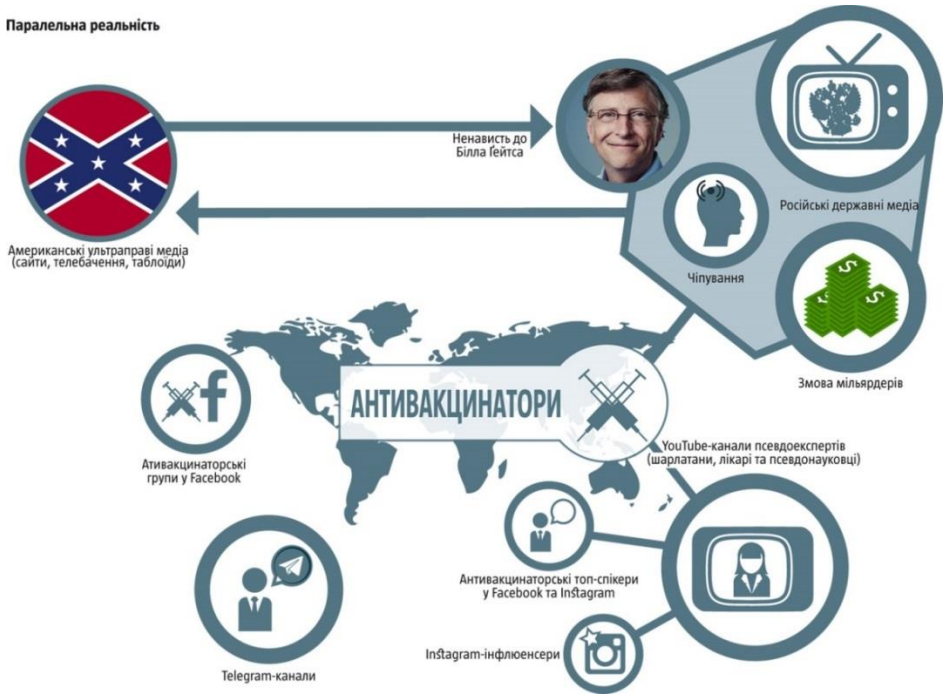


Рис. 2.6. Фейк про чип Білла Ґейтса

Джерело https://tyzhden.ua/Pandemic/243855 [99]

Висновки до розділу 2

Досліджено питання інформаційних воєн, дезінформації, фейків, дискредитації Збройних Сил України, добровольчих батальйонів. Також було досліджено інформаційні війни, методи ведення інформаційної війни, яка використовує Російська Федерація, «Доктрину Герасимова», використання Російською Федерацією ІДІЛ, як дезінформацію проти України.

Розглянуто питання конспірологічного руху на прикладі Qanon та використання його під час інформаційних воєн, впливу гумору під час інформаційних воєн, пропаганду, дезінформацію та використання гумору у політичній агітації. Розглянуто питання поширення фейків та дезінформації під час обсервації в санаторії туристів з Китаю у Нових Санжарах, Полтавської області. Використання Російською Федерацією блогерів, іноземних громадян для поширення дезінформації та маніпуляцій проти Збройних сил України.

Також розглянуто антивакцинаторські рухи, які маніпулюючи інформацією спричиняють зменшення довіри громадян до вакцинації, що в свою чергу тягне за собою збільшення захворюваності на інфекційні захворювання, збільшення смертності населення та загрозу національної безпеки.

Отже, недовіра громадян України до державних інституцій, а також до самої держави в цілому, тільки підсилювала ворожу дезінформацію, фейки, манімупуляції. Російській Федерації це було легко зробити, оскільки України сотні років перебувала у російськомовному інформаційному середовищі, яке паразитувало на питаннях «єдиного народу», «однієї країни» тощо.

На маю думку, якщо б держава починаючи з 1991 року займалася державною інформаційною політикою (патріотичне виховання, культурна пропаганда), освітою громадян, розвивала Збройні сили України, то можливо б такої катастрофи, яка сталась 2014 року, не було.

Життєво важливо для України проводити інформаційні кампанії щодо своєї культури, як в середині країни, так і на міжнародному рівні. Також необхідно

«виховувати» своїх громадян, навчати їх бути громадянами своєї країни, починаючи із дошкільних навчальних закладів.

Отже, за відсутністю державної інформаційної політики, твоє інформаційне поле захоплює Російська Федерація.

Освіта – це фундамент держави, стратегічна інвестиція, яка окупиться за десятки років.

Я прийшов до такого висновку – якщо ти не займаєшся «промиванням мізків» населенню, то ці «мізкі» буде промивати своєю пропагандою через «м’яку силу» Російська Федерація.

РОЗДІЛ 3. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Інформаційна безпека в умовах поширення COVID-19

Інформаційні загрози у сфері національної безпеки, що пов'язані із поширенням COVID-19

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

У Стратегії національної безпеки України-2020 визначено поширення COVID-19 як загрозу національній безпеці України [101].

Серед основних інформаційних загроз у сфері національної безпеки, пов'язаних із поширенням COVID-19, є: зростання правопорушень в інформаційній сфері (кіберзлочинності).

У Концепції розвитку сектору безпеки і оборони України серед нерозв'язаних проблем у секторі безпеки і оборони визначено неефективність механізму запобігання та нейтралізації сучасних загроз національній безпеці України [102].

У Стратегії національної безпеки України 2020 р. проголошено, що «людина, її життя і здоров'я, честь і гідність, недоторканність і безпека – найвища соціальна цінність в Україні», а також визначено, що однією із загроз національній безпеці України є поширення COVID-19. Крім того, поширення COVID-19 в Україні загострило та відкрило системні проблеми у сфері охорони здоров'я, біобезпеки й соціального захисту, недостатню готовність держави до дій у надзвичайних ситуаціях [101].

Відповідно до Постанови Кабінету Міністрів України від 12 березня 2020 р. № 211, на території України запроваджено карантин [103], який пов'язаний із заходами запобігання поширенню COVID-19.

20 лютого 2020 року повернувся літак із евакуйованими з Уханю (Китай) громадянами України та іноземцями. Автобусами пасажирів літака повезли на обсервацію в Нові Санжари (Полтавська обл.).

Автобуси із евакуйованими пасажирами місцеві мешканці зустріли протестом [104] та сутичками із поліцією [105] (рис. 2.7).

Відео, як жінки кидають каміння в автобуси на залізничній станції неподалік від Нових Санжар 20 лютого можна подивитись у Youtube, Джерело: https://www.youtube.com/watch?v=U6u0vk1Av0M

Відео «Провокатори у Нових Санжарах чіпляються до правоохоронців», Джерело: https://www.youtube.com/watch?v=DLi8wZPg6MI&t=1s

Любов Величко у своїй статті «Майстри паніки. Як проросійська мережа в Україні організувала бунт в Нових Санжарах» [106] пише про організацію та підтримку паніки серед місцевих жителів в Нових Санжарах (рис. 2.8).

Рис. 2.7. Зустріч мешканців евакуйованих з Уханю (Китай) на обсервацію в Нові Санжари (Полтавська обл.). Джерело: https://cutt.ly/HxXfbIZ

Рис. 2.8. «Скріншот із фейсбук-групи ГО "Голос Санжарщини" поширювався у вайбер-групах та в Інстаграмі ввечері 19 лютого»

В липні 2020 року Кримська правозахисна група опублікувала дослідження «Кримські медіа не надають людям вичерпної інформації про коронавірус (результати моніторингу)» [137], мета дослідження показати, як засоби масової інформації показуюсь ситуацію із пандемією в окупованому Криму [137]. Більшість публікацій у засобах масової інформації в період з квітня по червень 2020 року, відсутня критична інформація щодо пандемії, а також висловлювання представників окупаційної адміністрації однобоку та без висвітлення іншої точки зору на ситуацію із пандемією [137].

У соціальні мережі Facebook 30 квітня 2021 року користувач під іменем Alexander Snesar поширив пост [138] про інтерв'ю із доктором медичних наук Александром Редьком, де пан Редько стверджує, що після щеплення проти COVID-19 «людина виділяє з себе вірус, вона захворіватиме у два рази частіше, ніж до щеплення, а хворіти – важче». Фактчекери із порталу StopFake досліди цю інформацію і становили, що це фейк, оскільки жодна вакцина, яка дозволена для застосування Всесвітньою організацією охорони здоров'я проти COVID-19, не має у складі живий вірус [139]. Про те, що у вакцини проти COVID-19 має живого вірусу, також вказує Центр з контролю і профілактики захворювань США [140].

В соціальній мережі Facebook з'являться інформація про те, що «В Ізраїлі вакцина від Pfizer «вбила» у 40 разів більше людей похилого віку, ніж коронавірус» [141]. Авторка публікації наводять слова «інженера Хаїма Ятіва і доктора Ерве Селігмана», без жодних посилань на першоджерело [142]. 04 березня 2021 року цей фейк, що вакцинація викликає серйозну хворобу та приводить до смерті частіше, спростовує Міністерство охорони здоров'я Ізраїлю [143]. «При визначенні ефективності вакцини вимірюється ризик зараження хворобою серед людей, вакцинованих двома дозами вакцини, в порівнянні з людьми, які не були вакциновані взагалі. Згідно з найостаннішими даними встановлено, що вакцина дуже ефективна щодо захворюваності, важкого перебігу захворювання, госпіталізацій і смертності» [143]. Висновки

Міністерства охорони здоров'я Ізраїлю були зроблені на підставі звіту про ефективність щеплення проти COVID-19 відділу епідеміології Міністерства охорони здоров'я Ізраїлю [143].

Кібербезпека. Загрози в умовах COVID-19.

Глобальна мережа McAfee, що є одним з провідних лідерів досліджень загроз у сфері кібербезпеки, зареєструвала зростання на 605% загальної кількості виявлених загроз в умовах COVID-19 за другий квартал 2020 р. [107].

Після першої чверті, яка призвела світ до пандемії, у другому кварталі 2020 року підприємства та установи продовжили свою діяльність та адаптовувалися до роботи удома, а кібербезпека мала новий виклик. McAfee контролює мільярд датчиків у всьому світі, та захищає бізнес та особисті активи громадян [107, с. 4].

У звіті за листопад 2020 р. розглядаються загрози та інциденти безпеки, які проявилися в умовах COVID-19 у другому кварталі 2020. Результати досліджень (третій квартал до другого) показують: збільшення загроз, в середньому – 419 на хвилину, поява нових шкідливих програм для Office та їх зростання на 103%. Регіональний розподіл загроз представлено у Додатку А.

Зловмисники перенаправили все більш витончені методи в сторону підприємств, урядів, шкіл і співробітників, які продовжують ще стикатися з проблемами, що пов'язані з обмеженнями COVID-19 [107].

У цих умовах для співробітників важливо дотримуватися протоколів безпеки, остерігатися використовувати зовнішні вкладення електронної пошти і неперевірені посилання, фішингові точки входу, через які можуть бути доставлені програми-вимагачі та шкідливі програми. Найбільша кількість хмарних інцидентів сталося в Таїланді, менше – в США, Україна – за меншої їх кількості – на третьому місці після США і Гонконгу. (Додаток Б) [107].

У другому кварталі 2020 року компанія McAfee зафіксувала близько 7,5 мільйона зовнішніх атак на хмарні облікові записи, збираючи дані про використання хмарних технологій від більш ніж 30 мільйонів користувачів по всьому світу. Ці дані моніторингу представляють компанії з основних галузей по

всьому світу, такі як: фінансові послуги, охорону здоров'я, державний сектор, освіту, роздрібну торгівлю, технології, виробництво, енергетику, комунальні послуги, юридичні послуги, нерухомість, транспорт та бізнес-послуги [107].

McAfee Labs нарахував 561 публічно розкритий випадок у другому кварталі 2020 р. (Додаток В). Розкриті випадки, були спрямовані на Північну Америку та становили 29% від загальної кількості інцидентів, зменшившись на 30% порівняно з попереднім кварталом. Розкриті інциденти, націлені на США в другому кварталі 2020 року, знизилися на 47%, у Великобританії – на 29%, а в Канаді – на 25% в порівнянні з попереднім кварталом [107].

Кількість розкритих випадків, що виявлені у другому кварталі 2020 року у сфері науки і технологій, збільшилася на 91% в порівнянні з попереднім кварталом. У кількох галузях економіки їх кількість зросла на 25%, у промисловості показник знизився на 10%, у державному секторі знизився на 14%, у приватному секторі знизився на 28% [107].

У період з січня по квітень цього року США урядовий сектор зафіксував зростання використання хмари підприємствами та установами на 45%, через продовження соціально віддаленої роботи. Звіт про загрози лабораторій McAfee, листопад 2020 р [107, с. 14]

Успішна інтеграція багатохмарного середовища створює реальні виклики для всіх секторів, зокрема для таких, як державний сектор. Керування безпекою в різних хмарах середовища можуть бути в переважній більшості ускладненими для IT-співробітники, тому їм потрібні інструменти, які можуть автоматизувати їх завдання та забезпечують постійний захист чутливої інформації, куди б вона не потрапляла всередину або поза хмарою. Компанія McAfee пропонує навчити користувачів та громадськість про потенційні ризики, пов'язані зі шахрайством. Підступні групи намагаються зібрати дані користувачів. Мета їх полягає в крадіжці облікових даних користувачів OneDrive. У фальшивому урядовому електронному листі-приманці шахраї вдають, що вони з урядових установ і доставлять документи, які містять найновіші дані анкети щодо COVID-19. Запам'ятайте: уряди, зазвичай, не надсилають електронною поштою

незатребувані документи. Користувач повинен перевірити адреси електронної пошти відправника та місцезнаходження в заголовках електронних листів і відвідати офіційний урядовий сайт, щоб перевірити, чи є там інформація про COVID-19. Звіт про загрози лабораторій McAfee, листопад 2020 р [107, с. 26].

Шевчук О. пропонує оцінювати таку загрозу на трьох рівнях: безпеки особи (особистості), суспільства та держави [108]. Автор зазначає, що поряд із позитивним впливом заходів карантину на стримування та запобігання розповсюдженню пандемії COVID-19 мали місце негативні моменти, що пов'язані з обмеженнями прав людини [108, с. 325-328].

З початком дії положень Постанови Кабінету Міністрів України від 12 березня 2020 р. № 211 [103] передбачено втручання держави у права людини. Основними з них є обмеження стосовно права: на повагу до приватного життя; на свободу й особисту недоторканність – примусове поміщення громадян в обсервації; на свободу пересування, на свободу мирних зібрань, на освіту на свободу релігії, доступу до медичної допомоги [109, с. 327].

Андрощук Г. до актуальних проблем поширення COVID-19 у Європейському Союзі вказує такі чинники: «збільшення кількість кібератак проти організацій і приватних осіб як результат зростання кіберзлочинності (поширення різних пакетів шкідливих програм); шахрайство (розвиток схем телефонного шахрайства, шахрайства з поставками спиртовмісних гелів і масок); збільшення продажів контрафактної медичної та санітарно-гігієнічної продукції, а також засобів індивідуального захисту тощо» [110].

Так, ООН розроблена класифікація безпеки суспільства, яка визначає її основні рівні, серед яких: економічний, продовольчий, суспільний, політичний, екологічний, особистої безпеки, охорони здоров'я. Безпека держави характеризує рівень захищеності держави від внутрішніх і зовнішніх загроз шляхом застосування комплексу політичних, економічних, соціальних, воєнних, інформаційних і правових заходів, які слугують забезпеченню стабільної життєдіяльності суспільства [111, с. 295].

Також дослідники наголошують на поширенні злочинності в інформаційній сфері, спричиненої розповсюдженням COVID-19 у різних сферах життя людини та суспільства в цілому: зростання кількості шахрайств, які зумовлені продажем, а також придбанням медичних засобів або засобів індивідуального захисту та продуктів харчування, зокрема продажів у мережі «Інтернет» ліків для лікування COVID-19; поширення кіберзлочинності, зумовлене шахрайством у вигляді дзвінків чи смс-розсилок про фінансові компенсації державою витрачених на лікування коштів або інших виплат, які мають на меті поширення паніки серед населення тощо [112, с. 37].

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

Європейським Союзом прийнято низку документів з метою боротьби з дезінформацією про COVID-19: Action Plan against Disinformation (План дій проти дезінформації) [113] та упроваджено Code of Practice on Disinformation (Кодекс практики проти дезінформації) [114].

Action Plan against Disinformation (План дій проти дезінформації) дезінформацію визначає, як оманлива, не правдива інформація, яка поширюється для введення суспільства в оману, що спричиняє шкоду суспільству [113].

Шкода суспільству це в першу чергу знищення демократії, благам суспільства громадянам Європейського Союзу [113].

Code of Practice on Disinformation (Кодекс практики проти дезінформації) підписаний такими соціальними мережами Facebook, Google, Twitter, Microsoft [114].

3.2. Інструменти протидії загрозам в інформаційній сфері

Є.Ф. Штефанюк, І. Р. Опірський, О. І. Гарасимчук, у статті «Аналіз застосування існуючих технік розпізнавання фейкових новин для протидії інформаційній пропаганді» опублікованої в електронному журналі «Безпека інформації» вказують чотири особливості пропаганди російської федерації, а саме [115]:

1. «великий об’єм це поширення великою кількістю користувачів та ЗМІ. Фактично створюючи ілюзію достовірності інформації;
2. неконсистентність це неузгодженість фейків із загальною пропагандою;
3. велика кількість каналів поширення це ЗМІ, соціальні мережі, інформаційні портали;
4. фальсифікація та викривлення фактів» [115].

Критерії для ефективного виявлення фейків такі: [115]:

1. знаходити фейки на ранній стадії;
2. коефіцієнт виявлення фейків має бути на високому рівні;
3. контент та реакцію користувачів на пости, повинні враховуватись;
4. враховувати, що у соціальних мережах можуть бути боти [115].

Захист інформації про особовий склад Збройних Сил України.

Автор брав участь у розробленні Аналітичної записки «Як забезпечити захист штабної інформації, інформації про особовий склад ЗСУ», де було проаналізовано основні проблеми захисту інформації. Замовником визначено Міністерство оборони України, Генеральний Штаб України. Мета вирішення проблеми визначена як захист інформації про особовий склад Збройних Сил України, впровадження кібербезпеки. Альтернативні варіанти висвітлені у

Додатку Д. Рекомендований варіант політики: Впровадження новітньої інформаційної системи на основі симетричного алгоритму блочного шифрування Advanced Encryption Standard (AES). Це дасть змогу підвищити обороноздатність, безпеку та захистити життя військовослужбовців та їх родин, оперативно прийняти рішення на полі бою, ефективно виконувати службу підрозділами Армії тощо.

В Україні існує величезна проблема захисту інформації, як персональних даних громадян та чутливої інформації (цілком таємної, інформація про персональні дані військовослужбовців тощо). Було багато випадків погроз у вигляді телефонних дзвінків та текстових повідомлень зі сторони Російської Федерації до ветеранів, діючих військовослужбовців, ветеранів та членам їх сімей [116]. Були випадки витоку інформації із штабів про особовий склад батальйонів, рот, взводів.

Також неодноразово витікала персональна інформація про пацієнтів. Так, 08 жовтня 2020 з'являється повідомленнями від Національного координаційного центру кібербезпеки при Раді безпеки і оборони України, який проводив моніторинг, про витік персональної інформації (медичні дані) найбільшої клініки Дніпра [117].

Інформація яка попала у відкритий доступ є такою:

- персональні дані клієнтів.
- персональні дані працівників клініки.
- дані медичної картки.
- списки хворих на COVID-19 [117].

В Армії командири використовують комп'ютерну техніку, яка не сертифікована (ніяким чином не захищення), часто використовують піратське програмне забезпечення, є випадки використання російських антивірусних програм. Також низька цифрова освіта громадян та військовослужбовців, яка призводить до не розуміння захисту інформації в кіберпросторі зокрема [118].

Гумор-розвага, гумор-пропаганда як інструменти інформаційної війни

Як говорив американський гуморист James Thurber [119] «Humor is a serious thing. I like to think of it as one of our greatest earliest natural resources, which must be preserved at all cost» [120], яка перекладається «Гумор - це серйозна річ. Мені подобається думати про це як про одне з наших найбільших».

Наукова праця «StratCom сміється: у пошуках аналітичної основи» досліджує вплив гумору на дискредитації політиків, дезінформації, інструмент пропаганди та контрпропаганди [121].

Також треба розділяти на 2 види гумору [121, с. 7]:

1. Гумор-розвага.
2. Гумор-пропаганда.

Максим Кияк у 4 розділі дослідженні «StratCom сміється: у пошуках аналітичної основи» [121], «Ситуаційне дослідження: використання гумору для заохочення солідарності, очернення і зняття напруги в українських ЗМІ під час російської агресії (2014-2016 р.р.)» [121, с. 127], стверджує що на початку військової агресії Російської Федерації Україна мала протидіяти масовій інформаційній війні, без досвіду боротьби з контрпропагандою.

Українські засоби масової інформації є головним інструментом контрпропаганди. Є багато прикладів використання гумору на українському телебаченні: ICTV (Антизомбі), Канал 24 (Вєсті Кремля) та інші програми, карикатуристи, журнали, газети, співак Антін Мухарський (в образі Ореста Лютого) [121, с. 128].

Один із головних методів контрпропаганди – це зведення пропаганди до абсурду. Один із таких прикладів – відео бійців полку «Азов», які піднімають прапор США, говорять англійською. Вони в гумористичній манері розповідають про пропаганду Російської Федерації щодо військ НАТО на Донбасі та інших стереотипах російської пропаганди.

Бійці «Азова» у жартівливому відео підняли американський прапор над Широкіним [122]. Відео із відеохостингу YouTube https://www.youtube.com/watch?v=1p7JIN7dxBY «Широкино доброволец из полка Азов поднял флаг США».

Також дуже вдало використовує гумор та музику Антін Мухарський в образі Ореста Лютого. Його пісні основані на совєцькій музиці, на котру накладено антикремлівський, патріотичний, гумористичний текст українською [121, с. 134]. Приклад жартівливої пісні Ореста Лютого «А я не москаль», відео https://www.youtube.com/watch?v=1euHQ8SDHCo&list=PLcnaspc0quf7oLvBhHIAQEo422wFZKSpo&index=3.

Гумор, як елемент контрпропаганди, вдало використовує висміювання пропагандиських наративів та доводить їх до абсурду, які створює Російська Федерація під час інформаційних війн проти України [121, с. 136].

3.3. Пріоритети, механізми та інструменти формування політики у сфері інформаційної безпеки

Пріоритети державної політики в інформаційній сфері

Пріоритети державної політики в інформаційній сфері прописані у Доктрині інформаційної безпеки України [47] (рис. 2.11.)

Рис. 2.11. Пріоритети державної політики в інформаційній сфері

Джерело: [47]

«Пріоритетами державної політики в інформаційній сфері мають бути:

1) щодо забезпечення інформаційної безпеки: створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет;…, забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;… розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України; боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;…тощо» *Пріоритети державної політики в інформаційній сфері* [47]

2) «щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію: стимулювання розвитку національного виробництва текстового і аудіовізуального контенту…; розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;…, удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;…, пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз тощо» [47]

3) «щодо відкритості та прозорості держави перед громадянами: розвиток механізмів електронного урядування;…, проведення реформи урядових комунікацій; розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень; сприяння формуванню культури суспільної дискусії» *Пріоритети державної політики в інформаційній сфері»* [47];

4) «щодо формування позитивного міжнародного іміджу України:

– ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені; розвиток публічної дипломатії, у тому числі культурної та цифрової;…, сприяння поширенню та розвитку системи іномовлення України; створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства;…, участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності; запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини». *Пріоритети державної політики в інформаційній сфері* [47].

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

На даний час проти України ведеться новий тип військових дій, які описані у так званій «Доктрині Герасимова» [68] і в першу чергу інформаційна війна ведеться проти цивільного населення. Тобто задача посіяти паніку, недовіру до політиків, а також до державних інституцій.

На думку аналітика з безпекових питань пана Юрія Костюченка, на запитання у статті пані Ірини Шторгін «Якою має бути інформаційна політика України в умовах війни?», він надає таку відповідь: що вигоду від ведення бойових дій набувають не тільки держава агресор, а також окремі групи впливу у самій державі агресора. Тобто, головна задача держави агресора – це створення постійного конфлікту, в середині суспільства. Якщо громадяни вірять у фейки та ворожу пропаганду, то вона присутня в інформаційному середовищі держави [123].

Громадяни для держави – це є діти, яких необхідно постійно виховати та давати якісну освіту. Тобто, держава має забезпечувати виховання громадян з молодшого віку ще у дошкільному навчальному закладі.

Державний механізм протидії дезінформації

31.03.2021 року при Міністерстві культури та інформаційної політики було створено Центр стратегічних комунікацій та інформаційної безпеки (ЦСКІБ) [124] з метою протидії дезінформації. ЦСКІБ об'єднав зусилля громадських організацій та влади у боротьбі із дезінформацією, швидкого реагування на фейки, а також на промоцію українських наративів. У структурі діятиме при МКІП, але у співпраці з Центром протидії дезінформації РНБО [124].

Основними напрямками діяльності ЦСКІБ передбачено такі (рис. 2.12):

Рис. 2.12. Напрямки діяльності Центру стратегічних комунікацій та інформаційної безпеки (Побудовано на основі [124, 125]).

09 квітня 2020 року створюється Facebook сторінка Центру. Вже в цей день з'являється перший пост про дезінформацію щодо загибелі дитини на окупованих територій [125].

На брифінгу 12 квітня 2020 року в Укрінформ Центр стратегічних комунікацій та інформаційної безпеки разом із представниками ГО «Детектор медіа», інтернет-проекту «Стопфейк» [126].

Спікери повідомили, що інтернет-видання Страна.ua та «Вести», ці медіа писали найбільше про загибель п'ятирічної дитини в Олександрівському біля Горлівки, Донецької області (тимчасово окуповані території) [127].

За словами представника ГО «Детектор медіа» Галини Петренко [126] що в Страна.ua та «Вести» були різні акценти до написання новини. Так Страна.ua акцентувала увагу на загибель хлопчика та інші події на Донбасі – це підготовка до великомасштабної війни або провокація України, можливо так званої ДНР. В свою чергу «Вести» зосереджувались на критиці [126].

Загалом російські пропагандистські інформаційні ресурси повідомляли про 2 квітня почали поширювати новину про смерть дитини в Олександрівську нібито вбито внаслідок удару українського безпілотнику. Населений пункт де загинула дитина знаходиться близько 15 кілометрів до лінії зіткнення, що ставить під сумнів застосування безпілотника [126].

За словами керівниці Центру, порівняння російською владою загибелі п'ятирічного хлопчика із діями президента Югославії Слободана Мілошевича у Сербії (масове вбивство у місті Сребриця в Боснії та Герцеговина) є не припустимим, оскільки сама росія підтримала резолюцію Радбезу ООН про масові вбивства в Сребриці та визнала це геноцидом [128].

Центр стратегічних комунікацій та інформаційної безпеки підготував публікацію, яка опублікована на порталі Укрінформ [129] за назвою «М'яка сила» Кремля в дії: як Росія експортує свій «культурний продукт» в Україну», про культурну пропаганду Російської Федерації, на прикладі російського репера Моргенштерна. Цей виконавець планував зробити в Україні три концерти (червень місяць), але за його словами він відмінив концерт тому, що йому страшно їхати в України з туром. Станом на 28 квітня 2021 року квитки на його концерти в Україні є у продажу [130]. Аудиторія Моргенштерна це російськомовна молодь у віці 12-19 років.

Попередній концерт в Україні цього репера відбувся в Одесі 08 грудня 2019 року в Одесі, в день жалоби за загиблими в Одеському коледжу економіки, права та готельно-ресторанного бізнесу [131]. Під час концерту Моргенштерн назвав траур «показухою» [132].

Як Моргенштерн використовується в російській пропаганді методом «м'яка сила» [129]:

1. Його вплив здійснюється на молоду аудиторію від 12 до 19 років.
2. Він напряму не закликає до військово інтервенції та поваги до Путіна.
3. Моргенштерн поважає Путіна за авторитет та особисті риси.
4. Нещодавно підтримував Навального, а зараз підтримує Путіна.

Виступи російських виконавців таких, як Моргенштерн, просувають російську пропаганду про «один народ», «одна мова», «братські народи» – це так звані непрямі методі пропаганди – «м'яка сила» із впливом на загальну аудиторію [129].

Україна на шляху до НАТО

Організація Північноатлантичного договору (НАТО) – міжнародна організація, військово-політичний союз [133]. Головна місія Організації Північноатлантичного договору це забезпечення свободи, безпеки, дотримання спільних цінностей демократії, верховенства права країн-членів [133].

У 2014 році запрацював Strategic Communications Centre of Excellence NATO (далі – Центр), штаб квартира знаходиться в місті Рига, Латвія. Центр не входить до структури НАТО, а є міжнародною військовою організацією [134]

Головна місія Центру це збільшення потенціалу НАТО та союзників у стратегічних комунікаціях [134].

Види діяльності Центру на 2021 рік, зазначені наступні: [134].

1. «Розробка політики та доктрини Центру.
2. Багатонаціональний експеримент з інформаційних операцій.
3. Багатонаціональна кампанія з розвитку спроможності.
4. Аналіз контр-наративних стратегій, розвиток та оцінка наративу.

5. Розробка концепції настільних вправ Центру та розробка концепції моделювання інформаційного середовища.

6. Розробка концепції навчального модуля моделювання дезінформаційної атаки.

7. Розробка концепції навчального модуля моделювання дезінформаційної атаки.

8. Розробка концепції НАТО з бойових дій.

9. Робота над вдосконаленням термінології Центру.

10. Звіти про роботизовані мережі в соціальних мережах, російські дезінформаційні кампанії в регіоні NB-8, система соціальних кредитів Китаю, роль посередників даних у маніпулюванні даними, вимірювання ефектів дезінформації та розвінчання.

11. Курс та конференція у соціальних мережах.

12. Підтримка освіти та тренінгів для АСТ» [134].

Центром було підготовлено наукове дослідження під керівництвом майором Томасом Балкусом та колективом дослідників: професор Жанет Озолія, професор Іварс Аустерс, доктор наук Солвіта Деніса-Лієпнієцє, доктор філологічних наук Юргіс Шкілтерс, докторант Сігіта Струьерга, доктор філософії Максим Кияк, по замовленню Міністерства оборони Латвійської Республіки «StratCom laughs: in search of an analytical framework», що перекладається як «StratCom сміється: у пошуках аналітичної основи» [121].

22 листопада 2018 року Верховна Рада попередньо схваливши Закон України «Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)», закріпивши стратегічний курс до Організації Північноатлантичного договору (НАТО) [144].

Співробітництво у військовій сфері Україна – НАТО виконується відповідно до Річної національної програми під егідою Комісії Україна – НАТО в межах Робочого плану Військового комітету Україна – НАТО [135]. Завдання співробітництва у військовій сфері: посилення обороноздатності та нарощення

оперативних спроможностей Збройних Сил України у сучасних безпекових умовах; досягнення взаємо сумісності Збройних Сил України зі збройними силами країн Альянсу; сприяння реформуванню та професіоналізації Збройних Сил України, впровадження у їх діяльність кращих військових стандартів; забезпечення участі Збройних Сил України у операціях з підтримання миру та безпеки під проводом Альянсу, залучення до Сил реагування НАТО [135].

Починаючи з 2015 року збільшується військове співробітництво у сферах системи управління та зв'язку, кібербезпека, медичне забезпечення, логістика, стандартизація, стратегічні комунікації [135].

Забезпечується лікування та реабілітація країнами-членами військовослужбовців, постраждалих під час війни на сході країни. Також Організація Північноатлантичного договору (НАТО) підтримує реформування Збройних Сил України та надало необхідні нормативно-правові документи для їх реформування [135].

Залучаються підрозділи Сил спеціальних операцій Збройних сил України до Сил реагування НАТО, після відповідного оцінювання НАТО [136].

До тридцятиріччя незалежності України було створено дискусійний майданчик Всеукраїнський форум «Україна 30» [145] в рамках якого проходить форум «Безпека країни» [145]. Головне завдання форуму «Україна 30. Безпека країни» [146]:

1. Дискусія на тему національної безпеки України під час стягування військ Російської Федерації на східні кордони України.
2. Комунікація та інформування громадян про заходи, які вживає державні інституції під час виконання стратегії безпеки.
3. Діалог із партнерами щодо національної безпеки
4. Реформування сектору безпеки та визначення першочергових кроків
5. Обговорення теми кібербезпеки та інформаційної безпеки
6. Кроки для членства в НАТО [146].

Отже, для забезпечення ефективності і результативності формування та реалізації чинної політики потрібно комплексно використовувати механізми та

інструменти правового, економічного, фінансового, організаційного, інформаційного, освітнього характеру. Система цих інструментів має відображати національні пріоритети та узгоджувати загальнодержавні інтереси [146].

Інструменти та механізми [146]:

у сфері фінансово-економічного забезпечення: довгострокове бюджетне планування; якісне використання коштів трастового фонду НАТО; проведення аналізу бюджетних запитів розпорядників бюджетних коштів із залученням центральних органів влади в процесі опрацювання проекту державного бюджету України на поточний рік з метою вмотивованого вирішення питань концентрації фінансових ресурсів на реалізацію пріоритетних цілей та програм в секторі безпеки і оборони України [146];

у сфері інституційного забезпечення: запровадження електронного урядування та документообігу; державна підтримка програм та проектів, що стосуються національної безпеки і оборони України; удосконалення стратегічного планування МО, РНБО, їх узгодження з цілями та напрямами національної політики, здійснення бюджетного планування відповідно до стратегічних пріоритетів; збереження курсу України в членство в Євроатлантичному Альянсі [146].

Висновки до розділу 3

Підсумовуючи вищезазначене, визначено, що інформаційні загрози у сфері національної безпеки, які пов'язані із поширенням COVID-19, – це витік персональних даних громадян, шахрайство, дезінформацій щодо лікування хвороби тощо.

Європейським Союзом вживаються заходи для боротьби з глобальним поширенням COVID-19 та підтримки систем охорони здоров'я, а також протидією дезінформації щодо COVID-19.

У Стратегії національної безпеки України-2020 визначено поширення COVID-19 як загрозу національній безпеці України.

Серед основних інформаційних загроз у сфері національної безпеки, пов'язаних із поширенням COVID-19, є: зростання правопорушень в інформаційній сфері (кіберзлочинності).

Важливо захищати персональні дані військовослужбовців, використовувати сертифіковане та ліцензійне програмне забезпечення при виконанні своїх службових обов'язків, навчати військовослужбовців цифровій та інформаційні грамотності.

Ми можемо і використовуємо гумор у своїй пропаганді нашої культури та контрпропаганді проти Російської Федерації.

Створення Центру стратегічних комунікацій та інформаційної безпеки Міністерства культури та інформаційної політики дасть можливість системно займатись протидією дезінформації та ворожій пропаганді, а закордонним партнерам спиратись на офіційну позицію Уряду.

Так, як економіка України в десятки разів менша за економіку Російської Федерації, і ми не можемо протидіяти сам на сам із нашим ворогом. Критично важливо постає питання вступу до НАТО. Оскільки вступаючи до НАТО на вас розповсюджується колективна безпека на напад третьої країни.

ВИСНОВКИ

Інтеграція новітніх мережевих технологій у життя стала невід'ємною складовою різноманітних сфер суспільного життя. Не стали винятком і Збройні Сили України. За роки війни значно зросло використання таких технологій у повсякденній діяльності та у процесі управління ЗСУ. Широке залучення інформаційних технологій дає можливість значно зменшити час на прийняття рішень, передачу наказів та обмін інформацією між підрозділами.

1. Верховною радою України прийнята низка законів що стосується національної безпеки. Так, для забезпечення державної інформаційної політики у сфері національної безпеки було прийнято Закон України «Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)» (2019), який передбачає стандартизацію ЗСУ до стандартів НАТО, в тому числі та діджиталізацію та захист інформації про особовий склад та боротьбу з кібератаками.

Стратегія національної безпеки України (2015) передбачає досягнення цілей: мінімізація загроз державному суверенітету та створення умов для відновлення територіальної цілісності України у межах міжнародно-визнаного державного кордону України, гарантування мирного майбутнього України як суверенної і незалежної, демократичної, соціальної, правової держави; утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО. Загрозою національної безпеки у Стратегії національної безпеки України визначено інформаційно-психологічну війну.

Визначено, що важливим нормативно-правовим документом є Доктрина інформаційної безпеки України (2017), де передбачено, що технології гібридної війни, які застосовує Російська Федерація проти нашої країни перетворило інформаційну сферу на головну боротьбу за свідомість громадян.

2. У магістерській роботі досліджено міжнародний досвід державної інформаційної політики у сфері національної безпеки, насамперед, досвід Сполучених Штатів Америки, де головним федеральним виконавчим органом у військовій сфері та питанні національної безпеки є Міністерство оборони США. У складі Міністерства оборони США діє Агентство національної безпеки, повноваження якої є збір та аналіз закордонної розвідувальної інформації, захист інформаційних систем і комп'ютерних мереж.

Агентство національної безпеки є складовою частиною системи безпеки країни разом з ЦРУ та іншими агентствами, однак на відміну від ЦРУ не займається використанням агентів в інших країнах. Кіберкомандування Армії США та Управління програм з інформаційної Міністерства оборони виконує такі основні функції: захист інформаційних мереж Армії та Міністерства оборони; реагування на кібер-атаки; підтримка союзників США. Важливим для України є також досвід у сфері інформаційної безпеки потужних армій світу: Ізраїлю, Південної Кореї, Туреччини.

3. Визначено проблеми реалізації державної політики у сфері інформаційної безпеки, що виникли через поширення COVID-19. Проаналізовано заходи політики, які застосовуються для боротьби з поширенням COVID-19 та підтримки систем охорони здоров'я в Україні та світі. Після проголошення у березні 2020 року ВООЗ пандемії Європейським Союзом прийнято низку документів з метою боротьби з дезінформацією про COVID-19, як то: план дій проти дезінформації та кодекс практики проти дезінформації. В Україні також було оголошено про поширення пандемії Постановою КМУ від 12 березня 2020 р. та вжито низку заходів протидії.

У Концепції розвитку сектору безпеки і оборони України, в Стратегії національної безпеки України-2020 р. наголошено на неефективності механізму запобігання та нейтралізації нових загроз та визначено поширення COVID-19 як загрозу національній безпеці. Визначено, що нині в Україні та світі активно поширюється антивакцинаторський рух. Основними майданчиками для

розповсюдження антивакцинальної інформації стали соціальні мережі. Приведено конкретні приклади.

Досліджено основні інформаційні загрози у сфері національної безпеки, що пов'язані з поширенням COVID-19, такі як: зростання правопорушень в сфері кіберзлочинності. Проаналізовано показники та тенденції, які розглянуті глобальною мережею McAfee, що є одним з провідних лідерів досліджень загроз у сфері кібербезпеки, Зокрема, зареєстровано зростання на 605% загальної кількості виявлених загроз в умовах COVID-19 за другий квартал 2020 р. Визначено, що найбільша кількість хмарних інцидентів сталося в Таїланді, менше – в США, Україна – за меншої їх кількості – на третьому місці після США і Гонконгу.

Аналіз досліджень науковців дав можливість оцінювати загрози на трьох рівнях: безпеки особи, суспільства та держави та закцентував увагу на тому, що поряд із позитивним впливом заходів карантину на стримування та запобігання розповсюдженню пандемії COVID-19 мали місце негативні моменти, що пов'язані з обмеженнями прав людини, оскільки, з початком дії положень Постанови Кабінету Міністрів України від 12 березня 2020 р. передбачено обмеження стосовно права: на повагу до приватного життя, на свободу й особисту недоторканність, на свободу пересування, на свободу мирних зібрань, на освіту на свободу релігії, доступу до медичної допомоги тощо.

Визначено, що ще однією загрозою, яка пов'язана із застосуванням карантинних заходів COVID-19, є витік персональних даних громадян, які перебувають на лікуванні, карантині або самоізоляції. Також, наголошено, що держава зобов'язана забезпечувати достовірне інформування суспільства про COVID-19.

4. Обґрунтовано механізми формування та реалізації державної політики у сфері інформаційної безпеки. Для забезпечення ефективності і результативності формування та реалізації чинної політики потрібно комплексно використовувати інструменти правового, економічного, фінансового, організаційного, інформаційного, освітнього характеру. Інструменти та

механізми, що застосовуються у сфері фінансово-економічного забезпечення мають враховувати довгострокове бюджетне планування, здійснювати аналіз бюджетних запитів розпорядників бюджетних коштів із залученням органів влади в процесі підготовки проекту державного бюджету України на поточний рік тощо; у сфері інституційного забезпечення: запроваджувати електронне урядування та системи документообігу; надавати державну підтримку програм та проектів стосовно національної безпеки і оборони України, узгоджувати стратегічні плани з цілями та напрямами державної політики, продовжувати курс України до членства в Євроатлантичному Альянсі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дай Томас Р. «Основи державної політики». Р. 1. Аналіз політики. Р. 2. Модель політики: підр. для ВНЗ. – Одеса: АО БАХВА, 2005. – 468 с. URL: https://books.google.com.ua/books?hl=uk&lr=&id=gYwzprJAEDAC&oi=fnd&pg=PA11&dq=related:wbVezAvgX50J:scholar.google.com/&ots=XUJH3D4Kel&sig=Wc9dWLoErkgF3-yt_NjaT9rmbDc&redir_esc=y#v=onepage&q&f=false
2. Кондратюк Т.В. Концептуальні моделі як відображення різних аспектів державної управлінської політики. *Науковий вісник Академії муніципального управління*. Серія : Управління. – 2012. – Вип. 1. С. 133. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nvamu_upravl_2012_1_19.pdf
3. Knill C., Tosun J. Policy Making. In: Daniele Caramani (ed.), Comparative Politics. Oxford: Oxford University Press, 2008, pp. 495-519. – URL: https://www.researchgate.net/publication/30014974_Policy_making
4. Baumgartner F.R., Breunig C., Green-Pedersen C., Jones B.D., Mortensen P.B., Neytemans M., Walgrave S. Punctuated equilibrium in comparative perspective. *American Journal of Political Science*. – 2009. – Vol. 53. – No. 3. – P. 602—619. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-5907.2009.00389.x
5. Shepsle K. A. Rational choice institutionalism/ / The Oxford handbook of political institutions / [edited by R. A. W. Rhodes, S. A. Binder and B. A. Rockman]. – New York : Oxford University, 2008. – P. 23-38. URL: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199548460.001.0001/oxfordhb-9780199548460-e-2
6. March J. G. Olsen J. P. Elaborating the «new institutionalism». The Oxford handbook of political institutions / [edited by R. A. W. Rhodes, S. A. Binder and B. A. Rockman]. –New York : Oxford University Press, 2008. – P. 3-20. URL: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199548460.001.0001/oxfordhb-9780199548460-e-1
7. Bechtel M., Tosun J. Changing economic openness for environmental policy convergence: when can bilateral trade agreements induce convergence of environmental regulation. *International Studies Quarterly*. – 2009. – Vol. 53. – No. 4. – P. 931-953. URL: http://mbechtel.com/wp-content/uploads/2015/12/bechtel_tosun_polcon.pdf
8. Пал Л.А. Аналіз державної політики. Основи, 1999. – 424 с. URL: http://kyiv-heritage.com/sites/default/files/%D0%9F%D0%90%D0%9B%20-%20%D0%90%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%20%D0%B4%D0%B5%D1%80%D0%B6%20%D0%BF%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B8%201999%20424%D1%81.pdf
9. Young E. and Quinn L. Writing Effective Public Policy Papers A Guide for Policy Advisers in Central and Eastern Europe. Local Government and Public Service Reform Initiative. 2002. URL:

https://www.icpolicyadvocacy.org/sites/icpa/files/downloads/writing_effective_public_policy_papers_young_quinn.pdf

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

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

12. Тертичка В. Аналіз державної політики і політологія. *Політичний менеджмент*. №6 , 2004. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/11578/01-Tartuchka.pdf?sequence=1

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

14. Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650), URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

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

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

17. Закон України «Про національну безпеку України», (Відомості Верховної Ради (ВВР), 2018, № 31, ст.24), URL: https://cutt.ly/Ct5Fcca

18. Linebarger Paul M. A. Psychological Warfare. URL: https://books.google.com.ua/books?id=bD9wCwAAQBAJ&printsec=frontcover&hl=uk&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

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

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

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

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

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

24. Alotaibi Mutlaq, Furnell Steven, Clarke Nathan L. (2016). Information security policies: A review of challenges and influencing factors. Conference: 2016

11th International Conference for Internet Technology and Secured Transactions (ICITST). URL: https://www.researchgate.net/publication/313804253_Information_security_policies_A_review_of_challenges_and_influencing_factors
DOI: 10.1109/ICITST.2016.7856729

25. Lutaaya Shafiq (2019). Information Security Policy for Ronzag. URL: https://www.researchgate.net/publication/338142467_Information_Security_Policy_for_Ronzag#fullTextFileContent

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

27. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України*. Серія: державне управління. № 3 (2019). URL: http://periodica.nadpsu.edu.ua/index.php/governance/article/view/296

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

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

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

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

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

33. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Абзац другий пункту 13. URL: https://zakon.rada.gov.ua/laws/show/537-16#top

34. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y

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

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

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

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

39. Network and Information Security: Proposal for A European Policy Approach. Brussels, 6.6.2001. URL: https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN

40. Towards a general policy on the fight against cyber crime. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560.

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

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

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

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

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

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

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

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

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

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

51. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини

України», Офіційний вісник Президента України від 09.10.2015 р., № 78, стор. 38, стаття 2592, URL: https://cutt.ly/nt5Vhe0;

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

53. Закон України «Про національну безпеку України», (Відомості Верховної Ради (ВВР), 2018, № 31, ст.24), URL: https://cutt.ly/Ct5Fcca

54. Міністерство оборони США, URL: https://cutt.ly/tysoz9N

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

56. Буга Л.В. Досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах. *Наукові записки Львівського університету бізнесу та права*. Том 19 (2018). – С. 174-178. URL: https://nzlubp.org.ua/index.php/journal/article/download/68/66/

57. Гребенюк М.В., Леонов Б.Д., Досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право*, 2018, № 2(25). – С. 45-50. URL: http://ippi.org.ua/sites/default/files/6_9.pdf

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

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

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

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

62. Kovács László. Cyber Security Policy and Strategy in the European Union and Nato, *Land Forces Academy Review*, Vol. XXIII, No 1(89), 2018 URL: https://www.researchgate.net/publication/325147671_Cyber_Security_Policy_and_Strategy_in_the_European_Union_and_Nato

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

64. State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks, URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193

65. Warsaw Summit Communiqué, URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

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

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

68. Murphy Martin (2016). Understanding Russia's Concept for Total War in Europe. The Heritage Foundation. URL: https://www.heritage.org/defense/report/understanding-russias-concept-total-war-europe

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

70. Конспірологи з QAnon разом з іншими штурмували Капітолій. Розробник ігор аналізує, як функціонує цей рух. texty.org.ua. 2021-01-26 URL: https://texty.org.ua/articles/102817/konspirolohy-z-qanon-shturmuvaly-kapitolij-rozrobnyk-ihor-analizuye-yak-vynyk-cej-ruh/

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

72. Mishara Aaron L. (2010). Klaus Conrad (1905–1961): Delusional Mood, Psychosis, and Beginning Schizophrenia. *Schizophrenia Bulletin*, Volume 36, Issue 1, January 2010, Pages 9–13. URL: https://doi.org/10.1093/schbul/sbp144

73. The New York Time, Operation InfeKtion. URL: https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html?auth=login-google1tap&fbclid=IwAR06stlwY0SEs57VlhtPhhRyBkS0SN-3rZT3OgIEliECMq-71bZBkMuAJjw&login=google1tap

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

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

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

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

78. Terrorisme : que peut la démocratie? *France Inter*. 27.03.2016 URL: https://www.franceinter.fr/emissions/agora/agora-27-mars-2016

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

80. Пуляєв П. Фейк: Украина стала центром легализации боевиков ИГИЛ. *StopFake* від 8.04.2017. URL: https://www.stopfake.org/fejk-ukraina-stala-tsentrom-legalizatsii-boevikov-igil/

81. Сошников А. Искусство фейка: как арт-центр в Донецке превратили в «базу ИГИЛ». *Русская служба Би-би-си* від 2.12.2016. URL: https://www.bbc.com/russian/features-38109630

82. Mamon Marcin. IN MIDST OF WAR, UKRAINE BECOMES GATEWAY FOR JIHAD. The Intercept. 26.02.2015. URL: https://theintercept.com/2015/02/26/midst-war-ukraine-becomes-gateway-europe-jihad/

83. Накрыт блокпост карателей под Волновахой. *Censor.net*. ФОТОфакт від 13.01.15 URL: https://censor.net.ua/photo_news/319755/nakryt_blokpost_karateleyi_pod_volnovahoyi_opolchentsy_priznalis_chto_eto_oni_unichtojili_avtobus_s

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

85. Чередніченко С. facebook.com від 19 лютого 2020 року, URL: https://www.facebook.com/permalink.php?story_fbid=2517384035203212&id=100007949194303

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

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

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

89. UkraineHistoryArchive. ГО «Український мілітарний центр». Фейки Шарія. Ч. 1 від 18.07.2019. Ч. 2 від 6.01.2020. URL: https://mil.in.ua/uk/author/ukrainehistoryarchive/

90. Україна видворила журналіста Russia Today. *LB.ua* від 25 липня 2014, URL: https://lb.ua/society/2014/07/25/274176_ukraina_vidvorila_zhurnalista_russia.html

91. Грэм Филлипс. Дебальцево. Танки российской армии Т-72Б3 [15.02.2015] URL: https://www.youtube.com/watch?v=3sRF15WFKtQ&t=12s

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

93. Vaccines and immunization: What is vaccination? URL: https://www.who.int/news-room/q-a-detail/vaccines-and-immunization-what-is-vaccination?adgroupsurvey=%7badgroupsurvey%7d&gclid=EAIaIQobChMIzpbrwfbe7wIV0e5RCh0cCw3WEAAYAiAAEgIRy_D_BwE

94. 100+ відповідей на запитання про вакцинацію проти COVID-19 для медичних працівників та пацієнтів URL: https://drive.google.com/file/d/1L0r19z2S8IW19aNp4jCE_ob4YzcDM4rx/view?fbclid=IwAR3RxZE8Fgy4-pVkTwKt6f0daX176SHsAiQhTMpeuwB83l4KNwNRu7TkeKs

95. James Gillray and the Art of Caricature, The Morgan Library & Museum James Gillray (British, 1756-1815), The cow-pock,-or-The wonderful effects of the new inoculation! - Vide - the Publications of ye Anti-Vaccine Society, 1802, URL: https://www.themorgan.org/exhibitions/gillray

96. Мілютін З., 02 березня 2020 року, URL: https://www.facebook.com/permalink.php?story_fbid=3111774268857515&id=100000749169919

97. Токсичний алюміній у вакцинах викликає аутоімунні захворювання та невропатології. [Колектив авторів]. VoxUkraine. Аналітична платформа, 14 липня 2020 URL: https://voxukraine.org/uk/fejk-toksichnij-alyuminij-u-vaktsinah-viklikaye-autoimunni-zahvoryuvannya-ta-nevropatologiyi/

98. What is an adjuvant and why is it added to a vaccine?, URL: https://www.cdc.gov/vaccinesafety/concerns/adjuvants.html

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

100. Bill & Melinda Gates Foundation, URL: https://www.gatesfoundation.org/

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

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

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

104. У Нових Санжарах перекрили дорогу і палять шини, щоб не пустити людей із Китаю. *Українська правда*. URL: https://www.pravda.com.ua/news/2020/02/20/7241079/

105. Биті вікна і барикади з вогнем: на Полтавщині відтіснили протест і завезли людей з Уханю. *Українська правда* URL: https://www.pravda.com.ua/news/2020/02/20/7241165/

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

107. McAfee Labs Threats Report November 2020. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

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

109. Шевчук О.М. Заходи адміністративного запобігання поширенню пандемії COVID-19 та права людини: досвід Великобританії. *Science and practice of today* : збірник праць міжнародної конференції, November 16–19, 2020. Ankara, 2020. 695 p. С. 325–328. URL: https://ifsk.sumdu.edu.ua/images/doc/IX-Conference-16-19-Ankara-Turkey-Book.pdf.

110. Андрощук Г. Проблеми національної безпеки в умовах COVID-19: аналіз кримінального ландшафту в ЄС. *Yurgazeta*. URL. https://yurgazeta.com/publications/practice/kriminalne-pravo-ta-proces/problemi-nacionalnoyi-bezpeki-v-umovah-covid19-analiz-kriminalnogo-landshaftuv-es-.html

111. Кланца А.І. Охорона здоров'я як структурна складова національної безпеки держави : дис. ... докт. наук з держ. управл. : 25.00.02 / Інститут підготовки кадрів державної служби зайнятості України. Київ, 2019. 571 с. URL: http://ipk.edu.ua/wp-content/uploads/2019/06/dis_ KLANTSA.pdf

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

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

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

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

116. Як бойовики погрожують бійцям АТО через СМС. *Espreso.tv*. URL: https://espreso.tv/news/2015/07/22/yak_boyovyky_pogrozhuyut_viyskoym_ato_cherez_sms

117. Виявлено витік персональних даних пацієнтів в одній із найбільших приватних клінік Дніпра. *Ua.interfax* URL: https://ua.interfax.com.ua/news/general/692350.html

118. Продукти «Лабораторії Касперського» під забороною в держагентствах США. Що цьому передувало? (розслідування). *Radiosvoboda*. URL: https://www.radiosvoboda.org/a/28864734.html

119. James Thurber. URL: https://en.wikipedia.org/wiki/James_Thurber

120. Humor is a serious thing URL: https://www.brainyquote.com/quotes/james_thurber_393634

121. StratCom laughs: in search of an analytical framework URL: https://www.stratcomcoe.org/stratcom-laughs-search-analytical-framework

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

123. Шторгін І. Якою має бути інформаційна політика України в умовах війни? *Radiosvoboda*. URL: https://www.radiosvoboda.org/a/28338927.html

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

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

126. Загибель дітей на окупованих територіях: як Росія ескалює ситуацію в інформаційному полі. URL: https://www.ukrinform.ua/rubric-presshall/3224498-zagibel-ditej-na-okupovanih-teritoriah-ak-rosia-eskalue-situaciu-v-informacijnomu-poli.html

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

128. Цибульська назвала цинічними російські заяви про «Сребреницю» на Сході України URL: https://www.ukrinform.ua/rubric-polytics/3226041-cibulska-nazvala-cinicnimi-rosijski-zaavi-pro-srebrenicu-na-shodi-ukraini.html

129. «М'яка сила» Кремля в дії: як Росія експортує свій «культурний продукт» в Україну». *Укрінформ*, 28 квітня 2021, URL: https://www.ukrinform.ua/rubric-society/3235466-maka-sila-kremla-v-dii-ak-rosia-eksportue-svij-kulturnij-produkt-v-ukrainu.html

130. Моргенштерн 16+, *Контромарка*, https://kontramarka.ua/uk/morgenstern-kiev-66102.html

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

132. Російський артист Morgenshtern під час виступу в Одесі… від 09 грудня 2019 року URL: https://afisha.24tv.ua/rosiyskiy_artist_morgenshtern_pid_chas_vistupu_v_odesi_nazvav_den_zhalobi_yonoyu_pokazuhoyu_n1245929

133. North Atlantic Treaty Organization (NATO) URL: https://www.nato.int/cps/en/natohq/index.htm

134. Strategic Communications Centre of Excellence NATO URL: https://www.stratcomcoe.org/about-us

135. Співробітництво Україна – НАТО у військовій сфері. URL: https://nato.mfa.gov.ua/ukrayina-ta-nato/spivrobitnictvo-ukrayina-nato-u-vijskovij-sferi

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

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

138. Alexander Snesar, 30 квітня 2021 року, https://www.facebook.com/teleportator.trafalgator/posts/3900430573397489

139. Фейк: Після вакцини від COVID-19 людина стає носієм інфекції, колектив авторів, 06 травня 2021 року, https://www.stopfake.org/uk/fejk-pislya-vaktsini-vid-covid-19-lyudina-staye-nosiyem-infektsiyi/

140. Myths & Facts, CDC, https://www.cdc.gov/coronavirus/2019-ncov/vaccines/facts.html

141. Вера Лёдов, «ПЕРВЫЕ РЕЗУЛЬТАТЫ ПЛАНОВОЙ ВАКЦИНАЦИИ в ИЗРАИЛЕ» 01 березня 2021 року https://www.facebook.com/groups/1100662226943371/permalink/1480564268953163/

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

143. Правда: установлено, что вакцина очень эффективна в отношении заболеваемости, тяжелого течения заболевания, госпитализаций и смертности, МОЗ Ізраїлю, 04 березня 2021 року, https://www.gov.il/ru/departments/news/fake-efficacy

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

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

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

ДОДАТКИ

Додаток А

Публічно розкриті інциденти безпеки за регіонами, 2020

Джерело: McAfee Labs Threats Report November 2020. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

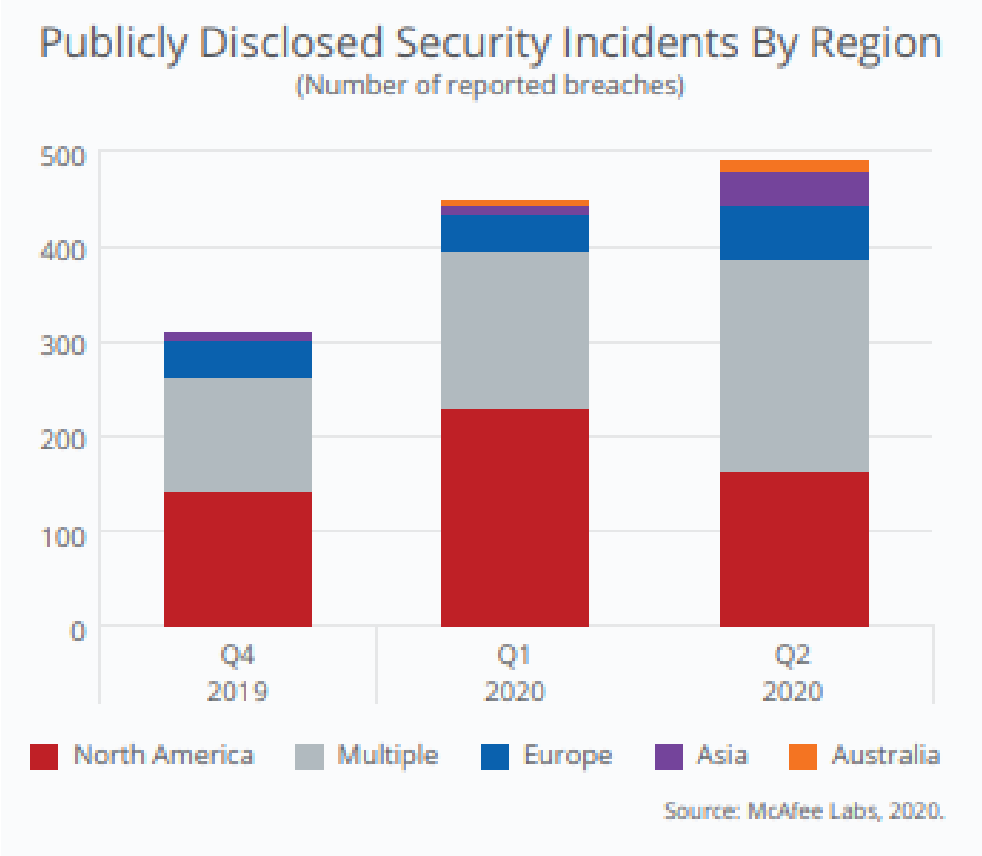


Figure 2. McAfee Labs counted 561 publicly disclosed security incidents in the second quarter of 2020, including those in which the region target was non-applicable, an increase of 22% from Q1 of 2020. Disclosed incidents targeting North America accounted for 29% of total incidents, a decrease of 30% over the previous quarter, while Europe was targeted in 10% of total incidents.

Додаток Б

Топ 10 країн з інцидентами в хмарних технологіях, 2020

Джерело: McAfee Labs Threats Report November 2020. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

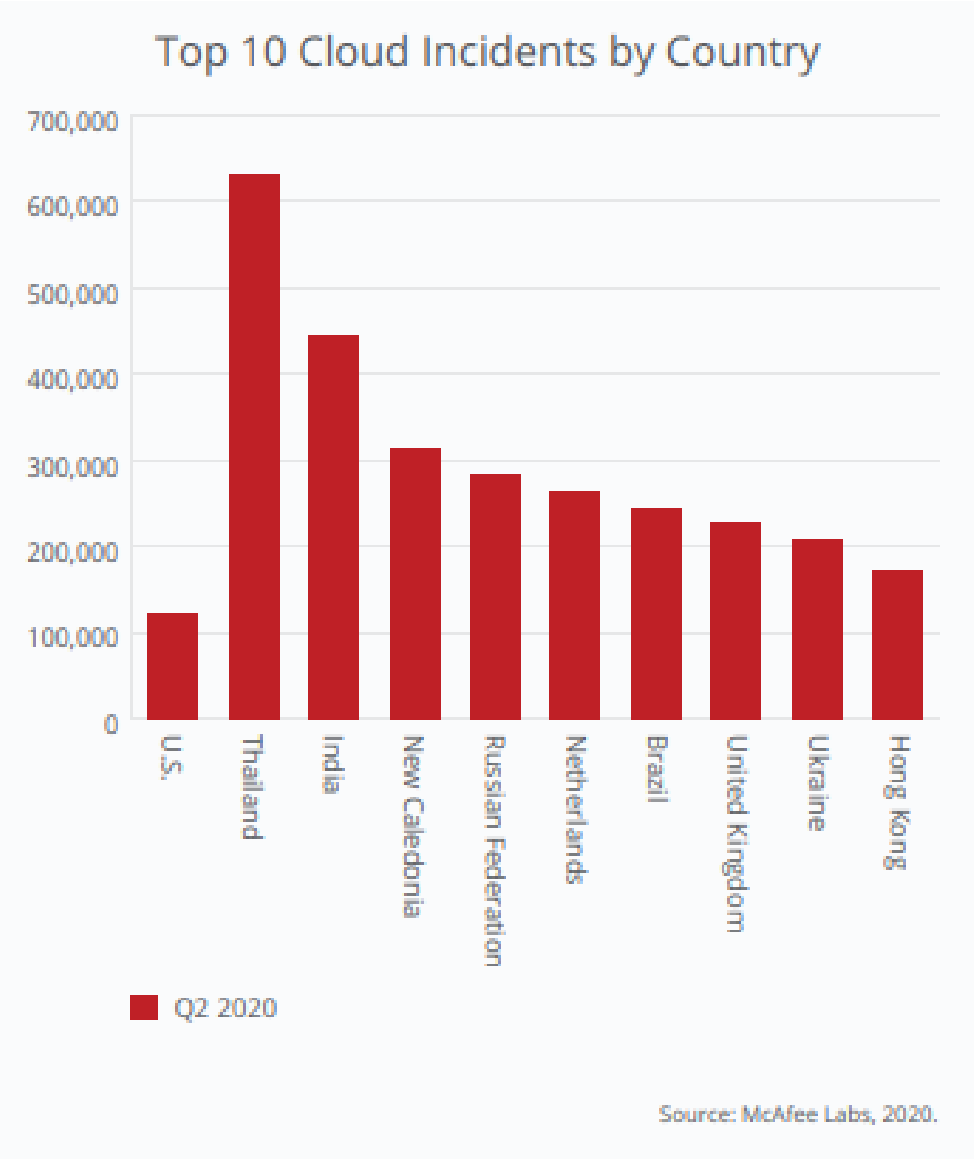


Figure 3. McAfee observed approximately 7.5 million external attacks on cloud accounts, aggregating and anonymizing cloud usage data from more than 30 million McAfee MVISION cloud users worldwide during the second quarter of 2020. This data set represents companies in all major industries across the globe, including financial services, healthcare, public sector, education, retail, technology, manufacturing, energy, utilities, legal, real estate, transportation, and business services.

Додаток В

Топ 10 цільових країн, розкриті інциденти, 2020

Джерело: McAfee Labs Threats Report November 2020. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

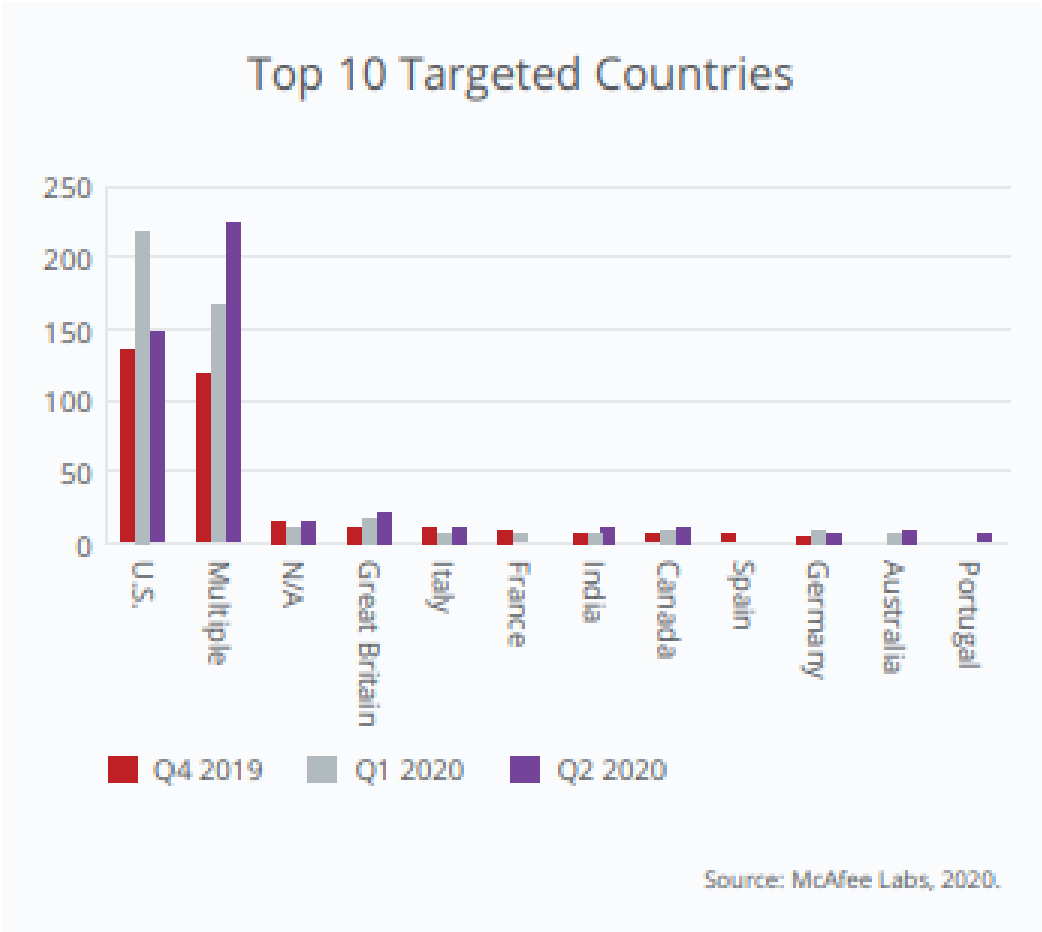


Figure 4. Disclosed incidents targeting the United States in Q2 2020 decreased 47%, Great Britain increased 29%, and Canada increased 25% over the previous quarter. Nearly 27% of all publicly disclosed security incidents took place in the U.S.

Додаток Г

БІЛА КНИГА СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ ПРОТИ УКРАЇНИ 2014 – 2018

За ред. Д. Ю. Золотухіна

Джерело: https://mip.gov.ua/files/pdf/white_book_2018_mip.pdf

Додаток Г (продовження)

Додаток Д

Об'єкти впливу, вигоди, витрати альтернатив (Аналітична записка)

Альтернатива №1

Об'єкт впливу	*Вигоди*	*Витрати*
Держава	продовження існуючої політики	політика не потребує додаткових витрат, крім тих які закладені в бюджеті, інформаційна політика призводить до додаткових побічних витрат : виплати постраждалим військовослужбовцям, втрата техніки ЗСУ
Громадські організації	відсутні	додаткові засоби захисту, дозвіл на зброю, купівля легальної зброї, лікування
Місія України при НАТО	продовження існуючої політики	не виконання плану по впровадженню стандартів НАТО та стратегічного партнерства

Альтернатива 2

Об'єкт впливу	*Вигоди*	*Витрати*
Держава	ефективне управління ЗСУ, зменшення втрат на Сході України, (людей, техніки), відокремлення від російського впливу, реформа Сектору Безпеки і Оборони України трастовий фонд НАТО 2 мільйони 90 тисяч євро	політика потребує додаткових витрат, крім тих які закладені в бюджеті, корупційна складова
Громадські організації	Захист персональних даних, безпека життя свого та своїх рідних та близьких	Час та громадський контроль по впровадженню інформаційних систем, виявлення корупційної складової

Місія України при НАТО	виконання плану-заходу реалізація політики “курс на НАТО”, імплементація стандартів	Людський та робочий ресурс, час на впровадження та контроль виконання , політика не потребує додаткових витрат, крім тих які закладені в бюджеті

Альтернатива 3

Об'єкт впливу	*Вигоди*	*Витрати*
Держава	ефективне управління ЗСУ, зменшення втрат на Сході України, (людей, техніки), відокремлення від російського впливу, реформа Сектору Безпеки і Оборони України, робочі місця	політика потребує більш додаткових витрат, крім тих які закладені в бюджеті, корупційна складова, довгострокове впровадження, людський ресурс, можливий негативний результат політики без допомоги міжнародних організацій.
Громадські організації	Захист персональних даних,безпека життя свого та своїх рідних та близьких	Час та громадський контроль по впровадженню інформаційних систем, виявлення корупційної складової
Місія України при НАТО	унікальність продукту, немає контролю з боку виконання політики	ризик невідповідності стандартам НАТО, довготривалий процес, залучення великої кількості людського ресурсу,