МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, професор	доктор економічних наук, професор
_____ С.В. Легомінова	_____ С.В. Легомінова
«___»_____2022 р.	«___»_____2022р.

КВАЛІФІКАЦІЙНА РОБОТА

другого магістерського рівня вищої освіти

на тему:

ЗАСАДИ ПРОТИДІЇ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ В УКРАЇНІ

СТУДЕНТ: Баленко Ольга Анатоліївна _____

(підпис)

КЕРІВНИК: к.держ.упр., доц. Мужанова Тетяна Михайлівна _____

(підпис)

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Миколайович _____

(підпис)

Київ – 2022

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність 125 Кібербезпека
Спеціалізація Управління інформаційною та кібернетичною безпекою
Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 2022 р.

ЗАВДАННЯ
на кваліфікаційну роботу

студенту Баленко Ользі Анатоліївні

Тема роботи: «ЗАСАДИ ПРОТИДІЇ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ В УКРАЇНІ», затверджена наказом по університету № 122 від «12» жовтня 2022 р.

1. **Термін здачі** студентом оформленої роботи «24» грудня 2022 р.

2. **Об'єкт дослідження:** спеціальні інформаційні операції.

3. **Предмет дослідження:** засади протидії спеціальним інформаційним операціям в Україні.

4. **Мета дослідження** полягає у вивченні засад протидії спеціальним інформаційним операціям в Україні.

5. **Перелік питань, які мають бути розроблені:**

5.1 Дослідити теоретико-методологічні основи проведення спеціальних інформаційних операцій.

5.2 Проаналізувати досвід реалізації спеціальних інформаційних операцій в Україні.

5.3 Вивчити засади протидії спеціальним інформаційним операціям в Україні, розробити рекомендації щодо їх удосконалення.

6. **Дата видачі завдання «**15» вересня 2022 р.

Науковий керівник _____ Т.М. Мужанова
Підпис

Завдання прийнято до виконання _____ О.А. Баленко
Підпис

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «15» вересня 2022 р.

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	23.09.2022	
2.	Збір та аналіз літератури.	30.09.2022	
3.	Дослідження теоретико-методологічних основ проведення спеціальних інформаційних операцій	17.10.2022	
4.	Аналіз досвіду реалізації спеціальних інформаційних операцій в Україні	01.11.2022	
5.	Вивчення засад протидії спеціальним інформаційним операціям в Україні, розробка рекомендацій щодо їх удосконалення	15.11.2022	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2022	
7.	Оформлення роботи.	04.12.2022	
8.	Оформлення презентації.	21.12.2022	
9.	Отримання рецензії на роботу.	24.12.2022	
10.	Захист в ДЕК.	17.01.2023	

Студент О.А. Баленко

(підпис)

Науковий керівник Т.М. Мужанова

(підпис)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню засад протидії спеціальним інформаційним операціям в Україні та розробці рекомендацій щодо їх удосконалення. Робота складається зі вступу, трьох розділів, що містять 6 рисунків, висновків та списку використаних джерел, що містить 60 найменувань. Загальний обсяг роботи становить 80 аркушів, з яких 6 аркушів займає список використаних джерел.

Об'єктом дослідження є спеціальні інформаційні операції.

Предметом дослідження є засади протидії спеціальним інформаційним операціям в Україні.

Метою роботи є вивчення засад протидії спеціальним інформаційним операціям в Україні та розробка рекомендацій щодо їх удосконалення.

Для цього у роботі використовуються методи класифікації, порівняння, узагальнення, системного аналізу, комплексного і процесного підходів, теорії управління та інформаційної безпеки.

Як результат у роботі досліджено теоретико-методичні основи проведення спеціальних інформаційних операцій; проаналізовано досвід реалізації спеціальних інформаційних операцій в Україні; вивчено засади протидії спеціальним інформаційним операціям в Україні та розроблено рекомендації щодо їх удосконалення.

Галузь застосування. Розглянуті підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства, зокрема при використанні процесного підходу та моделі ПВПД.

Ключові слова: СПЕЦІАЛЬНА ІНФОРМАЦІЙНА ОПЕРАЦІЯ, СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ В УКРАЇНІ, ПРОТИДІЯ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ В УКРАЇНІ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АІВ	акція інформаційного впливу
ГО	громадська організація
ЗІБ	забезпечення інформаційної безпеки
ЗМІ	засоби масової інформації
ІБ	інформаційна безпека
ІВ	інформаційна війна
ІДІЛ	Ісламська держава Іраку та Леванту
ІП	інформаційне протиборство
ІПсВ	інформаційно-психологічний вплив
МКІП	Міністерство культури та інформаційної політики України
ПсО	психологічна операція
СІО	спеціальна інформаційна операція

ВСТУП

Актуальність теми. Досвід вирішення військових конфліктів останніх десятиліть свідчить про те, що суперництво в інформаційній сфері стає їх невід'ємною частиною. Більше того, від ефективності інформаційної боротьби в загрозливий період (від етапу зародження конфлікту до етапу кризи) у значній мірі залежить успішне вирішення конфлікту загалом.

Сьогодні Україна перебуває у стані збройного конфлікту і змушена вступати в інформаційне протиборство з державою-агресором, проводити й реагувати на спеціальні інформаційні операції противника. Незважаючи на досить успішні зусилля української сторони щодо протидії негативному інформаційному впливу, методи протидії спеціальним інформаційним операціям, а також заходи щодо покращення обізнаності громадян з цих питань потребують удосконалення. З огляду на зазначене дослідження засад протидії спеціальним інформаційним операціям в Україні та розробка рекомендацій щодо їх удосконалення є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає у вивченні засад протидії спеціальним інформаційним операціям в Україні та розробці рекомендацій щодо їх удосконалення.

Для досягнення цієї мети в роботі необхідно виконати такі **завдання**:

1. Дослідити теоретико-методологічні основи проведення спеціальних інформаційних операцій.

2. Проаналізувати досвід реалізації спеціальних інформаційних операцій в Україні.

3. Вивчити засади протидії спеціальним інформаційним операціям в Україні, розробити рекомендації щодо їх удосконалення.

Об’єкт дослідження - спеціальні інформаційні операції.

Предмет дослідження – засади протидії спеціальним інформаційним операціям в Україні.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, ситуаційного та процесного підходів, теорії управління та інформаційної безпеки.

Наукова новизна одержаних результатів. У результаті аналізу сценаріїв проведення СІО РФ в Україні виділено перелік цілей деструктивного інформаційно-психологічного впливу держави-агресора. На основі дослідження сформовані рекомендації щодо вдосконалення нормативно-правової бази України у сфері інформаційної безпеки, а також представлена методика виявлення СІО для використання у діяльності органів державної влади.

Практичне значення одержаних результатів. Застосування напрацювань сприятиме вдосконаленню вітчизняної практики нормативно-правового та інституційного забезпечення інформаційної безпеки, а засад планування й реалізації СІО відповідними органами державної влади.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

1.1 Спеціальна інформаційна операція: поняття й етапи

У сучасних умовах прискореного розвитку інформаційного суспільства, цифровізації усіх сфер життєдіяльності суспільства інформація стає найважливішим і найбільш цінним ресурсом, а встановлення контролю над її виробництвом і обігом в інформаційному просторі є метою запеклої боротьби між різними політичними й економічними суб'єктами – інформаційного протиборства (далі - ІП).

ІП (у широкому розумінні) – це форма боротьби, що становить сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) методів, способів і засобів вигідного впливу на інформаційну сферу об'єкта зацікавленості та захисту власної інформаційної сфери в інтересах досягнення поставлених цілей.

ІП (у вузькому розумінні – у військовій, оборонній сферах) – це комплекс заходів інформаційного характеру, здійснюваних з метою захоплення й утримання стратегічної ініціативи, досягнення інформаційної переваги над противником і створення сприятливого пропагандистського підґрунтя при підготовці й веденні бойової й іншої діяльності збройних сил [29].

Формами ведення ІП є інформаційні війни (далі - ІВ), спеціальні інформаційні операції (далі - СІО) та акції інформаційного впливу (далі - АІВ).

Розглянемо сутність та співвідношення цих понять (Рис. 1.1).

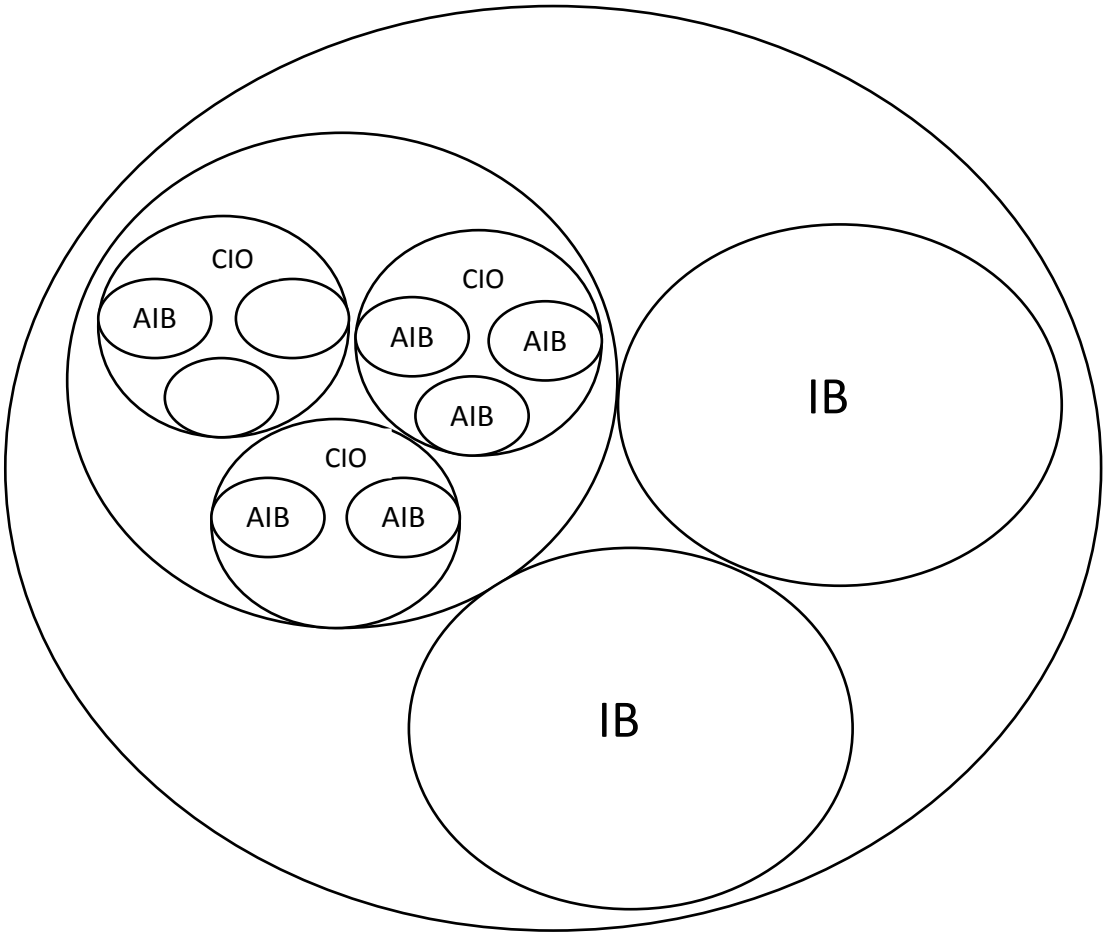

Рис. 1.1 Співвідношення понять ІВ, СІО та АІВ

Варто відзначити, що ІВ, зазвичай, складається із багатьох СІО, а СІО, в свою чергу, з низки АІВ. Однак, можливим є проведення окремих СІО, які не є елементами більш масштабного і довготривалого протистояння в інформаційному просторі. Так само, як і АІВ можуть бути одиничними і спрямованими на досягнення конкретних короткострокових інформаційних цілей.

ІВ – форма ведення ІП між різними суб’єктами (державами, неурядовими, економічними або іншими структурами), що передбачає здійснення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони й захисту власної інформаційної безпеки (далі - ІБ).

СІО є основою ведення ІВ, вони є самостійним видом оперативного забезпечення, який реалізує на полі бою концепцію ІВ.

Варто відзначити, що в науковій літературі присвячено багато уваги дослідженню сутності поняття СІО, водночас єдиного підходу ще не вироблено. Наведемо декілька визначень від різних авторів.

СІО – дії, що вживаються для досягнення інформаційної переваги в забезпеченні національної військової стратегії шляхом впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації, інформаційних систем та інфраструктури.

СІО – це комплекс взаємопов'язаних за метою, місцем і часом заходів і акцій, спрямованих на ініціалізацію і управління процесами маніпулювання інформацією, з метою досягнення і утримання інформаційної переваги шляхом впливу на інформаційні процеси в інформаційних системах супротивника. При цьому інформаційні системи розглядаються в широкому сенсі, тобто, не тільки автоматичні і автоматизовані технічні системи, але і держава, суспільство, які теж розглядаються як інформаційні системи.

СІО – дії, що вживаються з метою вплинути на інформацію та інформаційні системи супротивника і захистити свої власні інформацію та інформаційні системи [1].

Але, не дивлячись на велику кількість можливих визначень, що, часто, описують лише один аспект природи поняття СІО, найбільш повним і досконалим, на нашу думку, є таке визначення:

СІО – це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію з метою схилення до прийняття управлінських рішень або (та) вчинення дій, вигідних для суб’єкта інформаційного впливу. СІО можуть передбачати також вплив на інформаційно-технічну інфраструктуру, але для більш ефективного впливу на свідомість і поведінку людей [2].

АІВ – одноразова акція інформаційно-психологічного та інформаційно-технічного впливу, яка передбачає спланований вплив на свідомість і поведінку людей шляхом поширення упередженої, неповної чи недостовірної інформації та (або) інформаційно-технічну інфраструктуру об’єкта (об’єктів) [3].

Мета СІО – досягнення інформаційної переваги над противником.

Інформаційна перевага – здатність збирати, обробляти і розподіляти безперервний потік інформації про ситуацію, перешкоджаючи противнику робити те ж саме. Інформаційна перевага також може бути визначена і через показники динаміки обробки інформації.

Інформаційна перевага – здатність забезпечувати такий темп проведення операції, який перевершує будь-який можливий темп противника, дозволяючи домінувати протягом її проведення, залишаючись непередбачуваним і діяти, випереджаючи противника в його діях у відповідь [1].

СІО здійснюються в кілька етапів і можуть бути довгостроковими (більше місяця), середньостроковими (два-чотири тижні) й короткостроковими (один-два тижні). АІВ тривають один-три дні. Слід зауважити, що СІО складається з поєднаних між собою часом, метою, завданнями, силами й засобами проведення АІВ.

Перед здійсненням СІО може відбутися низка АІВ для «розігріву» цільової аудиторії, крім випадків, коли потрібен фактор несподіваності. Як правило, СІО проводяться від двох тижнів до місяця, оскільки цього часу достатньо для ефективної обробки цільової аудиторії. Водночас тривале поширення негативної інформації притупляє сприйняття її людською психікою, що призводить до зниження ефективності СІО. До того ж значна тривалість СІО зумовлює її ґрунтовну підготовку, а також потребу в додаткових силах, засобах і фінансах.

Підготовка СІО передбачає планування операції, визначення форм та способів її здійснення, цілей, завдань, сил і засобів, прийомів та методів впливу, цільової аудиторії. У екстрених випадках підготовка до СІО може проходити в стислі терміни.

СІО здійснюються за приблизно однаковою схемою (Рис. 1.2):

1. Інформаційний етап передбачає створення інформаційного приводу – конкретної або вигаданої події, яка використовується в СІО.

2. «Розкручування» інформаційного приводу забезпечує поступове зростання напруження (кількості повідомлень і їх сенсаційності, тенденційності, емоційності та, як правило, недостовірності).

3. Загострення напруження є основною частиною СІО, що полягає у використанні інформаційного приводу для досягнення цілей операції.

4. Вихід із операції або етап закріплення – забезпечення плавного завершення СІО після досягнення поставленої мети. Якщо мету не досягнуто, як правило, готується нова СІО.

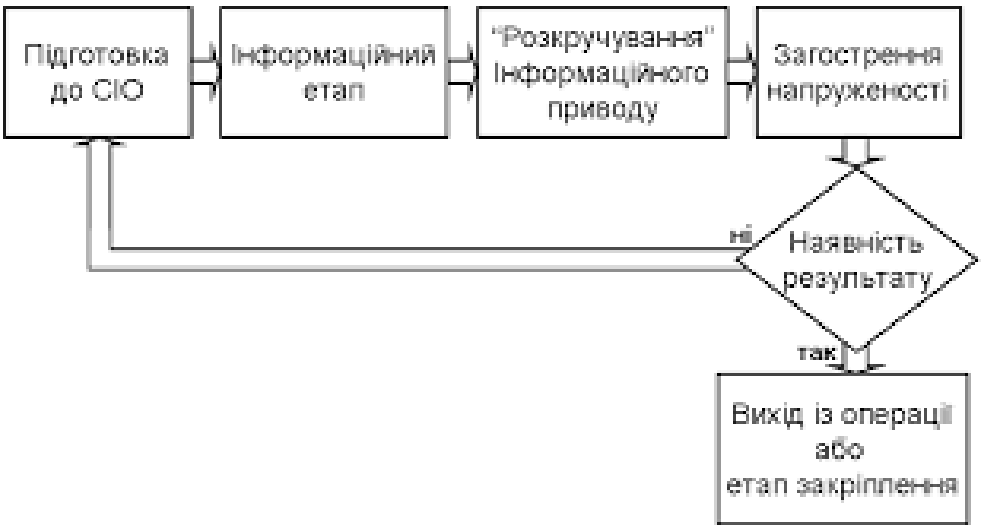

Рис. 1.2 Етапи СІО

Слід виокремити основні ознаки проведення СІО:

1. Збільшення кількості повідомлень негативного змісту з певної соціально-політичної або (та) економічної тематики.

2. Зростання емоційності.

3. Зростання тенденційності.

4. Збільшення сенсаційності.

5. Лавиноподібність (на першому етапі – поступове, на другому – значне, на третьому – різке зростання напруження).

6. Взаємоузгодження дій суб’єктів проведення СІО.

7. Час проведення (від одного тижня до двох місяців, але переважно від двох тижнів до місяця).

Необхідно визначити суб’єктів проведення СІО:

1. Керівництво іноземної держави – головний суб’єкт, всі інші – виконавці.

2. ЗМІ (іноземні та підконтрольні вітчизняні).

3. Неурядові організації (іноземні й підконтрольні вітчизняні).

4. Спецслужби іноземної держави.

5. Інтернет-ресурси.

6. Агентура впливу іноземних держав і підконтрольні лобістські структури із представників влади, управління, місцевого самоврядування, політичних партій, громадських і релігійних організацій, відомих діячів культури.

Представники військової науки не використовують термін «спеціальна інформаційна операція», а послуговуються поняттям «інформаційно-психологічна операція» або «психологічна операція» (ПсО). Причому СІО називають довгостроковими та середньостроковими ПсО, а АІВ – короткостроковими ПсО. У зв’язку із синонімічністю цих понять термін «психологічна операція» можна використовувати для опису цих операцій і акцій у військовий час.

СІО та АІВ передбачають досягнення таких цілей:

1. У мирний час: домінування в інформаційному просторі, вплив на соціально-політичну ситуацію в регіоні, формування власного позитивного іміджу.

2. У воєнний час: інформаційно-психологічне забезпечення діяльності вищого військово-політичного керівництва.

3. У післявоєнний час: забезпечення процесу формування лояльної влади, сприяння соціально-економічному розвитку в регіоні, впровадження програм гуманітарної допомоги.

СІО та АІВ поділяють залежно від спрямованості на такі види:

- проти суб’єктів, які ухвалюють рішення;
- компрометуючі та такі, що завдають шкоди опонентам;
- дестабілізуючі політичну (економічну) ситуацію.

СІО й АІВ замовляє, як правило, керівництво іноземних держав, але можуть організовувати і транснаціональні структури, й навіть приватні особи зі світовим рівнем авторитету та капіталу.

СІО й АІВ спрямовані на ідеологічний, ідейно-політичний і соціальний вплив на особу, групу осіб чи суспільство загалом із метою їх переорієнтації на інші цінності й ідеали; а також можуть використовуватися для підштовхування до вчинення протиправних дій із підриву державного й суспільно-політичного устрою.

1.2 Основні методи СІО та АІВ

У ході проведення СІО та АІВ використовують різноманітні методи інформаційно-психологічного впливу. До основних методів СІО та АІВ відносять дезінформування; пропаганду; диверсифікацію громадської думки; психологічний тиск і поширення чуток (Рис. 1.3).

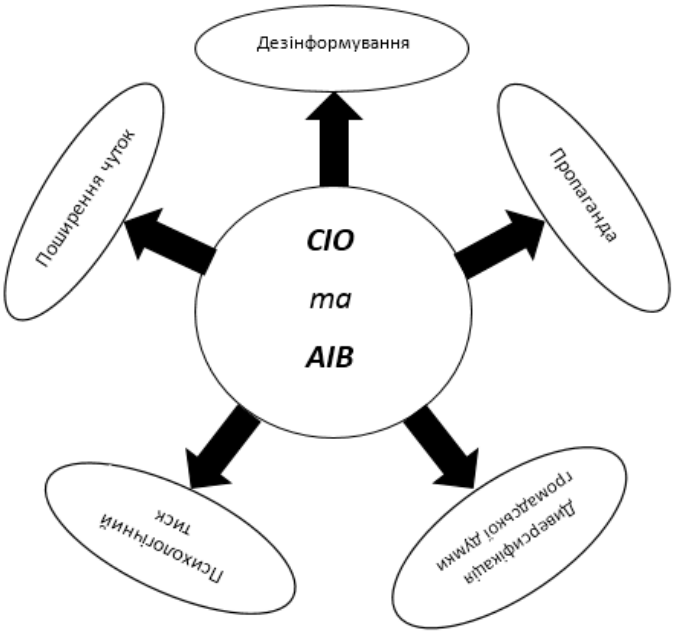

Рис. 1.3 Методи СІО та АІВ

Розглянемо детальніше сутність цих методів.

Дезінформування – це метод, який передбачає обман чи уведення об’єкта впливу в оману щодо справжності намірів для спонукання його до запрограмованих дій.

Найчастіше у світовій практиці застосовуються такі форми дезінформування:

- тенденційне викладення фактів – полягає в упередженому висвітленні фактів чи іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних. Як правило, використовуючи цей метод, об’єкту впливу доводять дозовано, із постійним зростанням напруження, спеціально сформовану інформацію. Такий напружений стан об’єкта підтримується шляхом постійного «підкидання» нових порцій суворо обмежених і дозованих даних у середовище інформаційного дефіциту;
- дезінформування «від зворотного» – відбувається шляхом подання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об’єктом впливу як неправдиві. Внаслідок застосування подібних заходів виникає ситуація, коли об’єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно та неготовий протистояти негативному впливу;
- термінологічне «мінування» – полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативно-прикладного характеру;
- «сіре» дезінформування – передбачає використання синтезу правдивої інформації з дезінформацією;
- «чорне» дезінформування – означає застосування переважно неправдивої інформації [2, с. 50].

У загальному вигляді акції дезінформування можуть проводитися шляхом створення видимості випадкового витоку закритої інформації, успіхів розвідки іноземних партнерів, використання засобів масової інформації (власні інформаційні агентства, теле-, радіокомпанії, друковані видання, «кишенькові» журналісти й т. ін.).

Пропаганда – поширення політичних, філософських, наукових, художніх, інших мистецьких ідей із метою їх упровадження в громадську думку та активізації використання цих ідей у масовій практичній діяльності населення. Водночас до пропаганди належать повідомлення, які поширюються для здійснення вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення чи поводження певної групи людей у напрямі, безпосередньо чи опосередковано вигідному організаторам.

Форми проведення пропаганди:

- пропаганда способу життя (соціологічна) – натуральний показ досягнень, переваг, перспектив конкретної держави тощо;
- формулювання та створення нових ідей;
- коригування наявних думок.

Пропаганда також поділяється залежно від мети на позитивну й негативну.

Мета позитивної пропаганди – сприяти соціальній гармонії, злагоді, вихованню людей у дусі загальноприйнятих цінностей. Позитивна пропаганда виконує виховну та інформаційну функції в суспільстві. Вона здійснюється на користь тих, кому адресована, а не обмеженого кола зацікавлених осіб; не допускає обману та приховування фактів. У цьому її відмінність від негативної. Позитивна пропаганда не містить маніпулятивної мети, тому використовується не для проведення СІО та АІВ, а для захисту населення від них.

Завдання негативної пропаганди – нав’язати людям певні переконання за принципом «мета виправдовує засоби». Мета негативної пропаганди – розпалювання соціальної ворожнечі, ескалація соціальних конфліктів, загострення суперечностей у суспільстві, пробудження похітливих інстинктів у людей тощо. Це дає змогу роз’єднувати людей, робити їх слухняними щодо волі пропагандиста. Технологія створення «образу ворога» дає можливість згуртувати натовп навколо пропагандиста, нав’язати людям потрібні переконання та стереотипи. Основна функція негативної пропаганди – створення ілюзорної, паралельної реальності з «хибною» системою цінностей,

переконань, поглядів. При цьому активно використовується низька критичність та навіюваність мас із метою маніпулювання останніми на користь обмеженої групи осіб.

Диверсифікація громадської думки – це розпорошення уваги панівної еліти держави на різні штучно акцентовані проблеми й відволікання цим від вирішення нагальних завдань суспільно-політичного та економічного розвитку для нормального функціонування суспільства й країни.

Форми диверсифікації громадської думки:

- дестабілізація обстановки в державі чи окремих її регіонах;
- активізація кампаній проти політичного курсу панівної еліти та окремих її лідерів різними міжнародними установами;
- ініціювання антидемпінгових кампаній й іншого роду скандальних судових процесів, застосування міжнародних санкцій з інших причин.

Психологічний тиск – це вплив на психіку людини шляхом залякування, погроз із метою її спонукання до запланованої моделі поведінки.

Форми психологічного тиску:

- доведення до об’єкта впливу відомостей про реальні чи неіснуючі загрози та небезпеки;
- прогнози щодо репресій, переслідувань, убивств тощо;
- шантажування;
- здійснення вибухів, підпалів, масових отруєнь, захоплень заручників, інших терористичних акцій.

Поширення чуток – це діяльність щодо поширення різної інформації (переважно неправдивої) серед широких верств населення здебільшого неофіційними каналами з метою дезорганізації суспільства та держави або їхніх установ чи організацій.

За одним із визначень, чутки – це циркулююча форма комунікації, за допомогою якої люди, котрі перебувають у неоднозначній ситуації, об’єднуються, утворюючи зрозумілу їм інтерпретацію цієї ситуації, спільно використовуючи при цьому власні інтелектуальні можливості.

Чутки можна класифікувати за трьома параметрами: експресивними (емоційні стани, виражені в змісті чутки, і відповідні типи емоційних реакцій), інформаційними (ступінь достовірності сюжету чутки) та за ступенем впливу на психіку людей.

За експресивною характеристикою визначають чутки-бажання, чутки-залякування й роз'єднувальні агресивні чутки.

1. Чутки-бажання. Інформація поширюється з метою викликати розчарування з приводу нездійснених очікувань і деморалізацію об'єкта впливу.

2. Чутки-залякування. При їх поширенні в особи ініціюється стан тривоги, непевності. Це можуть бути чутки про смертельну суперзброю, якою володіє противник (сторона, що поширює чутки), про нестачу продовольства, зараження місцевості, питної води тощо.

3. Роз'єднувальні агресивні чутки. Поширювана інформація має на меті внести розлад у суспільство, порушити соціальні зв'язки.

За інформаційною характеристикою чутки поділяються на абсолютно недостовірні, недостовірні, недостовірні з елементами правдоподібності та правдоподібні.

Самопоширювані чутки. Їхня природа базується на інформації, яку важко втримати. Особа обов'язково має розповісти про почуте комусь іншому. Достатньо створити відповідну чутку та запустити її в обіг у потрібному місці в слушний час. «Людський поголос» зробить решту. Позитивний чинник використання цієї форми СІО полягає ще й у тому, що практично немає ефективних засобів протидії чуткам.

На офіційному рівні зупинити чутки неможливо: офіційні заходи протидії викликають прямо протилежний ефект: для людей, яких безпосередньо цікавлять чутки, це є підтвердженням правдивості останніх. Чим численніші намагання їх спростувати, тим більша упевненість у їхній достовірності. Єдиний можливий спосіб подолання ефективності чуток – цілковите їх ігнорування. Як правило, через деякий час напруження спадає, зайва активність

в обговоренні уже неактуальних новин згасає, інтерес до порушеної в чутках проблеми зникає. Поява нових проблем повністю нейтралізує можливі небезпечні наслідки дезорганізації суспільства та держави.

СІО становлять комплекс заходів інформаційно-психологічного характеру, що здійснюються за єдиним планом із метою порушення системи державного та військового управління, впливу на морально-психологічний стан військово-політичного керівництва, населення й особового складу військ визначеного об’єкта, запобігання інформаційному та психологічному впливу на власні сили й засоби.

СІО та АІВ належать до специфічних форм і методів впливу, ефективне використання яких потребує відповідної підготовки та високої майстерності, ґрунтовних наукових розробок і постійного практичного вдосконалення. Для організації та ведення СІО й АІВ використовуються традиційні канали ІПсВ – теле-, радіопропаганда, поліграфічні засоби, усне мовлення, наочна агітація, робота з місцевим населенням; нові способи – супутникові, оптоволоконні системи, телекомунікаційні засоби, інтернет; нетрадиційні форми впливу – нейролінгвістика, парапсихологія, психотропні засоби, інфразвук, 25-й кадр, тобто такі, що застосовуються для здійснення впливу на підсвідомість.

Сучасна розвинена держава спроможна за допомогою СІО та АІВ отримати певну перевагу над противником ще до застосування традиційних бойових засобів. За оцінками фахівців, СІО якісно змінюють характер бойових дій, про що наочно свідчать останні локальні конфлікти та війни: перемагає той, хто здобув інформаційну перевагу.

Здійснення СІО й захист від них є невід’ємною передумовою забезпечення національної безпеки держави, вони проводяться як за мирного часу, так і у воєнний період. Основні аспекти СІО – психологічний, культурний, інтелектуальний, технологічний та економічний.

Концепції національної безпеки багатьох провідних країн світу визначають основні напрями застосування збройних сил у XXI столітті. Підкреслюється, що головною рисою нового століття буде перенесення

акцентів у галузь інформаційного протиборства, а досягнення інформаційної переваги стане обов’язковою умовою перемоги над будь-яким противником [2].

1.3 Особливості СІО в мережі Інтернет

В умовах широкого розповсюдження ЗМІ нового типу – сайтів, форумів, блогів, соціальних мереж тощо – основна боротьба за право адекватного відображення дійсності переходить в Інтернет. Нові форми подання та поширення інформації створюються майже в режимі реального часу, і в їх «розкручування» вкладаються значні кошти. Якщо в минулому столітті при збройній агресії ступінь охоплення аудиторії країни з метою перепрограмування був серед малозначущих параметрів, то сьогодні, після впровадження в промислово розвинених країнах демократичної форми правління, підвищення рівня охоплення – це значимий параметр за умови грамотного оформлення пропонованого матеріалу.

Будь-яка війна починається з певної послідовності дій з боку супротивника. Дії, будучи для будь-якого зовнішнього спостерігача подіями, знаходять відображення в новинах, які здобуваються як з відкритих джерел інформації, так і за допомогою спеціальних технічних засобів і технологій.

У рамках протиборства в інформаційному просторі без переходу до гарячої фази конфліктуючими сторонами можуть вирішуватися такі два класи завдань (Рис. 1.4):

1. Виявлення загроз. Фільтрація і аналіз вмісту заданої множини сайтів, інтегрування результатів і розробка управлінської стратегії.

2. Проведення СІО.

СІО в мережі Інтернет, включають в себе:

- знищення реальних об'єктів і інфраструктури, наприклад, за допомогою комп'ютерних вірусів і закладок;
- знищення, блокування, дискредитація Інтернет-ресурсів;

- створення, розкручування, рекламування, нав'язування Інтернет-ресурсів.

Рис. 1.4 Завдання інформаційного протиборства в мережі Інтернет

Під терміном «розкручування» (просування) ресурсу розуміється комплекс заходів, спрямованих на підтримку і зростання позицій ресурсу в пошукових системах мережі Інтернет, збільшення цільової відвідуваності ресурсу, створення сприятливого іміджу і впізнаваності в Інтернеті. Розкрутка ресурсу стає можливою завдяки наявності в Інтернет таких сервісів, як пошукові системи, якими регулярно користуються практично всі відвідувачі мережі. Пошукові системи збирають дані за ключовими словами і словосполученням разом з посиланнями на ресурси, де ці ключові слова знаходяться. Обсяг видачі пошукової системи в залежності від запиту користувача може змінюватися в дуже широких межах, як повна відсутність видачі, так і тисячі посилань, які неможливо переглянути в розумний час. Вважається, що ресурс добре розкручений, якщо за основними термінами, що відображають суть даного ресурсу, пошукові системи поміщають посилання в Топ-10 знайдених посилань.

- зниження рівня напруженості в заданому регіоні або підвищення рівня напруженості в заданому регіоні.

- формування громадської думки на заданих інтернет-ресурсах. Зокрема, підготовка громадської думки для прийняття противником законодавчих актів збиткового для противника характеру.
- формування іміджу (позитивного або негативного) за допомогою цілеспрямованої комунікаційної політики. Зокрема, підвищення або зниження статусу певної країни, організації, людини та інше.

Для підготовки відповідних керуючих впливів здійснюється створення мультимедійного контенту за заданою проблематикою і доставка цього контенту до об'єкта впливу. Основними принципами виконання цих дій є:

- підготовка мультимедійного контенту в режимі «реального часу» на базі наявних типових заготовок;
- контент може мати текстову, відео- і аудіо- форму.

При підготовці мультимедійного контенту необхідно дотримуватися таких вимог:

- формування текстових матеріалів в заданому стилі, за зразком текстів конкретного автора;
- формування аудіо-матеріалів на заданому аудіо-фоні (шум моря, аеропорт, вулиця, приміщення з людьми, приміщення без людей і т.п.);
- формування аудіо-матеріалів з заданими базовими голосовими характеристиками (чоловічий голос, жіночий голос, голос молодої людини, голос людини середнього віку, голос літньої людини) на основі вихідного аудіо-матеріалу;
- формування аудіо-матеріалів з заданими голосовими характеристиками конкретної людини на основі вихідного аудіо-матеріалу;
- формування відеоматеріалу на заданому відео-фонів (вулиці конкретних міст в різний час доби, різні приміщення: музеї, театри, диппредставництва тощо);
- формування відеоматеріалів з заданими базовими відео-характеристиками для головних дійових осіб (стать, вік, національність);

- формування відеоматеріалів з відео-характеристиками, що дозволяють глядачам впізнати в дійових особах конкретних людей.

У більшості випадків, говорячи про СІО в мережі Інтернет, мають на увазі проведення спеціальних дій в умовах анонімності. Суб'єкт, який ініціює СІО, так і той, що її здійснює, виступає як актор (лат. Actor – діяч) – індивід, громадська група, інститут або інший суб'єкт, який здійснює конкретні дії; сторона, що бере участь в конфлікті.

Таким чином, в рамках рольових концепцій результат СІО є результатом реалізації різних ролей задіяних акторів. Виконавцями дій є не тільки люди, здатністю до виконання цілеспрямованої дії наділені і віртуальні суб'єкти, наприклад, програмні роботи та боти і навіть віруси. У програмуванні актор – програмна сутність заданої структури і механізмів взаємодії; містить дані і процедури і може породжувати повідомлення. Актори так само, як в театрі, «грають ролі» на інформаційній арені (сцені) Інтернету за сценаріями або спонтанно. Їх поділяють на акторів технічної і гуманітарної сфери (Рис. 1.5).

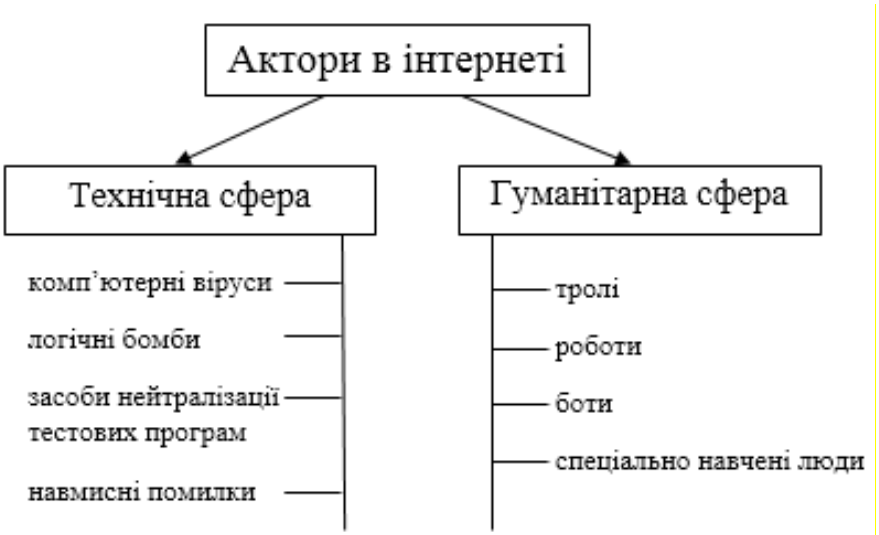

Рис. 1.5 Актори технічної і гуманітарної сфери в Інтернеті

Досягнення інформаційної переваги шляхом знищення, перекручення або розкрадання інформаційних масивів, подолання систем захисту, забезпечення допуску незаконних користувачів, дезорганізації роботи технічних засобів і комп'ютерних систем орієнтується на високоточні і максимально приховані,

анонімні способи впливу масштабного руйнування. Акторами технічної групи, що може займатися такими діями, виступають:

- комп'ютерні віруси, здатні впроваджуватися в програмне забезпечення інформаційних систем, розмножуватися, передаючись по лініях зв'язку, мереж передачі даних, виводити з ладу системи управління і тому подібне;
- логічні бомби – програмні закладки, які завчасно впроваджують в інформаційно-керуючі частини системи, щоб по команді або в призначений час привести їх в дію;
- засоби нейтралізації тестових програм;
- навмисні помилки, що вводяться противником в програмне забезпечення об'єкта впливу.

Таким чином, актори технічної сфери, представляють собою інформаційну зброю на основі програмного коду, «відповідальні» за проведення наступних спеціальних дій в ході здійснення інформаційних операцій в телекомунікаційному середовищі:

- проникнення в інформаційну систему противника;
- подолання систем захисту;
- власне маскування і анонімність;
- збір даних, що циркулюють в інформаційній системі противника;
- доставка і впровадження певних команд або інформаційних матеріалів в конкретне місце інформаційної системи (інтернет-ресурсу);
- створення або модифікація віртуальної реальності (імітація голосів, створення відео-зображень конкретних людей і т.п.);
- модифікація інформації, що зберігається в базах даних інформаційних систем противника або відображається на його інтернет-ресурсах;
- прихована зміна алгоритму функціонування програмного забезпечення в заданий момент часу або при настанні певної події в системі тощо.

Крім вищевказаного в ході СІО, зокрема, повинні вирішуватися завдання зменшення або збільшення інформаційних повідомлень, що розміщуються на довірених і розкручених в Інтернеті інформаційних ресурсах (новинних сайтах і стрічках, в соціальних мережах, в коментарях, де має місце вираження ставлення до проблеми). Неживими акторами соціальної сфери в цих явищах виступають медіавіруси в разі соціального програмування, тролі і роботи та боти в разі астротерфінга, а також спеціально навчені люди.

Медіавірус – медіаподія, що викликає прямо або опосередковано певні зміни громадської думки.

Астротерфінг – створення штучної громадської думки за допомогою спеціальних програм і технологій на базі середовища Інтернет.

Інтернет – середовище, в якому одночасно живуть як люди, так і програмні модулі, які мало чим відрізняються від людей. У літературі вони називаються по-різному: боти, аватари, програмні роботи. В силу того, що ці програмні роботи в частині діалогового інтерфейсу мало чим відрізняються від людей, а часом навіть їх перевершують по ряду комунікаційних параметрів, вони можуть створювати «думка більшості», до якого часто прислухаються люди.

Громадська думка на базі ресурсів Інтернету являє собою сукупність взаємопов'язаних індивідуальних думок з конкретного питання, яке торкається групи людей. Ці думки зафіксовані у вигляді мультимедійних матеріалів на ресурсах мережі Інтернет. Наприклад, у вигляді коментарів до будь-якої новини. Новина є тим вузлом, який збирає ці думки навколо себе. Грамотний вибір потоку новин впливає і на кількість коментарів, які, в результаті, і створюють цю громадську думку.

Принципово важливо, що відвідувач приходить на той чи інший ресурс не безпосередньо сам, а опосередковано, через відповідне ПЗ – браузер. Браузер – звичайна комп'ютерна програма, і їй все одно, хто її запускає – людина або інша комп'ютерна програма. Але при переході на сайт і внесенні туди деякої

інформації або повідомлень у робота можуть виникнути проблеми, з якими йому може допомогти впоратися людина:

- спеціально навчена людина на сотнях різних Інтернет-ресурсів самостійно реєструє роботів;
- спеціально навчена людина ставить завдання роботам у вигляді безлічі текстів коментарів, на базі яких роботи повинні формувати схожі і розміщувати їх на заданих ресурсах;
- спеціально навчені і організовані люди за завданням роботів розпізнають капчи і видають результат. Сьогодні ця платна послуга широко представлена в Інтернеті. При зіткненні з капчею робот звертається за допомогою на відповідний платний ресурс, демонструє людям капчу, отримує відповідь, відповідає і йде далі.

Капча (англ. Captcha) – назва застосовуваних в Інтернеті прийомів, призначених для перевірки на приналежність до людей. Зазвичай проходження капчі полягає у вирішенні задачі розпізнавання текстових, голосових, математичних образів, які може розпізнати людина, але не може програма.

Отже, теоретично люди могли б поставити перепону роботам, але роботам, яким допомагають такі ж люди, поставити перепону практично неможливо.

Зрозуміло, що все-таки люди більше довіряють людям, здатним, на відміну від робота, приймати рішення в нестандартних ситуаціях і оперативно діяти згідно з ними. Щоб створити інтелектуального робота, потрібен час і інші витрати на його підготовку для проведення спеціальних дій в ході інформаційної операції. Тому надійними виконавцями як і раніше залишаються спеціально найняті відвідувачі, які за певну плату або з ідейних міркувань періодично заходять на задану множину сайтів і виконують обумовлені з замовником дії. Вони реєструються під кількома іменами і масово просувають певну ідею.

Необхідною складовою сучасної війни є постійний моніторинг інформаційного простору на предмет виявлення фактів початку інформаційних

операцій. Моніторинг доцільно здійснювати в мережі Інтернет як найбільш динамічній складовій інформаційного простору, на базі добре зарекомендувавших себе образів, слоганів, слів і словосполучень.

До ознак інформаційної загрози в Інтернеті можна віднести:

- збільшення і підтримання на певному рівні частоти повторення новин певної тематики і замовних коментарів до них, відповідно до вказаної кількісної оцінки;
- територія, на яку спрямовано вплив відповідної інформації (об'єкт впливу);
- джерела інформації (суб'єкт впливу).

Виявлення інформаційних загроз, як і будь-яких інших загроз, доцільно починати з аналізу підходів і методів цілеспрямованого перепрограмування інформаційних систем, чи то технічні системи, чи соціальні структури, або люди. Виділення послідовності властивих інформаційній операції подій, а потім виявлення цих подій в загальному «життєвому шумі» – це класичний шлях вирішення подібних завдань. Даний шлях складається з наступних етапів:

Етап 1. Послідовність подій, що становлять загрозу, завжди пов'язана з метою. Досягнення мети передбачає перепрограмування суб'єктів інформаційного протиборства. Щоб розуміти, наскільки досягнута мета, бажано вміти оцінювати результати перепрограмування і власні можливості, кажучи іншими словами – ступінь можливого ураження інформаційною зброєю тієї чи іншої системи. Одні об'єкти знищити і перепрограмувати не складає труднощів, з іншими – завдання може виявитися нерозв'язною за виділені для цієї мети ресурси і, в першу чергу, часові ресурси.

Етап 2. Оцінка і обґрунтування частоти появи подій, при якій вже можна говорити про початок інформаційної операції по перепрограмуванню.

Етап 3. Оперативне і доступне подання інформації користувачу в разі виявлення небезпечних тенденцій.

Якщо система управління вже піддалася інформаційному ураженню, його ступінь можна оцінювати через відкритість цієї системи для зовнішніх

цілеспрямованих інформаційних впливів. Перерахуємо якісні ознаки відкритості системи управління для противника.

1. Ключові суб'єкти з системи управління «прив'язані» противником (переможцем) до сфери своїх інтересів.

2. Для ключових суб'єктів з системи управління противником забезпечена «база» у себе. Родичі подібних суб'єктів («агентів впливу»), як правило, переселяються, проживають, навчаються за межами своєї країни.

3. У разі перемоги противник, як правило, перебудовує систему управління ураженого об'єкта. Перебудова ця здійснюється в ключі, зручному для розуміння і подальшого таємного управління. Найчастіше перебудова системи управління за своєю формою спрямована на відповідність образом і подобою системі управління переможця [4].

Висновки до розділу 1

В розділі було розглянуто основі поняття та дані визначення поняттю «спеціальна інформаційна операція», її етапи та яким чином вона може проводитися. Виходячи з цього СІО можна розглядати як вид бойового забезпечення і оперативного супроводу політичного і військового керівництва держави, яким може користуватися не тільки наша країна, а й активно використовує противник.

СІО необхідно розглядати, як систему інформаційно-психологічного впливу скоординованої і взаємозалежної по цілям і завданням, об'єктам і суб'єктам прямого цілеспрямованого придушення конкуруючих опонентів у всіх сферах інформаційного протиборства ймовірного противника.

СІО можуть проводитися з метою оперативного або стратегічного маскування своїх реальних військових, геополітичних, політичних, економічних задумів, завдань і намірів, а також з метою дискредитації дій ймовірного противника, його державної політики, економічних структур.

Встановлено, що на глобальному рівні в операції можуть бути задіяні, агенти, резиденти, розробники і їх інформаційно-ударні комплекси, розташовані на території ймовірного противника. Операція може проводитися на території декількох держав одночасно, протягом великого проміжку часу, тому з метою реалізації СІО інколи доцільно задіяти всі інформаційні ресурси держави, а так само сили і засоби ІП системи національної безпеки.

Оскільки проведення СІО – це творчий процес, оперативне мистецтво, що потребує неординарного підходу, то планування і реалізація СІО є дуже складним, багаторівневим і багатоходовим оперативним завданням, а протидія їм - ще складніший процес.

РОЗДІЛ 2
РЕАЛІЗАЦІЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В УКРАЇНІ

2.1 Загальна характеристика СІО в Україні протягом 2014-2022 років

Спеціальні інформаційні операції відбуваються постійно, але мають різний масштаб і різні напрями впливу, тому, для захисту держави, необхідно зосереджувати увагу не на всіх наявних СІО, а лише на тих, що можуть їй зашкодити.

Протягом останніх років, починаючи з 2014 року, Російська Федерація здійснила велику кількість СІО, що наносили шкоду іміджу України та збентежували її населення. Ці СІО об’єднувалися в серії поєднаних спільними сценаріями дій, що поступово нарощують соціальну напругу. Відомо, що російські навіювання та дезінформаційні прийоми мають високий ступінь ефективності саме завдяки повторюваності в медіа.

Офіційно неоголошена війна РФ проти України визначається як «гібридна», «нелінійна», або «війна керованого хаосу». Така війна поєднує військові, інформаційні, терористичні та інші агресивні дії, скоординовані з центру і спрямовані на досягнення визначеної стратегічної мети. Метою цієї війни є повне підпорядкування України російському керівництву.

Зміст, характер і особливості такої війни істотно відрізняються від традиційних моделей минулих воєн. Сутність війни керованого хаосу полягає в геополітичному знищенні держави-жертви, нейтралізації її геополітичних характеристик – розміру території, чисельності населення, статусу держави в світі, економічних можливостей, військової могутності, сукупного потенціалу.

При такій війні в державі-жертві або в окремих її регіонах ініціюються певні внутрішньополітичні процеси, які, по суті, є акціями стратегії керованого хаосу. Справжні роль, місце, інтереси й цілі держави-агресора виводяться зі сфери суспільної уваги, ховаються за «інформаційним сміттям» і демагогією.

У цій новій війні ставка робиться на використання цивільного населення для нагнітання масової істерії і опору законній владі в якості «живого щита» для прикриття озброєних бойовиків.

При цьому медійна складова відіграє чи не найважливішу роль для формування «правильного» з точки зору агресора образу жертви в цій війні, що, по суті, є набагато важливішим, ніж отримання власне перемоги. Вбивство чужих солдатів не є головною метою – в сьогоднішній війні досить вбивати своїх воїнів і забезпечувати при цьому необхідний інформаційний супровід. В ході такої війни агресор приписує жертві те, що робить сам.

Основним об'єктом впливу в гібридній війні є не противник, а населення, яке «звільняється». Завдання і метод такої війни – спонукання громадян до зради власної держави і підтримки агресора. Також задіюються всі засоби для формування кращої для загарбника картини подій в очах міжнародної громадськості.

Така схема ведення війни надзвичайно складна для протидії, оскільки немає формальних підстав воювати з країною-агресором, яка лише неофіційно (але надактивно) підтримує бойовиків і терористів.

Навіть сьогодні в нашій країні діє розгалужена агентура спецслужб РФ, російські диверсанти і найманці. А Росія постачає їх зброєю і новими бойовиками, веде обстріл наших позицій зі своєї та окупованої території.

В офіційно неоголошеній війні проти України РФ активно застосовує методи інформаційно-психологічної війни, прагнучи зруйнувати моральний стан військовослужбовців і цивільного населення нашої держави.

Привід для початку російських СІО в Україні. Інформаційна війна проти України перейшла в «гарячу фазу» 6-5 жовтня 2013 року, коли відбувся боксерський 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. Річ у тім, що російський інформаційний простір був максимально розігрітий перед боєм, а

вся російська політична еліта зробила ставку на перемогу «руського вітязя». Тож виграш українського боксера запустив механізм «реваншу» через соцмережі. Завданням «тролів» було різко критикувати українців та все українське, розповсюджуючи ненависть до України. Тоді більшість просто не звернула уваги на сплеск мови ворожнечі стосовно українців.

Відтоді тактика Кремля змінилася. За вісім років спостереження за діяльністю російських спецслужб стало очевидним, що ключові лозунги були модифіковані, а СІО, спрямовані проти України, набули більш систематичного характеру. Більшість лозунгів можна об'єднати за кількома напрямками, кожен з яких відповідає одному сценарію, що просувається у світовий інформаційний простір і розрахований на конкретну цільову аудиторію [5].

У дипломній роботі буде проаналізовано низку основних сценаріїв СІО, організованих РФ і спрямованих на досягнення різних цілей. Загалом усі розглянуті сценарії можна класифікувати за кількома критеріями – цілями деструктивного впливу (Рис. 2.1).

Рис. 2.1 Види сценаріїв СІО РФ, спрямованих проти України

2.2 Сценарії СІО, що були реалізовані в Україні

2.2.1 Зв'язок України з ІДІЛ

Починаючи з 2013 року, Кремль активно просував в глобальний інформаційний простір міф про зв’язок України та Ісламської держави Іраку та Леванту (ІДІЛ). На даний момент, в світовому інформаційному просторі ІДІЛ розцінюється як безумовне зло, джерело загроз і небезпеки для всього людства, організація, яка прагне знищувати усе, до чого може дотягнутися. Екс-президент США Д. Трамп на початку своєї каденції назвав ІДІЛ «загрозою номер один».

Не важко розгадати мотиви російських спецслужб та політичних еліт, які роками намагалися довести світовій спільноті, що між Україною та ІДІЛ є зв’язок.

Запускаючи відповідні повідомлення в інформаційний простір, провокуючи їх, здійснюючи для цього спеціальні інформаційні, російські спецслужби та підконтрольні їм медіа створювали з нашої держави образ країни, яка допомагає джихадистам влаштовувати теракти на території Європи.

Метою цього частіше за все була дискредитація та руйнація іміджу України у світовій спільноті. Однак, окрім іншого, російська сторона також переслідувала ціль виправдання агресії проти України та розширення повноважень своїх спецслужб та правоохоронних органів. Зокрема, щодо подальших обмежень та державного контролю над Інтернетом та онлайн-сервісами.

Для закріплення у інформаційному просторі та у свідомості людей ідеї про зв’язок між Україною та ІДІЛ Кремль намагався декілька років підтримувати просування чотирьох ключових тем:

1. На території України знаходяться, підтримуються та фінансуються «табори», де майбутні бійці ІДІЛ проходять підготовку, військовий вишкіл та отримують «промивання мізків», для того щоб в подальшому за підтримки керівників цих «таборів» потрапити на територію Сирії, Іраку, щоб брати

участь у джихаді. Особливу увагу слід приділити окремому напрямку роботи російських спецслужб, який зводився до намагання Кремля створити з українського міста Одеси образ перевалочного пункту для ІДІЛ.

2. Добровольчі батальйони та підрозділи української армії, які боряться з агресором, це насправді бойовики-терористи, які мають тісний зв'язок з ісламськими радикалами та мережею ІДІЛ, в тому числі, тією, що працює на території України. Ключовою цільовою аудиторією цих меседжів для Кремля звичайно була політична еліта та громадяни країн ЄС. Таким чином, російські спецслужби намагалися закріпити за Україною образ країни, яка підтримує тероризм, а отже Кремль має усі права з нею воювати.

3. Україна здійснює постачання або контрабанду зброї та амуніції терористичним угрупованням, що є частинами ІДІЛ в різних країнах. Ключовою аудиторією для цієї дезінформації є предстставники політичних еліт країн-партнерів України, а також масштабні гравці міжнародного ринку озброєнь. Ні для кого не є секретом той факт, що Україна та Росія постійно конкурують на міжнародному ринку озброєнь, оскільки мають працювати з одним і тим самими країнами-споживачами, що закуповують товари військового призначення. У зв'язку з цим, російська сторона часто вдається до неконкурентної боротьби, шляхом використання «чорного піару» та поширення дезінформації, щоб усунути конкурента з ринку, або прикрити власні незаконні оборудки.

4. Громадяни України та іноземці, що перебувають на території України, можуть в будь-який момент стати жертвами терористичних атак, які плануються до здійснення бойовиками ІДІЛ.

2.2.2 Дискредитація ЗСУ

З початком війни на Донбасі російська пропаганда почала масштабну інформаційну кампанію для дискредитації дій України на Сході. Основними її цілями стали Збройні Сили України та добровольчі батальйони, яких у фейкових новинах представляли як «карателів» і «фашистів», намагаючись

провести паралелі з Другою світовою війною. Заразом щодо російських військ вживався термін «ополченці», який, за твердженням дослідників з «Media Sapiens», «має чіткі конотації з героїчною боротьбою «радянського народу» проти німецької агресії під час Другої світової війни, для позначення і водночас виправдання заколоту проти української держави». Також активно використовувалася риторика «геноциду, який здійснюють українські війська», для підтвердження якого використовували фейки про, нібито, «злочини» ЗСУ та добровольчих батальйонів.

Все це було спрямовано на демонстрацію внутрішньому російському споживачеві інформації про агресію з боку України щодо «російськомовного населення Донбасу» і таким чином виправдання вторгнення російських військ на українську територію для його захисту. Разом з цим, для міжнародної спільноти створювалася викривлена картина подій, яка повинна була змусити західних партнерів України відмовитися від надання Києву підтримки.

Ключовими цільовими аудиторіями для російських спецслужб та медіа, що співпрацюють з ними, в контексті висвітлення цього кремлівського навіювання, є, в першу чергу, мешканці окупованих регіонів; громадяни та мешканці Росії; громадяни й політичні еліти країн Західної Європи та Америки.

Мешканці окремих районів Донбасу, де точиться збройне протистояння вже вісім років, стали жертвою щоденної російської «промивки мізків», що мала на меті переконати в безальтернативності російського вибору, оскільки з українського боку на російськомовне населення Донбасу чекають тільки звірства і насильство.

Для внутрішньо-російської аудиторії ці навіювання були важливі для легітимізації російської агресії проти України. Відповідно до поширюваних наративів російськомовне населення має підтримати путінський режим, в іншому випадку – воно буде знищене радикальними українськими націоналістами. Ще кращим варіантом для мешканців Донбасу може бути взяти до рук зброю та воювати проти українців. Цей лозунг був вкрай успішним серед російської аудиторії.

Для європейської аудиторії, яка на той час здебільшого споживала новини про події в Україні з близьких до Москви джерел, просувалася ідея, що Україну не слід підтримувати, оскільки вона нічим не відрізняється від Росії, а військові злочини скоюють обидві сторони.

2.2.3 Звинувачення України в збитті малайзійського боїнгу

З моменту катастрофи малайзійського боїнгу MH17 Російська Федерація почала формувати стратегію «інформаційного захисту», ключовою метою якого було – відвести підозри про злочин від себе, звинуватити у збитті літака Україну, зробити її «співучасником» злочину. Зробити все можливе, щоб факти щодо безпосередньої причетності Кремля до збиття цивільного авіалайнера, доведені Міжнародною спільною слідчою групою, були максимально розмиті фейками і різними версіями, що поширювалися в інформаційному просторі.

Насправді ж, інформація про справжні причини катастрофи була надіслана до Кремля достатньо швидко, так само як і відомості про виконавців атаки на цивільний літак. Однак задля того, щоб якомога надійніше приховати усі нюанси цього акту агресії, російські спецслужби розробили довгострокову стратегію, спрямовану на відтермінування процесу розробки єдиної можливої версії, яка звучить так: малайзійський Boeing збили терористи, використавши при цьому російський зенітно-ракетний комплекс «Бук».

Однак, коли стало зрозуміло, що саме росіяни та підконтрольні їм бандформування збили малазійський авіалайнер, російські спецслужби вигадали фейк про «диспетчера Карлоса», який, як стане відомо пізніше, виявився злочинцем, якому росіяни, вірогідно, сплатили значну суму грошей задля розповсюдження хибної інформації. Кремль одразу поширив інформацію про те, що ця катастрофа сталася з вини України, а українські військові насправді намагалися збити літак президента РФ, який мав летіти в тому районі.

Головну тезу, яка є мета-темою, що її просував Кремль у міжнародний інформаційний простір, стала фраза журналіста та письменника Пітера

Померанцева, якою він назвав свою книгу про російську пропаганду: «Ніщо не правда і все можливо». Створюючи щоразу нові версії, російські спецслужби використовували, так званий, «принцип Алі-Баби», який використовується піарниками в комерційній сфері, коли стоїть задача врятувати чи відкоригувати репутацію людини чи бренду в інфопросторі та соцмережах.

«Принцип Алі-Баби» не так часто згадується у широкому вжитку, оскільки він є специфічним прийомом вузького кола спеціалістів і його назва не є усталеною. Цей «маневр» називають по різному, але суть його полягає у використанні прийому, описаного у казці «Алі-Баба та 40 розбійників»: поставити хрестики на всіх дверях, щоб не можна було виявити двері будинку, де жив герой. У випадку СІО, організованих РФ в Україні, цей прийом полягав у наступному: якщо немає можливості зняти обвинувачення зі справжнього зловмисника - винуватця події, то треба зробити винними у реалізації злочину всіх, кого тільки можливо.

Отже, головною метою російських спецслужб було звинуватити усіх причетних - «поставити хрестики на усіх дверях», щоб максимально розмити істину й уникнути правосуддя. Для цього було вигадано безліч історій. І для кожної з них було сфабриковано «докази».

2.2.4 США і НАТО в Україні

У кремлівських ЗМІ було оприлюднено нескінченну кількість фейків про нібито масову участь громадян країн Заходу у війні на боці України. Адже РФ не може визнати, що військові успіхи й ефективні тактичні операції реалізовуються українською армією. А отже їй, буцімто, допомагають «афроамериканські вояки НАТО», «ельфи Середзем'я» та «балтійські снайпери». Таким чином, російські пропагандисти у висвітленні подій в Україні не обмежуються лише однією дискредитацією українських військових.

Особлива роль відводиться НАТО та США: «факти» щодо присутності їхніх військ в Україні ще з самого початку конфлікту 2014 року стали логічним продовженням теми російської пропаганди про «організований заходом

Євромайдан» і «зовнішнє управління Україною». Однак регулярними військами справа не обмежується, у фейках також постійно фігурують приватні військові компанії різних країн.

Впродовж усієї історії незалежності України російська сторона всіляко підкреслює, що Україна є сферою інтересів Кремля. А відтак, будь-яка співпраця з Північно-Атлантичним Альянсом є загрозою для національної безпеки Росії, оскільки може призвести до розширення НАТО і використання території України для розміщення озброєнь або військових баз.

Тому, з перших днів Революції гідності і дотепер кремлівські спікери та експерти підкреслюють, що Кремль веде боротьбу не з українцями, а з американцями та натівцями на території України.

Крім безпосередньої участі Альянсу в бойових діях пропагандисти також поширюють інформацію про діяльність секретних американських лабораторій із виготовлення біологічної зброї на території України.

Головною мотивацією тут виступає бажання зобразити Україну ареною геополітичного протистояння, де вже активно діють США та НАТО. Через це Росія не може залишатися осторонь і «вимушена» брати участь у конфлікті не з Україною, а саме з, нібито, її «заокеанськими кураторами», а населення РФ – підтримувати інтервенцію російських військ в Україні.

2.2.5 Протидія євроінтеграції України

Масштабна протидія процесам євроінтеграції України та повернення українського суспільства до європейсько-орієнтованої парадигми майбутнього після століть штучної відірваності від західної цивілізації – була головним завданням Кремля ще задовго до Революції гідності. Унеможливлення європейської інтеграції України було метою багатьох російських та українських політиків, яка не справдилася через принципову позицію українського народу та готовність її захищати на Майдані.

Після подій Революції гідності Російська Федерація також намагалася активно завадити процесу євроінтеграції України. Кремль не лише намагався

використати проти офіційного Києва економічні та військові важелі, а й активно застосовував інформацію як зброю.

Ключовими аудиторіями СІО російських спецслужб були як європейська спільнота, так і українські громадяни. Намагаючись зірвати підписання Угоди про асоціацію України з ЄС, Росія розповсюджувала фейкові новини як в українському інформаційному просторі, так і в європейському.

Так, Кремль докладав значних зусиль, щоб перешкодити процесу ратифікації документу державами-членами ЄС, яскравим прикладом цього є референдум у Нідерландах, де російські спецслужби застосували усі можливі засоби до та під час волевиявлення голандців.

В Україні за допомогою медійних та політичних груп Кремль намагався переконати суспільство в тому, що в Європі на українців ніхто не чекає, і їм вона також не потрібна. Дуже потужні атаки були спрямовані на процес отримання безвізового режиму.

Росія і досі поширює неправдиві дані про невигідність цієї Угоди, акцентуючи на тому, що українська економіка порівняно із економікою ЄС є неконкурентноспроможною, а вітчизняні підприємства не виживуть без підтримки Росії.

2.2.6 Анексія Кримського півострова РФ

Окупація Криму стала першим актом фізичної агресії РФ проти України після Революції гідності. Кремль продемонстрував, що не менш активно, аніж живу силу, Росія використовує свій пропагандистський ресурс для війни в інформаційному просторі. На початку агресії російські ЗМІ для виправдання анексії Криму використовували фейкові ідеї про «фашизацію» України та «смертельну небезпеку для усіх російськомовних», які й досі активно підтримуються російською пропагандистською машиною.

Після зміщення акценту пропаганди на українських військових на Донбасі, Кремль продовжував поширювати фейки про Крим. Переважно вони стосувалися того, наскільки позитивно вплинуло на півострів його

«приєднання» до Росії, відсутності в українців бажання повертати його та негласної підтримки анексії міжнародною спільнотою. Для цього російська пропаганда активно використовувала офіційні візити представників інших держав. Таким чином Росія намагалася показати світовій спільноті правомірність анексії, а українському населенню - марність сподівань на повернення півострова до складу України.

Анексія Криму безперечно залишається одним з тяжких злочинів Російської Федерації, а також одним з найгрубіших порушень міжнародного права після Другої світової війни. Намагаючись хоча б якось виправдати свою протиправну поведінку в очах світового співтовариства, у Кремлі вирішили зробити основну ставку на просування розкрученої пропагандою РФ тези про абсолютну підтримку кримчан ідеї приєднання півострова до Росії.

2.2.7 Експорт української зброї

Нова ера постійного інформаційного переслідування України за підозри у незаконних оборудках зі зброєю почалася в 2005 році після виходу на світові екрани голлівудського фільму «Збройний барон» (Lord of War), який зібрав у прокаті по всьому світу 73 мільйони доларів. Стрічка розповідає про емігранта з України, який у змові зі своїми українськими родичами, що продовжували служити в українському війську, за безцінь скуповує все, що лежить на українських складах зброї.

Очевидно, що зазначений фільм став чудовим пропагандистським засобом в умілих руках російських пропагандистів. Новини про те, що Україна експортує зброю в гарячі точки, регулярно з’являлася в ЗМІ. За 10 років до початку війни фейки повідомляли про українські поставки озброєння до Грузії, Судану, Нігерії, Тайланду, Ірану та навіть ІДІЛ.

Причин актуалізації таких звинувачень декілька. По-перше, у зв’язку з вторгненням Росії, світова спільнота звертає на Україну більше уваги. По-друге, відкриті дані демонструють, що як виробник і експортер, Україна дійсно

досягає значних успіхів у військово-технічній сфері і в деяких аспектах переважає над РФ, яка є найближчим конкурентом на цьому ринку.

У зв'язку з цим, РФ намагалася підірвати довіру іноземних держав до українського військово-промислового комплексу й вітчизняного виробника озброєння. Для цього застосовувалися всі можливі засоби, починаючи від активних заходів на кшталт фіктивних поставок і закінчуючи СІО. Таким чином РФ прагнула заблокувати військове співробітництво України з основними регіональними (Туреччина) і глобальними (США та ЄС) партнерами.

2.2.8 Розгляд суперечок між РФ та Україною в міжнародних судах

Російська Федерація вела активну інформаційну боротьбу проти України й у залах міжнародних судових установ. Нині, коли суди міжнародного рівня розглядають протиправні дії агресора, які були і досі є направлені проти політичного ладу України та економічного добробуту її населення, Кремль та підконтрольні йому спецслужби були вимушені активізуватися й на цьому напрямку.

Щоб відстоювати свої права, закріплені в міжнародних договорах, компетентні органи української влади забезпечили звернення до міжнародних судів з метою встановлення справедливості. Зокрема, щодо підтримки російською стороною міжнародного тероризму, факти якого було зафіксовано на Сході України (МН17, обстріл під Волновахою, обстріл мікрорайону «Східний» в Маріуполі), порушення міжнародного законодавства шляхом анексії Криму та економічної суперечки між українською компанією «Нафтогаз» та російською «Газпром».

Кожний судовий процес, в якому задіяна російська сторона, перетворюється на змагання по розповсюдженню дезінформації. Спочатку в суді, коли Росія озвучувала свою юридичну позицію та аргументи, на яких вона ґрунтується, а потім в російських та лояльних до Кремля медіа, в яких висвітлюється судовий процес.

Міністерство інформаційної політики України, з березня 2020 року Міністерство культури та інформаційної політики України (далі – МКІП) з початку березня 2017 року уважно стежить за темами, які просуває російська сторона, стосовно своїх позицій в судових процесах. Таким чином, було сформовано ключові тези, які є основою російської брехні:

1. «Події на сході України є не військовою агресією, а внутрішньо-українським конфліктом». Хоча де-факто створення, фінансова підтримка й воєнний вишкіл відповідних парамілітарних організацій на Донбасі проводився російськими силами ще у 2009-му році в рамках підготовки до активних дій проти України. Крім того, державні органи та громадські організації України надавали безліч підтверджень про присутність російських військ на суверенній території України.

2. «MH17 міг бути збитий українськими військовими, оскільки відповідні частини ЗСУ й техніка також могли знаходитися в наближенні до місця катастрофи. Міжнародна розслідувальна комісія навмисно не враховує російських доказів». Насправді ж, розслідувачами вже давно відтворені усі факти і аспекти того, як БУК-М1, з якого було вражено літак, внаслідок чого загинуло 298 осіб, був привезений на територію України з Росії, знаходився під контролем російських найманців, і випустив ракету зі встановленого місця.

3. «На Донбасі немає російської зброї та російських військових». Насправді ж, СБУ, недержавні організації InformNapalm, Bellingcat, Stop Terror, та Atlantic Council, журналіст Саймон Островський та багато інших суб'єктів представили багато доказів того, що представники регулярних російських військових частин знаходилися на Донбасі, постачали зброю і важку техніку російського виробництва терористам, а також використовували її самі, брали участь у бойових зіткненнях.

4. «Україна не дотримується Мінських домовленостей». Насправді ж, ескалація в Авдіївці була спровокована проросійськими терористами через 5 годин після телефонної розмови Володимира Путіна з Дональдом Трампом. Волонтери міжнародної спільноти InformNapalm зафіксували бронетехніку й

важку артилерію, яка знаходилася у безпосередній близькості до лінії зіткнення, що порушує норми домовленостей в рамках Мінських угод.

5. «Блокада торгівлі з окупованими територіями свідчить, що Україна сама може бути спонсором тероризму». Насправді ж, на українських підприємствах, які ще не встигли вкрасти росіяни, працювали громадяни України, які отримували зарплатню та сплачували податки до українського бюджету. Ці громадяни України утримувалися і досі утримуються в заручниках і потребують допомоги міжнародної спільноти й захисту в міжнародному суді.

2.2.9 Держава, що не відбулася

Після перемоги Революції гідності Росія активно почала транслювати у медіа тему, відповідно до якої Україна описувалася як «держава, що не відбулася». РФ використовувала її для дестабілізації України психологічно та задля надання легітимності окупації Криму та початку війни на Донбасі. Цим напрямом своєї пропаганди вона намагалася:

для іноземних партнерів України - обґрунтувати необхідність захоплення Криму в умовах «політичного колапсу», який нібито відбувався в Україні на початку 2014 року, а також переконати в необхідності російського патронажу над Україною задля забезпечення її нормального розвитку. Водночас Кремль прагнув знищити міжнародну підтримку вітчизняних реформ, які робили і роблять Україну незалежною від Москви;

для внутрішнього споживача – перевести увагу з внутрішніх проблем Росії на зовнішні подразники, в центрі яких перебуває Україна, пояснити необхідність російської підтримки самопроголошених «республік» як частини «руського міра». Окрім того, показати безальтернативність путінського режиму, оскільки нібито тільки завдяки його успішному керівництву вдасться уникнути в Росії такого хаосу, який нібито відбувається в післяреволюційній Україні;

для українського населення – показати неспроможність української влади вирішувати внутрішні проблеми держави, хибність вибраного шляху

європейської інтеграції, неспроможність керівництва України здійснювати реформи.

2.2.10 Відверта брехня

Російська пропагандистська машина намагається вкладати окремі лозунги в цілісні наративи для формування вигідного Кремлю медіаконтексту стосовно конкретних питань. Однак, нерідко в роботі пропагандистських механізмів відбуваються збої, які можуть бути викликані «інформаційними перегинами на місцях» або нечітким формулюванням позиції керівництва. Внаслідок цього у ЗМІ дивні й часто абсолютно відірвані від реальності сюжети, наприклад повідомлення про участь Арсенія Яценюка у Чеченській війні, створення концтаборів для російськомовних, поїдання голодними українцями снігурів тощо.

Поширення російськими дезінформаторами таких фантастичних історій можна пояснити прагненням наповнити медіапростір такою абсурдною інформацією, у порівнянні з якою будь-яка менш сюрреалістична брехня РФ буде сприйматися як достовірна інформація. Крім того, такі новини мають не стільки інформувати, скільки вражати й навіть шокувати аудиторію, формуючи образ максимально відмінної та ворожої України [5].

Крім абсурдних фейків, які є результатом невдалого виконання завдань російськими пропагандистами, але в яких можна знайти хоч якийсь сенс, зустрічаються також «творчі ініціативи на місцях», які, очевидно, були створені без вказівки керівництва і є взагалі відірваними від реальності. Яскравими прикладами таких новин є такі: декомунізація масляної, віднесення Діда Мороза до персон нон-грата в Україні, політ п’яного президента в Росію для «розборок» з Путіним, дитячий хрестовий похід на Донбас, заборона виїзду української молоді за кордон та багато інших.

Створення й поширення такої неправдивої інформації є основою для обгрунтованої критики і викриття фактів дезінформації, а також висміювання російської пропаганди та методів її роботи як в Україні, так і в усьому світі.

Висновки до розділу 2

У результаті дослідження встановлено, що керівництво РФ неодноразово планувало і проводило проти України різнопланові СІО, спрямовані на досягнення різних політичних та економічних цілей, ще задовго до початку повномасштабного вторгнення в Україну та навіть задовго до гібридної агресії в Криму і на Донбасі.

Головними гравцями на «інформаційному полі бою» були, зазвичай, російські ЗМІ, які транслювали спеціально спотворені інформаційні повідомлення. Збройні сили Росії і їх інформаційні структури також вчилися використовувати інформацію, як зброю масового ураження. Ще в мирний час вони відточували майстерність ведення бойових дій з використанням мирного населення в якості щита, реалізували тактику виправдання військових злочинів.

У роботі проведено аналіз низки сценаріїв реалізації СІО, організованих РФ на території України, з якого випливає, що всі вони мали на меті здійснення деструктивного інформаційно-психологічного впливу на населення України, керівництво держави та ЗСУ, зокрема звинувачення України в порушеннях, до яких вона не причетна, та зв’язках з терористичними державами; звинувачення української влади у неспроможності й залежності від країн Заходу й НАТО; просування хибності ідеї європейської та євротлантичної інтеграції для України; дискредитація і звинувачення ЗСУ в обстрілах і геноциді; просування ідей перспективності путінського режиму й безальтернативності економічної співпраці України з РФ; виправдання неправомірних дій РФ, легітимізація анексії Криму.

РОЗДІЛ 3
ЗАСАДИ ПРОТИДІЇ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ В УКРАЇНІ

3.1 Нормативно-правове й інституційне забезпечення протидії СІО в Україні

З моменту набуття незалежності в Україні сформовано нове національне законодавство, що регулює суспільні відносини в інформаційній сфері, у тому числі щодо забезпечення інформаційної безпеки держави (далі – ЗІБ). Законодавчі норми у цій сфері істотно впливають на нормативно-правове регулювання відносин між суспільством, його членами і державою, між фізичними та юридичними особами тощо. Тобто на сучасному етапі інформаційні відносини виступають, з одного боку, змістовним наповненням будь-яких відносин у житті країни, суспільства та громадян, з іншого – тими підвалинами, на яких формується законодавство в інших сферах їх існування.

У свою чергу, для створення сучасної та ефективної системи ЗІБ істотного значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити усі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави й ефективно реалізовувати політику національної безпеки в інформаційній сфері.

Законність функціонування є однією з головних вимог до системи ЗІБ. Ця законність повинна базуватися на сукупності законів і підзаконних нормативних актів, які спрямовані на створення необхідних умов для захисту національних інтересів в інформаційній та інших сферах життя країни.

В Україні за час її незалежності сформовано необхідні законодавчі основи системи ЗІБ, зокрема було прийнято великий масив нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері. Акти національного законодавства, які визначають

правовий статус державних органів, організацій і громадян, встановлюють у т.ч. повноваження державних органів щодо ЗІБ України.

З огляду на викладене, нормативну базу забезпечення національної безпеки України в інформаційній сфері доцільно розглядати з урахуванням існуючої ієрархії нормативних актів.

На найвищому рівні знаходяться норми Конституції України, які закріплюють концептуальні положення національної безпеки України, а також Стратегії національної безпеки України [24], Воєнної доктрини України [37], Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» [30], Закон України «Про основні засади забезпечення кібербезпеки» [31], Закон України Про основні засади забезпечення кібербезпеки [32], Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України [33], Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України» [34], Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки» [35]. Ці документи враховують основні положення міжнародних договорів і угод, ратифікованих Україною, які стосуються її національної безпеки в усіх сферах, у т.ч. й інформаційній.

На другому рівні знаходяться закони конститутивного напрямку, в яких визначаються важливі положення щодо забезпечення національної безпеки в інформаційній сфері (Закон України від 9 січня 2007 року № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [11], Закон України від 2 жовтня 1992 року № 2657-XII «Про інформацію» [12], Закон України від 21 січня 1994 року № 3855-XII «Про державну таємницю» [13], Закон України від 1 червня 2010 року № 2297-VI «Про захист персональних даних» [14], Закон України від 13 січня 2011 року № 2939-VI «Про доступ до публічної інформації» [15], Закон України від 4 лютого 1998 року № 74/98-ВР «Про Національну програму інформатизації»

[16], Закон України від 16.12.2020 № 1089-IX Про електронні комунікації [38], Закон України від 4 лютого 1998 року № 75/98-ВР «Про Концепцію Національної програми інформатизації» [17], Закон України від 5 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах» [19], Закон України від 20 листопада 2003 року № 1296-IV «Про захист суспільної моралі» [20] тощо).

На третьому рівні – закони України інституційного рівня, де закріплені основні завдання та форми діяльності державних органів у процесі забезпечення національної безпеки в інформаційній та інших сферах життєдіяльності особи, суспільства та держави (зокрема, Закон України від 6 грудня 1991 року № 1932-XII «Про оборону України», Закон України від 06 грудня 1991 № 1934-XII «Про Збройні Сили України», Закон України від 25 березня 1992 року № 2229-XII «Про Службу безпеки України» [21], Закон України від 23 лютого 2006 року № 3475-IV «Про Державну службу спеціального зв'язку та захисту інформації» [22] тощо).

У структурі нормативно-правової бази забезпечення національної безпеки України в інформаційній сфері особливе місце посідають укази та розпорядження Президента України та постанови Кабінету Міністрів України. Такі підзаконні нормативні акти видаються з метою конкретизації та підвищення якості вирішення завдань ЗІБ, визначених на законодавчому рівні.

Міністерства й відомства України в межах визначеної законами компетенції та відповідальності згідно з нормами чинного законодавства про національну безпеку України, а також відповідно до рішень Президента та Кабінету Міністрів України розробляють відомчі накази, інструкції, положення, спрямовані на реалізацію програм захисту життєво важливих інтересів людини, суспільства, держави в інформаційній сфері: Наказ МОУ «Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України» [39], Доктрина зі стратегічних комунікацій ЗСУ [40], проект Указу Президента України «Про затвердження концепції розвитку стратегічних комунікації сектору безпеки і оборони» [41].

Не дивлячись на те, що інформаційна агресія проти України почала розгортатися дуже несподівано та швидко, а наша країна була повністю не підготовлена не тільки для надання опору інформаційній, а й фізичній агресії, що стало результатом згубної для України політики тогочасного керівництва держави, все таки, спочатку силами добровольців був покладений початок, а згодом і силами державних служб – розвинена протидія фізичній та інформаційній агресії.

Функції виявлення та протидії деструктивному інформаційному впливу (в тому числі СІО) на керівництво, Збройні Сили та громадян України виконують усі органи виконавчої влади. Однак, ключові повноваження у цій сфері розподілені між декількома центральними органами виконавчої влади, такими як Рада національної безпеки та оборони України, Міністерство оборони України, Міністерство культури та інформаційної політики.

Центр протидії дезінформації при РНБО України.

Центр протидії дезінформації при РНБО України - створений з метою протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, ефективної протидії пропаганді, деструктивним дезінформаційним впливам та кампаніям, недопущення маніпулювання громадською думкою [42].

Управління стратегічних комунікацій МО України.

Основними завданнями Управління стратегічних комунікацій є:

- організація, координація, синхронізація та контроль за реалізацією заходів стратегічних комунікацій у Збройних Силах України;
- забезпечення ефективної взаємодії суб'єктів стратегічних комунікацій Збройних Сил України;
- розвиток спроможностей Збройних Сил України з питань стратегічних комунікацій та проведення їх оцінювання;

- розробка та уточнення планувальних документів стратегічного застосування Збройних Сил України, інших складових сил оборони в частині, що стосується питань стратегічних комунікацій.

Центр стратегічних комунікацій та інформаційної безпеки МКІП.

Ключові завдання стратегічних комунікацій та інформаційної безпеки МКІП розбудова стратегічних комунікацій (розробка контрнаративів РФ, проведення інформкампаній, включення українських наративів у щоденну комунікацію Уряду);

- протидія дезінформації та формування стійкості до неї. Постійне сповіщення про інформаційні атаки проти України на ресурсах Центру, зокрема на web-порталі, FB-сторінці, та Telegram-каналі;
- підвищення обізнаності про гібридні загрози (розробка та проведення тренінгів для державних службовців, зокрема для представників комунікаційних підрозділів);
- регулярне інформування про гібридну агресію з боку Росії на міжнародному рівні, напрацювання механізмів протидії дезінформації спільно з міжнародними партнерами [43].

Варто акцентувати на значному внеску МІП у справі просування інформації про СІО для широкої громадськості. Так, у 2019 році МІП представило хрестоматію – «Білу книгу спеціальних інформаційних операцій проти України 2014-2018», яка була створена на основі аналізу СІО, що проводилися Росією в останні роки перед загостренням ситуації [5].

Книга складається з добірки фейків російської пропаганди, спрямованих на підрив територіальної цілісності України. Вона яскраво демонструє, які теми найбільш часто використовувалися в інформаційних атаках проти України.

Книга структурована у вигляді набору «серіалів» з «сезонами», адже кожну масштабну тему російської дезінформації можна порівняти з «серіалом», який ділиться на «сезони» – складні комплекси ідей всередині нього. Кожна окрема «серія» зображує одну конкретну ситуацію, яка відповідає лінії сценарію, сезону і серіалу. Всього в книзі описано 10 «серіалів».

З моменту першої презентації видання – 12 лютого 2019 року, зафіксовано понад 10000 завантажень pdf-версії, а більше тисячі примірників МІП направило в київські вищі навчальні заклади та інші державні і недержавні інститути. Але такі обсяги є дуже малими для того, щоб викликати достатні зміни в реакції населення на СІО, що, потенціально, ще неодноразово проводитимуться Росією на території України.

Важливу роль у протидії дезінформуванню та СІО відіграє вітчизняна громадськість. Громадська організація «Український кризовий медіа-центр» (далі – УКМЦ) була створена у березні 2014 року, як швидке реагування на російську окупацію Криму та з метою захистити суверенітет України, її національні інтереси у глобальному інформаційному просторі. Від часу свого заснування УКМЦ розвинувся у центр міжнародних стратегічних комунікацій з активним поширенням інформації на аудиторії як в Україні, так і закордоном.

Експертиза УКМЦ охоплює унікальний медіа-центр, виняткові проєкти у сфері реформування урядових комунікацій, медіа підтримку великим іноземним ініціативам з допомоги Україні, глибинну роботу з регіональними журналістами, комунікацію реформ, що тривають, події та заходи у сфері культури, поширення медійної грамотності молоді, комплексний аналіз дезінформаційної діяльності у медійному просторі [44].

3.2 Рекомендації для вдосконалення засад протидії СІО в Україні

3.2.1 Рекомендації щодо внесення змін до законодавчої бази

Одним з найпотужніших важелів просування певної думки, позиції чи настроїв, а також покращення чи погіршення іміджу певної особи чи організації є реклама, адже це мультимедійний продукт, що може бути практично довільного змісту, який важко регулювати або цензурувати.

Відомо що всі комерційні телеканали та радіохвилі існують за рахунок надходження грошей за ефірний час, який вони продають. Частіше за все цей ефірний час зайнято рекламою, проте при факті існування соціальної та

політичної реклами під неї якнайкраще маскуються відео- та аудіо-матеріали, спрямовані на зміну настроїв населення. Схожу ситуацію можна бачити і в Інтернеті. Практично всі недержавні інтернет-ресурси існують за рахунок місця на сторінці, яке вони продають, частіше, іншим інтернет-ресурсам. Такі повідомлення, що платно розміщуються на сторінці інтернет-ресурсу та мають посилання на інший підпадають під категорію інтернет-реклами, при чому не важливо що мають на меті такі розміщені повідомлення та що знаходиться за їх посиланнями.

Найбільшою проблемою є те, що за допомогою подібних банерів створюється загальний настрій. Повідомлення на банері може містити частину фрази або фразу цілком, що виставлятиме в певному світлі особу або організацію, фото або частину відео, розміщеного з тією ж метою та звукову доріжку, що вмикається автоматично, без дозволу на те користувача комп'ютера. Тобто, навіть якщо за посиланням людина потрапляє на інформаційний ресурс, де розміщена стаття або інші матеріали, що описують лише імовірність факту, зазначеного в тексті банеру або інформацію, що не має ніякого відношення до вказаної теми взагалі це все одно становить велику небезпеку, оскільки дуже велика кількість населення не переходить за посиланнями, що знаходяться за цими банерами, але бачить їх та, при великій кількості однотипних банерів чи банерів на певну тему спрацьовує ефект запам'ятовуваності за рахунок частого повторення певної інформації.

Вбачаючи, що наразі більша частина населення країни користується мережею Інтернет для отримання інформації частіше ніж іншими засобами (наприклад телебачення, газети, книжки тощо), можна із впевненістю сказати, що банери в Інтернеті мають набагато більшу продуктивність і більший вплив на споживачів, ніж матеріали в інших ЗМІ.

Отже, за рахунок банерів в Інтернеті можливо продуктивно впливати на населення, що користується мережею, проте, можливо знизити цей вплив за допомогою врегулювання на законодавчому рівні. Не дивлячись на те, що реклама в Інтернеті є найвпливовішою та найпопулярнішою і може

застосовувати весь можливий потенціал мультимедіа для представлення інформації, вона не регулюється нормативними актами. 08.09.2008 року була спроба просування законопроекту «Про Інтернет рекламу» [8] народним депутатом України Уколовим В.О., проте він не отримав підтримку при розгляданні його Верховною Радою України, тому так і залишився на етапі пропозиції.

Ідея нормативного регулювання банерів в Інтернеті є абсолютно логічною та необхідною до розгляду, проте, такий крок, як пропозиція окремого закону є невдалим, оскільки створення великої кількості законів є непродуктивним, а саме цей законопроект більшою частиною свого тексту копіює основний Закон України від 3 липня 1996 року № 270/96-ВР «Про рекламу» [7]. Тому набагато кращим рішенням було б внесення змін в існуючий закон відповідно до пропозицій, наявних в проекті закону «Про Інтернет рекламу» [8], а також інші додаткові зміни, до інших нормативно-правових актів.

Крім інтернет-банерів згубний плив на суспільство має трансляція теле- та радіопередач країни, що має на меті проведення СІО, направлених на завдання шкоди іміджу України, оскільки такі дії проводяться не тільки на території нашої країни, але й країни-противника також. Тому, при виявленні такого впливу з боку іншої держави, необхідно обмежити доступ для транслювання телеканалів та радіохвиль, що надходять з країни-агресора. Доцільним буде внести пропозицію внесення змін до Закону України від 21 грудня 1993 року № 3759-XII «Про телебачення і радіомовлення» [23], що заборонять трансляцію відповідних телеканалів. Всі пропозиції щодо внесення змін до нормативно-правових актів викладено в додатку А.

Через велику кількість брехні в ЗМІ, особливо, в новинах, доцільним є накладання адміністративної або кримінальної відповідальності за ненадання джерела інформації в новинах, неправдиве надання джерела або надання джерелом неправдивої інформації, за якого у перших двох випадках покарання накладатиметься на відповідальну особу радіо- або телеканалу, а в третьому –

на джерело інформації в розмірі, визначеному судом, а також подальше висвітлення правдивої інформації на тому ж телеканалі. Оскільки ефект закріплення інформації якнайкраще працює на телебаченні, необхідно обмежити транслювання однієї теми новин до 20 хвилин на день для запобігання частого повторення інформації, яка може бути згубною для держави, але не підпадати під інші заборони.

3.2.2 Рекомендації щодо змін у технічній сфері

Відомо, що для проведення СІО, а саме для створення штучної суспільної думки та для переконання широкого загалу використовуються запрограмовані боти, створені з метою реєстрації їх, а надалі і розміщення ними коментарів на задану тему на певних інтернет-ресурсах. Звісно, такою діяльністю займаються не тільки боти, а й спеціально найняті люди, проте від ботів захиститися трохи простіше, ніж від людей.

Протягом останнього часу якість розробки ботів зросла і вони вже спроможні самі розпізнати деякі капчі, наприклад шляхом підвищення контрастності зображення, що пропонуються сайтами для вирішення, тому необхідно ускладнити проходження таких задач для роботів і спростити для людей, оскільки не завжди людина може пройти це завдання навіть не з першої спроби, що може істотно знизити рейтинг ресурсу. Єдиним можливим шляхом реалізувати вищесказане є застосування відмінностей людей та роботів.

Необхідно створювати капчі, що засновані на дефектному сприйняті кольорів оком людини через контраст із розміщеними поряд кольорами. На виході капча повинна мати вигляд пропозиції вибору блоків, визначеного в умові кольору, з усіх запропонованих. Людина обиратиме ті, що вважатиме необхідними, на основі того, що сприйматиме її око, а робот обере ті, код кольору яких співпадатиме з кольором, вказаним в умові. Для людини це завдання є доволі простим, оскільки не потребує ні розумових навантажень ні обдумування вибору віднесення певного блоку до потрібних, а для ботів це завдання сильно ускладнюється, оскільки, фактично, до потрібних за умовою

можуть відноситись більше блоків, ніж може обрати людина, або взагалі жодного.

Також можна змінити підхід до капчі з математичною умовою. Частіше за все подібні капчі зустрічаються з умовою, що пропонує ввести результат вирішення прикладу, а на зображенні, що додається присутні легко розпізнавані цифри та математичні оператори. Продуктивнішим було б застосування зображення без попередньої умови, записаної на сайті, а з умовою, зображеною відразу на ньому, після якої зазначається сам математичний приклад, написаний на зображенні текстом, проте результат якого людина матиме ввести цифрами.

Але навіть такий захист, що не під силу ботам, є все одно неідеальним. Враховуючи факт того, що існують організації, що надають оплачувані послуги по розшифровці капчі, необхідним також є введення обмеження по часу на введення відповіді настільки, щоб бот не встигав переслати капчу спеціальній людині, прийняти від неї відповідь та ввести її на сайті.

Із доступом на інтернет-ресурси спеціально навчених людей боротися складніше, ніж з доступом ботів, проте є можливість його мінімізувати. Для захисту державних інтернет-ресурсів є доцільним, для вчинення користувачем будь-яких дій на сайті, що будуть видимими для інших користувачів, обов’язкова реєстрація за даними паспорта та коду платника податків на державних ресурсах усіх рівнів.

Для захисту українських сайтів, відповідно, доцільною є реєстрація за номером телефону, оскільки одна людина може писати з великої кількості профілів, їх кількість можна зменшити саме таким чином, адже кількість телефонних номерів обмежена і, навіть, група осіб неспроможна купити безмежну кількість номерів та витрачати гроші на їх обслуговування, на відміну від створення електронних поштових адрес. Також, за потреби, можна не пропускати до реєстрації осіб певної країни, оскільки код країни вказується в телефонному номері.

Нашою державою вже були здійснені дії, направлені на обмеження впливу російської пропаганди, спілкування із оплаченими чи ідейно налаштованими спеціально навченими людьми та ботами, які просувають руйнівні ідеї у вигляді блокування доступу до деяких російських інтернет-ресурсів та соціальних мереж, проте не всі українці ще відмовились від користування цими ресурсами і продовжують це робити шляхом застосування VPN – технології, що забезпечує одне чи кілька мережевих з'єднань в іншій мережі шляхом побудови логічної мережі, що захищається криптографічними засобами.

Для того, щоб знизити використання російських ресурсів необхідно всі організації, що надають подібні послуги, зобов'язати надавати їх виключно на платній основі в абонементному порядку. Це істотно знизить бажання людей користуватись послугами VPN, проте на основних клієнтів постачальників даних послуг це не вплине, оскільки ними користуються комерційні підприємства й організації для налаштування конфіденційного зв'язку між собою вже на основі регулярної оплати.

3.2.3 Рекомендації щодо змін у гуманітарній сфері

Більшість населення і в Росії, і в Україні, і в країнах Євросоюзу не здатні розрізнити спотворене повідомлення від правдивого, не можуть критично оцінювати інформацію з різних типів медіа. Брак медіа-грамотності, тобто знань, які дозволяють людині аналізувати й протистояти пропаганді і брехні, відчувається серед усіх категорій населення. Це тим більш небезпечно для України, проти якої Росія веде війну.

Також велику проблему складає критично мала кількість спеціалістів достатнього рівня у сфері інформаційної безпеки. Часто держслужбовці, зайняті в цій сфері не мають відповідної освіти. Навіть, досягнувши певних результатів протягом службової діяльності, співробітник може підняти свій професійний рівень не так високо, наскільки може з відповідною освітою.

У разі, якщо певна кількість кадрів у вищевказаних службах є настільки цінними, що їх заміна персоналом з відповідною освітою буде нераціональною, доцільним є таких людей зараховувати на курси підвищення кваліфікації, які необхідно створити на базі державних університетів України із залученням провідних фахівців з Військового інституту Київського національного університету імені Тараса Шевченка, ІСЗЗІ КПІ ім. Ігоря Сікорського, Національної академії СБУ та Державного університету телекомунікацій.

Але найбільш обгрунтованим є набирати до лав, наприклад, Ради національної безпеки та оборони України чи МКІП фахівців, що проходили навчання в університетах, за умови, що в навчальних програмах всіх спеціальностей буде збільшено кількість годин викладання дисциплін, пов’язаних з інформаційною безпекою держави та її забезпеченням. Крім того реформ потребують інші військові та цивільні вищі навчальні заклади, де для формування критичного мислення необхідно ввести дисципліну «Інформаційне протиборство», що закріпить результати бази, необхідної для введення в школах.

Оскільки Інтернет тепер відіграє значущу роль в житті будь-якої людини, яка має до нього доступ, необхідним є реформування в навчальних закладах дисципліни «Безпека життєдіяльності», в рамках якої освітяни, окрім вже наявних тем в програмі, навчатимуться перевіряти інформацію, що містять ресурси на корисність та правдивість на базовому рівні. Доцільно вводити подібний предмет ще з початкової школи, адже отримавши мінімальні навички читання діти користуються мережею.

На початку цієї дисципліни може розглядатися, яким ресурсам можна довіряти, а яким – ні, необхідність перевіряти всі умови при скачуванні файлів та встановленні програм, основи протидії інтернет-злочинцям (на кшталт вимагачів грошей чи збоченців), а надалі, у старших класах, теоретичне ознайомлення з різницею між видами правди, неправди та дезінформування. Також, протягом програми, необхідно запевнити освітян в тому, що офіційним державним ресурсам необхідно беззастережно довіряти. Учні, що

проходитимуть таку програму будуть набагато більш захищеними від ворожої пропаганди починаючи зі шкільного віку та протягом життя.

Окрім молоді у групі ризику невмілого користування Інтернетом знаходяться також громадяни зрілого та літнього віку, для яких користування Інтернетом не є буденністю. Яскравим прикладом є те, що вищевказана категорія людей вірить даним, що знаходяться за першим-ліпшим посиланням, або часто сприймає спам за правдиві пропозиції, що несуть в собі корисний зміст або певну вигоду. Це нерідко призводить до втрати ними свого часу та грошей. Якщо додати до цього «сум за минулим», то російська пропаганда отримує для себе ідеальну жертву, особливо враховуючи, що ці вікові групи складають велику частину населення України.

Для захисту цих вікових груп необхідно розробити коротку інструкцію з користування Інтернетом саме для них, яку, по-перше, необхідно зобов’язати розмістити на офіційних сайтах інтернет-провайдерів, про що провести соціальну рекламу, а по-друге зобов’язати їх надавати інструкцію у друкованому вигляді при кожному новому підключенні абонентів.

Вищезазначених дій може бути недостатньо, оскільки далеко не всі люди читають інструкції, а пам’ять у молоді може виявитись доволі короткою, тому, для більшої продуктивності, необхідно застосувати розповсюдження соціальної реклами у вигляді плакатів, реклами в Інтернеті та на телебаченні, що закликатиме до обережності та перевірки змісту інформації на правдивість при її перегляді, особливо з російських ресурсів та інших ресурсів, якщо автором інформації зазначено громадянина держави-агресора, певну неперевірену особу або автора матеріалу не зазначено взагалі.

Також в перелік небезпечних матеріалів необхідно додати книжки, оскільки у наш час будь-яка людина може видати книжку, чи будь-яке друковане чи недруковане видання, за умови, що вона має на це гроші. При цьому видання може містити в собі абсолютно будь-яку інформацію агітаційного, пропагандистського, дестабілізуючого свідомість та іншого змісту, яка може виправдовуватися шляхом зазначення, що присутні у виданні

матеріали не мають нічого спільного з реальними людьми чи подіями або що матеріли наведені в якості прикладу та є вигаданими.

Навіть якщо обман викриється та видання відкличуть з продажу або іншого виду розповсюдження, це не убезпечить від згубного впливу тих людей, що його вже отримали. При чому такі видання можуть позиціонуватися не тільки як художня чи література для широкого загалу, а й і як дитяча чи, навіть, наукова література.

Оскільки за часів Радянського Союзу була розповсюджена думка про те, що книга – найкращий подарунок, книга не може нести шкоди, в книзі та інших друкованих виданнях міститься лише перевірена та корисна інформація (звісно, адже все, що видавалось того часу дійсно перевірялося на наявність політично та науково некоректного змісту), частина населення держави, що народилася і здобула хоча б загальну середню освіту за часів СРСР часто повністю довіряє інформації, викладеній у книжках та друкованих матеріалах. Саме тому необхідним є проведення соціальної реклами про перевірку на правдивість інформації, отриманої не тільки зі ЗМІ, а і з книжок та друкованих матеріалів.

Окрім ЗМІ та друкованих матеріалів загроза пропаганди надходить від людей, зацікавлених у її розповсюдженні. Намагатися переконати окремих людей або певні категорії громадян у своїй правоті та прийняти шкідливу точку зору можуть як люди, дії яких було профінансовано (на постійній основі, як працівника, що займається пропагандою серед мас, чи на договірній основі, як підробіток для людини, що хоче отримати гроші, не переймаючись результатами своєї оплачуваної діяльності) так і люди, що піддалися російській пропаганді та підтримують її позицію в інформаційному протиборстві. Для зосередження уваги людей на обережності при спілкуванні з такими особами доцільно провести соціальну рекламу, що нагадуватиме їм, що ворог може виявитися поруч.

Окрему групу ризику складають громадяни, що занадто серйозно відносяться до релігії. Проблему складає наявність в Україні православної церкви московського патріархату, особливо, такого відомого релігійного

осередку як Києво-Печерська Лавра. Через проповіді служитель може легко вплинути на розум, думки й наступні дії прихожан, пов’язавши з релігією політичні та інші події, інтерпретувати їх з будь-яким, корисним для проповідника сенсом. Для захисту прихожан від такого впливу необхідно взагалі відмовитись від його існування на території нашої держави, в окремих випадках дозволивши проповідання російською мовою.

Певна частина пропозицій пов’язана із запровадженням соціальної реклами, на яку необхідно витрачати бюджетні кошти. Проте видатки на неї можливо мінімізувати шляхом проведення повністю відкритого конкурсу на найкращу соціальну рекламу в певній сфері, для участі в якому необхідно, на задану в умові тематику та відповідно до вказаних вимог, представити готовий продукт реклами, а винагородою за перемогу зазначити вказання авторства реклами у вигляді імен творців або назви студії.

Таким чином видатки обмежаться проведенням конкурсу, а його переможці отримають можливість вперше вийти на екрани або підняти свій рейтинг в сфері реклами. Крім скорочення витрат на соціальну рекламу, із залученням до її створення широкого загалу, вона матиме вигляд поради одним людям від інших, що спростить її сприйняття масами.

3.3 Методика протидії спеціальним інформаційним операціям в Україні

Неможливо заздалегідь визначити імовірність проведення СІО, суб’єкт, який буде її проводити, й тему, на яку вона буде проводитись, неможливо визначити, якими саме шляхами потрібно протидіяти СІО, проте можливо сформувати методику протидії у вигляді певного списку дій, які, в залежності від етапу, на якому було виявлене проведення СІО, необхідно виконувати для протидії їй. Оскільки в попередньому розділі роботи були вказані зміни, які буде доцільно внести для протидії СІО, логічним буде розглядати створення методики протидії СІО саме в контексті цих змін.

Якщо підозра про проведення СІО виникла ще на інформаційному етапі, то необхідно провести наступні дії:

1. На початку:

- проаналізувати інформацію, що надійшла та, в залежності від її небезпечності, дати висновок про нагальність реакції на неї;
- визначити країну, що, ймовірно, проводить СІО, як можливу країну-агресора;
- скласти список небезпечних ресурсів цієї країни, доступ до яких буде заблокований, щойно статус країни агресора для неї набуде чинності;
- проаналізувати, які країни можуть співпрацювати з нею, та перевірити їх ресурси.

2. Якщо підозра про проведення СІО виправдана:

- надати країні, що проводить СІО, статус держави-агресора із подальшим блокуванням доступу до її ресурсів, трансляції її телеканалів та радіопередач на території України;
- прореагувати на інформацію, що вже надійшла у вигляді спростування її або висвітлення її у вигідному для держави світлі;
- перевірити дії та ресурси держав, що можуть співпрацювати з державою-агресором і, в залежності від небезпечності надаваного контенту, заблокувати або пропустити;
- проводити соціальну рекламу, давати сюжети новин, що висвітлюють країну, що проводить СІО, як вороже налаштовану, а інформацію, що від неї надходить, як неправдиву, повторювати в разі необхідності, наприклад надходження нової небезпечної інформації;
- якщо СІО повністю або частково проводилось проти певного об’єкта (наприклад, особи, групи осіб або організації), то цей об’єкт повинен вчинити певні дії, відповідно до ситуації, для покращення власного іміджу.

Якщо інформаційний етап було пропущено через рішення про безпідставність підозри про проведення СІО, необхідно:

- в якомога короткий термін часу переконатися в тому, що СІО дійсно проводиться шляхом аналізу даних, що поступали з ворожих ресурсів (держави, що імовірно проводить СІО та держав, що з нею імовірно співпрацюють за останній час (тиждень або місяць);
- виконати дії, вказані в другому пункті попереднього списку дій.

Якщо інформаційний етап не було помічено, а етап розкручування пропущено через рішення про безпідставність підозри про проведення СІО, необхідно:

- якнайшвидше заблокувати доступ до ресурсів країни-агресора та країн, що, можливо, з нею співпрацюють, після чого перевірити на небезпечність і розблокувати ті, що не несуть в собі небезпеки;
- запустити новини на усіх можливих ресурсах, включаючи телебачення та радіомовлення, що дискредитуватимуть країну-агресора, користуючись віднайденими або вигаданими підтверджуючими фактами;
- виконати дії, вказані в попередньому списку.

Якщо всі попередні етапи, включаючи етап загострення напруги, були пропущені, або якщо факт проведення СІО було виявлено вже після її завершення, необхідно:

- для недопущення ефекту закріплення, тимчасово переключити увагу людей з основної теми, що просувалася протягом СІО, на будь-яку найбільш сенсаційну новину, що викличе зацікавленість якомога більшої кількості людей та, за можливості, не нагадувала про основну ідею СІО;
- для того, щоб запобігти проведенню наступної СІО, виконати дії, вказані в попередньому списку.

Доцільним є покласти виконання кроків даної методики на МКІП, яке зможе шляхом видання власних актів або актів на основі рішень Міжнародної дорадчої ради регулювати дії ЗМІ.

Висновки до розділу 3

У розділі проаналізовано нормативно-правове й інституційне забезпечення протидії СІО в Україні, зокрема встановлено, що основними суб'єктами виявлення та протидії деструктивному інформаційному впливу на керівництво, ЗСУ та громадян України є: РНБО України, при якій діє Центр протидії дезінформації; Міністерство оборони України, у структурі якого функціонує Управління стратегічних комунікацій, і Міністерство культури та інформаційної політики, яке виконує завдання у сфері стратегічних комунікацій. Важливу роль у протидії дезінформуванню та СІО відіграє також вітчизняна громадськість.

У результаті дослідження розроблено рекомендації щодо вдосконалення засад протидії СІО в Україні, зокрема щодо внесення змін до законодавчої бази, змін у технічній та гуманітарній сферах, а також представлено методику протидії СІО в Україні, шляхом застосування яких можливо продуктивно протидіяти СІО, що проводитимуться іншими державами на території України. Проте, важливою умовою успіху є їх комплексне застосування: необхідно спочатку втілити вказані рекомендації і, в разі проведення СІО, застосувати розроблену методику протидії. У разі неприйняття пропозицій застосування методики протидії не дасть позитивних результатів.

ВИСНОВКИ

У дослідженні розглянуто сутність ключових понять у сфері інформаційного протиборства: інформаційна війна, СІО та АІВ. Під СІО розумітимемо вид бойового забезпечення і оперативного супроводу політичного і військового керівництва держави, яким може користуватися не тільки наша країна, а й активно використовує противник.

СІО можуть проводитися з метою оперативного або стратегічного маскування своїх реальних військових, геополітичних, політичних, економічних задумів, завдань і намірів, а також з метою дискредитації дій ймовірного противника, його державної політики, економічних структур.

Встановлено, що планування і реалізація СІО є дуже складним, багаторівневим і багатоходовим оперативним завданням. Водночас, СІО включає такі типові етапи: створення інформаційного приводу; «розкручування»; загострення напруги; вихід із операції або закріплення.

З'ясовано, що керівництво РФ неодноразово планувало і проводило проти України різнопланові СІО, спрямовані на досягнення різних політичних та економічних цілей, ще задовго до початку повномасштабного вторгнення в Україну та навіть задовго до гібридної агресії в Криму і на Донбасі.

Аналіз сценаріїв реалізації СІО, організованих РФ на території України, показав, що всі вони мали на меті здійснення деструктивного інформаційно-психологічного впливу на населення України, керівництво держави та ЗСУ, зокрема звинувачення України в порушеннях, до яких вона не причетна, та зв'язках з терористичними державами; звинувачення української влади у неспроможності й залежності від країн Заходу й НАТО; просування хибності ідеї європейської та євроатлантичної інтеграції для України; дискредитація і звинувачення ЗСУ в хибних злочинах; просування ідей перспективності путінського режиму й безальтернативності економічної співпраці України з РФ; виправдання неправомірних дій РФ, легітимізація анексії Криму.

У результаті вивчення нормативно-правового й інституційного забезпечення протидії СІО в Україні встановлено, що основними суб'єктами виявлення та протидії деструктивному інформаційному впливу на керівництво, ЗСУ та громадян України є: РНБО України, при якій діє Центр протидії дезінформації; Міністерство оборони України, у структурі якого функціонує Управління стратегічних комунікацій, і Міністерство культури та інформаційної політики, яке виконує завдання у сфері стратегічних комунікацій. Важливу роль у протидії дезінформуванню та СІО відіграє також вітчизняна громадськість.

За підсумками дослідження розроблено рекомендації щодо вдосконалення засад протидії СІО в Україні, зокрема щодо внесення змін до законодавчої бази, змін у технічній та гуманітарній сферах, а також представлено методику протидії СІО в Україні, шляхом комплексного застосування яких можна продуктивно протидіяти СІО, що проводитимуться іншими державами на території України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монографія. СПб. : Наукоемкие технологии, 2017. – 546 с.

2. Інформаційно-психологічне протиборство: підручник / за загальною редакцією В.М. Петрика. К.: Видавництво ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 388 с.

3. Історія інформаційно-психологічного протиборства: підручник; за загальною редакцією д.ю.н., проф., засл. юриста України Є.Д. Скулиша. К. : Наук.-вид. відділ НА СБ України, 2012. 212 с.

4. Расторгуев С.П., Литвиненко М.В.. Информационные операции в сети Интернет. За загальною редакцією А.Б. Михайловського. М. : АНО ЦСОиП, 2014. 128 с.

5. Біла книга спеціальних інформаційних операцій проти України 2014-2018 / За загальною редакцією Д.Ю. Золотухіна. К. : Мега-прес груп, 2018. 384 с.

6. Петрик В.М., Присяжнюк М.М., Мельник Д.С. Забезпечення інформаційної безпеки держави: підручник / за загальною редакцією О.А. Семенченка та В.М. Петрика. К. : ДНУ «Книжкова палата України», 2015. 672 с.

7. Про рекламу: Закон України від 3 липня 1996 року № 270/96-ВР // ВВР, 1996. – № 39. – ст. 181.

8. Про Інтернет рекламу : Проект Закону України від 08 вересня 2008 року № 3126. [Електронний ресурс] – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JF2EU00A.html.

9. Про радіочастотний ресурс України : Закон України від 1 червня 2000 року № 1770-III // Голос України, 2000. – № 36. – ст. 298.

10. Протидія російській інформаційній агресії : спільні зусилля задля захисту демократії. Аналітичний звіт. К. : Телекритика, 2015. 7 с.

11. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 9 січня 2007 року № 537-V // ВВР, 2007. – № 12. – ст. 102;

12. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII // ВВР, 1992, № 48. – ст. 650.

13. Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII // ВВР, 1994. – № 16. – ст. 39.

14. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI // ВВР, 2010. – № 34. – ст. 481.

15. Про доступ до публічної інформації : Закон України від 13 січня 2011 року № 2939-VI // ВВР, 2011 – № 32. – ст. 314.

16. Про Національну програму інформатизації : Закон України від 4 лютого 1998 року № 74/98-ВР // ВВР, 1998. – № 27-28. – ст. 181.

17. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР // ВВР, 1998. – № 27-28. – ст. 182.

18. Про телекомунікації : Закон України від 18 листопада 2003 року № 1280-IV // ВВР, 2004. – № 12. – ст. 155.

19. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР // ВВР, 1994. – № 31.

20. Про захист суспільної моралі: Закон України від 20 листопада 2003 року № 1296-IV // ВВР, 2004. – № 14. – ст. 192.

21. Про Службу безпеки України: Закон України від 25 березня 1992 року № 2229-XII // ВВР, 1992. – № 27. – ст. 38.

22. Про Державну службу спеціального зв'язку та захисту інформації: Закон України від 23 лютого 2006 року № 3475-IV // ВВР, 2006. – № 30. – ст. 258.

23. Про телебачення і радіомовлення: Закон України від 21 грудня 1993 року № 3759-XII // ВВР, 1994. – № 10. – ст. 43.

24. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 року № 287/2015 // Урядовий кур’єр, 2015. – № 95.

25. Про пресу та інші засоби масової інформації: Закон Союзу радянських соціалістичних республік від 12 червня 1990 року № 1552-I // ВВР, 1990. – № 26. – ст.492.

26. Питання діяльності Міністерства інформаційної політики України: Постанова КМУ від 14 січня 2015 р. № 2 // Урядовий кур'єр, 2015. – № 11.

27. Про Міжнародну дорадчу раду: Указ Президента України 16 грудня 2015 року № 706/2015 // Урядовий кур’єр, 2015. – № 237.

28. Кодекс України про адміністративні правопорушення // ВВР, 1984. – додаток до № 51, ст.1122.

29. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене [В. М. Петрик, В. В. Бедь, М. М. Присяжнюк та ін.]; за заг. ред. В. В. Бедь, В. М. Петрика. К.: ПАТ «ВІПОЛ», 2018. 386 с.

30. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. №392/2020.

31. Про основні засади забезпечення кібербезпеки : Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст.403

32. Про основні засади забезпечення кібербезпеки : Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст.403

33. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. №96/2016.

34. Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47.

35. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : указ Президента України від 28.12.2021 р.

36. Воєнна доктрина України: Указ Президента України від 24.09.2015 р. № 555/2015.

37. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. Офіційний вісник України. 26.01.2021 р. № 6, стор. 10, стаття 306.

38. Наказ МОУ Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України

39. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил: Наказ МОУ від 22.11.2017 р. № 612.

40. Проект Указу Президента України про затвердження концепції розвитку стратегічних комунікації сектору безпеки і оборони. [Електронний ресурс] – Режим доступу: https://goal-int.org/proekt-ukazu-prezidenta-ukraini-pro-zatverdzhennya-koncepcii-rozvitku-strategichnix-komunikacii-sektoru-bezpeki-i-oboroni-proekt/.

41. «Про створення Центру протидії дезінформації»: Указ Президента України від 19 березня 2021 року. [Електронний ресурс] – Режим доступу: № 106/2021 https://www.president.gov.ua/documents/1062021-37421.

42. Про Міністерство культури та інформаційної політики України. [Електронний ресурс] – Режим доступу: https://mkip.gov.ua/content/centr-strategichnih-komunikaciy-ta-informaciynoi-bezpeki-pri-ministerstvi-kulturi-ta-informaciynoi-politiki.html

43. Про Український кризовий медіа-центр. [Електронний ресурс] – Режим доступу: https://uacrisis.org/uk/pro-nas.

44. Руснак І.С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18-23.

45. Литвиненко А.В. Специальные информационные операции и пропагандистские кампании: моногр. / А.В. Литвиненко. [Електронний ресурс] – Режим доступу: https://psyfactor.org/infops.htm.

46. Конах В.К. Роль інформаційних операцій та інформаційних воєн у державній політиці США / В.К. Конах // Стратег. панорама. – 2004. – № 1. – С. 164-169.

47. Бойко О. Д. Політичне маніпулювання. / О. Д. Бойко. — К., 2010. — 432 с.

48. Волковский Н. Л. История информационных войн. / Н. Л. Волковский; в 2 ч. — СПб.: Полигон, 2003. — Ч. 1. — 502 с.

49. Інформаційна боротьба: теоретичні та воєнно-прикладні аспекти: навчальний посібник. / [Рось А. О., Явтушенко А. М., Жарков Я. М. та ін.] / за ред. В. Б. Толубка. — Київ: НАОУ, 2003. — 218 с.

50. Ліпкан В. А. Тероризм і національна безпека України / В. А. Ліпкан. — К.: Знання, 2000. — 184 с.

51. Мельник Д. С. Предупреждение манипулирования общественным сознанием с использованием средств массовой информации / [Мельник Д. С., Лашкет Е. С.] // Юридический советник. — 2006. — №3 (11). — С. 133-137.

52. Музичко О. Є. Проросійські суспільно-політичні організації на півдні України як фактор дестабілізації ситуації в регіоні: сучасний стан проблеми та шляхи її вирішення / О. Є. Музичко // Стратегічні пріоритети. — 2006. — № 1. — С. 42-43.

53. Нарис теорії і практики інформаційно-психологічних операцій / [Дзюба М. Т., Жарков Я. М., Ольховой І. О., Онищук М. І.]: навч. посібник / за заг. ред. В. В. Балабіна. — К.: ВІТІ НТУУ «КПІ», 2006. — 468 с.

54. Петрик В. М. Інформаційно-психологічне протиборство (еволюція та сучасність): навч. посіб. / [Петрик В. М., Бакалинський О. О., Жарков Я. М. та ін.] — К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2012. — 248 с.

55. Петрик В. М. Інформаційна безпека держави: підручник/ [Петрик В. М., Присяжнюк М. М., Мельник Д. С. та ін.]; в 2 т. — К.: Вид-во ІСЗЗІ НТУУ «КПІ», 2016. — Т. 1. — 264 с.

56. Почепцов Г. Г. Информация и дезинформация / Г. Г. Почепцов. — К.: Ника-Центр, Эльга, 2001. — 256 с.

57. Техніки маніпуляції. Розпізнавання і протидія / Андреас Ендмюллер, Томас Вільгельм. — «Омега-Л», 2006. — 131 с.

58. Толубко В. Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): монографія / Толубко В. Б. — К.: НАОУ, 2003. — 315 с.

59. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. [Електронний ресурс] – Режим доступу: file:///C:/Users/%D0%97%D0%B0%D0%BC_%D0%BD%D0%B0%D1%87/Desktop/Nvnudpsu_2014_2_10.pdf.

60. Патрикеева Н. Общественный контроль СМИ в Украине: реальное состояние и перспективы. 29-04-2015. [Електронний ресурс] – Режим доступу: http://www.mediakrytyka.info/ohlyady-analityka/hromadskyy-kontrol-zmi-vukrayini-realnyy-stan-ta-perspektyvy.html.

ДОДАТКИ

Додаток А

Пропозиції щодо удосконалення чинного законодавства України з протидії негативному інформаційно-психологічному впливу

Нормативний акт, редакція, виконавці	Пропозиції щодо внесення змін	Вихідний варіант
1	2	3
Положення про Міністерство культури та інформаційної політики України [26] Редакція від 20.03.2018 МІП	Внести зміни до частини 3: Основними завданнями МІП є: 1) забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації та заборони поширення суспільно шкідливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів; 2) забезпечення здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації та заборони поширення суспільно шкідливої інформації шляхом видання актів Міністерства інформаційної політики які реалізують рішення Міжнародної дорадчої ради та є обов'язковими до виконання особою, що зазначена виконавцем в акті, протягом 48 годин. Виконавцями актів Міністерства інформаційної політики можуть бути: Засоби масової інформації; оператори телекомунікацій з надання послуг доступу до Інтернету.	Частина 3: Основними завданнями МІП є: 1) забезпечення формування та реалізація державної політики у сферах інформаційного суверенітету України та інформаційної безпеки, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами; 2) забезпечення здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації.

1	2	3
	Внести зміни до пункту 5 частини 4. МІП відповідно до покладених на нього завдань: 5) здійснює нормативно-правове регулювання у сфері забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації та заборони поширення суспільно шкідливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів.	Пункт 5 частини 4. МІП відповідно до покладених на нього завдань: 5) здійснює нормативно-правове регулювання у сфері забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів.
Положення про Міжнародну дорадчу раду [27] Редакція від 13.05.2020 Міжнародна дорадча рада, МІП	Внести зміни до абзацу 2 частини 7: У разі потреби рішення Ради реалізуються шляхом видання актів Президента України. В сфері забезпечення інформаційної безпеки рішення Ради реалізуються шляхом видання актів Міністерства інформаційної політики, що є обов’язковими до виконання особою, що зазначена виконавцем в акті, протягом 48 годин.	Абзац 2 частини 7. У разі потреби рішення Ради можуть реалізовуватися шляхом видання актів Президента України.
Кодекс України про адміністративні правопорушення [28] Редакція від 06.11.2022 Правоохоронні органи, Національна комісія, що	Додати 5 та наступні частини, включити статтю 164^9 в наданій редакції. Незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних: Поширення примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз	3 та наступні частини відсутні та пропонується вперше.

1	2	3
здійснює державне регулювання в сфері зв’язку та інформатизації	даних, реклами що містить інформацію, заборонену актами Міністерства інформаційної політики через мережу Інтернет шляхом невиконання даних актів у встановлений строк операторами телекомунікацій з надання послуг доступу до Інтернету – тягне за собою накладення штрафу від тисячі неоподатковуваних мінімумів доходів громадян та попередження про припинення ліцензії. Та сама дія, вчинена особою, яку протягом року було піддано адміністративному стягненню за одне з правопорушень, зазначених у частині п’ятій цієї статті, –тягне за собою накладення штрафу у подвійному розмірі із припиненням ліцензії.	
Положення про Національну комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації Редакція від 11.11.2014	Додати пункт до частини 4 статті 38: Повноваженнями національної комісії є: заборона ретранслювати радіохвилі та супутниковий сигнал, що надходять з країн, які загрожують національній безпеці наявним інформаційним конфліктом.	Даний пункт в частині 4 статті 38 відсутній та пропонується вперше.
Закон України Про телебачення і радіомовлення [23] Редакція від 19.11.2022	Внести зміни до пункту 4 статті 4: Основні принципи державної політики у сфері телебачення і радіомовлення: Держава не чинить перепон	Пункт 4 статті 4. Держава не чинить перепон прямому прийому телевізійних і радіопрограм та передач з інших країн, які

Національна рада України з питань телебачення і радіомовлення	прямому прийому телевізійних і радіопрограм та передач з інших країн, які транслюються мовою національної меншини або подібною до неї регіональною мовою, окрім передач, що надходять з країн, які загрожують національній безпеці наявним інформаційним конфліктом.	транслюються мовою національної меншини або подібною до неї регіональною мовою.
	Внести зміни до пункту 1 статті 42: Ретрансляція телерадіопрограм та передач. Ретрансляція телерадіопрограм та передач, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення, на території України не обмежується. Забороняється ретрансляція телерадіопрограм та передач, зміст яких загрожує національній безпеці наявним інформаційним конфліктом з країною походження. Порядок ретрансляції регулюється цим Законом.	Пункт 1 статті 42. Ретрансляція телерадіопрограм та передач, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення, на території України не обмежується. Порядок ретрансляції регулюється цим Законом.
Закон України Про рекламу [7] Редакція від 10.10.2022 Центральний орган виконавчої влади, що реалізує державну політику у сфері державного контролю за додержанням законодавства	Внести правки відповідно до законопроекту «Про Інтернет рекламу»; Додати пункти у частину 1 статті 8: У рекламі забороняється: • поширювати інформацію щодо товарів, на які розповсюджуються обмеження, встановлені законодавством та/або виробником послуги, товару чи контенту на ресурсах, на які не розповсюджуються відповідні вікові обмеження; • застосування в Інтернеті	Дані пункти у частині 1 статті 8 відсутні та пропонуються вперше.

про захист прав споживачів - щодо захисту прав споживачів реклами.	аудіо-супроводу реклами по замовченню, без дозволу користувача;	
	У статтю 8 додати частини: • Забороняється розміщення динамічної банерної реклами на сторінці таким чином, за якого вона перекриватиме частину сторінки інтернет-ресурсу, де розміщена основна інформація. Забороняється розміщати рекламу на Інтернет-ресурсі таким чином, щоб вона займала більше, ніж 25% від загальної площі розміру екрану монітору, крім Інтернет-ресурсів, що не займаються іншою діяльністю крім розміщення реклами.	Дані частини в статті 8 відсутні та пропонуються вперше.
	Внести зміни до абзацу 5 частини 4 статті 27: Повторне вчинення перелічених порушень протягом року тягне за собою накладення штрафу у подвійному від передбаченого за ці порушення розмірі. Для інтернет-реклами – обмеження доступу інтернет-ресурсу порушника до мережі Інтернет шляхом видання актів Міністерства інформаційної політики на термін, визначений актом.	Абзац 5 частини 4 статті 27: Повторне вчинення перелічених порушень протягом року тягне за собою накладення штрафу у подвійному від передбаченого за ці порушення розмірі.