КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Навчально-науковий інститут
міжнародних відносин

ОКСАНА ЗАПОРОЖЕЦЬ

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Навчальний посібник

2-е видання

Київ
VADEX
2025

УДК 327:316.77(075.8)
З-33

Рекомендовано до друку
Вченою радою Навчально-наукового інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка
протокол №14 від 10 червня 2025 року

Рецензенти:
Надія БІЛАН – доктор наук із соціальних комунікацій, Київський національний університет імені Тараса Шевченка.
Ніна РЖЕВСЬКА – доктор політичних наук, Державний університет «Київський авіаційний інститут».

Запорожець О. Ю.
Технології інформаційного протиборства : навчальний посібник. 2-ге вид., випр. і допов. Київ : ВАДЕКС, 2025. 167 с.

ISBN 978-966-972-128-0

Навчальний посібник присвячено концептуальним та прикладним аспектам інформаційного протиборства в системі сучасних міжнародних відносин. У виданні проаналізовано американську та китайську доктрини інформаційної війни, а також охарактеризовано сучасні технології впливу: від класичної пропаганди й дезінформації до складних кібератак та методів онлайн-астротурфінгу. Навчальний матеріал структуровано таким чином, що кожен розділ доповнено питаннями та практичними завданнями, спрямованими на закріплення знань і розвиток аналітичних навичок.

Для студентів закладів вищої освіти, науковців, фахівців у галузі міжнародних відносин та безпеки, а також усіх, хто цікавиться проблематикою інформаційних війн у сучасному світі

ISBN 978-966-972-128-0

ЗМІСТ

ПЕРЕДМОВА

У сучасному світі інформація перетворилась на потужну зброю, а інформаційний простір – на поле бою. Інформаційне протиборство (information warfare) сьогодні має місце не лише під час військових кампаній, але й у мирний час.

Протистояння в інформаційному просторі характеризується комплексним впливом як на громадську думку країни-об'єкта впливу, так і на об'єкти інформаційної інфраструктури. Специфіка інформаційної війни – відсутність видимих фізичних руйнувань, багатовимірність і множинність впливу на масову свідомість, що може спричинити незворотні і вкрай негативні наслідки для країни-об'єкта впливу. До того ж, технології інформаційного протиборства стрімко розвиваються, стаючи більш витонченими, різноплановими та таргетованими, що ускладнює їх своєчасну ідентифікацію, і підвищує вразливість будь-якого суспільства до зовнішніх інформаційних впливів.

Розуміння технологій ведення інформаційного протиборства, здатність виявляти і не піддаватись методам маніпулювання масовою свідомістю є надзвичайно важливими навичками у 21 столітті, формуючи суспільний «імунітет» до небажаних (деструктивних) інформаційних впливів з боку тих чи інших акторів міжнародних відносин.

Навчальний посібник присвячено теоретичним і прикладним аспектам ведення інформаційного протиборства у сучасних міжнародних відносинах.

Навчальний посібник складається з трьох розділів. У першому розділі охарактеризовано американський та китайський підходи до інформаційної війни, а також розглянуто специфіку операцій впливу. Другий розділ присвячено таким технологіям інформаційно-психологічного впливу, як пропаганда, дезінформація та рефлексивне управління. У третьому розділі представлено інструментарій інформаційного протиборства у кіберпросторі. Матеріал для розділу

підібрано так, щоб показати два аспекти використання кіберпростору в інформаційних війнах – інформаційно-технічний (кібератаки) та інформаційно-психологічний (інтернет-меми, онлайн астротурфінг). В розділах теоретичний матеріал підкріплено прикладами із сучасних міжнародних відносин. Кожний підрозділ містить питання для самоконтролю та практичні завдання.

Посібник призначено для викладачів і студентів вищих навчальних закладів, а також всіх, хто цікавиться темою інформаційних війн у міжнародних відносинах.

РОЗДІЛ 1.
КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

1.1. Американська концепція інформаційної війни

Вперше термін «інформаційна війна» (information warfare) було використано Томасом Рона у звіті «Системи зброї та інформаційна війна», підготовленому ним у 1976 році для компанії «Боїнг». У публікації Томаса Рона приділено увагу таким актуальним аспектам інформаційної війни, як збільшення обсягу власної інформації, створення перешкод для супротивника у доступі до правдивої інформації, розміщення в інформаційних потоках супротивника фальшивої інформації, що здається правдивою.

Томас Рона зазначав, що вплив на інформаційні потоки супротивника може призвести, зокрема, до того, що супротивник зрозуміє неадекватність своїх знань, а завдяки цій невизначеності утримається від агресивних дій [1].

Звіт Т. Рона зацікавив американських фахівців, передусім військових.

Офіційно термін «інформаційна війна» було введено в обіг Міністерством оборони США після операції «Буря в пустелі» 1991 року.

У грудні 1992 року основні положення концепції інформаційного протиборства було відображено у директиві міністра оборони США № TS-3600.1 «Інформаційна війна». Ідея інформаційної війни була сформульована у вигляді концепції «боротьби із системами управління» (БСУ).

БСУ – це комплексне проведення за єдиним задумом та планом психологічних операцій, заходів з оперативного маскування, радіоелектронної боротьби та фізичного знищення пунктів управління і систем зв'язку, з метою позбавлення супротивника інформації, виведення з ладу або знищення його систем управління при одночасному захисті своїх від аналогічних дій з боку супротивника [2].

В офіційних документах 1996 та 1998 років введено термін «інформаційна операція» як більш широке поняття, ніж «боротьба з системами управління».

Завдання БСУ – боротьба з системами управління і зв'язку як з цільовими об'єктами, а мета проведення інформаційних операцій – вплив на інформаційні системи супротивника і інформацію, що циркулює в них. Під час проведення інформаційних операцій БСУ інтегрується в них і стає невід'ємною складовою таких операцій.

За американським підходом, інформаційна війна реалізується у формі інформаційних операцій, які мають наступальний та оборонний аспекти. Наступальні інформаційні операції передбачають реалізацію комплексу заходів, спрямованих на здійснення впливу на свідомість людей, порушення процесу прийняття рішень супротивника, а також на виведення з ладу об'єктів інформаційної інфраструктури. Оборонні інформаційні операції передбачають заходи щодо захисту інформаційного середовища, розкриття ознак нападу, відновлення боєздатності та організації дій у відповідь на атаку [2].

1996 року на замовлення Міністерства оборони США експерти американської корпорації «RAND» представили звіт, в якому запроваджено термін Strategic Information Warfare – «стратегічне інформаційне протиборство». Суть такого протиборства полягає у «використанні державами глобального інформаційного простору та інфраструктури для проведення стратегічних військових операцій і зменшення впливу на власний інформаційний ресурс»[3]. Автори звіту виокремили стратегічне протиборство першого і другого покоління.

Стратегічне інформаційне протиборство першого покоління спрямоване на дезорганізацію функціонування систем управління і проводиться на підтримку дій традиційних сил і засобів. Основними завданнями інформаційного протиборства першого покоління є: вогняне придушення елементів інфраструктури державного та військового управління; ведення радіоелектронної боротьби; отримання розвідувальної інформації шляхом перехоплення і розшифровки інформаційних потоків; здійснення несанкціонованого

доступу до інформаційних ресурсів з наступним їх спотворенням або викраденням; формування і масове поширення дезінформації через інформаційні канали супротивника тощо.

Стратегічне інформаційне протиборство другого покоління – це принципово новий тип стратегічного протиборства, що включає у коло можливих сфер протиборства інформаційний простір та низку інших галузей (насамперед, економіку), і буде здійснюватися тривалий час. Розвиток стратегічного інформаційного протиборства ІІ покоління у перспективі може призвести до повної відмови від використання військової сили.

В рамках інформаційного протиборства другого покоління вирішуються такі завдання: створення атмосфери бездуховності, негативного ставлення до культурної спадщини супротивника; маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни для створення політичної напруги і хаосу; зниження рівня інформаційного забезпечення органів влади та управління; дезінформування населення про роботу державних органів, підрив їхнього авторитету; провокація соціальних, політичних, національних та релігійних конфліктів; ініціювання страйків, масових заворушень та інших акцій економічного протесту; ускладнення прийняття органами управління важливих рішень; підрив міжнародного авторитету держави, його співпраці з іншими країнами; нанесення шкоди життєво важливим інтересам держави у політичній, економічній, оборонній та інших сферах [3].

У 1998 році Міністерством оборони США затверджено «Об'єднану доктрину інформаційних операцій», в якій інформаційна війна визначається як комплексний вплив (сукупність інформаційних операцій) на систему державного та військового управління супротивника, на його військово-політичне керівництво, що вже у мирний час сприяв би ухваленню бажаних для країни-ініціатора інформаційного впливу рішень, а під час конфлікту повністю паралізував би функціонування інфраструктури управління супротивника [4].

Інформаційна війна реалізується на двох рівнях: державному та військовому.

На державному рівні мета інформаційної війни полягає у послабленні позицій конкуруючих держав, порушенні системи державного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери суспільного життя.

На військовому рівні інформаційна війна є складовою частиною військових кампаній і спрямована на досягнення інформаційної переваги шляхом впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації, інформаційних систем та інфраструктури [4].

Інформаційна перевага визначається як здатність збирати, обробляти та розподіляти безперервний потік інформації про ситуацію, перешкоджаючи супротивнику робити те ж саме.

Надалі в офіційних документах ЗС США термін «інформаційна війна» було замінено терміном «інформаційна операція» (ІО). Це зумовлено тим, що інформаційна війна фактично означає протистояння під час військової кампанії, у той час як інформаційні операції можуть проводитись як у воєнний, так і мирний час.

У документі 2000 року «Єдина перспектива-2020» (Joint Vision 2020) інформаційні операції визначаються як ефективний вплив на інформацію та інформаційні системи супротивника з одночасним захистом інформації та інформаційних систем американських збройних сил.

До інформаційних операцій, згідно з документом, відноситься будь-яка діяльність у небойових ситуаціях щодо захисту інформації та інформаційних систем держави, а також здійснення негативного впливу на можливість і процес виявлення інформації та інформаційних систем супротивником. Інформаційні операції можуть проводитися у мирний час, у кризовій ситуації та під час будь-якого конфлікту [5].

У Доктрині Повітряних сил США 2-5 «Інформаційні операції» (Air Force Doctrine Document 2-5 «Information operations») від 2005 року

інформаційні операції визначаються як заходи, що застосовуються для впливу на ворожу інформацію або інформаційну систему при одночасному захисті власної інформації та інформаційних систем [6].

В офіційному документі Збройних сил США 3-13 «Інформаційні операції» (Joint publication 3-13 «Information operations») від 2006 року представлено більш чітке визначення інформаційних операцій, визначено основні та допоміжні компоненти інформаційних операцій.

Згідно з документом, ІО – це інтегроване використання можливостей радіоелектронної боротьби, комп'ютерних мережевих операцій, психологічних операцій, операцій з введення в оману та операцій безпеки, з метою здійснення впливу, порушення процесу прийняття рішень супротивником при одночасному захисті власного (рішення) [6].

Кінцевою стратегічною метою інформаційних операцій є стримування потенційного або явного супротивника чи інші цільові аудиторії від вживання дій, які шкодять національним інтересам держави.

За доктриною, ключову роль у проведенні інформаційних операцій відіграють психологічні операції.

Психологічні операції (ПсО) – заходи з поширення спеціально підготовленої інформації, з метою впливу на емоційний стан, мотивацію й аргументацію дій, прийняття рішень й поведінку окремих керівників, організацій, соціальних або національних груп й окремих особистостей іноземних держав у сприятливому для країни-ініціатора та її союзників напрямку [7].

У Польовому статуті Армії США FM 33-1 ПсО визначаються як планова пропагандистська діяльність, націлена на іноземні ворожі, дружні або нейтральні аудиторії, з метою впливу на їхнє ставлення і поведінку у сприятливому напрямі для досягнення політичних та військових цілей держави.

Згідно зі Статутом, ПсО реалізуються на трьох рівнях [4].

Стратегічні психологічні операції здійснюються в інтересах досягнення довгострокових цілей, покликаних створити сприятливу

психологічну обстановку для ведення військових дій. Такі операції зазвичай мають глобальний характер.

Оперативні психологічні операції здійснюються в інтересах досягнення середньострокових цілей, на підтримку військових кампаній. Об'єктом таких операцій зазвичай є населення певного регіону.

Тактичні психологічні операції здійснюються в інтересах досягнення короткострокових цілей, на підтримку командирів тактичної ланки. Об'єктом таких операцій є окреме угруповання військ супротивника.

Наступним основним компонентом інформаційних операцій є **операції з введення в оману** (оперативне маскування) – це заходи, призначені для навмисного введення в оману військового керівництва супротивника щодо військових можливостей, намірів та операцій, аби спонукати супротивника до дій, які сприятимуть досягненню поставлених цілей [7].

Операції з введення в оману ґрунтуються на розумінні того, як командування супротивника мислить і планує дії, та як використовує інформаційний менеджмент для підтримки своїх зусиль.

Варто зазначити, що військові операції з введення в оману не обмежуються поширенням дезінформації. Для введення в оману використовуються різні стратагеми (військова хитрість), такі як маскування, макети, мімікрія, «інформаційне перевантаження» (перевантаження супротивника неважливою інформацією) тощо [8].

Для маскування військ та об'єктів використовуються захисні властивості місцевості, підручні матеріали, спеціальне фарбування бойової техніки, що спотворює видимий силует об'єктів тощо.

Макети призначені для демонстрації фальшивої мішені, яку ворог має атакувати. Макети відволікають увагу від реальних об'єктів. Наприклад, під час військової операції НАТО у Косово у 90-х роках 20 століття літаки НАТО декілька разів вражали макет мосту, створений сербами з поліетиленової плівки. Макет захищав від повітряних атак справжній міст, розташований за 300 метрів від фальшивого.

Мімікрія націлена на те, щоб представити щось чимось іншим, шляхом копіювання характеристик реального об'єкта. Прикладом успішного використання даного метода є операція «Фортитюд» під час Другої світової війни. Під час цієї операції англійці разом з американцями створили фіктивне військове угруповання США, аби посилити переконання німців про плани союзників зробити висадку у Па-де-Кале.

Важливим компонентом інформаційних операцій є **комп'ютерні мережеві операції** (кібероперації), що включають комп'ютерні мережеві атаки, мережевий захист та використання комп'ютерних мереж супротивника у своїх цілях [7].

Комп'ютерні мережеві атаки визначаються як дії, що реалізуються у відповідних мережах для пошкодження або знищення важливої інформації у комп'ютерах та комп'ютерних мережах або ж виведення з ладу самих комп'ютерів супротивника.

Під мережевим захистом розуміються заходи, що передбачають моніторинг та аналіз мережевих атак на комп'ютерні об'єкти Міністерства оборони США та захист від них.

До основних компонентів ІО, відповідно до американської доктрини, також відноситься **радіоелектронна боротьба**, яка включає радіоелектронне придушення і радіоелектронний захист.

Суть радіоелектронного придушення полягає у порушенні або ускладненні функціонування електронних засобів супротивника шляхом випромінювання, відображення електромагнітних, акустичних та інфрачервоних сигналів. РЕБ здійснюється автоматично, наземними, корабельними та авіаційними системами постановки перешкод.

Радіоелектронний захист передбачає такі дії, як захист своїх радіоелектронних засобів (РЕЗ) від перешкод, створюваних супротивником, і здійснення контролю за роботою РЕЗ союзників, з метою уникнення їхнього взаємного впливу один на одного.

Ще одним ключовим компонентом ІО є **операції безпеки** – процес ідентифікації критичної інформації та подальшого аналізу дій,

спрямованих на визначення даних, необхідних супротивнику для отримання точної інформації про сили і наміри союзників; заперечення критичної інформації супротивника про сили і наміри союзників; спонукання супротивника недооцінювати доречність відомої йому критичної інформації [7].

Планування операції безпеки передбачає реалізацію таких кроків:

1. *Ідентифікація критичної інформації*: визначення інформації, необхідної супротивнику.

2. *Аналіз загроз*: аналіз розвідувальних, контррозвідувальних та відкритих джерел інформації для виявлення потенційних супротивників планованої операції.

На цьому етапі потрібно відповісти на такі питання:

(a) Хто супротивник?

(b) Які цілі має супротивник?

(c) Яка стратегія у супротивника?

(d) Якою критичною інформацією володіє супротивник про операцію?

(e) Які розвідувальні можливості має супротивник?

3. *Аналіз вразливостей*: аналіз кожного аспекту операції для виявлення індикаторів, які можуть розкрити критичну інформацію та порівняння цих індикаторів з розвідувальними можливостями супротивника.

Індикатори – це дії та інформація з відкритих джерел, що можуть бути виявлені розвідкою супротивника та на основі яких супротивник може отримати критичну інформацію.

4. *Оцінка ризику*: визначення можливих заходів захисту для кожної вразливості; відбір конкретних заходів для реалізації, спираючись на результати оцінки ризиків.

5. *Застосування відповідних заходів безпеки*. Під час впровадження вибраних заходів відстежується реакція супротивника та оцінюється ефективність заходів.

В операціях безпеки використовуються такі заходи, як диверсії, маскування, приховування намірів, маніпулювання інформацією для введення в оману тощо.

Операції з введення в оману та операції безпеки доповнюють один одного. Операції з введення в оману спрямовані на те, щоб підштовхнути до неправильного аналізу і змусити супротивника дійти помилкових висновків. Операції безпеки передбачають заперечення достовірної інформації та запобігання вірної оцінки супротивником планів країни-ініціатора.

Допоміжними елементами інформаційних операцій є безпека інформації (Information Assurance), фізична безпека (Physical security), фізична атака (Physical Attack) на критично важливі об'єкти інформаційної інфраструктури супротивника та контррозвідка (Counterintelligence) [4].

Безпека інформації – це заходи щодо захисту інформації та інформаційних систем шляхом забезпечення їхньої доступності, цілісності, автентичності, конфіденційності та непідробленості.

Фізична безпека – це заходи щодо захисту персоналу, попередження неавторизованого доступу до обладнання, різним об'єктам, документам та захист їх від шпигунства, саботажу, пошкоджень і крадіжки.

Фізична атака може здійснюватись на підтримку ІО як засіб атаки на системи управління супротивника, аби вплинути на його здатність здійснювати управління і впливати на цільові аудиторії.

Контррозвідка – це збір інформації та діяльність, спрямована на захист від шпіонажу, інших дій розвідки, саботажу або вбивств, замовлених або здійснених від імені іноземних урядів, іноземних організацій або міжнародних терористичних груп.

Загалом, допоміжні компоненти ІО мають військові цілі, відмінні від цілей ІО, але вони або діють в інформаційному середовищі, або впливають на нього.

Доктрина Збройних сил США «Інформаційні операції» від 2012 року містить більш загальне визначення ІО: «інформаційні операції –

це інтегроване застосування під час військових операцій можливостей, що стосуються інформації, разом з іншими засобами операції, з метою впливу, руйнування, завдання шкоди, захоплення процесу ухвалення рішення супротивником при одночасному захисті власного» [6].

При цьому під можливостями, що стосуються інформації, розуміють інструмент, технологію або діяльність в інформаційному середовищі, які можуть бути використані для створення сприятливих умов проведення операції.

У документі охарактеризовано такі можливості, як зв’язки з громадськістю, військово-цивільні операції, психологічні операції, кібероперації, операції з введення в оману, радіоелектронна боротьба, операції безпеки, безпека інформації, фізична атака, фізична безпека, розвідка, космічні операції, залучення ключових лідерів тощо [7].

Згідно з документом, *зв’язки з громадськістю* - це комунікація Міністерства оборони США із зовнішньою і внутрішньою аудиторіями. Для цього використовується публічна інформація, інформація командування та взаємодія з місцевою аудиторією. Публічна інформація спрямована на інформування зовнішньої аудиторії. Інформація командування орієнтована на внутрішню аудиторію – солдатів, цивільних осіб Міністерства оборони та членів їх сімей. Зв'язки із громадськістю сприяють зміцненню довіри до армії та підвищенню її готовності проводити наземні операції.

Військово-цивільні операції – діяльність Міністерства оборони США, що реалізується відповідними цивільними чи військовими силами, спрямована на встановлення і підтримку відносин між збройними силами і населенням іноземної держави.

Під час військово-цивільної операції здійснюються такі заходи, як інформування населення про проведення операції, виправлення дезінформації та ворожої пропаганди, збір інформації про настрої місцевого цивільного населення тощо [7].

Кібероперації - це використання можливостей кіберпростору, де основною метою є досягнення цілей через кіберпростір. Кібероперації

зазвичай зосереджуються на інтеграції наступальних і оборонних можливостей, реалізованих у кіберпросторі і через нього.

Космічні операції підтримують ІО за допомогою функцій спостереження та розвідки космічних сил, попередження про ракетний напад, моніторингу довкілля, супутникового зв'язку; космічного позиціонування та навігації тощо.

Розвідка полегшує розуміння взаємозв'язку між фізичними, інформаційними та когнітивними вимірами інформаційного середовища. Розвідка передбачає використання різних інструментів для аналізу інформаційного середовища та виявлення уразливостей цільових аудиторій [7].

Операції з введення в оману націлені на те, щоб не просто ввести в оману, а підштовхнути супротивника до поведінки, вигідної суб'єкту впливу, наприклад, неправильно розподіляти ресурси, атакувати у той час і в місці, які є вигідними для країни-суб'єкта впливу, або взагалі уникати дій.

Залучення ключових лідерів (Key Leader Engagement) – сплановані зустрічі між військовими лідерами США та лідерами іноземної аудиторії, які прагнуть досягти певних цілей (наприклад, змінити політику країни). Така взаємодія може використовуватись для впливу на іноземних лідерів на стратегічному, оперативному і тактичному рівнях, а також може бути спрямована на певні групи, зокрема лідерів думок, аби, наприклад, посилити довіру до Збройних Сил США [7].

У документі Збройних Сил США ATP 3-13.1 The Conduct of Information Operations 2018 року, що містить інструкції з проведення інформаційних операцій, інструментарій ІО доповнено бойовою камерою, спеціальними технічними операціями, операціями із залучення солдат та поліцейських, а також заходами із забезпечення присутності та позиціонування збройних сил [9].

Бойова камера забезпечує оперативну зйомку, надає зображення, що підтримують стратегічний, оперативний та тактичний рівні війни, прискорює ухвалення рішень, а також сприяє вертикальному та горизонтальному потоку інформації.

Спеціальні технічні операції - це секретні операції, у яких використовуються спеціальні технічні можливості для здобуття вирішальної переваги над супротивником.

Залучення солдат і лідерів передбачає міжособистісну взаємодію військовослужбовців з аудиторією у районі операцій. Такі операції можуть проводитись особисто або дистанційно, за допомогою інформаційних технологій. Основна мета таких заходів – поширити заздалегідь розроблені повідомлення (на підтримку зв'язків з громадськістю або ПсО) для підвищення довіри до військових та посилення легітимності операцій збройних сил.

Залучення поліції відбувається серед співробітників поліції, організацій та населення, з метою підтримки громадського порядку. Військова поліція та співробітники Управління кримінальних розслідувань армії США взаємодіють із поліцією союзників, місцевою поліцією, цивільними лідерами та місцевим населенням для отримання важливої інформації, яка може вплинути на воєнні операції. Участь поліції спрямована на створення регулярної та надійної міжособистісної мережі, через яку важлива інформація може надходити до військової поліції.

Присутність та позиціонування військових. Проста присутність військових може суттєво вплинути на всю аудиторію у районі проведення операції. Розміщення, переміщення або спрямування військ у потрібне місце, у потрібний час може підвищити довіру до повідомлень, що доставляються іншими каналами, і зробити важливий внесок у стримування супротивника. Присутність може бути загрозливою або обнадійливою, залежно від ситуації. Потрібний ефект досягається завдяки ретельному і грамотному розрахунку кількості військ, їхнього позиціонування та діяльності.

Отже, за американським підходом, інформаційна війна є комплексним явищем, що передбачає скоординоване і чітко сплановане використання технологій психологічного впливу у поєднанні з інструментами впливу на об’єкти інформаційної інфраструктури супротивника, з метою зміни його поведінки у

сприятливому для суб'єкта впливу напрямі. Інформаційна війна реалізується у формі інформаційних операцій, які поєднують наступальний та оборонний аспекти. Ядром інформаційних операцій є зазвичай психологічні операції, операції з введення в оману, кібероперації та операції безпеки.

Питання для самоконтролю:

1. Як американські військові визначають термін "інформаційна війна"?
2. Якими є цілі інформаційної війни на державному та військовому рівнях за американським підходом?
3. З якого року американські військові почали використовувати термін "інформаційні операції" замість терміну "інформаційна війна"? Чому?
4. Що таке "інформаційна операція"?
5. Якими є основні та допоміжні компоненти інформаційної операції згідно з Доктриною інформаційних операцій 2006 року?
6. Яке значення мають допоміжні компоненти інформаційних операцій?
7. Які компоненти інформаційних операцій визначено в офіційних документах США 2012-2018 років?
8. Як взаємопов'язані психологічні операції та операції з введення в оману?
9. Як доповнюють один одну операції з введення в оману та операції безпеки?

Завдання:

1. Пояснити взаємозв’язок/співвідношення понять: інформаційна війна, інформаційна операція, психологічна операція, пропаганда, оперативне маскування, кібероперація, операція безпеки.
2. Пояснити спільні риси і відмінності між поняттями «інформаційна операція», «інформаційна кампанія», «піар-кампанія». Підтвердити прикладами.
3. Навести приклади психологічної операції, операції з введення в оману та кібероперації.
4. Навести приклади наступальних та оборонних інформаційних операцій у 21 столітті.
5. Навести приклади інформаційних операцій будь-яких країн під час конфлікту та у мирний період.

1.2. Китайська концепція інформаційного протиборства

З давніх часів Китай приділяє значну увагу технологіям маніпулювання масовою свідомістю. За оцінками дослідників, Китай має довгу історію ведення психологічних операцій – близько чотирьох тисяч років.

Сьогодні КНР вважається серйозним конкурентом США у веденні інформаційної війни. Спираючись на американський досвід, державне керівництво Китаю розробляє і впроваджує власні концепції та підходи до ведення інформаційної війни, що дали б змогу здобути переваги в інформаційній конфронтації та реалізувати стратегічно важливі національні інтереси і цілі.

Відомим стародавнім китайським джерелом, що містить китайські уявлення про війну та різні способи впливу на психіку і поведінку супротивника є стародавній трактат китайського мислителя Сунь-Цзи «Мистецтво війни».

Як зазначав Сунь-Цзи, мистецтво полководця полягає у досягненні перемоги над супротивником без застосування військової сили: «у війні, як правило, найкраща політика зводиться до захоплення держави цілісною; зруйнувати її значно легше. Взяти у полон армію супротивника краще, ніж її знищити. Підкорити супротивника без бою – це вершина мистецтва» [10].

Сунь-Цзи також вважав, що війна – це шлях обману, постійної організації хибних випадів, поширення дезінформації, використання хитрощів. Він виокремив такі способи психологічного впливу на супротивника: «розкладайте все гарне, що є в країні вашого супротивника»; «втягуйте провідних представників вашого супротивника у злочинну діяльність»; «використовуйте співробітництво самих підлих і мерзенних людей»; «розпалюйте сварки і зіткнення серед громадян ворожої країни»; «підбурюйте молодь проти старих»; «заважайте всіма способами діяльності уряду»; «перешкоджайте всіма способами оснащенню, забезпеченню і наведенню порядку у збройних силах»; «послаблюйте волю

супротивника безглуздими піснями і музикою»; «знецінюйте всі традиції ваших ворогів»; «будьте щедрі на пропозиції і подарунки для покупки інформації та спільників» [10].

Сучасна концепція ведення інформаційної війни почала розроблятися у Китаї у 90-х роках 20 століття.

Китайські дослідники визначають інформаційну війну як усі види військової діяльності, що передбачають руйнування і паралізацію інформаційних систем (ІС) супротивника з одночасним захистом власних ІС [11, 12].

У широкому значенні суть інформаційного протиборства полягає у тому, що обидві сторони ведуть боротьбу одна проти одної у політичній, економічній, культурній, науковій, соціальній та технологічній сферах. Боротьба ведеться за інформаційний простір та ресурси.

Основна мета – інформаційне домінування, яке означає здатність захищати свою інформацію й атакувати інформаційну інфраструктуру супротивника.

Зміст інформаційної війни полягає у боротьбі за здобуття і збереження ініціативи в отриманні, контролі та використанні інформації. Інформаційна війна спрямована, насамперед, на системи управління супротивника, аби підірвати готовність осіб, які приймають рішення, чинити опір.

Інформаційна війна реалізується у формі інформаційних операцій (ІО). За визначенням колишнього директора департаменту комунікацій Народно-визвольної армії Китаю генерала Дай Цінміна (Dai Qingmin), інформаційна операція - це комплекс заходів в інформаційному середовищі, націлених на воєнну інформацію та інформаційну систему, що проводяться у формі електронної війни і комп'ютерної мережевої війни. Такі операції засновані на знаннях і стратегіях. До таких стратегій, зокрема, відносяться:

- саботування ворожої інформації чи інформаційної системи;
- послаблення ворожих можливостей проводити інформаційну боротьбу;

- розсіювання сил ворога з одночасною концентрацією власних військ;
- відволікання уваги ворога і створення сприятливих бойових можливостей для себе;
- створення у ворога помилкового враження, що супроводжується раптовою інформаційною атакою на нього;
- спонукання ворога повірити, що правда- це брехня, а брехня – це правда;
- спонукання ворога до помилкового судження або дії [12].

Китайські експерти запозичили низку положень американської концепції інформаційної війни. Це стосується основної мети інформаційної війни (інформаційне домінування) і компонентів інформаційних операцій. Так, основними компонентами ІО, за китайською концепцією, є:

1. Фізичні атаки, в яких використовується високоточна зброя для знищення інформаційної інфраструктури супротивника;
2. Радіоелектронна боротьба – застосування електромагнітної зброї для впливу на системи збору інформації та розвідданих;
3. Комп'ютерні мережеві операції, що проводяться у формі хакерських атак та віртуальної війни (введення в оману супротивника за допомогою симульованих неправдивих команд);
4. Психологічні операції і введення в оману - поширення інформації або дезінформації для впливу на емоції, погляди та поведінку цільової аудиторії [11,12].

Водночас, китайський підхід до інформаційного протиборства має низку специфічних рис. Перш за все, Китай прагне до більшого впливу при мінімальних витратах. Метою інформаційної війни є не перемога над супротивником будь-якою ціною, а досягнення панування, виживання і процвітання власного народу. Супротивник не знищується, а його ресурси та можливості використовуються для задоволення державних інтересів і потреб.

Замість нарощування потужності технічних засобів Китай докладає зусиль для досягнення сприятливого розвитку подій та їхнього позитивного результату. Пріоритетними напрямами діяльності Китаю є накопичення значущої інформації, захист власної інформації, осіб, які приймають рішення, та національної єдності.

Крім того, Китай намагається приховати свої власні наміри від світової громадськості.

Специфічною рисою є також поєднання концепції «народної війни» з інформаційною війною.

Народна війна – це воєнно-політична стратегія, сформульована Мао Дзедуном. Основна ідея – заручитися підтримкою населення, затягти ворога у глибокий тил, де населення вимотає його партизанською війною. Народна війна передбачає уникнення прямих зіткнень із сильним ворогом, натомість надається перевага стратегії затяжної війни з ретельним вибором поля бою, на якому можна здобути перемогу.

Ідея поєднання народної війни з інформаційною втілюється у життя у півторамільйонних резервних силах Китаю. Народно-визвольна армія Китаю (НВАК) перетворює резервні сили деяких районах на міні полки ІО. Так, в окрузі Ечен, провінція Хубей, НВАК створила резервний полк мережевих операцій, об'єднавши в нього близько 20 міських управлінь. У 2003 році в Гуанчжоу були сформовані загони «міської міліції» з ІО, куди набирали не лише висококваліфікованих ІТ-фахівців, а й усіх, хто мав навички роботи з комп'ютером [12, 13].

Характерною рисою китайського підходу до інформаційного протиборства є особлива увага використанню мережі Інтернет. Фахівці Народно-визвольної армії Китаю (НВАК) визначили п'ять основоположних принципів досягнення перемоги у «мережевих війнах», а саме: позбавлення живлення головного комп'ютера мережі супротивника; удар по ключовим елементам мережі управління театром воєнних дій (система дистанційної розвідки, система зв'язку, система обробки даних, система управління військами та зброєю

тощо); перевантаження мережі супротивника помилковими і застарілими даними; зараження мережі супротивника вірусами; таємне проникнення у мережу супротивника [13].

Ще однією особливістю китайського підходу є використання стратагемних принципів. 36 стародавніх китайських стратагем не лише не втратили своєї актуальності, а набули нового сенсу в контексті інформаційного протиборства.

Стратагема – це хитрість, призначена, щоб ввести в оману або застати ворога зненацька. Мистецтво стратагем – вміння представляти попередні стратегічні розрахунки і плани у формі пасток.

Відмінною рисою хитрості служить не «обман» і «шахрайство», а «незвичайне». За словами Сунь-Цзи, «при зустрічі з супротивником військо стає непереможним завдяки поєднанню незвичайних і регулярних дій. У бою супротивника зустрічають регулярною позицією, а перемагають його нерегулярним маневром» [14].

Залежно від цілей, дослідники поділяють китайські стратагеми на такі категорії:

1. *Стратагеми підробки*, що передбачають створення ілюзорної дійсності. Наприклад, стратагема № 7 «Витягти щось з нічого». Це стратагема містифікатора, що має такі значення: представити вигадку реальністю; поширювати чутки; проводити брехливі, наклепницькі кампанії.
2. *Стратагеми приховування*, що передбачають приховування від ворога певних реальних обставин. Наприклад, це стратагема №1 «Обдурити імператора, щоб він переплив море» (суть - маскування цілі, шляху чи напрямку) та стратагема №8 «Начебто лагодити дерев'яні містки, а потай виступити у Ченьцан (суть – приховувати за звичайними діями щось незвичайне).
3. *Дезінформаційні стратагеми*, які передбачають повідомлення про невідоме як про щось відоме. Наприклад, це стратагема № 13 «Бити по траві, щоб сполохати змію» (стратагема провокації). За допомогою цієї стратагеми можна

змусити супротивника «розкрити свої карти», можна розпалити міжнародні суперечки, а також сильні негативні емоції у громадян тієї чи іншої країни.

4. *Стратагеми отримання вигоди*, що полягають у швидкому виявленні та використанні сприятливих обставин. Наприклад, це стратагема №9 «Спостерігати за пожежею з протилежного берега» та стратагема №19 «Витягати хмиз з-під котла». Суть стратагеми №9 – спостерігати за супротивником, що опинився у кризовій ситуації, не надаючи допомоги, поки ситуація не буде розвиватись у сприятливому напрямі. Стратагема №19 має такі значення: не виступати проти самої загрози, а усунути її причину; вибити грунт з-під ніг; позбавити опори. В інформаційних операціях це може бути використання шкідливих програм для виведення з ладу комп'ютерних мереж або підрив морального духу військ супротивника.
5. *Стратагеми втечі*, що передбачають ухиляння від несприятливих обставин. Так, згідно зі стратагемою №36 «Втеча – кращий варіант», якщо перемога супротивника неминуча, і битися з ним немає можливості, то потрібно або здатися, або домовлятися про мир, або втекти. Здатися означає поразку. Переговори про мир - поразка наполовину. Втеча не є поразкою. Уникнути поразки дуже важливо, бо це дасть змогу здобути перемогу у майбутньому [14].

2003 року була затверджена і у 2010 році скоригована **концепція «Трьох воєн»**, що визначає принципи та основні умови досягнення переваги в інформаційному протиборстві. Під трьома війнами мається на увазі медійна війна (public opinion warfare), психологічна війна (psychological warfare) та правова війна (legal warfare) [15].

Медійна війна (війна за громадську думку) передбачає формування сприятливої для державного керівництва громадської думки (як всередині країни, так і на міжнародній арені) шляхом поширення пропагандистських наративів через ЗМІ. Важливе значення має оперативність у поширенні власної інтерпретації фактів та

збільшення кількості джерел, які підтримують дану версію подій. Медійна війна має безперервний і довгостроковий характер.

Правова війна передбачає використання всіх аспектів права, включаючи національне законодавство, міжнародне право та закони війни, щоб забезпечити правову перевагу та делегітимізувати супротивника. Тобто мова йде про легітимізацію власних дій і здобуття підтримки з боку міжнародної спільноти.

Психологічна війна полягає у використанні конкретної інформації та засобів для військових дій, що впливають на психіку і поведінку цільової аудиторії. Психологічна війна, на відміну від медійної війни, частіше реалізується у воєнний період, і має на меті підірвати військову міць супротивника, здатність ухвалювати правильні рішення, шляхом загострення внутрішніх протиріч, внесення розколу у ряди супротивника.

Фахівці Народно-визвольної армії КНР виокремили чотири типи психологічних операцій: примусові операції, оманливі операції, операції відчуження (alienating) та оборонні операції [16].

Примусові операції націлені на деморалізацію супротивника. Такі операції спрямовані на те, щоб змусити супротивника відмовитися від своїх планів або від опору шляхом формування у нього переконання в тому, що опір не має сенсу. Мета такої операції досягається за допомогою демонстрації переваги у військовій могутності, в інформаційних технологіях, бойовій та психологічній підготовці військ, стратегічній позиції тощо. Успішний примус дає змогу уникнути військового конфлікту. До таких операцій відносяться, зокрема, китайські хакерські атаки.

Оманливі операції передбачають здійснення впливу за допомогою ЗМІ та різних Інтернет-технологій на когнітивні процеси супротивника, з метою їх спотворення, уповільнення чи блокування. Мета – дезорієнтація супротивника, формування помилкових вражень, оцінок, рішень та дій. При цьому акцент робиться на непомітному вбудовуванні помилок в існуючі вірування і системи цінностей супротивника. Реалізується принцип «сміття в смітті»: використання

помилкової інформації при прийнятті рішення веде до прийняття помилкових рішень.

Важливим елементом оманливих операцій є використання «підтверджувального упередження», тобто схильності людей шукати та надавати більше значення інформації, що підтверджує їхні існуючі переконання, відкидаючи інформацію, яка їм суперечить.

Операції відчуження націлені на розпалювання у таборі супротивника підозр, розбіжностей, непорозумінь і відчуження, на порушення зв'язків між населенням і керівництвом, між керівниками, між союзниками, між військовими і цивільним населенням. Для реалізації принципу «фортеці краще захоплювати зсередини» важливе значення має розуміння і врахування індивідуальної і групової психології супротивника, його слабкостей та уразливостей.

Оборонні операції покликані протидіяти спробам супротивника проводити примусові, оманливі операції та операції відчуження проти власної країни. Вони передбачають формування духовної, ідейної та соціальної єдності нації, «імунізацію» керівництва, населення, військовослужбовців проти ворожої пропаганди, утримання контролю над ЗМІ, з метою блокування деморалізуючих чуток і настроїв [16].

Крім того, останнім часом фахівцями Народно-визвольної армії Китаю (НВАК) розробляється нова концепція психологічних операцій – «cognitive domain operations», в рамках яких планується використовувати такі технології когнітивного впливу [17]:

- «Технологія когнітивних вимірів» (cognitive survey technology) переводить психологічні показники у кількісно вимірювані сигнали, щоб оцінити психологічну позицію супротивника – не лише сприйняття, а й мотивацію, емоції та потреби;
- «Технологія когнітивного втручання» (cognitive interference technology) призначена для проведення атак на психологічний стан супротивника за допомогою летальних та нелетальних засобів, таких як світлові хвилі, електромагнітні хвилі та

мікрохвилі, що можуть завдати психологічної шкоди, викликати галюцинації тощо;

- «Технологія зміцнення когнітивних здібностей» (cognitive strengthening technology) використовується для посилення власних когнітивних здібностей;
- «Технологія підсвідомої обробки інформації» (subliminal information processing technology) може використовуватись для збору та попередньої обробки контенту;
- «Технологія підсвідомого впровадження інформації» (subliminal information implantation technology) призначена для впровадження підсвідомих повідомлень у контент та створення «синтетичної інформації»;
- «Технологія виявлення підсвідомої інформації» (subliminal information detection technology) призначена для використання в оборонних цілях.

Таким чином, китайська концепція інформаційної війни базується на унікальних китайських уявленнях про війну, концепції «народної війни» та 36 китайських стратагемах. Провідну роль в інформаційній війні відіграють психологічні операції та операції з введення в оману, в яких використовуються різного роду хитрощі (стратагеми). Китай повною мірою користується можливостями і перевагами сучасних інформаційних технологій для ведення інформаційних операцій. При цьому Китай прагне діяти потай, виявляти і використовувати вразливості супротивника, тим самим уникаючи прямого зіткнення з ним. Особливість китайського підходу полягає також у залученні звичайних громадян до виконання поставлених державним керівництвом завдань в рамках інформаційного протистояння.

Питання для самоконтролю:

1. Які способи психологічного впливу на супротивника визначено у трактаті Сунь-Цзи «Мистецтво війни»?
2. Як китайські дослідники визначають термін «інформаційна війна»?
3. Яка мета інформаційної війни, за китайською концепцією?
4. Якими є компоненти інформаційних операцій за китайською концепцією?
5. Які специфічні риси притаманні китайському підходу до ведення інформаційної війни?
6. Чи коректно стверджувати, що стратагема є синонімом дезінформації?
7. Які типи китайських стратагем виділяють дослідники за цільовим призначенням?
8. В чому суть китайської концепції «Трьох воєн»?
9. Які типи психологічних операцій визначено фахівцями Народно-визвольної армії КНР?

Завдання:

1. Навести приклади інформаційних операцій КНР у 21 столітті.
2. Навести приклади використання китайських стратагем в інформаційних операціях 21 століття.
3. На прикладі окремої інформаційної операції показати, як на практиці реалізується китайська концепція «Трьох воєн».
4. На конкретних прикладах проаналізувати використання Китаєм мережі Інтернет в інформаційному протиборстві.
5. Охарактеризувати державні структури Китаю, відповідальні за проведення інформаційних операцій.

1.3. Операції впливу

Інформаційне протиборство у 21 столітті характеризується використанням урядовими та неурядовими акторами міжнародних відносин комплексу різнопланових, витончених технологій впливу на цільові аудиторії та нестандартних моделей і алгоритмів впливу. Інформаційна боротьба виходить за рамки конфліктів та військових кампаній, набуває довготривалого характеру і поєднує «жорсткий» та «м'який» інструментарій впливу. У зв'язку з цим термін «інформаційні операції» поступився місцем поняттю «операції впливу».

На сьогодні немає загальноприйнятого визначення терміну «операції впливу». Існуючі підходи до визначення даного терміну можна розділити на дві категорії: операції впливу – загальний термін для позначення будь-яких дій акторів міжнародних відносин в інформаційному просторі; операції впливу – різновид інформаційних операцій, що не обмежуються військовими кампаніями [18].

В аналітичній доповіді експертів американської дослідницької корпорації RAND під назвою «Основи ефективних операцій впливу» (2009 р.) операції впливу визначено як «скоординоване, інтегроване і синхронізоване застосування національних дипломатичних, інформаційних, військових, економічних та інших можливостей у мирний час, у кризах, конфліктах і постконфліктних ситуаціях для заохочення ставлення, поведінки або рішень з боку іноземних цільових аудиторій, які є сприятливими для реалізації інтересів і цілей держави» [19].

Американські експерти конкретизують, що операції впливу складаються здебільшого з комунікаційних та інформаційних дій, для впливу на когнітивні, психологічні, мотиваційні, ідеологічні та моральні характеристики цільової аудиторії, але можуть бути підкріплені діями у фізичному просторі. Операції впливу охоплюють військові та цивільні заходи, в тому числі інформаційну діяльність, яка не відноситься до сфери повноважень Міністерства оборони, таку як дипломатична діяльність зовнішньополітичного відомства та діяльність розвідувальних служб [19].

При плануванні операцій впливу проводиться ретельний аналіз цільових аудиторій (ЦА). Окрім визначення характеристик цільової аудиторії, каналів поширення інформації, меседжів та їхнього обсягу, при плануванні операцій впливу виявляються глибоко вкорінені у свідомість цільових аудиторій установки, які не піддаються змінам, а також визначається період часу для проведення операції.

Загальна модель планування операцій впливу передбачає відповіді на такі питання [19]:

1. Яку мету має країна? Чи ймовірно досягти поточні цілі з наявною стратегією та ресурсами, а якщо ні, то які наслідки це матиме?

2. Які суб'єкти та групи є пріоритетними для досягнення політичних і військових цілей?

3. Які стратегії найімовірніше вплинуть на ці групи та приведуть до потрібних результатів?

4. Які джерела інформації використовують цільові аудиторії та вважають найбільш достовірними?

5. Як позиції (ставлення) цільових аудиторій та наскільки стабільними вони є?

6. Які повідомлення цільові аудиторії вже отримують?

7. Які джерела повідомлень, контент і формати найімовірніше будуть сприйняті та сприятимуть зміні ставлення?

8. Скільки повідомлень потрібно надіслати? Які інші заходи слід вжити для досягнення цілей впливу?

Як зазначають фахівці RAND, операції впливу включають такі компоненти, як стратегічні комунікації, зв'язки з громадськістю, інформаційні операції, PR-складова цивільно-військових операцій [19].

В операціях впливу значна увага приділяється роз'ясненню та використанню реальних дій, створюючи для них позитивний контекст, і тим самим зміцнюючи довіру аудиторії, чи протидіючи заявам опонентів про такі дії фактичною інформацією. Мова йде про переконання окремих осіб або спільнот в тому, що певна дія (або бездіяльність) відповідає їхнім інтересам. Крім того, в операціях впливу важливо діяти до того, як супротивник ухвалить ключові рішення.

Операції впливу під час кризи можуть бути спрямовані на переконання супротивника і стримування ескалації ситуації, під час військових кампаній – на припинення війни на вигідних умовах, а під час операцій зі стабілізації – на відновлення стабільної післявоєнної політичної рівноваги.

У Доктрині інформаційних операцій ВПС США (AFDD 3-13) термін «операції впливу» розглядається як один з трьох типів інформаційних операцій (інші два типи – радіоелектронна боротьба та комп'ютерні мережеві операції). Згідно з Доктриною, операції впливу включають психологічні операції, військовий обман, операції безпеки, контррозвідку, зв'язки з громадськістю, контрпропагандистські операції і допоміжні дії, включаючи фізичний напад. Ефективність операцій впливу зумовлена поєднанням кінетичних і некінетичних можливостей, націлених на формування чи зміну сприйняття і поведінки лідерів, окремих груп або населення супротивника загалом [19].

Томас М. Сканзілло, Едвард М. Лопацієнські відмічають, що операції впливу мають проактивний характер і відіграють важливу роль не лише на стратегічному, але й на оперативному і тактичному рівнях. На локальному рівні такі операції здатні сформувати сприятливе операційне середовище для досягнення державних цілей. Для успіху операцій впливу критичне значення має розуміння обстановки і цільових аудиторій, робота з аудиторіями на місцях, підтвердження слів конкретними діями, узгодженість дій усіх задіяних підрозділів. Загалом, на думку дослідників, інформаційні операції варто перейменувати на операції впливу [20].

За визначенням Крістофера Пола, операція впливу – це завчасно спланована та синхронізована серія заходів, націлених на створення бажаної поведінки у супротивника шляхом прямого чи опосередкованого впливу, загрози чи фактичного використання військової могутності та можливостей держави для досягнення переваги чи бажаної кінцевої мети. Дослідник підкреслює, що операції впливу призначені для впливу на поведінку цільової аудиторії, а не для досягнення військових цілей [18].

Подібної точки зору дотримуються дослідники Роб Левінсон, Девід Ріген та Марсія Фражо, які зазначають, кінетичні дії можуть вважатись частиною операцій впливу, якщо їхня мета полягає у поширенні повідомлення для аудиторії, а не у послабленні можливостей супротивника чи захопленні території [18].

Паскаль Брангетто і Маттіс А. Венендаал розглядають операції впливу як загальний термін для позначення усіх операцій в інформаційному просторі, включаючи використання м'якої сили. Операції впливу передбачають використання невійськових [некінетичних] засобів у мирний час або під час збройного конфлікту для ослаблення сили волі противника, заплутування і обмеження його прийняття рішень, а також підриву його громадської підтримки, щоб досягти перемоги без єдиного пострілу.

На думку дослідників, операції впливу є ширшим поняттям, ніж інформаційні операції, що проводяться в рамках військових кампаній. До операцій впливу відносяться стратегічні комунікації, пропагандистська діяльність, дезінформаційні кампанії тощо [21].

Як зазначає Девід Таюрі, операції впливу можуть мати різні цілі та наслідки. У мирний час метою операцій впливу може бути просування бажаних ідей або спрямування груп населення у бажаному напрямку. Під час конфлікту або війни мета операцій впливу може полягати у тому, щоб викликати антиурядові дискусії, налаштувати громадську думку проти дій уряду, підірвати суспільну мораль (наприклад, створивши почуття незахищеності через дії уряду) тощо [18].

У своєму дослідженні Еліс Томас, Наталі Томпсон та Алісія Ванлесс дійшли висновку, що операції впливу не піддаються звичайній класифікації, оскільки часто не вписуються в існуючі політичні та законодавчі рамки. Операції впливу реалізуються у складному середовищі, де кордони розмиті, а мотивація учасників є різною, що ускладнює застосування правових норм. Агенти впливу знають, як обійти існуючі правила так, щоб їхня діяльність явно не суперечила політичним та правовим нормам. Фактично вони діють на межі допустимого [22].

Американські дослідники Герберт Лін і Жаклін Керр не розділяють поняття «операції впливу» та «інформаційна війна», характеризуючи «information warfare and influence operations» як діяльність, спрямовану на зміну інформаційного середовища в будь-якому або в усіх трьох його вимірах – фізичному, інформаційному та когнітивному, аби здобути перевагу над супротивником. Такі операції мають психологічний характер і проводяться за межами явного військового конфлікту організаціями, які не належать до збройних сил або військового командування. Їх сутність полягає у передачі аудиторії супротивника вибраної неправдивої, правдивої або частково правдивої інформації, що забезпечить зміцнення ставлення та поведінки супротивника у сприятливому для суб'єкта впливу напрямі.

Дослідники виокремили три види операцій впливу: білі, які чітко та коректно ідентифікують їх ініціатора; сірі, які не пов'язані з жодним актором міжнародних відносин; чорні, що публічно приписують певному актору, який насправді не є справжнім ініціатором впливу (так звані операції під «чужим прапором»). Такі операції також можуть передбачати обман, щоб спонукати супротивника (не) вжити певних дій для здобуття переваги або завдання йому збитків. Їх мета полягає у зміцненні упереджень супротивника, зосередженні його уваги на неважливих діях, відволіканні від важливих дій, створенні ілюзії сили там, де є слабкість, зниженні ситуаційної обізнаності супротивника тощо [23].

Специфіка операцій впливу полягає у невизначеності ефективності їх результату, оскільки вплив на цільову аудиторію не є однорідним – у суспільстві завжди будуть групи чи окремі особи, стійкі до зовнішнього впливу завдяки розвиненим інститутам верховенства права та високому рівню довіри до політичного керівництва.

В іншій публікації Герберт Лін відмічає, що операції впливу – це навмисне використання інформації суб'єктом впливу проти населення супротивника, аби заплутати, ввести в оману та зрештою вплинути на дії цільової аудиторії. Характерними рисами таких операцій є перебування за порогом збройного конфлікту і відсутність некомбатантів, адже кожна окрема особа серед населення супротивника є законною ціллю. Наслідки впливу таких операцій є

неочевидними, адже супротивник прагне за допомогою маніпуляцій перетворити більшу частину цільової аудиторії на мимовільних спільників: вони служать інтересам супротивника, але не знають, що їх обманюють [24].

Перемога в операціях впливу фокусується на волі супротивника, а не його фізичному знищенні. Використовуючи слова та образи задля переконання, інформування та введення в оману, суб'єкт впливу змушує супротивника не використовувати наявні в нього військові засоби, аби врешті-решт результат був таким самим, ніби ці військові засоби були знищені фізично.

Герберт Лін також відмічає односторонність такого впливу: через те, що він відбувається поза межами законодавчого рівня «застосування сили» або «збройного нападу», у міжнародно-правовому сенсі він не викликає застосування військової сили у відповідь. Основний фокус – не на фізичних артефактах, а на завданні шкоди знанням, правді та впевненості, провокуванні страху, тривоги і сумнівів під час прийняття рішень супротивником [24].

Аналізуючи операції впливу в онлайн середовищі, американські дослідники Дієго Мартін, Джейкоб Шапіро і Джулія Ільхардт виокремили зовнішні та внутрішні операції впливу. Метою обох кампаній є вплив на політичні рішення в державі, а особливість полягає в тому, що на відміну від традиційних інформаційних операцій, в яких підтримувані державою ЗМІ просувають певні наративи, в операціях впливу джерела походження контенту приховуються [25].

Зовнішні операції впливу – це скоординовані кампанії однієї держави,з метою впливу на один або кілька конкретних аспектів політики в іншій державі через медіа, включаючи соціальні мережі, шляхом створення контенту, який має виглядати характерним для країни-об'єкта впливу. За даними дослідника, більшість операцій впливу походять з рф (64%), КНР, Ірану, Саудівської Аравії та Об'єднаних Арабських Еміратів. Об'єктами впливу найчастіше були США та країни ЄС.

Внутрішні операції впливу – це скоординовані кампанії, що проводяться державою задля впливу на один чи кілька конкретних аспектів внутрішньої політики через різні медіа, а поширюваний

контент виглядає так, ніби його створили звичайні інтернет-користувачі. Кількість країн, які брали участь у внутрішніх операціях впливу є значно більшою, ніж тих, які проводили зовнішні операції, і деякі з них тривали щонайменше п'ять років. Такі операції часто використовувались для підтримки правління авторитарних режимів, доповнюючи традиційну тактику цензури та придушення політичної опозиції.

В операціях впливу найчастіше застосовувались стратегії переконання, спрямовані на зміну поглядів пересічного громадянина на ту чи іншу проблему. Менш поширеними, як зазначають дослідники, є стратегії дискредитації окремих осіб чи установ, поляризації суспільства, наклепу та інформаційного тиску. Інструменти реалізації – інтернет-тролі, боти, підроблені акаунти та викрадені хештеги. В обох типах операцій впливу просувались теми, які стосувалися політичних партій країн-об’єктів впливу, військових операцій, економічних та міграційних питань, контролю над озброєнням та кліматичних змін. Соціальні мережі та новинні платформи виявилися найпоширенішими платформами для операцій впливу, замаскованих під локальну політичну активність [25].

Шведські дослідники з Лундського університету (Pamment P., Nothhaft H., Agardh-Twetman H., Fjallhed A.) розглядають операції (інформаційного) впливу як скоординовані дії зарубіжного суб’єкта, націлені на здійснення впливу на політичні рішення та громадську думку іншої країни, що можуть негативно позначитись на суверенітеті, безпеці та інших інтересах країни-об’єкта впливу [26]. Основною характеристикою таких операцій є їх нелегітимність, оскільки вони вводять в оману громадськість, мімікруючи під легітимні способи і методи формування громадської думки, використовують вразливості суспільства та порушують правила конструктивних і відкритих дебатів.

В операціях впливу дослідники визначили три категорії цілей:

1. Конструктивні – утвердження чіткого наративу серед цільової аудиторії. Наприклад, це може бути масова ідеологічна пропаганда за допомогою різних засобів розповсюдження інформації.

2. Деструктивні – підрив довіри до існуючого наративу шляхом актуалізації спірних суспільних питань, що може призвести до внутрішніх конфліктів та суспільної поляризації.
3. Відволікаючі – відвернення уваги від важливих проблем за допомогою гумору, мемів та конспірологічних теорій [26].

Дослідниками виокремлено низку методів інформаційного впливу: когнітивне хакерство, соціальне хакерство, парасоціальне хакерство, дезінформація і фейки, «Потьомкінські села», фальшиві особистості, ботнети і тролінг, меми тощо.

Когнітивне хакерство не вимагає чіткого наративу і має за мету таємно вплинути на аудиторію. Прикладом такого хакерства може бути поширення компрометуючої інформації про політика напередодні виборів, коли політик вже не має можливості відповісти на такий закид. Когнітивне хакерство реалізується у двох формах: соціокогнітивне хакерство, націлене на експлуатацію когнітивних уразливостей індивіда у соціумі, та психографічне хакерство, націлене на окремих індивідів. У першому випадку відбувається активізація тригерів, що викликають сильні емоції. У другому випадку має місце ізоляція індивідів за допомогою соціальних медіа.

Соціальне хакерство передбачає використання уразливостей, породжених племінною природою та схильністю людей до конформізму. До таких уразливостей відноситься схильність приймати на віру те, у що вірять інші; прагнення приєднатись до більшості; схильність шукати і сприймати інформацію, яка відповідає власним переконанням (у соціальних мережах – ефект «інформаційної бульбашки»).

Парасоціальне хакерство передбачає експлуатацію парасоціальних (ілюзорних) відносин, які виникають, коли люди сприймають односторонні відносини як двосторонні. Завдяки соціальним мережам кожен індивід може налагодити парасоціальні відносини та обмінюватись інформацією з незнайомцями, знаменитостями і особами, які приймають рішення. Дана технологія може реалізуватись у таких варіантах, як формування відносин між інфлюенсером або пропагандистами, які прикидаються звичайними

користувачами, і цільовою аудиторією та створення віртуальної мережі друзів.

Технологія «Потьомкінські села» передбачає створення складних інституційних мереж, що контролюються та використовуються агентами впливу для просування і посилення конкретних наративів. До «Потьомкінських сел» можна віднести незаконні або фальшиві дослідження, (онлайн) журнали, неурядові організації або аналітичні центри, які публікують інформаційно-аналітичні матеріали з різної тематики тощо.

Дезінформація може використовуватися для побудови нових або альтернативних наративів, або підтримки конкретних існуючих наративів шляхом легітимації неправдивої інформації чи доказів, або шляхом заміни певних частин реальних історій помилковою, але переконливою інформацією, а також для створення «інформаційного шуму», що ускладнює пошук достовірної інформації.

Мемі можуть використовуватись як засоби прихованого впливу на громадську думку, для просування тих чи інших ідей, які аудиторією або не усвідомлюються, або не сприймаються як загрозливі [26].

Український дослідник Георгій Почепцов визначив декілька специфічних рис операцій впливу. Операції впливу є більш складним варіантом впливу, з акцентом на інформації про комунікатора, який має викликати довіру аудиторії [27]. Операції впливу відбуваються у такому форматі, що об’єкт впливу не сприймає це як цілеспрямований вплив. Це досягається тим, що об’єкт впливу занурюється у певні контексти та інтерпретації ситуацій чи подій. При цьому меседжі підбираються чітко під конкретні аудиторії, виходячи з їх вразливостей.

На відміну від інформаційних операцій, які жорстко програмують поведінку, операції впливу діють «м’якими» методами, надаючи аудиторії вибір (або створюючи ілюзію вибору).

Крім того, операції впливу мають дифузний характер, довгострокові цілі, не прив’язані до трансформації фізичного простору, а також можуть бути націлені як на утримання існуючої картини світу, так і на її зміну [27, 28].

Таким чином, операції впливу є широким поняттям, яке охоплює практично весь доступний акторам міжнародних відносин інструментарій впливу на цільові аудиторії. Ядром операцій впливу є психологічний вплив для управління сприйняттям та поведінкою цільових аудиторій. В операціях впливу відбувається синхронізація і координація дій в інформаційному та фізичному просторах. При цьому кінетичні дії використовуються також як інструмент психологічного впливу на цільові аудиторії, що підсилює ефект заходів в інформаційному просторі [18].

Операції впливу проводяться державними і недержавними акторами міжнародних відносин як у воєнний, так і у мирний час, та можуть мати як конструктивні, так і деструктивні цілі.

Операції впливу за своєю структурою, способами, методами і засобами реалізації виходять за рамки «традиційних» сценаріїв інформаційних операцій.

На відміну від інформаційних операцій з чіткими часовими рамками, операції впливу розраховані на довгострокову перспективу і можуть проводитись безперервно.

На відміну від інформаційних операцій, які націлені на ворожу інформацію та інформаційні системи, і передбачають наявність ситуації конфлікту і формування образу ворога, в операціях впливу дихотомія «свій-чужий», «друг-ворог», «добро-зло» є розпливчатою і неоднозначною.

Операції впливу проводяться постійно, з використанням сучасних інформаційно-комунікаційних технологій, відрізняються гнучкістю, варіативністю способів і методів впливу на цільові аудиторії, високим рівнем адаптивності до обстановки, множинністю ефектів тощо.

Питання для самоконтролю:

1. Як фахівці американської корпорації RAND визначили термін «операції впливу»?
2. Які характеристики операцій впливу розкрито у визначенні даного терміну фахівцями американської корпорації RAND?
3. Яку роль відіграють кінетичні дії в рамках операцій впливу?

4. Які специфічні риси операцій впливу виявили у своєму дослідженні Еліс Томас, Наталі Томпсон та Алісія Ванлесс?
5. Як характеризують операції впливу дослідники з Лундського університету?
6. Чому, на Вашу думку, частина дослідників вважає, що операції впливу є ширшим поняттям, ніж інформаційні операції?
7. За якими параметрами можна порівнювати інформаційні операції та операції впливу?
8. Що є спільного в термінах «інформаційні операції» та «операції впливу»?
9. Чим операції впливу відрізняються від інформаційних операцій?

Завдання:

1. Навести приклади операцій впливу у сучасних міжнародних відносинах.
2. На конкретному прикладі охарактеризувати інструментарій операції впливу.
3. На конкретному прикладі охарактеризувати державні структури та фінансовані державою організації (агенти впливу), задіяні в операції впливу.
4. Навести приклад інформаційної операції і приклад операції впливу та проаналізувати спільні і відмінні риси вибраних операцій.
5. Проаналізувати окрему операцію впливу, визначивши цілі операції, суб’єктів (ідеологів) та агентів впливу, період проведення операції впливу, цільові аудиторії, інструментарій (інформаційні та фізичні заходи), результати.

Список використаних джерел:

1. Почепцов Г. Информационная война: определения и базовые понятия. URL: https://psyfactor.org/psyops/infowar25.htm
2. Жуков В. Взгляды военного руководства США на ведение информационной войны. URL: http://pentagonus.ru/publ/22-1-0-175
3. Гриняев С. Информационное противоборство в современную эпоху. URL: https://psyfactor.org/infowar1.htm
4. Запорожець О.Ю. Інформаційне протиборство у зовнішній політиці США. URL: http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/223/199
5. Туляков О. Информационная война в планах Пентагона. URL: http://pentagonus.ru/publ/informacionnaja_vojna_v_planakh_pentagona_2015/19-1-0-2650
6. Панченко В. Інформаційні операції в системі стратегічних комунікацій. - http://ippi.org.ua/sites/default/files/panchenko.pdf
7. US Army Joint Publication 3-13 Information Operations. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf
8. Macdonald S. Propaganda and Information Warfare in the Twenty-First Century. Routledge, Abingdon, 2007. 204 p.
9. The Conduct of Information Operations. US Department of Army. URL: https://fas.org/irp/doddir/army/atp3-13-1.pdf
10. Сунь-Цзы Искусство войны. URL: https://librebook.me/the_art_of_war
11. Авраменко А., Старунский А. Психологические операции Народно-освободительной армии Китая. URL: http://psyfactor.org/lib/psywar37.htm
12. Vinod Anand Chinese Concepts and Capabilities of Information Warfare. URL: http://www.idsa.in/strategicanalysis/ChineseConceptsandCapabilitiesofInformationWarfare_vanand_1006
13. Mulvenon J. The PLA and Information Warfare. URL: https://indianstrategicknowledgeonline.com/web/The%20PLA%20and%20Information%20Warfare.pdf
14. Зенгер Х. фон. Стратагемы. О китайском искусстве жить и выживать. М: Изд-во Эксмо, 2004. URL: https://www.litmir.me/br/?b=122956
15. Kania E. The PLA's Latest Strategic Thinking on the Three Warfares. URL: https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/
16. Cheng D. Winning Without Fighting: The Chinese Psychological Warfare Challenge. URL: https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge#_ftn10
17. Beauchamp-Mustafaga N. Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations. URL:

https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/
18. Запорожець О.Ю. Операції впливу: концептуальний вимір. Медіафорум: аналітика, прогнози, інформаційний менеджмент. 2021. №9. С. 232-244.
19. Larson E. V., Darilek R. E., Gibran D., Nichiporuk B., Richardson A., Schwartz L., Thurston C. Q. Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities. URL: https://www.rand.org/pubs/monographs/MG654.html
20. Scanzillo T. M., Lopacienski E. M. Influence operations and the human domain. Case study. URL: https://www.hsdl.org/?view&did=814708
21. Brangetto P., Veenendaal M.A. Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. URL: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf
22. Thomas E., Thompson N., Wanless A. The Challenges of Countering Influence Operations. URL: https://carnegieendowment.org/2020/06/10/challenges-of-countering-influence-operations-pub-82031
23. Lin H., Kerr J. On Cyber-Enabled Information Warfare and Information Operations. Oxford Handbook of Cybersecurity, 2019. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680
24. Lin H. Developing Responses to Cyber-Enabled Information Warfare and Influence Operations. September 6, 2018. URL: https://www.lawfaremedia.org/article/developing-responses-cyber-enabled-information-warfare-and-influence-operations
25. Martin D.A., Shapiro J., Ilhardt J.G. Trends in Online Influence Efforts. August 5, 2020. URL: https://jns.scholar.princeton.edu/sites/g/files/toruqf2751/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_2020.pdf
26. Pamment J., Nothhaft H., Agardh-Twetman H., Fjallhed A. Countering Information Influence Activities: The State of the Art. URL: https://www.msb.se/RibData/Filer/pdf/28697.pdf
27. Почепцов Г. Операции влияния: современные представления военных и учёных.URL:https://ms.detector.media/ethics/manipulation/operatsii_vliyaniya_sovremennye_predstavleniya_voennykh_i_uchenykh/
28. Почепцов Г. Операции влияния вдали и вблизи. URL: https://ms.detector.media/trends/1411978127/operatsii_vliyaniya_vdali_i_vblizi/

РОЗДІЛ 2.
ПРОПАГАНДА І ДЕЗІНФОРМАЦІЯ
В ІНФОРМАЦІЙНОМУ ПРОТИБОРСТВІ

2.1. Пропаганда

Інформаційні війни базуються на технологіях маніпулювання масовою свідомістю. Відповідно центральним компонентом більшості інформаційних операцій є психологічні операції, що реалізуються у формі пропаганди.

У нейтральному значенні слово «пропаганда» означає поширення певних ідей [1]. Вважається, що термін «пропаганда» з'явився у XVI столітті, коли Папою Клементієм була створена конгрегація з просування віри – Congregeratio propaganda fide.

В англомовних словниках пропаганда визначається таким чином: розповсюдження ідей, інформації чи чуток, з метою підтримки чи завдання шкоди установі, справі чи особі [2]; інформація, часто неточна, яка розповсюджується політичною організацією, з метою впливу на людей [3]; інформація, особливо упередженого чи оманливого характеру, що використовується для просування політичної справи чи точки зору [4].

Американський дослідник пропаганди Гарольд Лассуелл у книзі «Техніка пропаганди у світовій війні» (1927 р.) визначив пропаганду як менеджмент колективних уявлень за допомогою маніпуляцій значимими символами. Мета – забезпечити мобілізацію та консолідацію мас навколо єдиної цілі. Ця мета є одночасно загальною для всіх, і особливою для кожної соціальної групи. Вона формулюється безліччю способів, кожен із яких розрахований на конкретний прошарок населення [5].

За Г. Лассуеллом, пропаганда активує базові примітивні людські інстинкти, тим самим забезпечуючи єдину реакцію на пропаганду. Чим вище рівень напруженості у суспільстві, чим сильніше виражені у ньому примітивні інстинкти, тим ефективніше працюватиме пропаганда, і тим легше люди повірять її повідомленням.

Американські дослідники Гарт Джоуетт та Вікторія О'Доннел визначили пропаганду як «цілеспрямоване та систематичне прагнення формувати сприйняття, маніпулювати знаннями та спрямовувати поведінку для досягнення реакції, що сприяє реалізації бажаної пропагандистом мети» [1]. Завдання пропаганди полягає у тому, щоб поширити серед аудиторії певну ідеологію задля досягнення заздалегідь сформульованої мети.

Цілі пропаганди встановлюються апріорі. Пропаганда прагне «втиснути» інформацію у певні рамки та відвернути реципієнта від будь-яких питань, що виходять за ці рамки.

Пропагандист прагне контролювати потік інформації для спрямованого впливу на громадську думку і маніпулювання поведінкою людей. Контроль над інформацією реалізується двома способами: контроль ЗМІ як джерела поширення інформації та поширення викривленої інформації з джерела, який здається надійним [1].

Відмінність пропаганди від інших інформаційних процесів полягає в інтерпретаційному та емоційно забарвленому характері повідомлень, а також у спрямованості на досягнення цілей суб'єкта впливу, а не на досягнення взаєморозуміння.

Дослідник пропаганди Л. Войтасик виокремив у структурі пропагандистського повідомлення два основних елементи: пропагандистські насичена інформація про факти та їх оцінку; заклик, спрямований на те, щоб згуртувати людей навколо певної ідеї чи справи. Заклик завжди містить деякі вказівки, яка саме дія очікується від тих, на кого розраховане це повідомлення [6].

Практично будь-яке пропагандистське повідомлення будується так, начебто у ньому зацікавлений адресат (реципієнт), інтереси адресанта (комунікатора) у повідомленні замовчуються.

Американський дослідник, професор Йельського університету Леонард Дуб визначив пропаганду як систематичну спробу індивіда чи індивідів контролювати настанови груп індивідів через використання навіювання і, внаслідок цього, контролювати їхні дії [7].

На думку Л. Дуба, психологічний механізм пропаганди працює через збудження (актуалізацію) тих чи інших настанов навіюваннями, що є по суті підготовчим етапом пропаганди. Пропаганда повною мірою починає виявляти себе, коли індивід стикається зі стимулами чи стимулами-ситуаціями, на які реагує у відповідності із актуалізованими пропагандистом настановами.

Вплив на індивіда залежить від стереотипів, соціальних цінностей, сприйняття його оточення. Саме через оточення і здійснюється навіювання та систематично контролюється поведінка індивідів. Для ефективного впливу на індивіда пропагандист має обрати сильне повідомлення, яке буде зрозумілим, буде відповідати раніше сформованим настановам, буде поширено через найбільш ефективний канал комунікації. Психологічна мета пропагандиста полягає в інтеграції настанов індивіда у нову настанову для досягнення практичної пропагандистської цілі [7].

Леонард Дуб зазначає, що пропагандист стикається зі сферою невизначеності (непередбачуваності), тобто з тим, що його наміри та цілі не обов'язково та не повною мірою втілюються у поведінку реципієнтів пропаганди. Зменшити рівень невизначеності можна такими способами: збудження підпорядкованої настанови щодо стимул-ситуації; включення у стимул-ситуацію осіб та об'єктів з позитивними соціальними цінностями; створення ілюзії універсальності своїх повідомлень; використання принципу селективності пропаганди (тобто обирати відкриту або приховану пропаганду); використання принципу повторення для актуалізації стимулів-ситуацій; спотворення та придушення шкідливих настанов тощо [7].

Ключові характеристики, принципи та правила пропаганди були сформульовані у роки першої та другої світових війн. Ці принципи є актуальними сьогодні й активно використовуються акторами міжнародних відносин в інформаційному протистоянні.

Принципи військової пропаганди викладено у книзі британського дипломата лорда Понсонбі «Брехня під час війни» (1928 р.).

Перший принцип «ми не хотіли війни» полягає у тому, щоб переконати власний народ, що керівництво країни не бажало війни, війну розпочала інша сторона, і за таких умов країна змушена захищатись.

Другий принцип полягає у тому, що не обов'язково змушувати ненавидіти весь народ іншої держави, достатньо персоніфікувати образ ворога, показавши своєму населенню, що лідер іншої країни є втіленням неприйнятних і жахливих якостей.

Третій принцип полягає у тому, щоб наголошувати на гуманітарних причинах війни, а не на економічних цілях, мотивувати свої дії принципами гуманності.

Четвертий принцип полягає у тому, щоб довести, що саме для супротивника жорстокість є нормальною справою, у той час як для власної армії це «вимушена необхідність» чи «прикра випадковість».

П'ятий принцип полягає у використанні принципу легітимності, тобто потрібно діяти від імені народу, ООН, світової спільноти чи всього людства.

Шостий принцип передбачає перебільшення своїх успіхів і втрат супротивника. Це означає створення позитивного іміджу власної сильної і добре підготовленої армії, та підкреслення слабкості військ супротивника.

Сьомий принцип передбачає поширення дезінформації і чуток, з метою зниження бойового духу супротивника, деморалізації населення супротивника, підриву міжнародного авторитету країни, провокації конфліктів, розпалювання недовіри, загострення політичної боротьби тощо [8].

У книзі "Майн кампф" Адольфом Гітлером сформулювано такі принципи пропаганди [9]:

1) Повторення. Пропаганди має бути багато, вона адресована лише масі, і маса має зустрічатися з її носіями постійно, у будь-якій точці простору, у будь-який проміжок часу.

2) Простота. Пропаганда має бути зрозумілою навіть для найбільш відсталих верств населення.

3) Одноманітність. Пропаганда має обмежуватись лише декількома пунктами і викладати ці пункти коротко, ясно і зрозуміло, у формі гасел, що легко запам'ятовуються.

4) Однозначність. Пропаганда спрямована на те, щоб «змусити масу повірити: такий факт дійсно існує, така необхідність дійсно неминуча, такий висновок дійсно правильний».

5) Емоційність. Пропаганда має впливати більше на почуття і лише незначною мірою на розум.

6) Пропаганда має шокувати. Тільки шокуюче нестандартне повідомлення люди будуть переказувати один одному.

Актуальні характеристики пропаганди викладено у книзі французького політолога та філософа Жака Елюля «Пропаганда. Формування людського сприйняття» (1965).

За його визначенням, пропаганда – це «сукупність методів, що використовуються організованою групою, яка прагне досягти активної чи пасивної участі у своїх акціях маси індивідів, згуртованих за допомогою психологічних маніпуляцій» [10].

Пропаганда має бути тотальною, використовуючи усі канали комунікації, аби занурити людину у світ почуттів і думок, граючи на її волі чи потребах, свідомому і несвідомому. Вона забезпечує його цілою системою, пояснюючи світ, забезпечує негайне спонукання до дії [11].

Пропаганда має сприяти квазі-одностайності, виключати можливість обговорення та спростування.

Пряма пропаганда може бути ефективною лише з попередньою пропагандою. Мета препропаганди – зробити людину сприйнятливою до певних впливів, підготувати її до специфічних дій. Це робиться за допомогою психологічних маніпуляцій, створення почуттів та стереотипів. Мета такої пропаганди – створення умовних рефлексів і міфів. Коли настає час, індивіда можна захопити дією, використовуючи активну пропаганду, запускаючи психологічні важелі та актуалізуючи у пам'яті міфи.

Пропаганда має бути безперервною і тривалою. Безперервність означає, що пропаганда має заповнювати всі дні громадянина. Тривалість означає, що пропаганда має діяти протягом дуже довгого періоду часу, аби сформувати потрібні образи, міфи та упередження [11].

Пропаганда завжди інституціоналізована у формі існування «апарату». Доки немає фізичного впливу, виробленого організацією на індивіда, до того часу немає пропаганди.

Пропаганда має бути вкорінена у дії, а також одночасно адресована індивіду і масам. Коли пропаганда адресована натовпу, у тому натовпі вона має зачіпати за живе кожного індивіда. Щоб бути ефективною, вона має справляти враження персональної адресованості [11].

На думку французького дослідника, мета сучасної пропаганди – провокувати дії. Вона змушує людину ірраціонально приєднуватись до процесу дії. Дії роблять ефект пропаганди незворотнім, оскільки тому, хто діє згідно з пропагандою, ніколи не вдасться все повернути назад. Індивід змушений вірити у пропаганду, адже без неї його дії здадуться абсурдними чи несправедливими.

Ж. Елюль розмежовує пропаганду як агітацію та пропаганду як інтеграцію. Агітаційна пропаганда найпомітніша. Це може бути агітація від опозиції, що спрямована на зміну існуючого ладу, а також урядова пропаганда у разі мобілізації країни на війну. Чим менш освічені люди, на яких спрямована ця пропаганда, тим більший успіх вона матиме у залученні індивіда до спільної справи [10].

Пропаганда інтеграції є ознакою розвинених країн. Це пропаганда згоди, коли від громадянина потрібно не просто проголосувати належним чином, а прийняти всі істини цього суспільства та його моделі поведінки. Інтеграційна пропаганда спрямована на стабілізацію соціосистеми, на об’єднання та посилення її. Така пропаганда вимагає не тимчасового підпорядкування конкретному завданню, а повного переформатування людини.

Щодо психологічних ефектів пропаганди Ж. Елюль наголошує, що пропаганда дає людям стереотипи. Пропаганда стандартизує ідеї та моделі мислення в усіх сферах. Ці колективні уявлення людина вважає своїми [10].

Ефективність пропаганди значною мірою залежить від сприйняття аудиторією джерела інформації та повідомлення. Якщо джерело сприймається як пропагандистське, яке намагається маніпулювати аудиторією, ефективність різко падає.

За словами британського політика Річарда Кросмана, який під час Другої світової війни проводив антинацистську пропаганду, «висококваліфікований пропагандист – це людина, яка говорить правду чи частину правди, причому у такому стилі, що реципієнт не сприймає це як пропаганду. Мистецтво пропаганди полягає не у тому, щоб брехати, а у тому, щоб вибірково представляти правдиву інформацію відповідно до мети, і змішувати її з іншою інформацією, яку аудиторія хоче почути» [12].

Для впливу на аудиторію у пропаганді використовуються як емоційні заклики, так і раціональні аргументи.

Якщо аудиторія сильно налаштована проти повідомлення, пропаганда буде більш ефективною, якщо в ній представлена двостороння аргументація. Навіть якщо аудиторія не налаштована проти, то ті, хто почує двосторонню аргументацію, надалі зможуть протистояти контрпропаганді.

Виходячи з ефекту первинності, якщо аудиторія не знайома з протилежними аргументами, то ефективніше надати спочатку аргументи на користь конкретної позиції. Якщо аудиторії відомі контраргументи, доцільно подати спочатку контраргументи, а потім аргументи на користь позиції комунікатора.

Пропаганда може містити явні та приховані заклики. Якщо тема відома, то ефективніше дати можливість аудиторії самій дійти певних висновків. Якщо тема невідома аудиторії, то краще чітко сформулювати висновки [12].

Як зазначає Георгій Почепцов, пропаганда задає координати світу й усіма засобами намагається утримати потрібну картину дійсності. Аби залишатись дієвою, пропаганда постійно мутує, і захоплює нові інформаційні простори.

Крім того, за словами Г. Почепцова, «пропаганда має власну логіку, яка дозволяє їй змінювати причинно-наслідкові зв'язки залежно від її внутрішніх цілей, що можуть не мати нічого спільного з реальністю» [10].

Пропагандистські кампанії можна ідентифікувати за такими параметрами:

- раптовий початок і таке ж раптове завершення всієї кампанії чи окремих її етапів;
- використання всіх жанрів;
- жорсткий відбір представників однієї точки зору для поширення у ЗМІ;
- залучення різного роду комунікативних «союзників», зокрема в інших країнах;
- підготовка комунікативних проектів у вигляді документального та художнього кіно, серії книг на певну тематику;
- використання такої мови опису, яка до цього була заборонена;
- різке завищення емоційного тону повідомлень [10].

В рамках пропагандистських кампаній використовується широкий спектр методів маніпулювання громадською думкою [13, 14].

Посилання на авторитет. Метод полягає у цитуванні висловлювань експертів/фахівців/дослідників та інших осіб, які мають авторитет для цільової аудиторії.

«Самоочевидні» твердження – ствердні висловлювання, які представляються як факт. Твердження представляються як самоочевидні, що не потребують доказів. Твердження можуть бути як правдивими, так і неправдивими.

Неминуча перемога. Даний метод має за мету переконати аудиторію поводитися так як інші, «приєднатися до натовпу»,

посилюючи природнє бажання людей бути на боці переможців. Ця техніка використовується для переконання аудиторії в тому, що ідея/програма підтримується більшістю, а отже в інтересах аудиторії приєднатися.

Блискучі загальності (Glittering generalities). Метод полягає у використанні емоційно насичених слів, пов'язаних зі значущими поняттями та віруваннями, які є переконливими без доказів. Це звернення до таких емоцій, як любов до Батьківщини та дому, бажання миру, свободи, гідності тощо. Часто використовувані слова мають нечіткий зміст, щоб аудиторія наповнила їх своїми інтерпретаціями.

Трансфер. Суть методу – проекція позитивних або негативних якостей однієї особи, об'єкту на інших, аби зробити їх прийнятними або навпаки дискредитувати. Даний метод часто використовується для перекладення провини з однієї сторони конфлікту на іншу.

Найменше з двох зол. Суть методу – визнання нинішнього курсу дій небажаним, але підкреслення, що інший курс призведе до ще гірших наслідків. Даний метод використовується для пояснення необхідності у жертвах або виправдання жорстких заходів, що викликають невдоволення аудиторії, чи обмежують громадянські свободи.

Навішування ярликів. Цей метод має за мету викликати упередження цільової аудиторії шляхом приписування об'єкту впливу тих характеристик, до яких аудиторія ставиться негативно. Навішування ярликів може бути прямим (прямі напади на супротивника або ідею) та непрямим (сарказм, кепкування).

Вибіркова подача інформації. Даний метод полягає у відборі і подачі лише тих фактів, які посилюють і підтверджують правильність точки зору пропагандиста. Спочатку пропагандист відбирає лише сприятливі факти і представляє їх аудиторії так, щоб викликати бажану реакцію. Потім пропагандист використовує ці факти як основу для висновків, намагаючись спонукати аудиторію прийняти ці висновки, прийнявши представлені факти.

Спрощення. Даний метод полягає у зведенні фактів до вірних або невірних. Цей метод дає прості рішення для складних проблем та пропонує спрощені інтерпретації подій, ідей, концептів, особистостей.

Порівняння. Даний метод передбачає порівняння двох або більше ідей, варіантів вибору і пояснення їхніх відмінностей.

Конкретні випадки. Метод полягає у наведенні конкретних прикладів, які допомагають довести певну точку зору (твердження).

Інформаційна блокада. Даний метод полягає у навмисному приховуванні інформації до тих пір, поки вона втратить свою актуальність, аби уникнути небажаних наслідків.

Маніпулятивне коментування. Повідомлення про факт супроводжується інтерпретацією коментатора, який пропонує аудиторії кілька розумних варіантів пояснення. Мета – створення такого контексту, в якому думки людини спрямовуються у потрібному напрямку.

Риторичні питання. ЗМІ ставлять перед аудиторією питання, залишаючи його без відповіді, але наділяючи певним контекстом, що змушує аудиторію міркувати і розвивати "підкинуту ідею" у потрібному для маніпулятора напрямі.

Напівправда. Даний метод передбачає подачу лише частини достовірної інформації, а інша частина, що пояснює першу, приховується.

Підміна понять. Даний метод передбачає використання сприятливих визначень для позначення несприятливих дій.

Зміщення акцентів. Даний метод полягає у тому, що небажане для маніпулятора подається на другому плані, а те, що потрібно, висувається на перший план.

Принцип контрасту. Метод полягає у поширенні необхідної інформації на фоні іншої, яка негативно сприймається більшістю аудиторії.

Емоційний резонанс. Суть методу – створення в аудиторії певного настрою з одночасним поширенням пропагандистської інформації.

Переписування історії. Цей метод полягає у штучному створенні викривленої картини історичної дійсності.

Класифікатори. Даючи назву об’єкту, людина підкреслює його певну особливість, ігноруючи інші характеристики. Те, як об'єкт описується (класифікується), і манера, у якій представляється образ дії, спрямовують думки та емоційні реакції у певне русло.

Створення проблеми. Даний метод передбачає цілеспрямований відбір інформації та надання високої значущості тим чи іншим подіям.

Створення загрози. Цей метод полягає у багатократному посиленні ілюзорної чи реально існуючої небезпеки того чи іншого явища.

Демонізація ворога. Цей метод передбачає цілеспрямоване створення негативного образу тієї чи іншої особи, заснованого на міфологізації, з елементами реальності.

«Свідки» подій. Даний метод полягає у тому, що ЗМІ демонструють опитування нібито випадкових людей, зі слів яких формується потрібний смисловий та емоційний ряд.

Повторення. Цей метод полягає у постійному повторенні певних тверджень, аби аудиторія до них звикла і сприймала не розумом, а на віру.

«Спільна платформа». Даний метод передбачає підбір суджень, висловлювань, фраз, що потребують одноманіття у поведінці, та створюють враження, що так роблять всі.

Пропаганда оперує наративами, тобто різноманітними «історіями», які характеризуються лінійним розгортанням у часі та просторі, за законами причинно-наслідкової детермінації, і створюють доступну для людського сприйняття і зрозумілу картину дійсності.

Наратив має свою особливу логіку і може пояснити, як і чому відбуваються певні події. Щоб наратив був ефективним, він має входити в резонанс із цінностями, інтересами і забобонами цільової аудиторії. Наратив формулює кінцевий стан і пропонує спосіб

досягнення мети, забезпечуючи громадськість розумінням і сенсом подій [15].

За словами Г. Почепцова, наратив не лише упорядковує модель світу, а й звужує простір можливого, оскільки зовнішній світ постає тепер винятково як варіант реалізації одного з можливих сюжетів [16].

Дослідники Е. Окс і Л. Капс виокремили у структурі наративу такі елементи: обстановка – інформація про час, місце знаходження; несподівана подія; психологічні/фізичні реакції; незаплановані дії – нецілеспрямовані дії та поведінка; спроба вирішення проблемної ситуації; наслідки [15].

Соціолінгвіст Уїльям Лейбов запропонував таку модель наративу [15]:

1. Анотація (Abstract). Як це все сталося і з чого усе почалося?
2. Орієнтація (Orientation). Хто/що були у це задіяні, коли й де?
3. Кульмінація (Complicating Action). Що ж трапилося?
4. Розв'язка (Resolution). Чим же це, зрештою, закінчилося?
5. Оцінка (Evaluation). Як до цього ставитися?
6. Фінал (Coda). Що це все означає?

Одним з яскравих прикладів пропагандистської кампанії, що відповідає основним принципам пропаганди, створює цілісну картину дійсності, і містить цілу низку маніпулятивних методів, – це пропаганда РФ під час анексії Криму 2014 року.

На початку 2014 року політична криза в Україні, зумовлена масовими акціями протесту (Євромайдан) проти зовнішньополітичного курсу тодішнього президента В.Януковича, не зовсім правомірне (з порушенням конституційних норм) усунення президента країни від влади, формування нового проєвропейські налаштованого уряду та нестабільна ситуація в східних і південних регіонах створили сприятливі умови для втручання РФ у ситуацію.

Політичне керівництво Росії розгорнуло масштабну пропагандистську кампанію через підконтрольні ЗМІ, з метою дискредитації нової влади в Україні та легітимізації свого втручання у внутрішні справи сусідньої країни [17].

Російські мас-медіа повідомляли про насильство і безлад в Києві, та цитували націоналістські висловлювання (вигадані або вирвані з контексту) українських політиків.

Для позначення загрози з боку України використовувалися слова-ярлики, які викликали негативні асоціації у російської аудиторії: фашисти, неонацисти, бандерівці, націоналісти, ультранаціоналісти, антисеміти, радикали, екстремісти [17].

Водночас, Крим позиціонувався як острівець спокою і стабільності. Однак, над цим острівцем нависла серйозна небезпека в особі радикалів, які прийшли до влади в Києві. Ознаками небезпеки, за твердженнями російських ЗМІ, були різного роду провокації, примусове запровадження української мови і спроби захоплення урядових будівель «людьми, направленими з Києва» [18,19].

Російські ЗМІ повідомляли про багатотисячні проросійські мітинги у Криму під гаслами «ні фашизму» та про зізнання мешканців півострову, які «свої надії на стабільність і підтримку миру на півострові пов'язують виключно з Росією» [17].

У такій ситуації Росія не могла залишатися осторонь і кинути напризволяще російськомовних громадян. Відповідно 1 березня 2014 року Президент Володимир Путін звернувся до Ради Федерації із проханням надати йому дозвіл на використання Збройних сил на території України у зв'язку з екстраординарною ситуацією, загрозою життю російськомовних громадян та Збройних сил РФ на території Автономної Республіки Крим. Рада Федерації одноголосно підтримала це звернення [17].

Через ЗМІ російське керівництво запевняло громадськість, що таке рішення спрямоване виключно на стабілізацію суспільно-політичної ситуації в Україні («братній країні») і є реакцією на багаторазові прохання з боку влади Криму і російських громадян, які проживають в Криму.

Під час півторагодинного спілкування з журналістами російський президент назвав зміну влади в Україні «антиконституційним переворотом і збройним захопленням влади», а нову владу –

нелегітимною, націоналістською і неонацистською. Коментуючи можливість введення військ на територію України, російський президент запевнив, що такі заходи будуть вжиті лише у крайньому випадку. Він також заперечив наміри примусово приєднати Крим до РФ, а лише на основі вільного волевиявлення жителів півострова [17].

На підтримку дій Росії державні ЗМІ цитували висловлювання окремих авторитетних осіб та посилались на спеціально підібрані матеріали з європейських мас-медіа. Так, 4 березня в ефірі Russia Today наводились висловлювання сербського кінорежисера Еміра Кустуриці, який назвав події в Україні справжньою катастрофою і підтримав рішення РФ захистити росіян, що живуть в Україні [17].

В «Российской газете» було опубліковано розгорнуте інтерв'ю з американським істориком Стівеном Коеном, який оцінив реакцію президента РФ на події в Україні як абсолютно адекватну і обгрунтовану. Він також зазначив, що відповідальність за такий розвиток ситуації несуть США і Євросоюз, які перейшли певну межу, розширюючи НАТО до кордонів Росії.

Російські ЗМІ також повідомляли, що європейські журналісти все більше переходили на бік Росії в інтерпретації подій в Україні: британський телеканал Бі-Бі-Сі показав нацистську символіку на Майдані; французька газета «Фігаро» назвала державний переворот в Україні нацистським путчем; німецька газета Der Spiegel зображувала членів Правого сектора у різко негативних тонах (головорізи, радикали, неонацисти) тощо [17].

Для переконання громадськості у добрих намірах Росії у своїх промовах російські високопосадовці підкреслювали щире співчуття і занепокоєння долею українського народу, і особливо російськомовної частини населення. За словами російського президента, «у нас болит душа за всё, что происходит сейчас на Украине, что страдают люди, что они не знают, как жить сегодня и что будет завтра»; «мы не просто близкие соседи, мы фактически один народ» [20].

У заяві МЗС РФ було зазначено, що Україна для Росії – братська країна, а не територія геополітичної гри, як розглядають її західні політики [21].

Практично відразу після надання Радою Федерації Росії згоди на використання президентом збройних сил на території України парламент Криму почав швидко діяти, як за заздалегідь заготовленим сценарієм: прем'єр-міністром Криму став лідер партії «Русское единство», який звернувся до Росії з проханням про допомогу у забезпеченні миру і спокою на території Криму; парламент АРК ухвалив рішення провести референдум про статус півострова; Верховна Рада Криму і Міськрада Севастополя проголосували за входження Криму до складу РФ за тиждень до референдуму [17]. Російськими ЗМІ ці рішення подавались як історичні та єдино вірні.

Паралельно повідомлялось, що дислоковані у Криму представники Збройних Сил України нібито масово почали переходити на сторону кримського керівництва, вважаючи накази нової центральної влади нелегітимними [17].

У період з 1 по 17 березня основна увага приділялась питанням підготовки і проведення референдуму про статус Криму. Для легітимізації референдуму російські ЗМІ проводили аналогії з оголошенням незалежності Косово. Для цього наводилися цитати європейських представників про те, що визнання незалежності є виправданим за наявності елементів державності (населення, територія, уряд), і що у міжнародному праві немає положення, яке забороняє ухвалення декларації про незалежність [17].

Посилаючись на коментарі окремих експертів, російські мас-медіа впроваджували у масову свідомість такі постулати: бажання кримчан увійти до складу Росії є більш легітимним і обґрунтованим, ніж створення західними країнами держави Косово; проголошенням незалежності Косово було створено прецедент, яким можуть скористатися інші нації; референдуми, подібні кримському, є поширеною у світі практикою (приклади Південного Судану, Еритреї,

регіону Венето в Італії, Квебека в Канаді, Каталонії в Іспанії, Шотландії у Великій Британії) тощо.

Крім того, значна частина повідомлень російських медіа містила цитування висловлювань жителів Криму, для яких референдум – це радісна і довгоочікувана подія, оскільки від української влади вони відчували постійні утиски і приниження, та не бачать перспектив соціально-економічного розвитку у складі України [17].

Процес підготовки до референдуму змальовувався досить детально, з акцентом на організованості, прозорості та забезпеченні максимально сприятливих умов для голосування. ЗМІ розповідали про створений прес-центр, підготовлені бюлетені трьома мовами (російською, українською і кримсько-татарською), а також кількість міжнародних спостерігачів з різних країн (135 спостерігачів з 23 країн, за даними російського Першого каналу).

Варто відмітити, що впродовж всього періоду підготовки до кримського референдуму повідомлення про спокійну обстановку в Криму і піднесені настрої жителів півострова супроводжувались новинами про безлад і свавілля націоналістів та екстремістів в Україні, які намагались організувати провокації, проникнути до Криму для дестабілізації ситуації тощо [17].

Для нагнітання обстановки російські ЗМІ поширювали викривлену або взагалі неправдиву інформацію. Це, зокрема, повідомлення про прибуття на територію РФ понад 140 тисяч біженців з різних регіонів України, підкріплене світлиною з чергою автомобілів нібито на україно-російському кордоні, хоча насправді це пункт перетину україно-польського кордону; новина про прибуття до Києва 300 іноземних найманців з американських воєнізованих приватних компаній; повідомлення про розстріл людей у Харкові і захоплення заручників бойовиками «Правого сектору» тощо.

День референдуму описувався як свято, на яке кримчани йшли цілими сім’ями і вітали один одного. У повідомленнях підкреслювалася рекордно висока явка виборців, атмосфера спокою, ентузіазму, а також відсутність серйозних порушень.

Офіційні результати референдуму стали відомі буквально наступного дня після референдуму: 96,77% жителів півострова проголосували за приєднання до РФ. За даними російських ЗМІ, міжнародні спостерігачі практично одноголосно визнали референдум зразковим і таким, що відповідав демократичним стандартам, а результати референдуму - чесними і об'єктивними [17].

Після референдуму російські ЗМІ повідомляли про підписання і ратифікацію російським парламентом пакету документів про прийняття Криму до складу РФ, а також транслювали висловлювання кримчан про почуття радості і щастя у зв'язку із возз'єднанням Криму з Росією.

Символічним завершенням успішної операції з «повернення Криму додому» був виступ російського президента перед Федеральними зборами у Кремлі 18 березня 2014 року [22]. У виступі відображено основні складові «картини дійсності», що створювалась російською пропагандою протягом попередніх місяців, а саме: Крим є споконвічно російською землею, незаконно переданою Україні за часів СРСР; після здобуття Україною незалежності Росія була готова фактично і юридично визнати Крим українською територією, але українська влада неодноразово порушувала права російськомовних громадян; після державного перевороту 2014 року в Києві Крим опинився у надзвичайно небезпечній ситуації, яку Росія вже не могла ігнорувати; Росія не здійснювала інтервенцію та анексію Крим, а лише забезпечила умови для вільного волевиявлення кримчан у відповідності з нормами міжнародного права; Крим є важливим чинником стабільності у регіоні і має знаходитись під сильним суверенітетом, який може забезпечити лише Росія; політичну кризу в Україні та подальше реагування РФ спровокували країни Заходу, насамперед США.

Отже, російською пропагандою було створено цілісну «картину дійсності», що відповідала інтересам російського керівництва. У російській пропагандистській кампанії чітко прослідковується модель наративу У. Лейбова.

Характерними рисами російської пропаганди є тотальність, безперервність, узгодженість, однозначність, послідовність і взаємодоповнюваність повідомлень російських високопосадовців і ЗМІ, образність та високий рівень емоційності.

Для впливу на громадську думку було використано такі пропагандистські методи, як «створення загрози», «навішування ярликів», «вибіркова подача інформації», «трансфер», «очевидці подій», «повторення», «блискучі загальності», «емоційний резонанс», «посилання на авторитети», «напівправда», «зміщення акцентів», «підміна понять», «одностороння перспектива», «спрощення», «порівняння», «принцип контрасту», «маніпулятивне коментування», «інформаційна блокада» тощо.

Російська пропаганда нагадувала телесеріал з динамічним і драматичним сюжетом, в якому герої проходять крізь важкі випробування, протидіють силам зла і врешті решт здобувають перемогу [17]. За стилем оповідання репортажі про події у Криму були схожі на добрі радянські фільми, викликаючи приємні спогади і ностальгію. Формат телесеріалу дав змогу тривалий час підтримувати інтерес до теми з боку аудиторії та посилювати емоційну залученість глядачів і читачів, знижуючи критичне сприйняття інформації.

Пропагандистські кампанії проводять не лише держави, а й недержавні актори. Яскравим прикладом є пропаганда терористичної організації «Ісламська держава».

Заснована у 1999 році йорданським радикалом Абу Мусаб аз-Заркаві під назвою «Організація Монотеїзму і Газавату», сьогодні «Ісламська Держава» (ІД) – невизнана мусульманська держава і міжнародна терористична організація. У 2015 році встановила контроль над територією з населенням 10 млн осіб в Іраку і Сирії.

Терористична організація ІД характеризує себе як мілітаристська група напрямку салафітський джихадизм. Салафітська ідеологія ґрунтується на месіанській ідеї «відродження ісламу», який з часом занепав і втратив свою автентичність та чистоту. Єдине ісламське світове співтовариство, «умма», має перемогти над національною

державою. Християнський Захід є найнебезпечнішим ворогом ісламу. Ведення джихаду – єдиний шлях боротьби із Заходом, який розуміє лише мову насилля [23].

Починаючи з 2004 року ця організація прагнула заснувати Ісламську Суннітську державу і встановити халіфат. Наприкінці червня 2014 року після захоплення значних територій Іраку та Сирії ІД формально проголосила встановлення халіфату. Халіфом було проголошено Абу Бакр аль-Багдаді.

Бакр аль-Багдаді закликав усіх правовірних мусульман приєднатися до халіфату та глобального джихаду, зазначивши, що справжній іслам – це не релігія миру, а релігія війни. Він процитував священне писання, аби пояснити, що ІД бореться з невірн ими і відступниками, які є ворогами ісламу, і хочуть, щоб мусульмани відмовилися від своєї релігії. Він також назвав арабські та інші ісламські країни, які співпрацюють із західними країнами, «рабами західних держав, що використовуються для пригноблення мусульманських народів».

Промова аль-Багдаді була записана та поширена разом із пропагандистським виданням «Це обіцянка Аллаха» (This is the Promise of Allah) у мережі інтернет 29 червня 2014 року.

Для ІД «битва за уми і серця» має важливе значення, і організація розгорнула масштабну пропагандистську діяльність, націлену на завоювання прихильників, об’єднання мусульман-суннітів, залякування внутрішніх і зовнішніх супротивників шляхом демонстрації жорстокості організації, поширення інформації про ефективне державне управління у Халіфаті.

Базовими наративами пропагандистської діяльності ІД є наступні:

1. **Встановлення халіфату**. Халіфат – це місце, де всі справжні мусульмани можуть мирно жити як члени умми (історична назва мусульманської громади) та отримувати підтримку держави, як навчав пророк Мухаммед.

2. **Джихад**, до якого мають бути залучені усі мусульмани, аби зберегти свою віру. Для джихадистів мир настане лише тоді, коли всі вороги ісламу будуть переможені.
3. **Вирішення соціальних проблем і образ кращого життя**. Звертаючись до соціальних питань у своїй пропаганді, ІД надають привабливий варіант для молодих людей, які почуваються покинутими у західних країнах та не мають ні особистих, ні фінансових перспектив. Соціальні наративи призначені для того, щоб спонукати аудиторію відчути, що вони можуть зіграти роль у чомусь значимому, що приєднання до ІД може допомогти розвинути себе і повністю висловити свої переконання за допомогою певного способу життя [24].

Цільовими аудиторіями ІД було населення територій в Іраку і Сирії, які опинились під контролем бойовиків терористичної організації та мешканці інших держав, які сповідують іслам суннітського толку (арабські країни, країни Європи та Північної Америки, пострадянські країни тощо). Пріоритетним об'єктом впливу для ІД є молодь.

Для поширення пропаганди ІД створено медіа імперію, що включала такі медійні організації, як «Аль-Хайят», «Аль-Фуркан», «Аль-Аджнад», «Аль-Ітіссам», інформаційну агенцію «Амак» тощо.

Аль-Фуркан – найстаріша медійна організація ІД, заснована у 2006 році для виробництва пропагандистської продукції (компакт-диски, плакати, брошури, інтернет-матеріали і офіційні заяви). Серед її продукції – фільм «Дзвін мечів» і серія відеороликів зі стратами американських журналістів Джеймса Фолі і Стівена Сотлоффа, а також британця Девіда Хейнса.

У фільмі «Дзвін мечів» звучить нашид «Наша держава переможна» і розповідається про бійців ІД, які готуються стати смертниками, дають клятви та беруть участь у бойових діях. У фільмі також показано падіннння військових баз, капітуляція міст, вбивства «колабораціоністів», якими джихадисти вважали іракських урядовців,

військових, поліцейських та інших службовців органів влади після 2003 року. За якістю цей фільм не поступається кінопродукції Голівуду.

Медіа організація *Аль-Ітісам* з моменту свого заснування у 2013 році і до закриття у 2015 році розробляла і поширювала пропагандистські відео, націлені на новобранців у країнах з мусульманською більшістю.

Медіа організація *Аджнад*, сворена у серпні 2013 році, спеціалізувалась на трансляції джихадських пісень та музичних творів, що прославляли іслам и його захисників.

Медіа-центр *Аль-Хайят*, створений у травні 2014 року, займався виробництвом і поширенням пропагандистського контенту для західної аудиторії. Так, у вересні 2014 р. центром «Аль-Хайят» було випущено 55-хвилинний фільм «Полум'я війни» («Flames Of War»), який висвітлює захоплення бази сирійської армії поблизу міста Ракка. Відеоматеріал показує спочатку сам напад на базу, а потім бійця ІД біля неї, який вільно розмовляє англійською з американським акцентом. Цей оповідач пояснює, що бойовики ІД просто намагаються встановити закон Аллаха на землі, але піддаються нападу з боку західних країн та інших супротивників [24].

Серед друкованої продукції, що випускалася медіа-центром «Аль-Хайят» – брошури «Ісламська Держава: Доповідь» і «Ісламська держава: Новини», журнали «Dabiq» і «Румійя», які публікувались декількома мовами, у тому числі англійською. Аль-Хайят також видавав цифровий журнал турецькою мовою під назвою «Konstantiniyye», інший французькою мовою – «Дар аль-Іслам». Всі журнали також були доступні у мережі інтернет.

Видання «*Ісламська Держава: Доповідь*» і «*Ісламська Держава: Новини*» – це інформаційні бюлетені обсягом 8-10 сторінок, які публікувались з певною періодичністю, починаючи з червня 2014 року. Вони містили текстовий та ілюстративний матеріал, що розповідав про різні аспекти діяльності «Ісламської держави».

Журнал «*Dabiq*» – повноцінний високоякісний глянцевий журнал обсягом від 25 до 50 сторінок, що містив короткі повідомлення з провокаційними світлинами і графічними зображеннями, подібні до тих, що друкуються у таблоїдних виданнях. На обкладинці та перших сторінках журналу зазвичай містились заголовки статей з гаслами про політику нового Халіфату. Маніфести та короткі репортажи супроводжувались світлинами, що ілюстрували успішні атаки ІД у Сирії та Іраку, зображення поранених солдатів та переможних маршів бойовиків у захоплених містах тощо. Інші фотографії з написами «Так проголосив Халіф», «Нова ера почалася», «Ісламська держава або потоп» показували жорстокі страти шиїтів, християн та езидів або ефектні терористичні атаки по всьому світу.

Журнал «*Румійя*» містив більше матеріалів рілігійного характеру, зокрема цитати з Корану і хадисів, міркування про стовпи ісламу, смерть і потойбічне життя. У виданні публікувались ісламські тексти про життя у раю.

Інформаційна агенція *Amaq* часто публікувала онлайн-репортажі про атаки ІД за кілька годин або днів до того, як офіційні медіа організації повідомляли про них. Агенція повідомляла про наземні дії в Іраку та Сирії, а також у регіональних вілаятах.

Співробітники ЗМІ в ІД складали «привілейований професійний клас» з вищим щомісячним доходом, ніж у бойовиків ІД, та були звільнені від виплати податків. Більшість співробітників були вихідцями із західних країн, та розуміли, який контент створювати для привернення уваги західної аудиторії.

Для впливу на цільові аудиторії ІД активно використовувала мережу інтернет. ІД створила акаунти різними мовами у найбільш популярних соціальних мережах: Facebook, Twitter, Instagram, Friendica тощо.

Станом на лютий 2015 года прихильники ІД у Твіттері щодня публікували понад 90 000 повідомлень від імені групи.

ІД мала офіційний акаунт, де викладались відеозвернення і заяви керівництва; акаунт для трансляцій з захоплених територій; акаунти

конкретних бійців, де вони ділились з підписниками подробицями участі у боях, емоціями і повсякденними побутовими деталями. Будь-який користувач Twitter міг поспілкуватись з джихадистами, які охоче йшли на контакт з усіма бажаючими.

Одна з найбільш успішних ініціатив ІД у соціальних мережах - додаток для Android під назвою «The Dawn of Glad Tidings» («Зоря радісних звісток»). Це офіційний сервіс, розроблений програмістами угруповання, щоб тримати лояльних користувачів Twitter в курсі останніх новин джихаду. Як тільки прихильники ІД реєструвались у додатку, він починав твітити від їх імені однакові повідомлення.

У січні 2014 року прихильники ІД оголосили про створення Медіа-батальйону Аль-Баттар, команди на базі Twitter, призначеної для просування пропаганди ІД і критики противників. До літа 2014 року принаймні 3000 користувачів працювали разом над створенням скоординованих кампаній із хештегами.

Для вербування західної молоді пропаганда ІД апелювала до потреби у соціальній приналежності, до обов'язку і послуху, честі і слави, до гендерних стереотипів, зачіпала проблеми дискримінації і маргіналізації тощо [25].

Так, ІД позиціонувала іслам як релігію, яка приймає людей всіх національностей, і закликала приєднатись до організації. Пропагандистські матеріали містили гасло «Ми всі - Ісламська держава», аби поєднати інклюзивність ісламу з ідеєю про приналежність мусульман до великої умми.

Пропаганда ІД містила заклик до мусульман приєднатись до джихаду, представляючи це як їхній обов'язок. Ідею про обов'язок західних мусульман приєднатись до джихадистських груп просував у мережі інтернет Анвар аль-Авлакі. У своїх промовах він стверджував, що основною вимогою ісламу є вчинення «хіджри» та ведення джихаду. Для мусульманина це основний обов'язок, і він має тривати вічно, доки іслам не переможе. Під впливом його промов група з шістнадцяти канадців та двох американців «Торонто 18» планувала розмістити вантажівки з вибухівкою навколо Торонто, штурмувати

канадський парламент та обезголовити прем'єр-міністра. Прихильниця аль-Авлакі, студентка Королівського коледжу Рошонара Чоудрі зарізала члена парламенту Великої Британії за голосування на підтримку вторгнення до Іраку.

На одному з пропагандистських плакатів зображений бойовик ІД із гвинтівкою за спиною, який йде територією, схожою на сирійське місто. Цитуючи Коран, він нагадує про слова Моїсея, коли той зіткнувся з військами фараона, який намагався перетворити його та його послідовників у рабів: «Мій Господь зі мною, і Він вестиме мене». Меседж - бойовики ІД, які блукають сирійськими вулицями, звільняються від тиранії і за підтримки Аллаха здатні протистояти більш потужним ворожим силам [25].

У своїй пропаганді ІД також зверталась до гендерних стереотипів, пропонуючи жінкам більш просте і щасливе життя, звільнене від вимог і обмежень західного суспільства, а чоловікам – можливість проявити себе, свою мужність. Так, ІД поширювала в інтернеті зображення жінок зі зброєю в руках або в оточенні матеріальних благ. Меседж – жінки у Халіфаті звільнені від обмежень західного суспільства.

Для привернення уваги молодих чоловіків у пропаганді ІД використовувались графічні фотографії та відеоролики з комп'ютерних ігор Grand Theft Auto та Call of Duty. Зображення з бойовиками містили такі заголовки, як «Справжній боротьбі потрібні справжні чоловіки» та «Боягузтво не продовжить моє життя».

Знаючи, що мусульмани у західних країнах стикаються з дискримінацією та маргіналізацією, ІД пропонувала вихід – приєднатись до організації. Одне із зображень бойовика ІД зі штурмовою гвинтівкою містило підпис: «Протягом багатьох років вони ставилися до нас як до другого сорту, хоча Аллах дав нам честь і настанови через іслам».

Інший пропагандистський пост у мережі інтернет містив зображення побитого поліцією чорношкірого чоловіка у Фергюсоні із написом «США» і поряд зображення двох озброєних бойовиків ІД

різних рас, які стоять бок о бок і посміхаються, з написом «Іслам». Над цими зображеннями – гасло «Іслам – це відповідь».

Коли адміністрації соціальних мереж почали активну боротьбу проти ІД, ісламісти перейшли на анонімні онлайн платформи обміну інформацією (justpaste.it, dump.to, sendvid.com, archive.org, dailymotion.com, liveleak.com), які не мали жорсткої політики щодо поширення контенту [26].

Після розпаду Халіфату ІД продовжувала підтримувати присутність у мережі інтернет. За даними дослідницької організації VOX-Pol, незважаючи на зменшення кількості матеріалів ІД до 300 онлайн-матеріалів у грудні 2017 року, їх виробництво збільшилося до 700 у січні 2018 року.

У січні 2019 року дослідники Міжнародного центру вивчення насильницького екстремізму (ICSVE) виявили понад 500 акаунтів Facebook албанською, арабською, англійською та турецькою мовами, які просували пропаганду ІД та антизахідний контент [27].

Пропагандистський контент часто поширювався з численних URL-адрес, що посилались на різні веб-платформи, аби у разі видалення деяких адрес зберегти матеріали у мережі інтернет.

Джихадистська пропаганда стала фрагментованою, більш розосередженою і, відповідно складніше контрольованою. Домінантними темами залишились насильство як відплата, демонстрація ідеологічної чистоти групи та легітимності державного будівництва.

Через розпад халіфату та втрату контролю над значною частиною територій на Близькому Сході, в онлайн пропаганді ІД акцентувала не на державності, а на демонстрації більш довготривалої стратегії з наративом про терпіння і майбутнє відродження халіфату. У пропаганді зберігається глобальний заклик приєднатися до ІД з постійним закликом до хіджри, поряд із заявами про необхідність боротьби за халіфат через гноблення мусульман на Заході.

Отже, пропаганда «Ісламської держави» є безпрецендентною за масштабами і якістю контенту. У пропаганді ІД використано

досягнення західного суспільства у сфері реклами та масової культури – ті ж самі образи та емоційні звернення. Пропагандистські кампанії терористичної організації базуються на таргетингу та сучасних цифрових технологіях. Завдяки соціальним мережам терористам ІД вдалось створити широку мережу ресурсів з пропагандистською продукцією та залучити до її поширення цільову аудиторію. Привабливість пропаганди ІД зумовлена не лише високоякісним і різноформатним контентом, а й грамотною апеляцією до потреб і вразливостей цільової аудиторії, створенням образу ідеального суспільства, в якому мусульмани зможуть знайти сенс життя і щастя. Іслам представлено не просто як релігію, а як шлях до вирішення усіх проблем і побудови кращого майбутнього.

Питання для самоконтролю:

1. Як визначено термін «пропаганда» у словниках?
2. Як трактує пропаганду Г. Ласвелл?
3. Які характеристики пропаганди визначено американськими дослідниками Г. Джоуетта та В.О'Доннел?
4. Як працює психологічний механізм пропаганди згідно з поглядами американського дослідника Леонарда Дуба?
5. Які принципи військової пропаганди сформулював британський дипломат лорд Понсонбі?
6. Які принципи пропаганди сформульовано Адольфом Гітлером?
7. Які характеристики сучасної пропаганди визначено французьким дослідником Жаком Елюлем?
8. Чому ефект пропаганди може бути незворотнім?
9. Чим відрізняється агітаційна пропаганда від інтеграційної?
10. Які чинники впливають на ефективність пропаганди?
11. За якими ознаками можна ідентифікувати пропагандистську кампанію?
12. Які маніпулятивні методи використовуються у пропаганді?
13. Який зв’язок між пропагандою і наративом?

Завдання:

1. Навести приклади пропагандистських кампаній в інформаційних операціях 21 століття.
2. Проаналізувати промову того чи іншого політичного лідера в умовах інформаційної війни з точки зору використаних методів пропаганди.
3. Проаналізувати пропагандистський документальний фільм за такими пунктами: тема і мета телесюжету, структура телесюжету; основні герої, їхні повідомлення; візуальні образи, представлені у сюжеті; цільові аудиторії; методи пропаганди, використані у фільмі; музичний супровід, його вплив на сприйняття сюжету; емоційна насиченість сюжету; переконливість сюжету для цільової аудиторії.
4. Навести приклади пропагандистських кампаній у мережі інтернет, визначивши суб'єктів впливу, наративи, цільові аудиторії, канали поширення пропаганди. Сформулювати особливості пропаганди у мережі інтернет та запропонувати способи протидії такій пропаганді.

2.2. Дезінформація і фейки

В інформаційних війнах для впливу на громадську думку і формування вигідної для суб'єкта впливу картини дійсності широко використовується дезінформація.

Дезінформація визначається як поширення викривлених або завідомо неправдивих відомостей для досягнення пропагандистських, військових або інших цілей.

У військовій сфері дезінформація розглядається як спосіб маскування, що полягає у навмисному поширенні неправдивих відомостей про об'єкти, їхній склад і діяльність, а також імітація їхньої діяльності відповідно до цих відомостей [28].

Автор книги «Секрети психологічної війни» В. Крисько визначив дезінформування як спосіб психологічного впливу, що полягає у навмисному наданні супротивнику такої інформації, яка вводить його в оману щодо справжнього стану справ [29].

Сутність застосування методу дезінформації образно сформулював великий полководець Сунь-Цзи: «Війна – це шлях обману. Тому, якщо ти і можеш що-небудь, показуй супротивникові, ніби не можеш; якщо ти і користуєшся чимось, показуй йому, ніби ти цим не користуєшся; якщо ти був близько, показуй, ніби ти далеко; якщо ти був далеко, показуй, ніби ти близько; заманюй його вигодою; приведи його в розлад і бери його ... » [30].

За словами американського розвідника, директора Центральної розвідки (1953-1961рр.) Аллена Даллеса, у розвідці поняття «дезінформація» охоплює широке коло заходів, за допомогою яких одна держава намагається ввести в оману іншу державу, зазвичай потенційного або фактичного противника, щодо своїх можливостей і намірів [31].

Аллен Даллес відмітив, що найбільш активно дезінформація використовується в ході війни або безпосередньо напередодні війни, коли її основне завдання полягає в тому, щоб відвернути сили оборони супротивника від ділянки, де намічається удар, або створити у нього

враження, що напад зовсім не планується, або просто ввести його в оману щодо своїх планів і цілей.

Один із фахівців у сфері дезінформації К. Фокс наголошує на її концептуальній відмінності від брехні, аргументуючи тим, що метою дезінформації є введення реципієнта інформації в оману, а для цього зовсім не обов'язково брехати – досить допускати двозначність, неточність, недоговорювати про якісь факти, деталі для того, щоб останній сам додумав потрібний для дезінформатора варіант.

За словами Наталі Грант, дезінформація може бути навіть на 99%, правдою. Це розумне поєднання правди з тим, що люди хотіли б, щоб було правдою, і з явною брехнею, яку багато людей не помітять, якщо вона грамотно представлена. Отже, дезінформація визначається не відсотком правди або відсотком брехні в ній, а тим, як вона спроектована, виконана і, врешті решт сприйнята або відкинута [32].

Г. Почепцов зазначає, що дезінформація «оперує віртуальними об'єктами, які або слабко піддаються перевірці, або спростовуються постфактум, коли дезінформація вже виконала свою негативну роль. Дезінформація ховається у потоці реальних фактів, оскільки до неї застосовуються всі ті ж методи розгляду, обговорення та передачі. Процес дезінформації конструює під себе потрібний факт. Потім факт перетворюється на інформацію, яка циркулює як у соцмедіа, так і у звичайних медіа» [33].

Крім того, за словами Г. Почепцова, з масовими дезінформаційними процесами складно боротись. Це зумовлено тим, що дезінформаційна кампанія спирається на вже наявні у масовій свідомості характеристики, тільки змінює їхню пріоритетність, акцентуючи те, що несе конфліктний потенціал; першою впроваджує у масову свідомість певну інформацію, що надалі ускладнює її спростування; працює з конкретними соціальними групами, виводячи їх на протистояння одна з одною, а решта населення стає свідком цієї боротьби. Крім того, поширювані наративи починають сприяти появі контр-наративів, чим посилюється протистояння, що переходить

спочатку з інформаційного простору у віртуальний, а потім може перейти у фізичний простір [33].

Дезінформація – це завжди усвідомлена політика і частина ширшого політичного поряду денного. Вона реалізується з чітким розумінням, що поєднання правди і брехні – корисно і ефективно. І ця мета переслідується до тих пір, поки дезінформація є ефективною [28].

Сценарій дезінформаційних заходів розробляється так, щоб надати ворогові шматочки здебільшого правдивої інформації, яка проте призводить до невірних висновків. Мета – змусити об'єкт впливу діяти на основі цього помилкового висновку.

Основними принципами дезінформування є такі:

Чітка спрямованість. Розробник дезінформації має чітко уявляти, кого і з якою метою він має ввести в оману, яка поведінка якого об’єкта дезінформації є кінцевою метою запланованих заходів.

Своєчасність. Дезінформування вимагає ретельного розрахунку часу.

Правдоподібність інформації. Поширювана дезінформація має містити частину правдивої інформації, корелювати з вже існуючими переконаннями об’єкта впливу, і забезпечувати можливість підтвердження при перевірці інших джерел.

Узгодженість. Дезінформаційні заходи вимагають тривалої і ретельної підготовки, тісної співпраці та координації дій всіх задіяних підрозділів суб'єкта впливу.

Секретність планування та проведення передбачає уникнення витоку інформації про цілі дезінформації, факт проведення дезінформаційних заходів, зміст модифікованої інформації і заходи з її розповсюдження. Секретність також передбачає диференційовану обізнаність виконавців щодо плану проведення заходів та завчасне розроблення легенди прикриття у разі часткового викриття заходів з введення в оману.

Доцільність. Вигода (політична, економічна, воєнна тощо) від проведення дезінформаційної операції має переважати ризики у разі часткового викриття, зриву чи провалу операції.

Багатоканальність. Неправдива інформація має бути представлена супротивнику через якомога більшу кількість інформаційних джерел. Підтвердження з різних джерел мають бути достатньо переконливими, аби викликати довіру об’єкта впливу [30].

Мистецтво дезінформації полягає у тому, щоб дати об'єкту інформацію, яка гранично близька до істинного стану справ і водночас містить щось таке, що має ввести її адресата в оману. Це може бути сильна деформація і посилення окремих фрагментів існуючого стану речей.

Так, під час військових дій в Боснії і Герцеговині з подачі PR-агенції «Ruder Finn» англійською телекомпанією було знято «документальний» фільм про «звірства» сербів. Головним лейтмотивом цього фільму був старий мусульманин у сербському фільтраційному таборі за колючим дротом. Надалі з'ясувалося, що хоча табір існував насправді, але колючого дроту там не було, він був лише на вікні будиночка, з якого знімав оператор [28].

Цілі дезіформаційних операцій формулюються у формі спеціальних і конкретних дій. Мета дезінформаційної кампанії розглядається як бажаний результат щодо введення в оману, виражений у вигляді того, що опонент має робити або не робити у вирішальний момент часу або місці. На практиці це означає, що у кожній операції, а можливо, і на кожному її етапі, цілі дезінформування будуть різними залежно від конкретних умов обстановки [28].

Введення супротивника в оману вважається активним методом і здійснюється наступними способами: відволікаючими, демонстраційними, імітаційними діями; поширенням неправдивих чуток або доведенням до супротивника помилкових планів. Кожен спосіб може застосовуватися окремо або разом з іншими [34].

Мета *відволікаючих дій* полягає в тому, щоб удари, що наносяться малими силами, супротивник прийняв за удари вирішальні, націлив на них свою увагу і ввів у дію резерви.

Демонстративними діями називається такий спосіб введення супротивника в оману, при якому демонструються заздалегідь

заплановані заходи і у супротивника створюється спотворене уявлення про справжні задуми і плани командування. Головне завдання цього способу – обдурити супротивника щодо складу, намірів і діяльності своїх військ без проведення активних дій і спонукати його зробити невигідні для нього кроки.

Імітаційні дії передбачають створення помилкових об'єктів із застосуванням різних макетів, пошкодженої техніки і інших подібних засобів. Для обману супротивника іноді можлива імітація звичайної повсякденної діяльності військ.

На думку М. Присяжнюка та О. Параніч, дезінформація може здійснюватися двома основними способами: дисимуляцією і симуляцією. Принцип дисимуляції полягає у тому, що суб’єкт намагається приховати явище або подію від об’єкта. Значення симуляції прямо протилежне і передбачає намагання суб’єкта змусити об’єкт впливу повірити в істинність наданої йому інформації [30].

До дисимуляції можна віднести маскування, камуфлювання (легендування), затінення обстановкою; до симуляції – конструювання, імітація, обманні (удавані) дії.

Маскування є найбільш простою формою дисимуляції і полягає у максимальному приховуванні об’єктом явища (інформації, подій, предметів), яке він не хоче розголошувати.

Камуфлювання (легендування) застосовується тоді, коли приховуване явище не можна зробити зовсім непомітним, тому здійснюється часткове маскування, що спотворює сприйняття цього явища/події об’єктом впливу, внаслідок чого його важко правильно ідентифікувати.

Затінення обстановкою передбачає реалізацію заходів, що стосуються обстановки навколо приховуваного явища, тобто якщо потрібно потай надіслати сигнал, навкол нього створюється такий шум, що всі, крім тих, кому він призначений, сприймають його як частину цього шуму.

Основні категорії симуляції (конструювання, імітація й обманні (удавані) дії) мають на меті створення видимості, демонстрацію події або явища, які насправді не існують.

Конструювання полягає у тому, що суб'єкт створює нове, але хибне явище і прагне, щоб об'єкт впливу сприйняв його як справжнє.

Імітація передбачає створення фальшивих мішеней для відвернення уваги супротивника від реальних об'єктів. Наприклад, під час операції "Буря в пустелі" іракська сторона використовувала хибні аеродроми, моделі танків, і американці здійснювали по них масовані авіаційні й артилерійські удари.

Обманні (удавані) дії. Даний метод полягає у проведенні відволікаючого маневру, внаслідок якого об'єкт сприймає одне явище за інше, тобто неадекватно або хибно оцінює його зміст. Удавані дії відрізняються від методів дисимуляції тим, що становлять реальні дії для відволікання уваги об'єкта від інших запланованих заходів (більш важливих) або з іншою метою.

Різновидом дезінформації є фейк. У перекладі з англійської мови слово fake означає підробку, фальшивку. У кембриджському словнику фейк визначається як об'єкт, створений так, щоб виглядати реальним або цінним, аби ввести людей в оману [35].

У словнику Меріам-Вебстер (Merriam-Webster) зазначено, що поняття fake news в англомовному інформаційному просторі з'явилося наприкінці XIX ст., з поширенням використання прикметника fake/fake news – «підроблений/підроблені новини» замість false/false news – «неправдивий/неправдиві новини». Різниця між цими поняттями полягає у тому, що false означає «неправдивий, «некоректний», у той час як fake означає «імітуючий», «підробний», тобто характеризує явища та предмети, що імітують ті, які реально існують [36].

Прототипом фейків можна вважати так звані «газетні качки», які з'явились у 17 столітті. «Газетні качки» – неперевірена або хибна інформація, що використовувалась редакторами газет для привернення уваги читачів і збільшення тиражу. Водночас, журналісти не бажали

втратити репутацію, і тому сумнівні і неперевірені новини позначали літерами NT, тобто non testatum – «неперевірений» [37].

Для журналістики кінця XVIII століття була характерною установка на розвагу читачів, і для цього журналісти часто використовували вигадку.

Як відзначив свого часу Бенджамін Франклін, «достовірність фактів не варто вважати абсолютною цінністю: занадто часто вони є менш захопливими, ніж вигадка, а цей дефект не такий нешкідливий, як здається на перший погляд» [37].

Для збільшення свого тиражу і заробітку газети не зупинялися ні перед чим, навіть могли розв'язати війни.

Так, коли відносини США та Іспанії стосовно Куби були напружені, американський медіамагнат Вільям Херст відправив своїх кореспондентів на Кубу. Згодом вони йому написали, що на Кубі все спокійно і немає ознак підготовки до війни. У відповідь Херст написав листа такого змісту: «Залишайтеся на Кубі. Забезпечте мене статтями, а я забезпечу вас війною». Після цього він опублікував у газеті «Жорнел» сфабриковані новини, щоб нацькувати лідерів двох держав один проти одного. Зрештою він досяг свого і розв'язав війну. В результаті кількість читачів його газети зросла у кілька разів [37].

Сьогодні існують два підходи до визначення фейків. У широкому значенні фейк – це не лише фейкові новини, а і люди, які видають себе за інших, світлини, підроблені, змонтовані у відповідних програмах; несправжні сайти або сайти, підроблені під справжні; несправжні сторінки від імені відомих осіб тощо [38]. Відповідно до вузького підходу, поняття «фейк» розглядається виключно тоді, коли йдеться про новини, а саме повністю вигадані історії.

Сутність фейкових новин чітко визначив Папа Римський. За його словами, «термін «фейкові новини» означає «неправдиву інформацію, засновану на неіснуючих чи змінених фактах, призначених для обману чи маніпулювання аудиторією. Ефективність фейків виходить з їх особливості імітувати справжні новини, здаватися правдоподібними. Ці фальшиві новини, що здаються достовірними, «прив'язливі»,

оскільки вони захоплюють увагу людей, апелюючи до стереотипів і соціальних забобонів і експлуатуючи миттєві емоції, такі як занепокоєння, зневага, гнів і розчарування. Неправдиві історії можуть поширюватися так швидко, що навіть авторитетне спростування не може зупинити завданої шкоди» [33].

За словами українського дослідника Г. Почепцова, «фейкові новини креативні, сенсаційні, привабливі для маси людей своїм пікантним характером і, отже, цікавіші, ніж тривіальні новини та факти. Фейки - це підсилювачі того, що вже було записано в індивідуальній і масовій свідомості до їхньої появи. Фейки експлуатують існуючі у суспільстві етнічні, расові, гендерні протиріччя» [33].

Крім того, на думку Георгія Почепцова, поширювачами фейків є звичайні люди, оскільки точкові інформаційні вкиди спрямовані на створення ланцюгової реакції масової свідомості. Фейк також дає можливість людині стати частиною групи однодумців. Як наслідок, така людина у колі «інформаційних друзів» стає здатною до групових дій, що суперечать очікуванням більшості [39].

І. Мудрая виокремила такі завдання фейкових повідомлень: дезінформувати аудиторію; пропагувати своє бачення, політику чи позицію; викликати агресію; похитнути позицію індивіда і змусити його засумніватися; посіяти паніку; змінити думку аудиторії; спонукати до певної дії; активувати увагу та зацікавити аудиторію; переконати аудиторію за допомогою вигаданих фактів; залякати аудиторію тощо [40].

Приклади. Одним з історичних прикладів успішної дезінформаційної операції є операція «Бодігард» під час Другої світової війни, з метою введення в оману німців щодо місця висадки союзників.

Мета операції – переконати німців у тому, що висадка сюзників у Нормандії відбудеться в іншому місці. Основними складовими операції «Бодігард» були операції «Фортитюд-Південь» і «Фортитюд-Північ». Перша була покликана переконати німців, що головний удар

супротивник завдасть у Кале, щоб відтягнути німецькі сили від берегів Нормандії, аби союзники мали більше часу для висадки піхоти [41].

З цією метою союзники сформували фальшиве угруповання – «перша армія США», яка базувалася неподалік Дувра, навпроти Кале. З метою введення в оману повітряної розвідки німців в зазначеному районі було розміщено макети танків, фальшиві військові табори і штаби, макети нафтовозів.

Для дезінформування німців була задіяна агентурна мережа. Протягом півроку подвійні агенти відправляли до Німеччини шифровки, більшість з яких містила справжні відомості, аби завоювати довіру супротивника. Агентам вдалося переконати німців, що головного удару союзники завдадуть у Кале чи Норвегії, і станеться це у липні 1944 року, а наступ у Нормандії – лише помилковий маневр, що має на меті відвернути увагу супротивника від головного удару в Кале.

Операція «Фортитюд-Північ» мала за мету змусити німців повірити, що вторгнення англо-американських військ розпочнеться з висадки на узбережжя Норвегії в районі Тронхейму. Для цього було створено ще одне фіктивне армійське угруповання – «Британська 4-та армія», дислокована в Единбурзі. На момент операції німці зосередили на узбережжі Норвегії 400 тисяч солдатів, на той випадок, якщо ворог десантується саме там [42].

Дезінформаційна операція також включала фіктивні удари по Іспанії, західному узбережжю Франції, західному узбережжю Італії, а також по Албанії, Греції, Румунії та Швеції.

Обман спрацював: у Нормандії залишалося значно менше німецьких військ, оскільки Адольф Гітлер перекинув їх на північний захід Європи.

Вперше узбережжя Нормандії зазнало масованого удару авіації за 9 годин до початку операції, тобто тоді, коли супротивник вже практично не мав можливості залучити резерви.

Рано-вранці 6 червня в Нормандії та Па-де-Кале в рамках операції “Титанік” висадилися загони барабанщиків у військовій формі. Вони

мали спеціальне шумове обладнання, яке імітувало звук стрілянини та повітряного нальоту. Їх головною метою було відвернути увагу ворога від основних сил союзників, що висадилися трохи західніше цього місця. За кілька годин до фактичного вторгнення для відволікання уваги противника союзники провели дві демонстративні висадки десантів, в яких було задіяно велику кількість катерів, барж і літаків.

Вночі британські літаки скидали у море в районі Па-де-Кале смужки фольги. Їх фіксували німецькі радари, і створювалася ілюзія, ніби до берегів Кале рухається армада військових кораблів. А ще у протоку вийшли 28 канонерок з прикріпленими до них аеростатами. Повітряні кулі були обклеєні металевими відбивачами: вони ловили сигнали німецьких радіолокаційних станцій і відображали у збільшеному вигляді. Складалося враження, ніби через Па-де-Кале рухається потужний військовий флот. І німці відкрили вогонь по фользі.

Німецьке командування до 6 червня зосередило майже всю 15-у армію в районі Кале-Булонь. Навіть тоді, коли почалася висадка в Нормандії, німці вважали, що це масштабна демонстрація.

Більш того, тільки через 10 днів - 16 червень 1944 року Гітлер віддав наказ передислокувати зі Східного фронту 2-й танковий корпус СС, а також 86-й армійський корпус з Південної Франції і частину 15-ї армії, що прикривали Па-де -Кале від неіснуючої загрози вторгнення. Однак нові дивізії без потрібного запасу палива і боєприпасів не змогли переломити ситуацію на свою користь. Завдяки цьому союзникам вдалося домогтися величезної переваги у силах і засобах в районах висадки в перший день вторгнення.

У сучасному світі дезінформація використовується не лише у воєнний період, але й у мирний час.

Актуальним прикладом є безпрецедентних масштабів російська дезінформація в інформаційній війні проти України, починаючи з 2014 року. Більшість повідомлень російських медіа про Україну є спотвореними і створюють викривлену картину дійсності.

Так, на початку квітня 2014 року російський телеканал НТВ показав сюжет про професора одного з харківських ВНЗ, який нібито був змушений звільнитись, тому що йому заборонили викладати російською мовою [43].

У сюжеті НТВ професор Олександр Міхілєв розповідав, що декану факультету раптом не сподобались «ідеологічні погляди викладача». Декан факультету нібито сказав професору, що враховуючи політичну ситуацію, «говорити, навчатись і навіть думати російською мовою – це просто зрада». Професору запропонували два варіанти – вивчити українську мову або звільнитись.

Як стало відомо, О. Міхілєв працював у Харківському національному університеті імені Каразіна на кафедрі зарубіжної літератури і класичної філології. За словами декана філологічного факультету, професор завжди читав лекції російською мовою й адміністрація університету не забороняла йому це робити.

Звільнення професора було добровільним, а не вимушеним. О. Міхілєв, порушуючи трудове законодавство, підписав контракт з іншим ВНЗ. Дізнавшись про це, адміністрація університету попросила його визначитись, в якому навчальному закладі він хоче працювати. Професор вирішив змінити місце роботи і написав заяву про звільнення за власним бажанням з 1 листопада 2013 року.

Однією з тем російської пропаганди з 2014 року є присутність військ НАТО та США на Донбасі. Так, 15 жовтня 2014 року російські медіа повідомили про прибуття чорношкірих найманців у Харків зі США. Основою для такої заяви стало відео із двору одного з харківських готелів, де дійсно були присутні вишикувані чорношкірі чоловіки у камуфляжі, які зупинялися у готелі «AN2-». Насправді, за даними «StopFake», це були технічні фахівці з Нігерії, які проходили практику на одному із харківських підприємств. А в жовтні скоріше всього та ж сама група людей проходила навчання з експлуатації автомобілів КрАЗ у Кременчуці [44].

19 лютого 2015 року на сайті «МИА Новороссия» із посиланням на американське видання «Vice News» було розміщено повідомлення,

що начебто «Захід визнав участь підрозділів НАТО у війні на боці ЗСУ». В якості доказу наводився лише той факт, що західне видання написало про командира з ім'ям Джексон, який вивів американський підрозділ із Дебальцевського котла. Насправді, в оригінальній публікації йшлося про українського військового із позивним «Джексон», який, за даними StopFake, неодноразово з'являвся у повідомленнях українських ЗМІ.

У серпні 2015 року російський веб-портал «Русская весна» та телеканал «Звезда» повідомили про те, що так звана розвідка ЛНР помітила на лінії розмежування американські танки «Абрамс» у той момент, коли українські військові нібито переганяли їх до свого укріпрайону. В якості доказу у матеріалі була розміщена світлина танків Абрамс, яка зустрічається на багатьох веб-сайтах у довідкових статтях про даний тип американських танків [44].

9 жовтня 2016 року російські ЗМІ поширили заяву спікера бойовиків Едуарда Басуріна про те, що на Донбас прибули снайпери зі США для участі у бойових діях на боці України. Ніяких інших фактів присутності американських солдатів на Донбасі, окрім як заяви Басуріна, наведено не було. За даними StopFake, троє американців дійсно підписали контракт з Міністерством оборони України, і в одного з них навіть взяли інтерв'ю на «Радіо Свобода». Але всі троє були добровольцями.

У квітні 2018 року Едуард Басурін заявив про підготовку провокацій українськими військами і переведення на Донбас групи військовослужбовців з країн-членів НАТО, яка «нібито прибула в зону АТО для ознайомлення з обстановкою». При цьому видання «Украина.ру» подало цю заяву як «Басурін: Військові з країн НАТО прибули на Донбас для здійснення провокацій».

Крім того, російські ЗМІ поширили заяву Едуарда Басуріна про те, що розвідка «ДНР» отримала секретну інформацію зі штабу АТО про інсценування ЗСУ спільно з натівськими радниками хімічної атаки по власним військам. На його думку, на Донбасі реалізується «сирійський сценарій» [39].

Для цілісності пропагандистського наративу про війська НАТО на Донбасі російські медіа повідомляли не лише про їх присутність, а про нібито існуючі втрати.

Так, 7 травня 2014 року видання «Взгляд» та ще кілька російських медіа з посиланням на «західні ЗМІ» повідомили про збиття двох українських гелікоптерів Мі17, внаслідок чого нібито загинули 13 найманців з ПВК «Greystone», які при цьому виявилися ще й агентами ЦРУ. «Взгляд» посилався на маргінальне видання «The European Union Times», а те, в свою чергу, – на ще більш маргінальний конспірологічний сайт «WhatDoesItMean.com».

За даними «StopFake», 2 травня у Слов'янську бойовики дійсно збили дві бойові одиниці, але Мі24, а не Мі17, і ще один гелікоптер Мі8 було пошкоджено. Однак, бойовики не знайшли «13 американських шпигунів-найманців», адже загинуло двоє українських військових і ще один потрапив у полон [44].

На початку грудня 2014 року проросійські ЗМІ опублікували інформацію із звіту «Міжрегіонального суспільного фонду сприяння стратегічній безпеці», в якому окрім втрат української армії на Донбасі, зазначено «втрати» іноземців, серед яких - 88 вбитих співробітників ЦРУ, ФБР та спецназу Міноборони США, а також 630 бійців «приватних армій» з їх стандартним переліком: «ASBS Othago», «Academi» і «Greystone». Слід зазначити, що сам фонд заснований колишніми співробітниками органів держбезпеки РФ, а у власному описі на сайті вказано, що він «дотримується чекістських традицій» [44].

17 травня 2018 року «Донецкое агенство новостей» і російські медіа повідомили про підрив військових НАТО на мінному полі біля Авдіївки. В Альянсі цю інформацію спростували, заявивши, що на Донбасі взагалі немає військових Північноатлантичного альянсу і жодна із країн-союзників не повідомляла про втрати.

У жовтні 2019 року деякі російські онлайн-медіа поширили новину під заголовком «В Нидерландах требуют признать вину Украины в крушении МН17» [45].

В самому повідомленні стверджується, що депутат від Партії Свободи Раймон де Роон вніс на розгляд парламенту Нідерландів питання про притягнення України до відповідальності за аварію малайзійського літака Boeing MH17 у 2014 році. За словами Роона, Київ мав не лише вагомі підстави, а й можливість закрити повітряний простір над територіями, де проходили бойові дії, до трагедії, що трапилася з авіалайнером.

Насправді у Палаті представників парламенту Нідерландів вимагали розслідувати «роль України» у трагедії рейсу MH17 у липні 2014 року над територією Донбасу. Мова йшла про те, щоб з'ясувати, чому Україна не закрила повітряний простір на Донбасі під час бойових дій [46].

У вересні 2020 року російські ЗМІ (зокрема, NewsFront, Украина.ру, Политнавигатор, Regnum, Федеральное агентство новостей) поширили повідомлення, в яких назвали військові навчання «Спільні зусилля-2020» та Rapid Trident 2020 «наглядним прикладом окупації країни». У статтях також повідомлялось про «незаконність» перебування військ НАТО в Україні, оскільки ці навчання відсутні у переліку, затвердженому Верховною Радою України у відповідному законі від 4 березня 2020 року [47].

У законі справді не згадувалися деякі військові навчання. Проте, вичерпні дані щодо кількості військовослужбовців інших країн та військового озброєння, які допускалися на територію України протягом 2020 року, містились у додатку до цього закону. У додатку чітко сказано, що, у період з червня по вересень в Україну допускалися до 3750 іноземних військовослужбовців із озброєнням та військовою технікою, до 50 кораблів (катерів та суден), до 2 підводних човнів, до 40 літаків та вертольотів, до 90 одиниць колісної техніки. Крім того, війська НАТО перебували в Україні тимчасово, лише на період міжнародних військових навчань.

Наприкінці вересня 2021 року деякі російські медіа поширили заяву політолога Олександра Семченко у програмі «60 хвилин» на російському телеканалі про те, що українська армія відпрацьовувала на

спільних навчаннях з НАТО дії щодо придушення мирного населення Донбасу. За його твердженням, сценарій навчань передбачав, що частина солдат перевдягалась у цивільне населення, і солдати вчилися придушувати мирне населення [48].

Насправді, за інформацією Міністерства оборони України, сценарій навчань «Об'єднані зусилля-2021» передбачав подолання заблокованої дороги та зустрічі військових з обуреними місцевими жителями. Завдання військових полягало у тому, щоб розблокувати дорогу та продовжити рух до пункту призначення. Під час навчань командир провів перемовини з представником протестуючих. Виявилось, що місцеві були налякані присутністю військових та страждали через нестачу питної води та їжі. Військові не лише змогли погасити конфлікт і продовжити рух, а й поділилися з «місцевими» їжею та водою із власних запасів, отримавши їхнє визнання.

Одним з методів введення в оману, що використовується російськими журналістами, є маніпуляції з перекладом матеріалів зарубіжних ЗМІ. Внаслідок таких маніпуляцій виявляється, що DieWelt називає «Білі каски» «псевдозахисниками прав людини» і звинувачує їх у розкраданні грошей; Foreign Policy пропонує різні сценарії повалення президента Білорусі Олександра Лукашенка; Newsweek «підтверджує» існування планів США щодо силового захоплення влади в Ірані тощо [49].

Російські журналісти діють за таким алгоритмом. Спочатку вони знаходять статтю у зарубіжних ЗМІ, в яку можна вставити потрібний текст, не викликаючи підозр. Потім журналісти пишуть власний матеріал російською мовою, роблячи вигляд, що цитують оригінальний матеріал. Але насправді вставляють у статтю факти чи заяви, які є або невірним перекладом, або повною фальсифікацією. Після цього стаття отримує новий заголовок, перекладається на інші мови і публікується здебільшого у маргинальних виданнях чи блогах.

Такі маніпуляції складно виявити, оскільки це вимагає певного рівня обізнаності, вміння і бажання перевіряти факти, володіння іноземними мовами тощо.

Після початку повномасштабного вторгнення на територію України 24 лютого 2022 року та оголошення Президентом України загальної мобілізації росія розпочала дезінформаційну кампанію, спрямовану на зрив мобілізації.

Антимобілізаційні меседжі базувались на реальних фактах, змішаних з маніпуляціями і фейками, та поширювалися не лише російськими пропагандистами, а й українцями, які потрапили під їх вплив.

Серед цих меседжів були такі: мобілізація незаконна через те, що в Україні «неправильний» воєнний стан; територіальні центри комплектації та соціальної підтримки (ТЦК) є не частиною ЗСУ, а «приватними фірмами», і тому не мають права проводити мобілізацію; ЗСУ зазнають великих втрат, командири не бережуть бійців, тому мобілізовані приречені на загибель; не варто воювати за корумповану владу, яка порушує права громадян, і закриває кордони; російська армія непереможна, чинити спротив немає сенсу [50].

Антимобілізаційна кампанія була націлена також на дискредитацію працівників ТЦК шляхом просування повідомлень про хабарництво, перевищення службових повноважень працівниками ТЦК, конфлікти за участю військових тощо.

Протягом 2022-2023 років дезінформаційна кампанія була спрямована на популяризацію пасивного ухилення від мобілізації (ігнорування військового обліку, уникнення контактів з ТЦК, створення фіктивних підстав для отримання відстрочки), а на початку 2024 року - активних форм ухилення (незаконний перетин кордону, насильство проти співробітників ТЦК, підпали автомобілів) [50].

Для просування дезінформації російські пропагандисти використовували медіаресурси (веб-сайти, профілі у соцмережах, Telegram-канали), ботоферми та фабрики тролів.

У 2022 було створено десятки регіональних Telegram-каналів, які поширювали повідомлення з локаціями, де нібито співробітники ТЦК видають повістки.

Як точку входу в український медіапростір російські пропагандисти використали TikTok, адже алгоритми рекомендацій цієї соціальної мережі починають просувати відео раніше, ніж його опрацюють алгоритми модерації, що відповідають за блокування та видалення контенту. Це означає, що українські користувачі TikTok мають дуже високі шанси побачити російську дезінформацію з популярними хештегами, навіть якщо вони не підписані на сторінки з таким контентом.

Так, до Топ-10 найпопулярніших хештегів увійшли відверто антимобілізаційні, такі як: #стоптцк, #народпротитцк, #спротивтцк, #протесттцк, а також антидержавний хештег #ценемояукраїна. Здебільшого вони супроводжувались відео (як реальними, так і постановочними) з конфліктами за участю співробітників ТЦК, а також вирваними з контексту переказами образливих історій та невдалими цитатами з інтерв'ю військових про необхідність мобілізації.

До антимобілізаційної теми російські пропагандисти включили також резонансні випадки, пов'язані з насильством та спробами самогубства. Так, коли жінка підпалила себе біля будівлі суду у Білоцерківському районі Київської області, російські пропагандистські ресурси подали це як «акт спротиву» через те, що суд не надав її чоловікові відстрочку від мобілізації (насправді відстрочки від мобілізації оформлюються у ТЦК, а не у судах). Протягом трьох днів фейк поширили понад 40 російських і проросійських веб-сайтів і Telegram-каналів. Поширення фейку відбувалося навіть після того, як поліція надала офіційне пояснення: суд розглядав справу щодо прав жінки і чоловіка на опіку над їхньою дитиною [50].

У 2022 році було виявлено також масштабну російську дезінформаційну кампанію відому як «Doppelganger» (Двійник). За даними ФБР, у кампанії «Двійник» були задіяні три організації: Social Design Agency (піар-агенція, яка спеціалізується на виборах, і належить політтехнологу Іллі Гамбашидзе), STRUCTURA (технологічна компанія з досвідом використання ботів і створення веб-сайтів) та АНО

«Діалог» (урядова організація, що працює у сфері інтернет-комунікацій, проводить моніторинг соціальних мереж та поширює онлайн пропаганду про війну в Україні).

Дезінформаційна кампанія здійснювалась під керівництвом Сергія Кирієнка з адміністрації президента рф [51]. Для просування російської дезінформації використано скоординовані коментарі ботів, які видавали себе за громадян інших країн, та підроблені версії справжніх новинних веб-сайтів.

Проросійські наративи поширювались через фейкові веб-сайти, які були майже повною копією реальних медіа, таких як The Washington Post, Fox Business, Der Spiegel, Fox News, Le Monde тощо. Фейкові статі приписувались реальним журналістам цих видань, а посилання на інші матеріали автора вели на справжній сайт ЗМІ.

Так, у Пенсильванії агенти ФБР виявили шість статей, опублікованих на сайті washingtonpost.pm, що мав майже однаковий із реальним медіа вигляд. Усі покликання, наприклад у меню навігації, перенаправляли читача на реальний портал The Washington Post. Фейковість веб-сайту видавали статті з проросійськими наративами.

Наприклад, одна зі статей під назвою «Білий дім прорахувався: конфлікт із Україною зміцнює Росію», автором якої нібито був репортер The Washington Post, містила такий текст: «Настав час нашим лідерам визнати, що подальша підтримка України є помилкою. Це була марна трата життів і грошей, а стверджувати інше – лише засіб подальшого знищення. Заради всіх учасників конфлікту адміністрація Байдена має просто укласти мирову угоду і рухатися далі» [51]. На справжньому веб-сайті The Washington Post такого матеріалу немає.

Публікації на сайтах-двійниках часто з’являлись паралельно з реальними статтями на таку саму тему. Наприклад, після злочинів у Бучі, які висвітлювали іноземні ЗМІ, «альтернативна» стаття різними мовами з'явилася на кількох підроблених сайтах: відповідно англійською – на сторінках несправжнього The Guardian, італійською – на ANSA та німецькою – на Der Spiegel. Цей контент поширювався

через рекламу у соціальних мережах, а коментували його переважно боти.

Фахівці урядової французької агенції VIGINUM з лютого 2023 року виявили близько 160 сторінок у Facebook, на яких розміщено понад 600 публікацій із покликаннями на веб-сайти, пов'язані з кампанією «Двійник».

Восени 2023 року в рамках кампанії «Двійник» було розпочато проєкт «The Good Old U.S.A» (Старі добрі Сполучені Штати Америки) [52]. Як з'ясували фахівці ФБР, до кампанії впливу на вибори у США була залучена піар-агенція Social Design Agency, яка мала чітко продуманий алгоритм дій. «Проєктний офіс», що складався з чотирьох команд, проводив моніторинг дописів законодавців від Республіканської партії у соціальних мережах та генерував ідеї і теми для подальшого висвітлення. Далі моніторингова група передавала дописи у «фабрику текстів», де всі теми скорочували до 4–5 основних питань, а також готували 8–10 базових дописів для соціальних мереж і 40–60 коментарів для мережі ботів під цими публікаціями. Інша команда під назвою «редакція манги» мала щодня генерувати три-чотири зображення включно з мемами. Відеокоманда випускала три-чотири відео щодня.

Мета кампанії «The Good Old U.S.A» – сформувати громадську думку, що Сполучені Штати мають спрямовувати свої зусилля на внутрішні проблеми, а не витрачати гроші на Україну та інші «проблемні регіони».

Фальшиві історії, замасковані під резонансні події, підживлювались масовим поширенням коментарів і мемів у Facebook та X (Twitter). За допомогою штучного інтелекту було створено контент для негативної реклами американських політиків. Деякі акаунти дублювали такі ЗМІ, як CNN California, Sacramento Inside, California News і California BBC [52].

У 2024 році кампанія «Doppelganger» була спрямована на нагнітання напруженості в США через прикордонну кризу в Техасі та

поширення неправдивих заяв про те, що такі знаменитості, як Тейлор Свіфт, підтримують вторгнення Росії в Україну.

За інформацією ФБР, організатори націлилися на наявні розбіжності в американському суспільстві, використовуючи расистські стереотипи й ультраправі нападки на прихильників екс-президента Дональда Трампа.

Один з документів російського полтітехнолога містив низку расистських і конспірологічних тверджень, зокрема про те, що республіканці є «жертвами дискримінації кольорових людей», що білі представники середнього класу зазнають дискримінації через високу інфляцію і зростання цін, тоді як «безробітні кольорові люди стають привілейованими групами населення» [53].

Окрім перемоги на виборах Дональда Трампа, вторинна мета кампанії «Двійник» полягала у збільшенні частки американців, які вважають, що США роблять забагато для допомоги Україні, до 51%, і зменшенні частки американців, які довіряють президентові Джо Байдену, до 29%.

Цільовими аудиторіями були жителі штатів, які вагаються, американські євреї, громадяни США латиноамериканського походження, а також спільнота американських геймерів, користувачі Reddit та іміджбордів, таких як 4chan.

В рамках кампанії передбачалось створення YouTube-каналів з протрампівським контентом, спільнот прихильників Дональда Трампа у Facebook, Twitter і Reddit, а також 18 «сплячих осередків» у соціальних мережах у кожному зі штатів, що вагаються, які можна було б активізувати у потрібний момент. Невідомо, чи були створені ці «сплячі осередки», і якщо так, то чи є вони досі на онлайн-платформах.

В рамках проєкту «Старі добрі Сполучені Штати Америки» планувалась також робота з інфлюєнсерами, які є «прихильниками традиційних цінностей, виступають за припинення війни в Україні та мирні відносини між США і Росією, а також готові долучитися до просування наративів проєкту» [53].

У документах російського політтехнолога також зазначалось, що для забезпечення ефективності кампанії впливу на вибори у США потрібно використовувати мінімум фейкових новин і максимум реалістичної інформації, а також повторювати меседж про те, що офіційні ЗМІ ніколи не розкажуть і не покажуть того, що відбувається насправді.

Дипфейк (DeepFake). За оцінками експертів, у найближчому майбутньому практично неможливо буде відрізнити підробку від оригіналу завдяки поширенню технології Deepfake. Дипфейк» складається із двох англійських слів: deep learning («глибинне навчання») та fake («підробка»).

Дипфейк – технологія створення підробленого аудіо чи відеоконтенту за допомогою штучного інтелекту. Основу дипфейків складають нейронні мережі, які дають змогу максимально правдоподібно підробити обличчя, міміку і голос окремої особи і вкласти в уста цієї особи те, що вона ніколи не говорила [54].

Відеодипфейк відтворює людину, її риси обличчя та манеру мовлення за допомогою алгоритмів. Таким чином створюється імітація справжнього зображення людини. Створення дипфейку починається зі збору світлин конкретної особи. Світлини завантажуються у спеціальну програму, яка встановлює зв’язок між візуальними і фізичними рисами особи (наприклад, між обличчям і тілом, між мімікою і словами тощо).

Для того, щоб відео виглядало реалістичним, використовуються генеративно-змагальні нейромережі (GAN), розроблені студентом Стенфордського університету Яном Гудфеллоу ще у 2014 році. Механізм такий: одна частина комп’ютерної програми генерує дипфейки, а інша частина намагається розпізнати фейк. Цей процес триває, доки друга частина програми не почне плутати копію з оригіналом [54].

Наприклад, у 2018 році американский режисер Джордан Піл та видання BuzzFeed опублікували начебто відеозвернення колишнього президента США Барака Обами, в якому він називає Дональда Трампа

«засранцем». Насправді Барак Обама нічого такого не казав. Відеоролик було створено за допомогою програми Fakeapp і графічного редактора Adobe After Effects [55].

Наприкінці травня 2020 року на Youtube та у соціальній мережі Facebook було поширено фейковий відеозапис, на якому спікер Палати представників США Ненсі Пелосі під час свого виступу виглядала нетверезою. Відео набрало близько 3 мільйонів переглядів. Перш ніж була виявлена підробка, це відео прокоментували президент США Дональд Трамп та інші американські політики [56].

Таким чином, дезінформація активно використовується в інформаційному протиборстві. Дезінформація – це цілеспрямоване і сплановане поширення викривленої, частково правдивої або сфабрикованої інформації, для впливу на громадську думку та формування вигідної суб'єкту впливу «картини дійсності». Дезінформацію можна грамотно «вбудовувати» у контекст вже поширюваних пропагандистських наративів, посилюючи існуючі стереотипи, уявлення і переконання цільової аудиторії. Сучасні технології розширюють можливості введення в оману та підвищують ефективність дезінформаційних кампаній, що можуть мати деструктивні наслідки для країни-об'єкта впливу.

Питання для самоконтролю:

1. Як визначається термін «дезінформація»?
2. Чому з дезінформацією складно боротись?
3. Якими є принципи дезінформування?
4. Якими способами можна ввести в оману супротивника?
5. Як співвідносяться поняття «дезінформація» та «фейк»?
6. Як визначається поняття «фейк»?
7. Чим зумовлена ефективність фейкових повідомлень?
8. Якими можуть бути цілі поширення фейкових повідомлень?
9. Що таке дипфейк?
10. Яка технологія створення дипфейків?
11. Чим небезпечні дипфейки?

Завдання:

1. Навести приклад використання дезінформації в окремій інформаційній операції (ІО) у 21 столітті: коротка характеристика вибраної інформаційної операції; приклади дезінформації в рамках вибраної ІО; суб'єкти/агенти впливу, цілі, формат і канали поширення дезінформації в рамках ІО.
2. Вибрати 2-3 інформаційні операції (ІО) та проаналізувати методи введення в оману, використані в ІО.
3. На веб-сайті stopfake.org у розділі Новини відібрати дезінформаційні повідомлення однієї тематики за один рік, і охарактеризувати вибрану дезінформаційну кампанію, відповівши на такі питання:
   - Яка тема дезінформаційних повідомлень?
   - Яка ціль дезінформаційної кампанії?
   - Скільки повідомлень було поширено в рамках вибраної дезінформаційної кампанії?
   - Які канали поширення дезінформації?
   - Які методи дезінформування було використано у повідомленнях?

2.3. Рефлексивне управління

Провідну роль в інформаційній війні відіграють технології управління сприйняттям реальності цільовими аудиторіями на національному і міжнародному рівнях. Змінюючи сприйняття, суб’єкти впливу змінюють моделі реальності у свідомості цільових аудиторій, що впливає на процес прийняття рішень. За допомогою ретельно підібраної інформації або дезінформації можна впливати на прийняття державних рішень та «програмувати» поведінку супротивника. Така технологія відома під назвою «рефлексивне управління».

Термін «рефлексивне управління» ввів в обіг радянсько-американський психолог і математик Володимир Лефевр.

В. Лефевр характеризує рефлексію як здатність встати у позицію «спостерігача», «дослідника» або «контролера» по відношенню до свого тіла, своїх дій, своїх думок, а також здатність встати у позицію дослідника по відношенню до іншого «персонажа», його дій і думок [57].

За визначенням В. Лефевра, рефлексивне управління – це процес передачі підстав для прийняття рішення одним із супротивників іншому.

Дослідник зазначив, що термін «рефлексивне управління» можна розуміти у двох сенсах: як мистецтво маніпулювання людьми та як специфічний метод соціального контролю.

Специфіка цього методу полягає у тому, що генерація інформаційних впливів спирається не стільки на природну людську інтуїцію, скільки на особливу модель керованого суб'єкта [57].

Успіх рефлексивного управління значною мірою залежить від якості моделі суб'єкта, яка використовується під час його реалізації. Модель суб'єкта має відображати не лише його поведінку, але і його здатність усвідомлювати себе і інших суб'єктів, включаючи і тих, які намагаються встановити контроль над його поведінкою.

В. Лефевр виокремив такі види рефлексивного управління:

- *Рефлексивне управління через плацдарм*. Сюди відноситься маскування своїх об’єктів та створення хибних об’єктів.
- *Рефлексивне управління шляхом формування цілі супротивника.* Найбільш поширеним типом такого управління є провокація.
- *Рефлексивне управління шляхом формування доктрини супротивника,* тобто алгоритму прийняття рішень.
- *Рефлексивне управління за допомогою зв’язування*. Суть – підштовхнути супротивника до потрібних висновків, показавши йому певний елемент дійсності.
- *Рефлексивне управління шляхом перетворення плацдарму*. Цей тип управління передбачає передачу супротивнику нібито власного погляду на ситуацію. Передача може реалізуватись у вигляді підкинутої документації або «підтверджень» того, що фальшиві об’єкти сприйняті як справжні (хоча насправді обман розкрито).
- *Рефлексивне управління шляхом перетворення цілі.* Таке управління націлене на формування у супротивника невірного уявлення про реальну мету суб'єкта.
- *Рефлексивне управління за допомогою зв'язування плацдарму та цілі.* За допомогою конфігурації і пересування військ супротивник підводиться до певних умовиводів щодо цілей суб’єкта. Власна ціль передається супротивнику шляхом передачі йому своєї картини плацдарму.
- *Рефлексивне управління масовими рішеннями*. Таке управління здійснюється за допомогою листівок, радіопропаганди та подібних засобів для формування «масових рішень» [57].

Ідеї В. Лефевра отримали подальший розвиток у публікаціях низки військових експертів.

Так, С. Леоненко зазначав, що рефлексивне управління відбувається, коли орган управління передає керованій системі спонукання та підстави, які стануть приводом досягти бажаного

рішення. Рефлексія спонукає процеси імітації міркувань супротивника чи імітації можливої поведінки супротивника, змушуючи його прийняти несприятливе для нього рішення [58].

За словами експерта, у війні, де використовується рефлексивне управління, сторона з найвищою якістю «рефлексії» (більш здатна до імітації думок опонента або передбачення його поведінки) матиме кращі шанси для перемоги.

У публікаціях генерал-майора М. Іонова зазначається, що мета рефлексивного управління – змусити супротивника робити певні дії, які ведуть до його поразки, впливаючи чи керуючи його процесом прийняття рішення.

Контроль над супротивником здійснюється через низку заходів, пов'язаних за часом, метою та місцем, що змушують супротивника відмовитися від свого первісного плану, вдаватись до невигідних дій або реагувати неправильно на їхню очевидну невигоду.

М. Іонов визначив чотири методи передачі інформації супротивнику для забезпечення контролю над ним, а саме [59]:

- *Тиск влади*, що включає використання переважаючої сили, демонстрацію сили, психологічні атаки, ультиматуми, погрози санкціями, військову розвідку, провокаційні маневри, випробування зброї, збільшення бойової готовності збройних сил, формування коаліцій, офіційне оголошення війни, організацію обмежених страйків, виведення з ладу окремих збройних сил, «нагнітання» та рекламування перемоги, демонстрація безжальних дій та демонстрація милосердя до союзника супротивника, який припинив опір;
- *Передача хибної інформації про ситуацію*, що включає маскування, створення хибних споруд, приховування справжніх взаємозв'язків між підрозділами, підтримання секретності нових видів зброї, блеф щодо зброї, зміна методів проведення операції чи навмисна втрата важливих документів;

- *Провокування супротивника до пошуку нових напрямків ескалації* або згортання конфлікту шляхом навмисної демонстрації особливого ланцюга дій, завдання удару по опорному пункту супротивника, підривної діяльності і провокацій, примусу супротивника здійснювати каральні дії, що призводять до витрачання збройних сил та інших ресурсів;
- *Вплив на алгоритм прийняття рішень супротивником*, що включає публікацію навмисно перекрученої доктрини, передачу неправдивих даних про ситуацію особам, які приймають рішення, вчинення дій для нейтралізації оперативного мислення супротивника, несподіваний початок воєнних дій тощо.

Полковник С.А. Комов, використовуючи поняття «інтелектуальні» методи інформаційної війни, перерахував такі елементи рефлексивного управління [58,59]:

- відволікання уваги (створення реальної або уявної загрози одній із життєво важливих дислокацій супротивника);
- перевантаження (надсилання супротивникові великого обсягу суперечливої інформації);
- параліч (створення сприйняття спеціальних загроз життєвим інтересам супротивника);
- виснаження (спонукання супротивника виконувати марні дії);
- брехня;
- розкол (переконання супротивника діяти всупереч інтересам коаліції);
- заспокоєння (спонукання супротивника думати, що проводяться навчання, а не підготовка до наступальних дій);
- залякування (формування враження непереборної переваги);
- провокація (нав’язування супротивнику дій, вигідних для суб’єкта впливу);
- пропозиція (надання інформації, яка зачіпає супротивника юридично, морально, ідеологічно тощо);
- тиск (поширення інформації дискредитаційного характеру).

О. Раскін та І. Тарасов розуміють під терміном рефлексивне управління нав'язування об'єкту управління певної стратегії поведінки за допомогою передачі йому підстав, з урахуванням яких він логічно вибудовує рішення, нав'язане йому суб’єктом впливу. Рефлексивне управління реалізується через будь-які обманні дії. Як технологія інформаційного впливу рефлексивне управління має два аспекти: інформаційно-психологічний, пов'язаний з впливом на усвідомлення конкретної ситуації людьми, зайнятими у процесі збирання, обробки, підготовки прийняття рішень; інформаційно-технічний, пов'язаний із впливом на технічні засоби збирання та обробки інформації [60].

В іншій публікації О. Раскін зазначає, що комп’ютерні технології підвищують ефективність рефлексивного управління. У мережі інтернет, на перший погляд, здається, що людина отримує доступ до різних поглядів, оцінок реальності. Здається, що користувач потрапляє у світ об’єктивної незалежної інформації, на основі якої він зможе сформувати справжні переконання і його подальші дії будуть мотивовані у правильному напрямі [61].

Насправді є модератори, які мають більше прав, ніж звичайні користувачі соціальних медіа, для управління інформаційними потоками. Вони мають право видаляти і редагувати повідомлення інших людей, видаляти сторінки користувачів, а також обмежувати права на редагування та перегляд користувачів тощо. Фактично мета модерації – підтримання порядку на сайті і контроль над контентом, а не над поведінкою користувачів. Але часто модератори не обмежуються цим.

Для впливу на мотивацію користувачів вони можуть використовувати «вкиди» спеціально підготовленої інформації, яка провокує ті чи інші настрої користувачів. Тут можуть бути використані чутки, розміщення інформації, яку не можна перевірити, а також відомостей, що дають змогу переконати громадськість в істинності тих чи інших подій. При цьому змістовне навантаження інформації може бути спотворене. Таким чином, здійснюється вплив на переконання та мотиваційний механізм прийняття рішень індивіда.

За словами О. Раскіна, погляди і переконання, сформовані у віртуальному середовищі, передаються у реальний світ. Людина з нестабільними поглядами легко потрапляє у «необхідний каркас соціальної поведінки» [61].

На думку військового експерта В. Махніна, суть рефлексивного управління полягає у тому, щоб за допомогою рефлексивних факторів впливати на розуміння ситуації супротивником і формувати картину ситуації. Відповідно з'являється можливість не прогнозувати, а зумовлювати дії супротивника чи рефлексивно керувати ним [62].

Експерт зауважує, що рефлексивний вплив на супротивника передбачає створення симулякра, тобто формування хибних реальних, інформаційних та психологічних образів об’єктів, процесів, явищ.

У рефлексивному впливі на супротивника найбільше значення мають заходи, що дають змогу замінити раціональні алгоритми такими шляхами: шаблонністю дій для забезпечення раптового застосування нового варіанта дій; передачею інформації, що вимагає прийняття рішення стосовно евристичних алгоритмів; дезорганізацією системи управління шляхом впливу на її елементи.

Британська дослідниця Maria de Goeij зазначає, що у рефлексивному управлінні ймовірність успіху залежить від правильного моделювання та інтерпретації сприйняття іншого проти власного сприйняття світу. Модель Я та іншого можна уявити як суб’єктивну чисту оцінку відносин між двома суб’єктами, включно з тим, як вони сприймають один одного та ситуацію, як вони, ймовірно, взаємодіятимуть або можуть взаємодіяти, і як їхню взаємодію можна змінити, щоб вплинути на результат.

Ключовою ідеєю, яка лежить в основі концепції рефлексивного контролю є визнання того, що, хоча об’єктивна реальність існує, малоймовірно, що сприйняття людей відповідає цій реальності. Тому навряд чи хтось виходить з об’єктивної реальності при прийнятті рішень. Рішення скоріше за все приймаються на основі сприйнятої версії реальності [63].

У цьому світі сприйняття такі суб'єктивні чинники, як етичні системи, довгострокові та короткострокові цілі, часові межі, доступні для прийняття рішень і дій, упередження, шум і слабкі місця, впливають на рішення акторів.

Застосування рефлексивного контролю теоретично складається з трьох кроків, які має виконати головний агент, перш ніж об'єкт впливу прийме рішення. Ці три кроки супроводжуються циклом зворотного зв'язку:

1. Побудова розуміння сприйняття ситуації: як, на думку іншого агента, виглядає ситуація?

2. Визначення цілей іншого агента і чого він повинен досягти, щоб задовольнити потреби основного агента: що інший агент вважає своїм найкращим вибором і яким він повинен бути?

3. Головний агент представляє «алгоритм» рішення, який аналізує можливі сценарії взаємодій і як на них впливати.

4. Виникає цикл зворотного зв'язку, щоб зрозуміти, яке рішення прийняв інший і чому [58].

Здійснення рефлексивного управління передбачає поєднання або послідовність різних впливів, дій і динаміки. Будь-який із цих елементів окремо не може позначатися як рефлексивне управління.

Історичним прикладом рефлексивних впливів шляхом застосування симулякра на стратегічному рівні є операції англо-американських військ «Оверлорд» (операція з форсування Ла-Манша) та «Енвіл» (десантна операція з висадки американських та французьких військ у Південній Франції, на захід від Канн). Мета операції "Оверлорд" полягала у висадці на французькому узбережжі, а операції «Енвіл» – відвернути німецькі війська від театру військових дій у північно-західній Франції.

До прикладів рефлексивного управління можна віднести російсько-грузинську війну 2008 року. За розрахунками російського керівництва, США, обтяжені війною з тероризмом і невдалою війною в Іраку, навряд чи зреагують на події у «зоні впливу» рф. За кілька

місяців до початку військової кампанії Кремль почав здійснювати тиск на прийняття рішення грузинською владою.

За російським задумом, причиною війни мала стати нерозсудливість тодішнього президента Грузії Міхеіла Саакашвілі. У травні 2006 року «Михаїл Саакашвілі: Психологічний профіль характеру» була видана колегією провідних західних інститутів, яких насправді не існувало. Хоча підробка була грубою, публікація викликала довіру і до 2008 року добре поширилася [64].

За три місяці до початку навчань «Кавказ-2008» російські контингенти Колективних миротворчих сил СНД на Північному Кавказі активізувались і були підкріплені матеріально-технічним та інженерним персоналом. До того ж, напередодні навчань мирне населення Південної Осетії було евакуйовано до рф. Такі дії свідчили про підготовку скоріше до війни, а не до навчань. Керівництво Грузії розуміло, що військові навчання історично були для Росії засобом маскування та підготовки до військового втручання.

Починаючи з 15 липня 2008 року навчання «Кавказ-2008» за участі 8000 військовослужбовців з різних видів військ (сухопутних, морських, десантних і повітряно-десантних сил, федеральної прикордонної служби та внутрішніх військ МВС) проходили в одинадцяти районах Південного федеральний округу, на узбережжі Чорного моря і майже в усіх гірських перевалах Великого Кавказького хребта. Навчання створили фон для погіршення загальної безпекової ситуації на кордоні Південної Осетії та Грузії. Ці навчання викликали занепокоєння грузинської влади.

4 серпня навчання офіційно завершилися. Водночас, було незрозуміло, скільки російських підрозділів повернулося до місця постійної дислокації мирного часу, скільки перебувало в дорозі та скільки підрозділів поверталися у зону конфлікту. Крім того, на початку серпня південноосетинські збройні формування вдавались до провокацій на кордоні з Грузією, зокрема почали обстрілювали грузинські села. Це змусило грузинських військовослужбовців відкрити вогонь у відповідь. Інтенсивність перестрілок між

ополченцями Південної Осетії та грузинськими збройними силами лише зростала [64].

Президента Грузії Міхеіла Саакашвілі також спонукала до дій видача паспортів Російської Федерації громадянам Південної Осетії та Абхазії, крок, який розглядався як акт «повільної анексії».

7 серпня підрозділи грузинської армії були спрямовані до Південної Осетії. Грузинські війська за кілька годин взяли під контроль більшу частину Цхінвалі, оплоту сепаратистів, та вбили декількох російських миротворців. Росія звинуватила Грузію в «агресії проти Південної Осетії», і розпочала повномасштабне наземне, повітряне і морське вторгнення у Грузію.

Британський військовий експерт Стів Тетем вважає, що рефлексивне управління було використано під час анексії Криму 2014 року. Тоді російська влада продемонструвала гарне розуміння ситуації та цільових аудиторій – російськомовних громадян Криму, української влади, міжнародної спільноти, особливо ЄС і НАТО, що дало змогу вірно спрогнозувати їхню поведінку [65].

Росія створила умови, аби нейтралізувати місцеве населення. Завдяки інтенсивній антиукраїнській пропаганді російськомовне населення Криму було налаштоване проти Євромайдану, що відбувався у Києві, а також було залякане приходом до влади в Україні «нацистів і бандерівців».

Коли на півострові з’явились російські військові без розпізнавальних знаків – «зелені чоловічки» або так звані «вежливые люди», місцеві жителі та українська влада були дезорієнтовані, і не могли відреагувати належним чином. Одночасно Росія почала нарощувати військову присутність на східному кордоні України, тим самим створюючи нові загрози і відволікаючи увагу від Криму. Внаслідок таких дій керівництво України було паралізовано, і не змогло оперативно зреагувати на ситуацію. Така операція з введення в оману також «обеззброїла» країни ЄС та США, які утримались від рішучих дій, дозволивши Росії анексувати Крим.

До прикладів рефлексивного управління можна віднести спроби перебільшити свою погрозу, свій потенціал в очах супротивника. Наприклад, президент РФ представляє себе як божевільного і непередбачуваного, і погрожує використати ядерну зброю. Специфіка цієї техніки в тому, що важко зрозуміти, де правда, а де брехня. І за таких умов інші країни утримуються від певних рішень і дій, побоюючись ескалації та вкрай негативних наслідків.

Питання для самоконтролю:

1. Як пояснює термін «рефлексивне управління» Володимир Лефевр?
2. Які види рефлексивного управління визначив В. Лефевр?
3. Як визначають термін «рефлексивне управління» військові експерти С. Леоненко, М. Іонов, В. Махнін?
4. Які методи передачі інформації, на думку М. Іонова, дають змогу встановити контроль над супротивником?
5. Які елементи рефлексивного управління виокремив полковник С. Комов?
6. Яким чином технологія рефлексивного управління була використана РФ під час операції з анексії Криму у 2014 році?

Завдання:

1. Навести приклади використання рефлексивного управління в інформаційних війнах 21 століття.
2. На конкретних прикладах показати реалізацію таких методів рефлексивного впливу: тиск влади, передача хибної інформації про ситуацію, вплив на алгоритм прийняття рішень супротивником.
3. Навести реальний приклад або змоделювати ситуацію інформаційного протистояння, в якій одна зі сторін для досягнення своїх цілей використовує ті чи інші елементи рефлексивного управління з переліку полковника С. Комова.

Список використаних джерел:

1. Джоуэтт Г.С., О'Доннел В. Пропаганда и убеждение. – Гуманитарный центр, 2021. 496 с.
2. Merriam-Webster dictionary. URL: https://www.merriam-webster.com/dictionary/propaganda
3. Collins Online Dictionary. URL: https://www.collinsdictionary.com/dictionary/english/propaganda
4. Lexico. URL: https://www.lexico.com/definition/Propaganda
5. Мозолин А. Исследования пропаганды в теориях массовой коммуникации. URL: http://rc-analitik.ru/file/%7B89440115-2a9a-4c24-a58c-9f7b01525937%7D
6. Киселев М.В. Психологические аспекты пропаганды. URL: https://psyfactor.org/propaganda7.htm
7. Павлов Д.М. Теорія пропаганди Леонарда Дуба. URL: http://politics.chdu.edu.ua/article/view/107070/102039
8. Сороченко В. Принципы военной пропаганды. URL: https://psyfactor.org/propaganda3.htm
9. Гитлер А. Моя борьба. URL: https://onemorelibrary.com/index.php/ru/knigi/sotsialnye-nauki/book/political-science-russian-187/m-ja-b-rib-197
10. Почепцов Г.Г. Пропаганда 2.0. Харків: Фоліо, 2018. 796 с.
11. Ellul Jacques. Propaganda: The Formation of Men's Attitudes. Характеристики пропаганды. URL: http://www.rc-analitik.ru/propaganda/teoriya_i_praktika_propagandy_hrestomatiya/vypusk__2_harakteristiki_propagandy/
12. Macdonald S. Propaganda and Information Warfare in the Twenty-First Century. Routledge, Abingdon, 2007. 204 p.
13. Сороченко В. Энциклопедия методов пропаганды. URL: https://psyfactor.org/propaganda.htm
14. Psychological Operations Field Manual No.33-1. URL:http://www.freerepublic.com/focus/fr/546409/posts
15. Ожеван М.А. Глобальна війна гранд-наративів у сучасну добу/ Стратегічні комунікації в міжнародних відносинах. Монографія. К: Вадекс, 2019. С. 60-94.
16. Почепцов Г.Г. Наратив як інструментарій: від літературознавства до боротьби з тероризмом//Політичний менеджмент. 2008. №4. С. 3-11.

17. Запорожець О.Ю. Російська пропаганда під час окупації Криму. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/2762
18. Жителей Крыма принуждают говорить на украинском языке. 28.02.2014. URL: http://russian.rt.com/article/23309
19. МИД РФ: Вооружённые люди, направленные из Киева, пытались захватить здание МВД Крыма. URL: http://russian.rt.com/article/23391
20. Верницкий А. Антиконституционный переворот и захват власти – Президент РФ дал оценку тому, что произошло в Киеве. URL: http://www.1tv.ru/news/polit/253452
21. Воробьев В. Миллионы своих на «восьмерку» не меняем. URL: http://www.rg.ru/2014/03/04/lavrov.html
22. Обращение Президента РФ Владимира Путина. 18 марта 2014 года. URL: http://www.1tv.ru/news/social/254389
23. Тихоненко І. В., Христодорова Ю.С. Ідеологія та організаційна структура «Ісламської держави» як фактори у веденні боротьби з тероризмом. URL: https://www.researchgate.net/profile/Iryna-Tykhonenko/publication/346523974_Ideologia_ta_organizacijna_struktura_Islamskoi_derzavi_ak_faktori_u_vedenni_borotbi_z_terorizmom/links/5fc61a8592851c301299bee6/Ideologia-ta-organizacijna-struktura-Islamskoi-derzavi-ak-faktori-u-vedenni-borotbi-z-terorizmom.pdf
24. Zgryziewicz M.R., Grzyb T., Fahmy Sh., Shaheen J. Daesh Information Campaign and its Influence. 2015. URL: https://stratcomcoe.org/publications/daesh-information-campaign-and-its-influence/156
25. Speckhard A. The Hypnotic Power of ISIS Imagery in Recruiting Western Youth. 2015. URL: https://www.academia.edu/17120997/The_Hypnotic_Power_of_ISIS_Imagery_in_Recruiting_Western_Youth
26. Shehabat A., Mitew T. Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. Perspectives on Terrorism. December 2017. URL: https://www.researchgate.net/publication/321995050_Black-boxing_the_Black_Flag_Anonymous_Sharing_Platforms_and_ISIS_Content_Distribution_Tactics
27. Speckhard A., Shajkovci A. Is ISIS Still Alive and Well on the Internet? February 13, 2019. URL: https://voxpol.eu/is-isis-still-alive-and-well-on-the-internet/
28. Доронин А.И. Бизнес-разведка. – М.: «Ось-89», 2006. 496 с.

29. Крысько В.Г. Секреты психологической войны. URL: https://www.gumer.info/bibliotek_Buks/Psihol/krusk/index.php
30. Шлапаченко В.М. Дезінформація як спосіб інформаційно-психологічного впливу. Інформаційна безпека людини, суспільства, держави. 2013. № 2 (12). С. 78-86.
31. Даллес А. Асы шпионажа. URL: https://www.e-reading.club/book.php?book=18012
32. Гобл П. Ложь, гнусная ложь и российская дезинформация. URL: https://www.stopfake.org/ru/lozh-gnusnaya-lozh-i-rossijskaya-dezinformatsiya/
33. Почепцов Г. (Дез)информация /Под общей редакцией Н. Лигачевой и Г. Петренко. К., 2019. 248 с.
34. Цапенко Н. Способы дезинформации противника. URL: http://pentagonus.ru/publ/sposoby_dezinformacii_protivnika_1976/19-1-0-2045
35. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/learner-english/fake
36. Невельська-Гордєєва О.П., Нечитайло В.О. Феномен «fake news» у контексті забезпечення інформаційної безпеки держави. URL: http://fil.nlu.edu.ua/article/view/250655/249738
37. Распопова С.С., Богдан Е.Н. Фейковые новости: природа происхождения. URL: https://cyberleninka.ru/article/n/feykovye-novosti-priroda-proishozhdeniya
38. Фейки як інструмент впливу на вибори. Аналітична доповідь / Дубов Д. В., Корецька І. О., Баровська А. В., Гнатюк С. Л., Ожеван М.А. та ін. URL: https://niss.gov.ua/sites/default/files/2020-01/fake_news_fin_full_clean.pdf
39. Почепцов Г. Фейки как информационно-виртуальный объект. URL: https://ms.detector.media/mediaanalitika/post/21965/2018-10-21-feyky-kak-ynformatsyonno-vyrtualnyy-obekt/
40. Мудрая И. Понятие «фейк» и его виды в СМИ. Теле- и радиожурналистика. 2016. Вып. 15. С. 184–188.
41. Friedman H. Deception and Disinformation. URL: http://www.psywarrior.com/DeceptionH.html
42. Хастингс М. Операция «Оверлорд»: Как был открыт второй фронт. URL: http://militera.lib.ru/h/hastings_m/index.html

43. Харьковский университет уличил НТВ во лжи об увольнении профессора за русский язык. 03.04.2014. URL: https://censor.net/ru/n279340
44. Золотухін Д. Ю. Біла книга спеціальних інформаційних операцій проти України 2014 – 2018. К., 2018. 384 с.
45. В Нидерландах требуют признать вину Украины в крушении MH17. URL: https://politobzor.net/204031-v-niderlandah-trebuyut-priznat-vinu-ukrainy-v-krushenii-mh17.html
46. Трагедия MH17. В Нидерландах хотят расследовать "роль Украины". 02.10.2019. URL: https://news.liga.net/politics/news/tragediya-mh17-v-niderlandah-hotyat-rassledovat-rol-ukrainy
47. Фейк: Войска НАТО в Украине находятся «незаконно» – это «оккупация». 25.09.2020. URL: https://www.stopfake.org/ru/fejk-vojska-nato-v-ukraine-nahodyatsya-nezakonno-eto-okkupatsiya/
48. Фейк: ВСУ отрабатывают на учениях действия по подавлению мирного населения Донбасса. 29.09.2021. URL: https://www.stopfake.org/ru/fejk-vsu-otrabatyvayut-na-ucheniyah-dejstviya-po-podavleniyu-mirnogo-naseleniya-donbassa/
49. С английского на русский, а потом – на чешский: повторный перевод как инструмент манипуляции. URL: https://www.stopfake.org/ru/s-anglijskogo-na-russkij-a-potom-na-cheshskij-povtornyj-perevod-kak-instrument-manipulyatsii/
50. Як російські спецопераційї намагаються зірвати мобілізацію в Україні. 07.08.2024. https://spravdi.gov.ua/yak-rosijski-speczoperacziyi-namagayutsya-zirvaty-mobilizacziyu-v-ukrayini/
51. Фейковий сайт WP та інші "двійники". Як працює мережа російської дезінформації під назвою Doppelganger. 10.05.2024. URL: https://texty.org.ua/fragments/112441/fejkovyj-sajt-wp-ta-inshi-dvijnyky-yak-pracyuye-merezha-rosijskoyi-dezinformaciyi-pid-nazvoyu-doppelganger/
52. “Старі добрі США”. Як дезінформаційна кампанія РФ працює на руку Трампу, – Wired. 17.09.2024. URL: https://texty.org.ua/articles/113401/stari-dobri-ssha-yak-dezinformacijna-kampaniya-rf-pracyuye-na-ruku-trampu-wired/
53. Операція «Двійник»: ФБР оприлюднило методички РФ із дезінформації. 11.09.2024. URL: https://www.rfi.fr/uk/міжнародні-

новини/20240911/операція-двійник-фбр-оприлюднило-методички-рф-із-дезінформації-частина1
54. Семенова Т. Эксплейнер: что такое дипфейк. 08.08.2019. URL: https://zn.ua/TECHNOLOGIES/ekspleyner-chto-takoe-dipfeyk-326315_.html
55. Технологія діпфейку стане найсучаснішою інформаційною зброєю – Associated Press. 05.07.2018. URL: https://www.radiosvoboda.org/a/29345082.html
56. Баловсяк Н. Deepfake: как видеофейки стали серьезной угрозой и объединили общество. URL: https://www.stopfake.org/ru/deepfake-kak-videofejki-stali-sereznoj-ugrozoj-i-obedinili-obshhestvo/
57. Лефевр В. А. Лекции по теории рефлексивных игр. М., 2009. 223 с.
58. Смолян Г. Рефлексивное управление – технология принятия манипулятивных решений. URL: https://gtmarket.ru/library/articles/7309
59. Томас Т. Рефлексивное управление в России: теория и военные приложения. URL: http://www.intelros.ru/pdf/stratagemi/Tomas.pdf
60. Раскин А.В., Тарасов И.В. Рефлексивное управление как технология информационного воздействия. Информационные войны. 2014. №2(30). С.15-17.
61. Раскин А.В. Рефлексивное управление в социальных сетях. Информационные войны. 2015. Т. 35. № 3. С. 18–22.
62. Махнин В.Л. О рефлексивных процессах в противоборстве боевых систем. Информационные войны. 2012. № 3. С. 48-58.
63. Maria W. R. de Goeij Reflexive Control: Influencing Strategic Behavior. 20.11.2023. URL: https://press.armywarcollege.edu/parameters/vol53/iss4/14/
64. Giles K., Seaboyer A., Sherr J. Russian Reflexive Control. October 2008. URL:https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control
65. Почепцов Г. Три модели построения информационных операций. URL: https://ms.detector.media/manipulyatsii/post/11571/2014-10-12-try-modely-postroenyya-ynformatsyonnykh-operatsyy/

РОЗДІЛ 3.
ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА У КІБЕРПРОСТОРІ

3.1. Характеристика кіберпростору

Термін «кіберпростір» (англ. cyberspace) складається з двох частин: «кібер» (cyber) та «простір» (space). В Оксфордському словнику зазначено, що префікс «cyber» походить від грецького слова κυβερνήτες, що перекладається як «мистецтво управління» [1].

За визначенням в англомовних словниках, «кібер» означає те, що відноситься до комп'ютерів, комп'ютерних мереж (зокрема мережі Інтернет) та віртуальної реальності; електронне середовище, в якому відбувається онлайн комунікація [1].

Вперше термін «кіберпростір» було введено в обіг письменником Вільямом Гібсоном у 1982 році у новелі «Спалення Хром» («Burning Chrome»). У 1984 році це поняття було більш детально розкрито у творі «Некромант» («Neuromancer»). На думку Гібсона, кіберпростір (cyberspace) – це злагоджена галюцинація, яку щодня переживають мільярди звичайних операторів у всьому світі. Це графічне представлення відомостей, збережених у пам'яті комп'ютерів всього людства [2].

З поширенням на початку 1990-х років мережі Інтернет термін «кіберпростір» використовується для позначення онлайн світу, в якому взаємодія індивідів та груп здійснюються за допомогою електронних мереж, сформованих інформаційно-комунікаційними технологіями.

Незважаючи на активне використання терміну «кіберпростір», сьогодні не існує загальноприйнятого визначення цього поняття.

Міжнародний союз електрозв'язку визначив кіберпростір як фізичний і нефізичний простір, що складається з комп'ютерів, комп'ютерних систем, мереж та комп'ютерних програм, комп'ютерних даних, контенту, даних трафіку та користувачів [1].

У Національній військовій стратегії США (2006 рік) кіберпростір розглядається як сфера, що характеризується можливістю використання електронних та електромагнітних засобів для

запам’ятовування, модифікування та обміну даними через мережеві системи, та пов’язана з ними фізична інфраструктура.

У документах Збройних Сил США кіберпростір визначається як глобальний простір в межах інформаційного середовища, що складається із взаємозалежної мережі об’єктів ІТ-інфраструктури, включаючи Інтернет, телекомунікаційні мережі, комп’ютерні системи, вбудовані процесори та контролери [1].

У Доктрині кібероперацій Збройних Сил США відмічається, що кіберпростір є особливим середовищем ведення військових операцій, відрізняючись від інших середовищ (моря, суши, повітря, космоса) штучністю, рукотворним характером, і потребує постійних зусиль з підтримки.

Кіберпростір є свого роду «сполучним середовищем» для всіх інших середовищ, забезпечуючи формування єдиного образу обстановки.

Взаємодіючи з іншими середовищами, кіберпростір безпосередньо пов'язаний з реальним світом, через розміщення в реальному світі кіберінфраструктури (наприклад, серверів) та через наявність у кіберпросторі образу реального простору.

Колишній радник Президентів США Б. Клінтона та Дж. Буша молодшого Річард Кларк у своїй книзі «Кібервійна: нова загроза національній безпеці та шляхи її подолання» визначив кіберпростір як всі комп’ютерні мережі світу і все, що їх об’єднує та контролює [1].

На думку П. Вуллей (Pamela Woolley) з Інституту технологій повітряних сил США, кіберпростір – це створене людиною цифрове довкілля, що використовується для миттєвого, безкордонного, глобального збору, зберігання і передачі даних та інформації між електронним обладнанням, без організаційних, культурних, національних чи політичних кордонів [3].

Американський дослідник Д. Копселл вважає, що кіберпростір складається з двох великих компонентів: обчислювальних машин (hardware) та програмного забезпечення (software). Комп'ютер є посередником при передачі інформації, а всі інформаційні процеси, що здійснюються таким шляхом, є комп'ютерно-опосередкованими феноменами (computer-mediated phenomena) [4].

Д. Копселл виокремив такі комп’ютерно-опосередковані феномени:

- Біти (от англ. Binary digits) – дрібні частинки інформації; фундаментальна одиниця кіберпростору, яка є основою кожного комп'ютерно-опосередкованого феномена.
- Байти – групи бітів, що використовуються комп'ютерами як самостійні одиниці.
- Слова («висловлювання» та «повідомлення») – упорядковані групи символів або бітів, які займають комірку пам'яті як самостійні одиниці.
- Алгоритми – деталізовані математичні чи логічні процедури для вирішення проблеми, що використовуються як комп’ютерними програмами, так і людьми у повсякденній діяльності.
- Програми – одиниці, що являють собою один чи декілька алгоритмів, з певним набором даних, потрібних для виконання конкретних функцій. Кожен елемент програмного забезпечення є окремою програмою. Отже, кіберпростір є безперервним процесом, до якого одночасно залучено мільйони людей.

За визначенням українських фахівців Національного інституту стратегічних досліджень, кіберпростір – це об’єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління, а також інформація, що в них циркулює [1].

Вітчизняний науковець О. Манжай наводить таке визначення кіберпростору: «це інформаційне середовище (простір), що виникає завдяки комп’ютерним системам при взаємодії людей між собою, взаємодії технічних (комп’ютерних) систем та управлінні людьми цими технічними (комп’ютерними) системами» [3].

А. Погорецький та В. Шеломенцев пропонують розуміти під кіберпростором «штучне електронне середовище існування інформаційних об’єктів у цифровій формі, що утворене внаслідок функціонування кібернетичних комп’ютерних систем управління й обробки інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів, вироблення електронних

інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо)» [3].

Дослідниця Д. Добринська розглядає кіберпростір у трьох вимірах: фізичний, інформаційний та соціальний [2].

З точки зору фізичного аспекту, для кіберпростору потрібні певні пристрої (комп'ютери, смартфони, засоби віртуальної реальності тощо), за допомогою яких цей простір створюється і функціонує. Кіберпростір – це віртуальне місце, створюване мережею взаємозалежних комп'ютерів, у якому взаємодіють агенти. У кіберпросторі реальні матеріальні об'єкти утворюють віртуальні місця, які не мають просторово-часової протяжності, проте є місцями взаємодії, де зберігаються значні обсяги інформації, а також створюються кордони для захисту цієї інформації.

З точки зору інформаційного виміру, кіберпростір – це сукупність численних інформаційних потоків, через які поширюється з надзвичайною швидкістю інформація у цифровій формі [2].

Соціальний вимір кіберпростору проявляється у соціальних взаємодіях, що мають місце у цифровому середовищі, у тому числі діяльність віртуальних спільнот.

Наведені визначення свідчать, що кіберпростір не обмежується мережею Інтернет, а охоплює середовище, створене сучасними інформаційно-комунікаційними технологіями, та безпосередньо обладнання, що відноситься до ІТ-інфраструктури.

Кіберпростір є керованою системою, в якій певним чином зберігається, обробляється і передається інформація. Дана система характеризується цілісністю, взаємозалежністю компонентів, динамічністю, глобальністю, вразливістю до зовнішніх впливів, здатністю до постійного копіювання і швидкого відтворення, а також постійно зростаючою кількістю суб'єктів впливу.

Кордони кіберпростору рухливі та мінливі і не зводяться до кордонів фізичного простору. Кіберпростір розсіяний всюди, і одночасно він не відображений на жодній мапі світу.

Кіберпростір жорстко не прив'язаний і не залежить від конкретного просторово-часового розташування. Місце взаємодії у кіберпросторі не вимагає, щоб суб’єкти взаємодії знаходилися в одному конкретному місці у певний момент часу для того, щоб їхня зустріч у кіберпросторі відбулася [2].

Кіберпростір не є чітко визначеним та заданим. Він подібний до динамічної мапи, яку неможливо побачити цілком, оскільки вона завжди відкривається лише частково і з будь-якого місця.

Олександр Войскунський характеризує кіберпростір як гіпертекст або мережу. Гіпертекст є нелінійним і містить безліч різнорідних зв'язків, що формує власне сприйняття кіберпростору у кожного суб’єкта, який перебуває у цифровому середовищі. Як мережа, кіберпростір характеризується децентралізацією та розмитістю кордонів [2].

Множинність зв'язків мережевої структури кіберпростору створює безліч варіантів індивідуальної репрезентації, а також можливостей для взаємодії у межах різних спільнот.

У кіберпросторі відбуваються соціальні інтеракції між реальними людьми, які можуть представлятись так само, як у реальному житті, або створювати свій новий образ за допомогою різних аватарів, тобто конструювати мережеві ідентичності.

У сучасному світі кіберпростір перетворився на поле бою, де використовуються технології інформаційно-психологічного та інформаційно-технічного впливу. Найпоширенішою формою інформаційно-технічного протистояння є кібератаки. Інформаційно-психологічний вплив здійснюється за допомогою Інтернет-мемів та Інтернет-тролінгу.

3.2. Кібератаки

Важливим компонентом сучасного інформаційного протиборства (information warfare) є кібероперації, що передбачають використання спеціалізованих програмно-апаратних засобів для впливу на інформаційні системи об’єктів критичної інфраструктури супротивника. Кібероперації реалізуються у формі кібератак.

За визначенням американських військових, кібератака – це ворожа дія з використанням комп’ютерних і подібних мереж, спрямована на виведення з ладу або руйнування ворожих критичних кіберсистем, пристроїв або функцій.

Дослідники визначають кібератаки таким чином:

- несанкціоновані спроби проникнення у комп’ютери, керовані комп’ютерними системами або мережами (Стівен Хілдрет);
- заходи, здійснювані для підриву безпеки систем чи реалізації загрози ресурсам інформаційних систем через використання їх уразливостей (В. Харченко);
- цілеспрямовані дії, що реалізуються у кіберпросторі і призводять до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість та психічний стан громадян) (Д. Дубов, М. Ожеван);
- результат використання технічних недоліків механізмів безпеки сучасного кіберпростору, з метою дезорганізації роботи його елементів (С. Мельник, О. Тихомиров, О. Лєнков);
- сучасна форма агресії, що здійснюється окремими особами, або групою осіб, метою якої є підрив інформаційної системи безпеки, підрив роботи будь-якої інфраструктури, комп'ютерної мережі та/або підрив роботи персональних комп'ютерів та інших пристроїв, зроблений будь-якими способами (Д. Вентре) [3,5,14].

У Законі України «Про основні засади забезпечення кібербезпеки України» кібератака визначається як «спрямовані (навмисні) дії у

кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) у комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [6].

Військовий експерт Дмитро Кандауров розрізняє три рівня кібервпливу. На першому рівні – виведення з ладу апаратних засобів обробки і передачі інформації, тобто так званого «заліза». Другий рівень – вплив на програмне забезпечення супротивника за допомогою шкідливих програм. Третій рівень – це вплив на контент або доступ до нього за допомогою апаратно-програмних засобів [7].

Основний принцип кібератак – використання вразливостей програмного, апаратного забезпечення, а також людського фактору (соціальна інженерія).

Кібератаки відбуваються у специфічному і незрозумілому для більшості людей просторі, за допомогою специфічних засобів (шкідливих програм). Громадськість фактично констатує лише наслідки таких атак. Те, як вони проводяться, якими способами і засобами – це сфера компетенції вузького кола фахівців в сфері інформаційних технологій (ІТ).

За способом дії кібератаки розділяють на шкідливе програмне забезпечення, фішинг, кібератаки через посередника, DDoS атаки, впровадження SQL-коду, атаки нульового дня, тунелювання DNS [8].

Шкідливе програмне забезпечення – це програмне забезпечення (ПЗ), яке за умови запуску, може призвести до блокування пристрою, крадіжки, видалення або шифрування даних,

отримання облікових даних, що дають змогу отримати доступ до систем або служб, якими користується індивід.

Шкідливе ПЗ часто потрапляє на пристрої через вкладення електронної пошти зі шкідливим кодом або через програми обміну файлами, які поширюють небезпечні матеріали, замасковані під музику або зображення.

Експерти Урядової команди реагування на комп'ютерні інциденти в Україні (CERT-UA) поділяють шкідливе ПЗ на такі типи [9]:

Бекдор (backdoor) – шкідливий програмний код, який впроваджується у систему, аби надати зловмиснику віддалений доступ. Бекдори зазвичай дозволяють підключитися до комп'ютера з мінімальною аутентифікацією або зовсім без такої, і виконувати команди у локальній системі.

Завантажувач (downloader) – шкідлива програма, єдиною метою якої є завантаження іншого шкідливого програмного коду.

Викрадач інформації (stealer) – шкідливе ПЗ, що збирає інформацію на комп'ютері жертви і, як правило, відправляє її зловмисникові. Дане шкідливе ПЗ використовується для отримання доступу до облікових записів інтернет-додатків, таких як електронна пошта або інтернет-банкінг.

Руткіт (rootkit) – шкідлива програма, що приховує існування іншого коду, і використовується разом з іншим шкідливим ПЗ, аби надати зловмисникові доступ до системи та ускладнити виявлення коду.

Залякуюче ПЗ (scareware) – шкідливе ПЗ, створене для залякування користувача та спонукання його до покупки програмного продукту. Маючи графічний інтерфейс, схожий з антивірусом, така програма повідомляє користувачеві про наявність в його системі шкідливого коду і переконує його вирішити проблему, придбавши певне «програмного забезпечення».

Програма для розсилки спаму (spam-sending malware) – шкідливе ПЗ, яке заражає комп'ютер користувача і потім з його допомогою розсилає спам.

Вірус-вимагач (ransomware) – тип шкідливого ПЗ, що блокує доступ до системи або унеможливлює роботу з файлами, після чого вимагає від жертви викуп для відновлення вихідного стану.

Наприклад, у травні 2017 року було виявлено програму-вимагача WannaCry. Об'єктом атаки стали телекомунікаційні і транспортні компанії, урядові та правоохоронні органи, лікарні й освітні установи у понад 100 країнах світу. Розробники шкідливої програми використали експлойт для Windows, відомий як EternalBlue. За допомогою експлойту зловмисники отримали віддалений доступ до комп'ютерів з ОС Windows 7 [10]. Після проникнення у папку з документами та іншими файлами WannaCry шифрувала їх, змінюючи розширення на .WNCRY. Після цього шкідлива програма вимагала купити спеціальний ключ вартістю від 300 до 600 доларів, погрожуючи видалити файли [11].

Кейлогер (keylogger) – тип ПЗ, що реєструє кожну дію користувача, наприклад з пристроїв вводу (рух комп'ютерної миші, натиснення кнопок клавіатури), і дає змогу зловмисникам отримати дані користувача.

Фішинг – розсилка повідомлень чи електронних листів зі шкідливим кодом. Як тільки користувач відкриває посилання, зловмисники отримують доступ до конфіденційних персональних даних.

Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Шахраї зазвичай маскуються під відомі компанії, додатки соціальних мереж, сервіси електронної пошти тощо.

Розрізняють декілька видів фішингу:

- spear-phishing – атаки, спрямовані на певних людей, наприклад, системних адміністраторів;
- whaling – атаки, спрямовані на керівників вищої ланки;
- smishing – атаки, що використовують текстові або SMS-повідомлення для привернення уваги жертви;
- email phishing – атаки через електронну пошту;
- vishing – атаки через голосову пошту [12].

Наприклад, у 2011 році компанія-розробник антивірусного ПЗ McAfee повідомила про п’ятирічну хакерську атаку Shady RAT, яка передбачала розсилку заражених «трояном» електронних листів співробітникам вибраних організацій. Усі атаки розпочиналися з фішингових повідомлень співробітникам компанії, які мали потрібні права доступу. Після відкриття повідомлення завантажувався шкідливий код, виконання якого призводило до відкриття бекдорів та встановлення зв'язку із сервером зловмисників. Об’єктами кібератаки були комп’ютерні мережі та сервери урядових структур різних країн світу і міжнародних організацій, зокрема, ООН, Асоціації держав Південно-Східної Азії (АСЕАН), Міжнародного олімпійського комітету (МОК) та Світової антидопінгової агенції. Загалом від хакерської атаки постраждали 72 організації.

Атака через посередника (Man-in-the-Middle) – кібератака, яка відбувається, коли хакери перехоплюють дані та обмін повідомленнями між двома людьми чи пристроями, зазвичай за допомогою публічної Wi-Fi-мережі або шкідливого ПЗ. Прикладом може бути підроблена точка доступу Wi-Fi, яка виглядає і працює як справжня, але при цьому перехоплює інформацію користувача [13].

«Відмова в обслуговуванні» (DoS-атака) – атака на комп’ютерну систему, що має на меті зробити комп’ютерні ресурси недоступними для користувачів за допомогою масового і безперервного потоку запитів до системи або серверу, що перевищує пропускну здатність системи/серверу, змушуючи його зупинити роботу. Розсилка запитів на веб-ресурс відбувається з одного пристрою.

Різновидом DoS атаки є DDoS атака (Distributed Denial of Service), в якій використовуються так звані ботнети – групи заражених шкідливими програмами комп’ютерів, які за командою хакерів одночасно надсилають запити на веб-ресурс. Розмір ботнету може складати від десятків до сотень тисяч пристроїв [14].

Наприклад, у вересні 2017 року компанія Google стала об’єктом рекордної за потужністю DDoS-атаки. За допомогою різних методів зловмисники одночасно атакували тисячі IP-адрес компанії. Атака тривала декілька місяців, а її потужність сягала 2,54 Тб/с. Згідно зі

звітом Google Threat Analysis Group, джерелом атаки були мережі китайських інтернет-провайдерів [15].

Впровадження SQL-кода – кібератака, яка передбачає впровадження шкідливого коду на сервер, що обробляє SQL-запити (Structured Query Language), тобто запити до структурованих баз даних.

Атака нульового дня (0-day) - це атака, в якій використовуються вразливості програмного забезпечення, невідомі користувачам чи розробникам ПЗ та проти яких ще не розроблені механізми захисту. Сам термін означає, що у розробників було 0 днів на виправлення дефекту: уразливість або атака стає публічно відомою до моменту випуску виробником ПЗ для виправлення помилок.

Тунелювання DNS (Domain Name System) – кібератака, що передбачає приховане впровадження керівних команд і даних у протокол DNS. Використовуючи DNS для обходу фаерволу, хакер тунелює протоколи поверх DNS та IP-трафік або переміщує викрадені дані.

Тунелювання дає змогу приховати дані і команди від комп'ютерних систем моніторингу. Для цього хакери можуть використовувати набори символів base32, base64, або шифрувати дані. Тунелювання DNS може використовуватись для прихованої передачі критичних даних, для завантаження на комп'ютер-жертву шкідливої програми та віддаленого керування комп'ютерами користувачів [16].

Кібератаки як інструмент інформаційного протиборства мають низку специфічних рис: невидимість впливу, надзвичайна швидкість проведення атак, відсутність фізичних, юридичних та інших перешкод, маскування (підлаштування під конкретні інформаційні системи і мережі), варіативність, одноразовість використання, націленість на системи і комплекси, що діють за чіткими алгоритмами.

Кібератаки зазвичай не знищують об'єкт впливу, а впроваджують певний набір даних і команд, що змінюють існуючі алгоритми функціонування системи й активізують потрібні реакції. У більшості випадків важко однозначно ідентифікувати організатора атаки, оскільки географічним джерелом кібератаки є часто зовсім не та держава, якій така атака може бути вигідною. Крім того, не завжди можна чітко визначити цілі, що переслідуються кібернападниками [1].

Зважаючи на неабиякий вплив кібератак на різні сфери діяльності суспільства і держави, постає питання про те, чи доцільно говорити у низці випадків не просто про кібератаки, а про кібервійну.

Дослідниками та експертами пропонується широкий спектр визначень кібервійни, зокрема:

- кібервійна – чітко скоординований цифровий напад однієї держави, спрямований на проникнення у комп'ютери та мережі іншої держави, з метою завдання шкоди або руйнування;
- кібервійна – конфлікт, що передбачає використання ворожих, незаконних атак на комп'ютери та мережі, з метою руйнування комунікацій та інших елементів інфраструктури як механізм завдання економічної шкоди або підриву системи оборони країни [1];
- кібервійна – застосування комп'ютерних технологій та мережі Інтернет однією державою, або за її безпосередньої підтримки, проти іншої держави, спрямоване проти її безпеки і оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї іншої держави [1];
- кібервійна – систематична боротьба у кіберпросторі між державами (групами держав), політичними групами, екстремістськими і терористичними та іншими угрупованнями, яка проводиться у формі атакуючих та оборонних дій [17]

Американський дослідник Мартін Лібікі визначає два рівні кібервійни: стратегічний та оперативний.

На стратегічному рівні кібервійна – це комплекс кібератак, націлених проти держави та її суспільства, з метою впливу на поведінку цієї держави. На оперативному рівні кібервійна складається з кібератак у воєнний період проти військових об'єктів та пов'язаних з військовими цивільних об'єктів [1].

Відкритим залишається питання, за яких умов кібератаку можна вважати актом кібервійни. Французькі дослідники намагались дати відповідь на це питання, виокремивши 6 рівнів кібератак за їхніми

наслідками для кіберпростору. На нульовому рівні – спроба кібератаки, яка була ідентифікована і зупинена антивірусними програмами та брандмауерами. Перший та другий рівні – інцидент і вторгнення в інформаційну систему, що вимагають втручання ІТ-фахівців, зокрема адміністраторів інформаційних систем. Третій рівень – злам інформаційної системи або серверу для перепрограмування або внесення змін у нормальне функціонування системи. До четвертого і п'ятого рівнів дослідники віднесли атаки, націлені на проникнення у державну мережу та порушення функціонування чи паралізацію (саботаж) об'єктів критичної інфраструктури. Цей рівень вимагає втручання державних служб безпеки, зокрема Комп'ютерних груп швидкого реагування (CERT).

Кібервійною можна вважати, на думку дослідників, масштабну кібератаку на шостому рівні, спрямовану на те, щоб паралізувати всю державну систему, особливо пов'язану з обороною і безпекою [18].

Одним з прикладів масштабної кібератаки в рамках інформаційного протистояння між країнами є використання вірусу Stuxnet для порушення роботи іранських підприємств зі збагачення урану.

Дана кібератака детально описана у книзі Енді Грінберга «Піщаний хробак або Sandworm» [19]. У 2005 році до влади в Ірані прийшов Махмуд Ахмадінежад, який заявив про намір зміцнити ядерний потенціал держави. За короткий період часу Іран припинив угоду з МАГАТЕ та відновив роботу ядерних центрів у Натанзі. За даними ізраїльської розвідки, Іран міг за декілька місяців створити ядерну зброю.

Американське керівництво почало шукати спосіб завадити реалізації іранської ядерної програми без військового втручання. Стратегічне командування Пентагону спільно з кіберкомандою Агенції національної безпеки та ізраїльською кібергрупою, відомою як Підрозділ 8200, почали розробку шкідливої програми, здатної перешкодити Ірану створити ядерну зброю.

Паралельно США з союзниками чинили тиск на Іран. Для цього використовувався широкий спектр технологій інформаційно-психологічного впливу, що підкріплювались обговоренням проблеми

на рівні Генеральної Асамблеї та Ради Безпеки ООН, економічними санкціями, демонстрацією сили і готовності розпочати військову операцію тощо [20].

Вже у 2008 році на заводі у Натанзі центрифуги почали виходити з ладу. Іранські інженери не могли зрозуміти, що відбувається, адже цифровий моніторинг центрифуг не виявляв жодних ознак проблеми. Наприкінці 2009 року представники МАГАТЕ повідомили, що іранці вивозять з ядерного центру центрифуги, зняті з експлуатації. За даними цієї організації, з 8700 центрифуг у Натанзі було пошкоджено близько 2000 машин.

Викриття Stuxnet сталося у червні 2010 року у маловідомій компанії «ВірусБлокАда». Розробник антивірусного ПЗ помітив, що комп'ютер одного з клієнтів в Ірані застряг у циклі повторюваних збоїв та перезапусків. Провівши аналіз, фахівець компанії виявив приховану форму шкідливої програми – руткіт, що закріпився у комп'ютері завдяки уразливості «нульового дня». Він також виявив, що Stuxnet потрапив у комп'ютерну мережу через звичайний USB-накопичувач.

Після повідомлення про шкідливу програму на форумі кібербезпеки інформацією зацікавалась компанія Simantec. Провівши дослідження, експерти компанії з'ясували, що шкідлива програма складалась з 500 кілобайтів коду, що у 20-50 разів перевищує «вагу» звичайної шкідливої програми. Шкідлива програма поширилась на 22 тисячі комп'ютерів в Ірані.

За даними різних експертів, Stuxnet атакував промислові об'єкти в Ірані у три етапи. Спочатку він націлювався на комп'ютери та мережі Microsoft Windows, неодноразово виконуючи своє самовідтворення. Потім він шукав програмне забезпечення Siemens Step7, яке також працює на Windows-платформі та використовується для програмування промислових систем управління, які керують обладнанням, таким як центрифуги. Зрештою, він компрометував програмовані логічні контролери.

Специфікою Stuxnet є оснащення краденими цифровими сертифікатами, які приймались ОС Windows, та дозволили встановити шкідливі драйвери [19].

Німецький експерт Ральф Лангнер (Ralph Langner) опублікував дослідження, в якому заявив про дві версії Stuxnet. Stuxnet Mark I датований 2007 роком, тобто з'явився на три роки раніше, ніж вже відомий Stuxnet Mark II.

Початковий варіант був націлений на те, щоб створити зайвий тиск у центрифугах шляхом саботажу системи, яка забезпечувала захист центрифуг.

Головною метою Mark I був саботаж іранської багаторівневої (каскадної) системи захисту, що керувала центрифугами, розробленими у 1970-х роках. Ця система дозволяла проводити збагачення урану, навіть у разі поломки тієї чи іншої центрифуги. У системі захисту використовувалися три запірні клапани, встановлені для кожної центрифуги. Завдяки цим клапанам поламані центрифуги ізолювалися від інших для подальшої заміни. Робочий процес при цьому не припинявся.

Система захисту використовувала промислові контролери Siemens S7-417 для керування клапанами та датчиками тиску в центрифугах. Stuxnet був розроблений для інфікування цих контролерів та встановлення контролю над ними.

Перший варіант Stuxnet перекривав газові клапани, блокуючи вихід газу і тим самим підвищуючи тиск на центрифуги. Підвищення тиску призводило до серйозних пошкоджень центрифуг. При цьому показники приладів не змінювалися, й інженери не бачили справжньої картини того, що відбувалося. До того ж, Stuxnet діяв так, щоб не допускати масштабних руйнувань, які могли б його викрити.

Дія другого варіанту Stuxnet була спрямована на прискорення та сповільнення роботи роторів центрифуг, поки вони не виходили з ладу.

За оцінками експертів, за допомогою Stuxnet було виведено з ладу понад тисячі центрифуг для збагачення урану, затримано запуск Бушерської АЕС в Ірані. І загалом, шкідлива програма відкинула іранську ядерну програму на два роки назад.

Іншим прикладом здійснення кібератак в рамках інформаційного протистояння є агресія РФ у кіберпросторі проти України, яка почалася ще під час масових протестів наприкінці 2013 року [21].

Вже тоді понад 20 підприємств та державних установ України було заражено комп'ютерним хробаком, що отримав назву «Uroboros». Головна мета – викрадення інформації, в тому числі персональних даних та паролів доступу до інформаційних ресурсів. Основними об'єктами ураження вірусу «Uroboros» були веб-ресурси органів державної влади, у тому числі силових структур, засобів масової інформації та великих промислових підприємств.

Uroburos – це руткіт, що складається з двох файлів: драйвера і закодованої віртуальної файлової системи. Цей руткіт може взяти під контроль заражений комп'ютер, заражати інші комп'ютери у локальній мережі, виконувати довільні команди і приховувати системну діяльність. Він може красти інформацію і може також перехоплювати мережевий трафік. Його модульна структура дає можливість легко додавати нові функції, що робить Uroburos не лише дуже складним, а й надзвичайно гнучким і небезпечним.

На кібератаку звернула увагу британська аерокосмічна і військова група BAE Applied Intelligence. За оцінками експертів, до кібератаки причетні державні структури, скоріше за все, російські спецслужби [22].

Наступна кібератака мала місце у травні 2014 року, під час президентських виборів, коли російські хакери на 20 годин вивели з ладу інформаційну систему Центральної виборчої комісії України «Вибори». Тоді російські хакери намагалися скомпрометувати результати виборів у пропагандистських цілях, вивівши лідера партії «Правий сектор» Дмитра Яроша на перше місце. У липні того ж року офіційний веб-портал Президента України зазнав потужної DDoS-атаки, внаслідок якої він декілька годин був недоступним [21].

З того часу кібератаки набирали обертів і почали охоплювати енергетичну сферу та державні фінансові установи. Так, в ніч на 23 грудня 2015 року російські хакери атакували внутрішню мережу «Прикарпаття обленерго». Через кібератаку було вимкнено близько 30 підстанцій, і близько 230 тисяч мешканців на кілька годин залишилися без світла. Для отримання доступу до корпоративної мережі компанії хакери заразили комп'ютер одного із співробітників трояном «BlackEnergy» [21].

Ще одну кібератаку на енергетичну сферу було здійснено 18 грудня 2016 року на підстанції «Північна» в Києві, коли протягом 2 годин через збій в автоматиці управління більшість споживачів північної частини правого берега Києва та прилеглих районів області залишилися без струму. Схоже, що хакери використали уразливості «нульового дня».

Того ж місяця було здійснено кібератаку на сайти Міністерства фінансів, Держказначейства, Пенсійного фонду. Внаслідок цієї кібератаки було знищено частину інформації, а також виведено з ладу обладнання, що призвело до затримки з бюджетними виплатами на сотні мільйонів гривень. Для виведення з ладу серверів державних фінансових установ зловмисники використовували «KillDisk» (програма для знищення файлів з комп'ютерів (серверів), принцип роботи якої полягає у знищенні або перезаписі критично важливих системних файлів), а також троянську програму «BlackEnergy» [21].

27 червня 2017 року Україна стала об'єктом масштабної кібератаки з використанням вірусу-шифрувальника «NotPetya». Внаслідок атаки було заражено близько 12 тисяч персональних комп'ютерів, більшість з яких належала приватним українським організаціям, а також уряду, банкам, державним енергетичним компаніям, київському аеропорту та метрополітену. Від атак постраждала значна кількість приватних компаній, торгові мережі («METRO Cash&Carry», «Novus», «Fozzy», «Епіцентр», «Рост» тощо), телеком-оператори («Київстар», «Vodafone», «Lifecell»), мережі заправних станцій («WOG»,»KLO«), транспортні та енергетичні компанії [21].

Російські хакери зламали сервера Linkos, що відповідали за розсилку оновлень бухгалтерського ПЗ M.E.Doc, яке використовували українські організації для електронного документообігу. NotPetya поширювався у комп'ютерних мережах компаній з надзвичайною швидкістю. Наприклад, для зараження внутрішньої мережі українського банку вірусу знадобилось 45 секунд.

В основі NotPetya – два потужних експлойта – EternalBlue та Mimikatz. EternalBlue – експлойт «нульового дня», що дає змогу скористатись уразливістю в одному з протоколів Windows, та

запустити сторонній код на комп’ютерах з операційною системою Windows. Mimikatz, створений французом Бенджаміном Дельфі у 2011 році, дає змогу вилучити автентифікаційні дані користувача, який залогінився у системі, а також використати їх для зламу інших доступних пристроїв.

Вірус NotPetya було створено виключно для того, щоб заподіяти шкоди. Шкідлива програма шифрувала завантажувальний сектор комп’ютера, що дає змогу пристрою «знайти» операційну систему. Після шифрування даних шкідлива програма вимагала викуп за ключ для розшифрування файлів. Однак, виплати не мали ефекту, і відновити файли було неможливо [23].

Значне зростання кількості кібератак спостерігалось на початку 2022 року. Масовані кібератаки проти державних структур України та бізнесу були частиною інформаційної війни РФ проти України та передували повномасштабному вторгненню російських військ на територію держави.

Так, у ніч на 14 січня 2022 року російські хакери атакували близько 70 сайтів органів влади України. Зокрема, хакерської атаки зазнали сайти Міністерства освіти та науки, Міністерства закордонних справ, Міністерства у справах ветеранів, Міністерства енергетики, Державної служби з надзвичайних ситуацій та «Дії». На урядових ресурсах було розміщено зображення з текстом українською, російською та польською мовами, який попереджав користувача, що нібито його особисті дані стали публічними, а інформація на комп'ютері знищується. Припис, що це «за ОУН УПА, за Галичину, за Полісся та за історичні землі» нібито вказував, що до атаки причетні «польські» хакери. Однак, «послання» українцям було написане ламаною польською мовою.

За інформацією Державної служби спеціального зв'язку та захисту інформації України від кібератаки постраждали 22 сайти органів державної влади: шість зазнали «значної шкоди», 70 – відключили за вказівкою Держспецзв’язку та Служби безпеки України. Роботу веб-сайтів було відновлено протягом трьох днів [24].

15 лютого 2022 року було здійснено серію DDoS-атак на українські урядові інтернет-ресурси та національні банки. Внаслідок

першої хвилі було втрачено доступ до сайтів Міністерства оборони та Збройних сил України, а також зафіксовано перебої у роботі сервісів ПриватБанку та Ощадбанку. Під час другої хвилі хакери атакували інші урядові сайти, зокрема сервіс Дія. DDoS-атак зазнали сайти 11 міністерств та урядовий портал [25].

Першими свою роботу відновили ПриватБанк та Ощадбанк. В основному кібератака стала причиною перебоїв у роботі мобільних додатків «Приват24» та «Ощад24/7». Роботу урядових сайтів було відновлено о півдні 16 лютого.

Безпосередньо напередодні повномасштабного вторгнення РФ на територію України, 23 лютого 2022 року масштабна DDoS-атака була націлена на сайти уряду, банків та структур безпеки України.

Внаслідок кібератаки не працювали сайти Верховної Ради, Кабміну, МЗС та СБУ. У відповідь на кібератаку, в якій Україна, Велика Британія та США звинуватили РФ, була задіяна команда швидкого реагування у складі експертів з Литви, Хорватії, Польщі, Естонії, Румунії та Нідерландів [26].

Загалом, за даними Державної служби спеціального зв'язку та захисту інформації, протягом місяця (з 15 лютого по 15 березня 2022 року) Україна зазнала понад три тисячі DDoS-атак. Найпопулярнішими видами атак були фішингові розсилки, розповсюдження шкідливого програмного забезпечення та DDoS-атаки. Об’єктами атак були інформаційні ресурси державних органів, установ і компаній фінансового сектору та сфери телекомунікацій [27].

Кібервійна проти України продовжується. Країна-агресор здійснює фішингові атаки через розсилання листів і повідомлень у месенджерах, кібератаки на об’єкти критичної інфраструктури, злами веб-сторінок місцевих органів влади та ЗМІ [28].

Показовою є кібератака у березні 2022 року проти десятка українських інформаційних ресурсів. Зокрема, було зламано стрічку новин в ефірі телеканалу «Україна 24». Зловмисники запустили «рядок титрування» із начебто зверненням Володимира Зеленського про капітуляцію. Хакери також атакували інші українські медіа (зокрема, «Сьогодні», Громадське, 0532.ua та інші), використовуючи вразливості рекламного застосунку Redtram.

Головними об’єктами кібератак є оператори мобільного зв’язку, інтернет-провайдери, державні органи, організації фінансового сектору, енергетики та сектору безпеки і оборони.

Кібератаки оперативно висвітлюються російськими ЗМІ. Фактично російські кібератаки координуються з психологічними операціями, створюючи потрібні медійні приводи для поширення пропагандистських наративів і дезінформації [28].

Питання для самоконтролю:

1. Як дослідники визначають термін «кіберпростір»?
2. Чи є тотожними поняття «кіберпростір» та «мережа Інтернет»?
3. Які специфічні риси притаманні кіберпростору?
4. Що таке кібератака?
5. На які види поділяються кібератаки за способом дії?
6. Якими є особливості кібератак як інструменту інформаційного протиборства?
7. Чому дослідники почали обговорювати питання кібервійни?
8. Як визначається термін «кібервійна»?
9. В яких випадках кібератаки переростають у кібервійну?
10. Яких цілей може досягти країна за допомогою кібератак?

Завдання:

1. Навести приклади кібератак як складової інформаційних операцій у 21 столітті, визначивши суб’єктів кібератак, цілі, типи кібератак, наслідки тощо.
2. Навести приклади використання в інформаційних війнах 21 століття таких видів кібератак: фішинг, DDoS атаки, шкідливе програмне забезпечення, атака нульового дня.
3. Навести приклади кібератак в рамках наступальної інформаційної операції та приклади кібератак в рамках оборонної інформаційної операції. Оцінити результати використання кіберзброї у вибраних інформаційних операціях.
4. Охарактеризувати діяльність кіберармій різних країн світу (на вибір).

3.3. Інтернет-меми

Одним з сучасних інструментів інформаційного протиборства у кіберпросторі є меми.

Мем походить від давньогрецького слова «мімезис», що означає наслідувати, відображати, імітувати.

Термін «мем» введено в обіг англійським біологом Річардом Докінзом у книзі «Егоїстичний ген» (1976 р.). Р. Докінз визначав меми як одиниці культурної передачі чи одиниці наслідування [29].

Розглядаючи меми як реплікатори, дослідник стверджував, що меми потрапляють з одного мозку до іншого у процесі імітації, а їх виживання зумовлене такими якостями, як довговічність, плодючість і точність копіювання.

За визначенням в Оксфордському словнику, мем – це ідея, що передається від одного члена суспільства до іншого людьми, які копіюють її; зображення, відео, фрагмент тексту тощо, які дуже швидко передаються від одного інтернет-користувача іншому, часто з невеликими змінами, що роблять його гумористичним [30].

Кіт Хенсон у своїй статті «Еволюційна психологія, меми та походження війни» визначила меми як інформацію, яка поширюється, впливає і зберігається. Меми можуть бути ідеями або символами, яскравими фразами, хештегами або словами, що мають культурне значення [31].

Американський філософ і когнітивіст Деніел Деннет визначив мем як складну ідею, яка самоорганізується в окрему одиницю, що запам’ятовується. На думку дослідника, мем має складний, впроваджений у культуру зміст, представлений у компактній формі, що легко запам'ятовується.

У книзі «Психічні віруси» Річард Броуді визначив мем як одиницю інформації, що міститься у свідомості. Дослідник виокремив три види мемів: меми-відмінності, меми-стратегії, меми-асоціації.

- ***Меми-відмінності*** дають змогу «порізати» світ на шматочки категорій, видавши кожній свій ярлик. Завдяки таким відмінностям, люди можуть оперувати окремими предметами, але одночасно втрачають з поля зору інші.

- ***Меми-стратегії*** – гнучкі правила практичної поведінки, які вчать людей, що можна зробити у певній ситуації для отримання бажаного результату.
- ***Меми-асоціації*** пов'язують два і більше мемів у людській свідомості один з одним. Якщо свідомість «запрограмована» мемом-асоціацією, увага до одного об'єкту негайно викликає іншу думку чи почуття [32].

Як зазначив дослідник, основними способами поширення мемів є повторення інформації, створення когнітивного дисонансу та вплив на «чуттєві точки» (метод троянського коня).

С. Катаєв вважає, що мем - це інформація, закодована у символі. Розкодування здійснюється шляхом асоціацій та культурних кліше, що формуються у процесі функціонування певної змістовної тематичної інформації.

Меми задають типізацію, за допомогою якої люди розпізнають сенс повідомлення. Крім того, меми можуть викликати «ментальну епідемію», формуючи стійкі образи у свідомості людини. Важливою характеристикою мема є його здатність до самовідтворення, знижуючи здатність великої кількості людей реагувати на раціональні доводи й аргументи, що суперечать мему [33].

Українська дослідниця Л. Смола вважає, що мем можна трактувати як образ, ідею, символ, дію, будь-яку культурну інформацію, яку скопіювала одна людина від іншої; спеціально створене інформаційне повідомлення, яке поширюється в інформаційному просторі та призначене для формування необхідної картини світу людини та прийняття відповідних рішень. Мем впливає на сприйняття дійсності та спонукає до дій. Коли мем перетворюється на загальнозрозумілий символ, він не тільки впливає на реальність, а трансформує її [34].

Вітчизняний дослідник Георгій Почепцов визначив меми як елементарні ментальні структури, за допомогою яких можна створювати чи руйнувати ідеї, та виокремив три важливі характеристики мема: яскрава форма і значення, самодостатність для саморозповсюдження та здатність створювати чи руйнувати ментальний захист [35].

Френсіс Хейліген у статті «What makes a meme successful?» визначив низку характеристик успішних мемів: конкретність, простота, актуальність, інваріантність, керованість, відповідність існуючим переконанням аудиторії, однозначність, виразність, легкість , корисність, конформність тощо.

Щоб бути відтвореним, мем має успішно пройти чотири послідовні етапи: 1) асиміляція індивідом; 2) збереження у пам'яті цієї людини; 3) відтворення індивідумом мема у вигляді мови, тексту, зображення, поведінки; 4) передача іншим. За цим останнім етапом знову слідує перший етап, тим самим замикаючи цикл реплікації [36].

У публікаціях С. Шомової визначено низку характеристик мему, як елементу комунікації, а саме: двошарова структура меседжу (шар політичного чи культурного контенту, та зовнішній асоціативний шар, що допомагає привернути до нього увагу індивіда); реплікація; іронічний зміст контенту; інтертекстуальність; інтерактивність; прив'язка до колективного несвідомого; суперечлива і двоїста природа (мем може бути спонтанним або цілеспрямовано створеним) [37].

Як зазначає В. Лавров, меми є лаконічними і не містять значущої інформації, а викликають певні асоціації, роблячи натяки. Мем містить більше сенсу, ніж може здатися на перший погляд. Мем подібний до айсбергу, більша частина якого прихована в історичному контексті або пам'яті людини.

Наприклад, у 2018 році Президент США Дональд Трамп у своєму офіційному аккаунті Twitter розмістив мем зі своєю світлиною, підписом «санкції близько» та датою впровадження антиіранських санкцій – 5 листопада.

На пост Д. Трампа іранський командувач К. Сулеймані відповів у такому ж дусі: у своєму Instagram-акаунті він розмістив мем з фразою «I will stand against you». Обидва меми було стилізовано під телесеріал «Гра престолів».

Ще однією важливою характеристикою мемів, що робить їх ефективним засобом впливу на масову свідомість, є те, що вони сприймаються аудиторією як «органічний» користувацький контент, і відповідно викликають довіру.

За стилістичними особливостями інтернет-меми поділяються на текстові, меми-зображення, відео-меми, креалізовані меми [38].

Текстовий мем – емоційно забарвлене висловлювання в афористичній чи гумористичній формі, що має певне значення. Різновидом текстових мемів є меми-анекдоти.

Мем-зображення – будь-яке зображення, що відображає певну ситуацію або виражає емоції. Різновидом такого мему є фотожаба – світлина, оброблена у графічному редакторі.

Відео-мем – короткий відеосюжет, що розповсюджується користувачами соціальних мереж.

Креолізований мем – мем, що складається з вербальної та візуальної частин. Вербальний компонент є коментарем до будь-якої реальної події. Візуальний образ задає загальну тему висловлювання, звужує сферу його вживання та передбачає емоційно-експресивне забарвлення інформаційного повідомлення.

У книзі «Меми як вони є» С. Шомова запропонувала класифікувати меми за цільовими функціями, розділивши їх на три категорії: меми-агресори, меми-протектори, меми-атрактори [37].

Меми-агресори націлені на підрив авторитету будь-якої особистості, політичної партії, ідеї, руйнування чинного статус-кво. Залежно від завдань, поставлених перед такими мемами, до таких мемів можна віднести меми-провокатори, меми придушення, меми безпорадності, конспірологічні теорії тощо.

Меми-протектори – меми, що захищають ту чи іншу ідеологію, персону, імідж організації чи держави, можуть бути як прямими, так і закамуфльованими.

Меми-атрактори – джерела хайпа – привертають увагу до події, персони, факту та створюють навколо них яскравий інформаційний контекст. Вони можуть діяти як у зв'язці з агресорами та протекторами, так і самостійно. У першому випадку вони стають компонентами негативних чи позитивних мемплексів, у другому – нейтральних.

Прикладні аспекти використання мемів в контексті інформаційного протистояння почали розроблятись американськими військовими приблизно з 2006 року.

У своїй публікації майор морської піхоти США Майкл Проссер зазначив, що якщо інформаційні операції націлені безпосередньо на супротивника, то об'єктом меметичних операцій є мирне населення своєї країни та країни-опонента [29].

2008 року на замовлення американської Агенції перспективних досліджень оборони (DARPA) та під керівництвом президента компанії Robotic Technology Inc. Роберта Фінкельштейна було підготовлено багатосторінковий «Memetics compendium», в якому відмічається наступне: «Щоб бути прийнятним для господаря, мем має відповідати існуючим ментальним конструкціям або системі переконань людини, або ж відноситись до парадигми поглядів, до якої індивід сприйнятливий» [29].

Джефф Гізі, автор статті «Настав час освоїти меметичну війну», розглядає меметичну війну як суперництво за наративи, ідеї та соціальний контроль на полі бою соціальних медіа. Меметична війна, на думку дослідника, – це цифрова версія психологічної війни. Меметичні кампанії можуть виглядати як піар-кампанії, проводитись з-за кордону, фінансуватись підставними особами, а не напряму урядом. Ефективність використання мемів залежить від розуміння специфіки аудиторії, та вимагає швидкості, адаптивності і креативності [39].

Автори дослідження Exploring the Utility of Memes for U.S. Government Influence Campaigns (Vera Zakem, Megan K. McBride, Kate Hammerberg), визначили три цілі використання мемів в інформаційному протиборстві [40]:

Inoculate: Меми можна використовувати для того, щоб запобігти чи мінімізувати вплив повідомлень супротивника (превентивна тактика). Для превентивних цілей часто використовується гумор/висміювання.

Наприклад, у 2015 році у відповідь на загрози з боку ІДІЛ користувачі іміджборду 4chan поширили сотні зображень бійців терористичної організації з гумовими качками замість голови. Такі меми стали популярними у Twitter, Facebook та інших соціальних мережах.

Infect: Меми можуть використовуватись для поширення повідомлень на користь суб'єкта впливу (наступальні дії).

Наприклад, під час президентських виборів у США 2016 року російська «фабрика тролів» поширювала низку мемів у мережі Інтернет, з метою поляризації американського суспільства та як наслідок здійснення впливу на результати виборів.

Treat: Меми можуть використовуватися для того, щоб стримувати ефект повідомлень супротивника (оборонна тактика)

Наприклад, 20 вересня 2015 року російський телеканал РЕН ТВ поширив новину про присутність посла США Джона Теффта на мітингу опозиції у Москві. Новина підкріплювалась світлиною Теффта, який стояв перед групою репортерів, на тлі мітингу опозиції. Російський телеканал також розмістив цю світлину у Твіттері з підписом «Посол США в РФ Джон Теффт прогулявся на мітингу опозиції у Мар'їно».

Посольство США з'ясувало, що новина була фейковою, і перетворило зображення Теффта на мем, створивши серію фотошоп-зображень. Через декілька годин після появи твіту РЕН ТВ посольство США в РФ відповіло твітом такого змісту: «Посол Теффт провів вчорашній вихідний вдома. Але завдяки фотошопу можна опинитись будь-де». Пости американського посольства зображували Теффта при посадці на Місяць, з Дугласом Макартуром на Філіппінах у 1945 році та на хокейному матчі. Твіти посольства США були ретвітнуті майже 1000 разів, в той час як початковий твіт РЕН ТВ мав менше 100 репостів.

Дослідники дійшли висновків, що візуальні меми виходять за рамки окремих культур, і можуть охоплювати різні аудиторії у мережевому середовищі; використовують гумор, іронію, сарказм для досягнення емоційного відгуку; можуть ефективно використовуватись як на тактичному, так і стратегічному рівнях.

У професійному бюлетені військової розвідки США у статті «Меметичні війни: майбутнє військової справи» Б. Дж. Хенкок зазначив, що «принцип меметичної війни полягає у тому, щоб витіснити або, іншими словами, перезаписати небезпечні патогенні меми на більш доброякісні, щоб кількість останніх була більшою» [41].

Для успішного витіснення небезпечних мемів потрібно створити інші заразливі меми, використавши привабливі для аудиторії формати та ефективні способи їх тиражування.

Загальний алгоритм створення і поширення мемів у мережі Інтернет включає декілька етапів.

На першому етапі визначається основна ідея, яку суб'єкт впливу хоче донести до цільової аудиторії. Якщо основна ідея є комплексною, тоді вона розбивається на компоненти.

На другому етапі проводиться підбір мемів для просування основної ідеї. Фахівці визначають не лише самі меседжі, але й вибирають формат і спосіб подачі мемів, аби зробити їх більш привабливими для аудиторії.

Третій етап – це меметична індоктринація. Індоктринація починається з лідерів думок, які мають своїх послідовників і можуть на них впливати. Для індоктринації використовуються різні методи впливу, такі як повторення, створення когнітивного дисонансу, гра на емоціях тощо. Постійно проводиться моніторинг ситуації та оцінка рівня індоктринації цільовими ідеями. Якщо рівень індоктринації є недостатнім, тоді агенти впливу повертаються до роботи над індоктринацією лідерів [41].

Заключний етап пов'язаний з ідентифікацією членів цільової аудиторії, які не індоктриновані ключовими ідеями. На цьому етапі вирішуються такі питання: чи буде ефективним тиск з боку індоктринованих членів і лідерів; чи становлять загрозу неіндоктриновані представники цільової аудиторії для поширення основних ідей; яким чином можна мінімізувати загрози тощо. Процес індоктринації продовжується до тих пір, поки не буде досягнуто бажаного рівня охоплення цільової аудиторії.

Загалом, інтернет-меми є дієвим засобом впливу в інформаційному протиборстві, оскільки привертають увагу громадськості і спонукають аудиторію до поширення тих чи інших ідей; формують певні шаблони сприйняття подій і ситуацій, граючи на почуттях, асоціаціях і пам'яті; можуть використовуватись як у наступальних, так й оборонних інформаційних операціях тощо.

Питання для самоконтролю:

1. Що таке мем?
2. Які характерні риси притаманні мемам?
3. Які види мемів визначено у книзі Річарда Броуді «Психічні віруси»?
4. Які характеристики роблять меми ефективними засобами впливу на масову свідомість?
5. Які класифікації інтернет-мемів Ви знаєте?
6. В чому полягає суть меметичної війни?
7. З якими цілями використовуються інтернет-меми в інформаційному протиборстві?
8. Яким є загальний алгоритм створення і поширення мемів у мережі інтернет?

Завдання:

1. Навести приклади використання інтернет-мемів в інформаційних операціях 21 століття.
2. Розробити сценарій психологічної операції (ПсО) у мережі інтернет з використанням мемів. Для цього потрібно визначити мету ПсО та цільові аудиторії; підібрати (знайти у мережі Інтернет) інтернет-меми, які підходять для ПсО; продумати алгоритм поширення інтернет-мемів.
3. Проаналізувати українські інтернет-меми у 2022 році з початком повномасштабної війни РФ проти України.

3.4. Онлайн астротурфінг

Однією з сучасних технологій інформаційно-психологічного впливу є астротурфінг, що полягає у створенні фіктивної громадської думки, імітації «масової підтримки» за допомогою численних фейкових повідомлень, замаскованих під «думки реальних осіб» [42].

У кіберпросторі астротурфінг використовується для витіснення думки реальних людей на веб-форумах, для організації підроблених (замовних) онлайн кампаній, які створюють враження, що велика кількість людей вимагають чогось конкретного, або виступають проти чого-небудь тощо.

Реалізація технології астротурфінгу передбачає створення команд для розміщення повідомлень на онлайн-платформах для просування чи висміювання певних ідей; поширення меседжів, які будуть ретрансльовані більшістю інтернет-користувачів; технічну «накрутку» переглядів потрібних повідомлень для підвищення їх рейтингу.

Найбільш поширеними інструментами астротурфінгу є тролі і боти, а також підставні організації, які позиціонують себе як некомерційні, що захищають інтереси громадськості.

Інтернет-тролінг можна визначити як вид інтернет-спілкування з порушенням етичних норм, що проявляється в агресивній та образливій поведінці учасників мережевої взаємодії. Відповідно троль – це користувач, який розміщує у мережі Інтернет провокаційні повідомлення, з метою створення соціальної напруги та конфліктів між учасниками інтернет-спільноти.

Дослідження тролінгу почалось у 1996 році. Тоді американська фахівець з сучасних медіа Джудіт Донат опублікувала статтю «Ідентичність і обман у віртуальному співтоваристві», в якій визначила тролінг як «гру у фальсифікацію особистості, що розігрується інтернет-користувачем без згоди інших учасників конкретної комунікативної ситуації» [43].

Ключова риса тролінгу, на її думку, - це провокативність комунікації, пов’язана зі створенням підробленої особистості. Як

зазначає Дж. Донат, основним мотивом дій троля є егоцентризм, бажання отримати задоволення від словесної атаки, опинитися у центрі уваги, спровокувати конфлікт. Тролі сприяють зниженню довіри між учасниками, розвитку параної в онлайн-співтоваристві, а також можуть зірвати обговорення тих чи інших тем.

За визначенням британської дослідниці К. Хардакер (C. Hardaker) тролінг – це діяльність, суб'єкт якої вдає щире бажання бути членом певної онлайн-спільноти та конструює необхідну для цього модель поведінки, насправді бажаючи посварити інших учасників, створити або підсилити конфлікт задля власного задоволення [44].

Дослідниця виокремила такі тактики тролів:

- *Відступ:* троль навмисно відводить дискусію від основної теми за допомогою звичайного спаму або винесення на обговорення неактуальної теми;
- *Критика*: троль надмірно критикує інших в антагоністичній манері, водночас лицемірячи;
- *Антипатія*: троль прагне сформувати емоційну відразу до користувача, приділяючи надмірну увагу до його висловлювань, аби його дискваліфікувати;
- *Ілюзія корисності*: троль прикидається корисним і дає поради. Але подібна інформація може бути фейковою чи потенційно небезпечною;
- *Шок:* троль постить образливі, грубі, обурливі коментарі на чутливі для громадськості теми;
- *Агресія*: троль нападає на користувача без будь-якого обґрунтування, щоб змусити його відповісти агресією;
- *Приховування*: тролі «зливаються» з онлайн-спільнотою на довгий час, але в якийсь момент різко стають антагоністами щодо певної теми чи питання;
- *Гра у жертву*: троль спочатку провокує дискусію, а потім робить вигляд, що це він зазнав кібербулінгу.

К. Хардакер зазначає, що перелік тактик тролів насправді набагато більший, і вони постійно модифікуються.

На її думку, троля можна виявити за такими ознаками: використання грубої, ненормативної лексики; агресивна і образлива поведінка для створення конфлікту або емоційної напруженості; ухиляння від відповідей на прямі запитання; перетворення конструктивної комунікації у безглузду суперечку; залучення якомога більшої кількості учасників.

Українська дослідниця Наталія Вовк вважає, що троля можна розпізнати за такими ознаками: «постійні спроби перейти на особистості в розмові; використання теми суперечки тільки для виклику емоційної реакції співрозмовника; удавана недалекість і непоінформованість або навпаки знання всього на світі; невихованість, хамська поведінка; зачіпання завідомо спірних провокаційних тем»[45].

Інша вітчизняна дослідниця В. Христенко виокремила такі ознаки того, що інформацію поширює троль:

- Скандальність тексту, теми чи коментаря;
- Популярність теми. Тролі зазвичай підігрівають інтерес до теми будь-якими засобами. Для цього троль реєструється під різними іменами;
- Швидкість відповіді. Троль завжди швидко реагує на чужі коментарі та оперативно відповідає усім учасникам дискусії;
- Зв’язаність коментарів. Це відноситься до тролей, які використовують в одній темі кілька ніків. В результаті коментарі троля логічно взаємопов’язані, і троль по суті веде дискусію сам із собою;
- Непримиренність. Троль завжди сперечається, і жодні аргументи не можуть змінити його точку зору [46].

Поширеними маніпулятивними тактиками тролів є гра на почуттях людей, офтоп (відхилення від теми дискусії), провокаційні коментарі, флуд (поширення великого обсягу інформації з мінімальною смисловою цінністю), подання власної думки як загальновизнаного факту, постановка навмисно наївних питань, поновлення або перефразовування спірної минулої теми дискусії, аргументація на основі хибного твердження або вигаданого факту тощо [47,48].

Крім звичайних тролів, які прагнуть задовольнити власні егоцентричні потреби, у мережі інтернет діють професійні тролі, які спонсоруються окремими державами або організаціями для впливу на громадську думку у бажаному напрямі.

Використовуючи різні вигадані імена та фіктивні акаунти, тролі створюють у звичайного користувача соціальних мереж відчуття, що інформація поширюється різними людьми, з різних джерел. Це підвищує довіру до повідомлень та знижує критичне мислення інтернет-користувачів.

Крім того, діючи організовано, тролі за допомогою лайків та численних репостів можуть підвищувати рейтинг своїх тем чи коментарів та занижувати рейтинг небажаних коментарів Інтернет-користувачів.

Під виглядом тролів працюють групи добре підготовлених людей, які отримують конкретні завдання від замовників. Професійні інтернет-тролі можуть просувати пропагандистські чи контрпропагандистські наративи, проводити дезінформаційні кампанії, створювати видимість масової підтримки чи масового невдоволення тими чи іншими політиками або урядом загалом.

Організовані групи тролів, які використовуються тими чи іншими країнами в інформаційному протиборстві, стали відомими під назвою «фабрики тролів».

У загальному вигляді «фабрики тролів» мають тролів-модераторів тв тролів-виконавців. Троль-модератор взаємодіє із замовником, формулює завдання тролям і відповідає за змістовне наповнення і спрямованість коментарів у мережі Інтернет. Завдання містить тему, ключові слова, мету тролінгу та перелік інтернет-платформ, на яких потрібно розмістити повідомлення. Тролі-виконавці поділяються на такі категорії: тролі-письменники, які розміщують текстові пости на відповідних інтернет-платформах; тролі, які створюють і поширюють фотоматеріали; тролі, які створюють і поширюють відеопродукцію. Серед тролів-виконавців може бути спеціалізація по конкретним інтернет-платформам [49].

Типова стратегія «фабрики тролів» передбачає реалізацію таких дій:

1. створення фіктивних акаунтів у соціальних мережах, враховуючи специфіку цільової аудиторії;
2. розробка детального плану дій щодо виконання поставленого завдання;
3. підготовка та розміщення постів певної ідейної спрямованості (залежно від поставлених замовником цілей);
4. моніторинг інформації, розміщеної тролями у соціальних мережах, та реакції цільової аудиторії.

Як з'ясувалося в ході опитування американських інтернет-користувачів у 2012 році, поширення тролями образливих коментарів призводять не до зміни поглядів, а навпаки до зміцнення існуючих переконань користувачів, що сприяє більшій поляризації точок зору на інтернет-платформах. Відповідно тролінг у мережі Інтернет слугує не засобом переконання, а інструментом залучення більшої кількості користувачів та створення інформаційного резонансу.

Як інструмент інформаційної війни, в якій об'єктами впливу є не лише українська громадськість, а й населення інших країн, інтернет-тролінг активно використовує росія.

Так, у 2015 році фінське онлайн-медіа Yle Kioski опубліковало звіт про проросійську тролінгову діяльність у Фінляндії. Під час розслідування журналісти Yle Kioski зібрали інформацію від різних експертів, фінських веб-сайтів та осіб, які були мішенню проросійських тролів, а також стежили за діяльністю кількох секретних профілів, які використовувалися для ведення інформаційної війни [50].

Наприкінці 2014 року-початку 2015 років на популярних фінських веб-сайтах проросійські тролі розміщували дезінформаційні повідомлення та світлини маніпулятивного характеру. Для більшої достовірності тролі ділилися новинами з джерел, які можуть здаватися надійними, наприклад Russia Today, Перший канал і Sputnik News.

Чітко у відповідності з російськими пропагандистськими наративами тролі поширювали одні і ті самі повідомлення на кількох сторінках Facebook і новинних веб-сайтах або надсилали фінським користувачам у Twitter. Повідомлення були такого змісту:

- «У Києві стався незаконний фашистський переворот, і незаконна військова хунта завоювала владу»;
- «Західні країни – фашистські, а лідери західних країн – нацисти»;
- «Фашисти захопили Східну Україну. Доказів присутності Росії на Сході України немає»;
- «Росія не порушила міжнародного права, анексувавши Крим»;
- «Фіни – расисти, які ненавидять росіян. Росія завжди була добрим сусідом Фінляндії і найважливішим стратегічним партнером».

Тролі також хейтили фінських політиків за антиросійську позицію і розпалювання війни.

Крім того, тролі поширили у фінських соціальних мережах світлину, на якій нібито зображені діти зі Східної України, які страждають від бідності та голоду. Зображення містило підпис «Мамо, чому вони нас вбивають?» і хештег #SaveDonbassPeopleFromUkrArmy. Так тролі намагалися переконати фінську аудиторію у жорстокості української армії, звинувачуючи її у вбивствах дітей та опосередковано виправдовуючи участь Росії у врегулюванні «української кризи».

Загалом, тролі діяли за такою схемою: якщо хтось наважувався критикувати російського президента та дії Росії, згадувати НАТО чи США або сумніватися у правдивості інформації, троль звинувачував людину у ненависті до Росії, підлабузництві до фашистського НАТО і називав «зрадником, який хоче зруйнувати добрі відносини Фінляндії та Росії». Одночасно тролі вихваляли президента РФ як «харизматичного лідера демократичної Росії, який має повну довіру всього російського народу і чиї міцні лідерські здібності довелося визнати навіть Заходу» [50].

Неабиякого резонансу набула справа про втручання РФ у президентські вибори у США 2016 року. Тоді головними претендентами на посаду президента були кандидат від Республіканської партії Дональд Трамп та кандидатка від Демократичної партії Гіларі Клінтон.

Підготовка до масштабної психологічної операції у мережі Інтернет почалась ще навесні 2015 року. Пропагандистські кампанії,

націлені на різні сегменти американських інтернет-користувачів, проводились російською «фабрикою тролів» – Агенцією Інтернет-досліджень, розташованою у Санкт-Петербурзі.

За даними Facebook, Агенція інтернет-досліджень проводила пропагандистські кампанії через 470 несправжніх сторінок і акаунтів. З червня 2015 року по травень 2017 року «фабрикою тролів» було опубліковано близько 3000 постів. Кожного тижня «фабрика тролів» генерувала близько однієї тисячі одиниць контенту – текстів, фотографій та відеороликів [51].

За два роки витрати «фабрики тролів» на просування пропагандистських повідомлень у соціальних мережах склали понад 100 тисяч доларів. Охоплення аудиторії – 10 млн. громадян США.

Агенція використала принципи цифрового маркетингу: розробила бренд, створила присутність на всіх інтернет-ресурсах, розширювала аудиторію за допомогою платної реклами, а також авторитетів і перехресних посилань. Агенцією також було створено медійні міражі – взаємопов'язані веб-ресурси для занурення цільових аудиторій у потрібний контент [52].

Для здобуття довіри цільових аудиторій співробітники Агенції створили акаунти у соціальних мережах під вигаданими іменами. Імена підбирались так, щоб складалося враження, ніби це акаунти американських громадян.

Російські тролі поширювали повідомлення не лише через Facebook, Instagram і Twitter, а й на YouTube, Reddit, Tumblr, Pinterest, Vine и Google+ тощо.

Російська «фабрика тролів» під час виборчих перегонів у США працювала за трьома напрямами:

- кампанії на підтримку Дональда Трампа - кампанії, націлені на консервативних виборців, яких спонукали підтримати кандидата від Республіканської партії;
- кампанії з дискредитації Хіларі Клінтон (дискредитації кандидата від Демократичної партії було присвячено переважну більшість повідомлень у соціальних мережах);
- кампанії щодо демотивації виборців, в рамках яких поширювались три варіанти наративів: повідомлення, що

вносили плутанину у правила голосування; повідомлення із закликами голосувати за третього кандидата; повідомлення із закликами бойкотувати вибори [52].

Контент створених акаунтів у соціальних мережах було розроблено з урахуванням специфіки та вразливостей кожної цільової аудиторії.

Основними цільовими аудиторіями російської «фабрики тролів» були афроамериканці, консервативні виборці, ЛГБТ-спільнота, ліберальні виборці, американські виборці мексиканського походження та американські виборці-мусульмани.

Повідомлення для афроамериканських виборців були спрямовані на те, щоб підвищити недовіру до політичної системи США, посилити існуюче невдоволення нерівністю, дискримінацією, бідністю, насильством з боку поліції тощо. Крім того, російські тролі намагались підштовхнути цю аудиторію до думки, що найкращий спосіб просунути справу афроамериканської спільноти – це бойкотувати вибори і сконцентруватись на інших питаннях.

Варто відмітити, що афроамериканська аудиторія була дуже важливим об'єктом впливу. Окрім десятків акаунтів у соціальних мережах, присвячених проблемам афроамериканців, Агенція інтернет-досліджень створила десятки веб-сайтів, замаскованих під афроамериканські з такими назвами, як blackmattersus.com, blacktivist.info, blacktolive.org, blacksoul.us. На платформі YouTube було створено канали «Don't Shoot», «BlackToLive», «Black Matters» тощо [53].

У повідомленнях для консервативних виборців акцент було зроблено на спірних питаннях, таких як проблема мусульманських меншин, питання зброї, погане ставлення до ветеранів тощо. Пропагандистські повідомлення часто містили патріотичні та антиімігрантські гасла, аби викликати обурення ліберальним умиротворенням інших за рахунок американських громадян.

Мета впливу на ЛГБТ-спільноту і ліберальних виборців полягала у тому, щоб знизити довіру до політичної системи і посилити поляризацію між лібералами і консерваторами стосовно прав ЛГБТ.

Апелюючи до американських виборців мексиканського походження російські тролі розкручували теми депортації, поганого ставлення до мігрантів, дискримінації тощо [52].

Для впливу на американських виборців-мусульман використовувались позитивні історії про іслам і мусульман, що поєднувались із критичними коментарями політики американського уряду.

За кількістю лайків і репостів найбільшої популярності набули такі створені «фабрикою тролів» акаунти у соціальних мережах:

- Being Patriotic,
- Stop A.I. (All Invaders),
- Heart of Texas,
- Blacktivist,
- United Muslims of America,
- Army of Jesus,
- Brown Power (запущена після виборів),
- LGBT United,
- South United,
- BM (Black Matters).

Приклади пропагандистських повідомлень російської «фабрики тролів» у період президентських виборів у США 2016 року представлено у Додатку А.

Лише протягом шести місяців 2016 року через ці 10 акаунтів було поширено 9373 пости, з яких 4596 (49%) були націлені на консервативних виборців, а 2355 (25%) орієнтовані на афроамериканців [52].

Поряд з онлайн-кампаніями, Агенція інтернет-досліджень залучала американських активістів для проведення оффлайнових заходів. Адміністратори акаунтів контактували з місцевими активістами під вигаданими іменами, просили дати інтерв'ю. Після інтерв'ю активісти отримували листи з проханням долучитись до проведення тих чи інших акцій, мітингів та флешмобів. Наприклад, у жовтні 2016 року у місті Шарлотт (Північна Кароліна) «фабрикою тролів» через спільноту BlackMattersUS та за підтримки місцевих

активістів було організовано мітинг афроамериканців проти поліцейського насильства. Загалом, за два роки (2016-2017 роки) «фабрикою тролів» було організовано близько 40 оффлайнових заходів [51].

2018 року американські спецслужби, які моніторили соціальні мережі, аби запобігти можливому втручанню у президентські вибори США, виявили підозрілі акаунти, що поширювали негативні пости про французького президента Емануеля Макрона.

ФБР проінформувала Facebook про підозрілі акаунти у самій мережі та в Instagram, сліди яких вели за кордон. За результатами перевірки було виявлено неавтентичну скоординовану поведінку низки акаунтів.

На основі цієї інформації Facebook заблокував 99 акаунтів в Instagram, 36 акаунтів і 6 сторінок у соціальній мережі Facebook. Серед цих акаунтів, 12 акаунтів в Instagram і 6 сторінок на Facebook генерували контент французькою мовою.

Схоже, що напередодні виборів у Франції була розгорнута онлайн-кампанія проти Емануеля Макрона з використанням тролів. Публікації в соціальних мережах містили переважно теги #macrondegage (Макрон, геть) або меми [54].

Експерти припускають, що можливою метою кампанії було зниження рейтингу Емануеля Макрона та створення сприятливих умов для обрання президентом Франції Марін Ле Пен.

За даними компанії Facebook, завдяки двом соціальним мережам було охоплено 76 000 підписників, з них – 12 400 були безпосередньо з Франції. Операція була вчасно виявлена, тому не встигла ще набути таких масштабів, як під час виборів у США 2016 року.

Франкомовні акаунти концентрувались на залученні аудиторії, а також публікували політичний контент, зокрема з нападками на Емануеля Макрона.

Як і в 2016 році, тролі привертали увагу аудиторії, апелюючи до актуальних суспільних проблем, особливо тих, які викликали суперечки.

Так, акаунт *@espoir_de_france* з 3000 підписників регулярно публікував антимакронівські меми, особливо на тему міграції, а також

на більш загальні економічні та політичні теми. Зокрема, було поширено декілька дописів зі світлинами Е. Макрона з такими написами: «Анти-французький!», «Я надаю перевагу мігрантам перед французами», «Мені подобається ображати французів!» [54].

Інший акаунт *@femme_combattante* (4 267 підписників) сконцентрувався на афро-французькій жіночій аудиторії та позитивних публікаціях про африканських жінок.

Акаунт *@france__rouge* (588 підписників) містив пости, в яких Е. Макрон поставав лицеміром і троцькістом, тобто послідовником революціонера, радянського комуністичного діяча Лева Троцького (1879-1940 рр.).

У дописах акаунту @france_pour_tous (3 353 підписники) акцент було зроблено на проблемах бідності та міграції. Колишній банкір Е. Макрон змальовувався як елітарний правитель, далекий від звичайних людей, який побоюється, що «народ прокинеться» [54].

Жоден інший французький політик не був об'єктом такої кількості негативних постів у соціальних мережах. Інтернет-тролі працювали переважно через меми, апелюючи до наболілих проблем, існуючих стереотипів та створюючи потрібні асоціативні ланцюжки.

Незважаючи на схожість з діяльністю російської «фабрики тролів», компанія Facebook заявила про відсутність достатніх доказів причетності Агенції інтернет-досліджень до проведення онлайн-кампанії проти Емануеля Макрона.

Технологію астротурфінгу використовує також Китай. Мета – поширення проурядової пропаганди, витіснення загрозливого для керівництва країни контенту і формування позитивного сприйняття країни з боку внутрішньої та зовнішньої аудиторій.

Для впливу на громадську думку у мережі інтернет Комуністична партія Китаю (КПК) використовує команди онлайн-коментаторів та контент-ферми.

До роботи онлайн-коментаторами залучаються репортери чи колумністи з традиційних ЗМІ, державні службовці, а також спеціально завербовані індивіди, які працюють анонімно та отримують невелику грошову винагороду за кожний пост (від 10 до 50 центів).

Обов’язки онлайн-коментаторів зазвичай включають моніторинг онлайн-думок, спрямування громадської думки шляхом участі в обговоренні актуальних тем, створення оригінальних дописів для просування пріоритетів діяльності уряду; роз’яснення політики та заходів, вжитих партією тощо. У кризових ситуаціях основним завданням онлайн-коментаторів є нейтралізація несприятливих соціально-політичних подій, особливо тих, які можуть спровокувати масові заворушення [55].

Проурядових онлайн-коментаторів у ЗМІ та низці наукових публікацій охрестили «50-центовою армією Китаю». Однак, американські дослідники Гері Кінг, Дженніфер Пан та Маргарет Робертс, проаналізувавши 43 757 публікацій китайських онлайн-коментаторів у соціальних мережах, отриманих з архіву електронних листів за 2013-2014 роки, надісланих відділу пропаганди району Чжангун міста Ганьчжоу в провінції Цзянсі, з’ясували, що переважна більшість коментаторів були державними службовцями і працювали у різних державних установах. Розміщення коментарів у соціальних медіа, скоріше за все, було частиною їх роботи на державній службі [56].

За вказівкою партійного керівництва онлайн-коментатори мали сприяти єдності і стабільності за допомогою позитивних наративів та активно керувати громадською думкою під час надзвичайних подій (тобто подій, які можуть спричинити колективні дії).

На прикладі вибірки дописів у соціальній мережі Weibo дослідники показали, що понад 70% дописів містили патріотичні гасла, мотиваційні цитати, неаргументовану похвалу партії та урядових програм; 20% – фактичну інформацію про державні програми, проекти та ініціативи; 6% – аргументовану похвалу державного керівництва або критику опонентів влади.

Екстраполювавши масштаби пропагандистської кампанії на решту Китаю, дослідники дійшли висновку, що урядові онлайн-коментатори щороку розміщують у соціальних мережах близько 448 мільйонів повідомлень [56].

Прокитайські наративи у мережі інтернет також поширюють націоналістично налаштовані групи інтернет-користувачів, яких ще

називають «добровільною 50-центовою армією». Для них характерним є скептичне ставлення до Заходу і розуміння ключової ролі державного керівництва у згуртуванні нації та індустріалізації країни.

Такі групи проводять онлайн кампанії проти опонентів китайської влади, апелюючи здебільшого до доказів і логіки. Так, члени групи можуть протистояти своїм опонентам, вказуючи на їхні логічні та фактичні помилки чи розбіжності у позиціях. Вони також вдаються до висміювання опонентів, використовуючи перебільшення, іронію та пародію, щоб підкреслити нелогічність їх аргументації. Ще однією тактикою є фішинг, що передбачає поширення сфабрикованого повідомлення на онлайн-платформі, збір даних про поширення фейку цільовою аудиторією та глузування над довірливістю опонентів [57].

Прикладом такої спільноти націоналістично налаштованих інтернет-користувачів є «Diba» (帝吧), що складається з китайців, які проживають за кордоном, та китайських студентів. Станом на 2019 рік група налічувала 20 мільйонів користувачів у соціальних мережах, включаючи Facebook, Twitter і Weibo [58].

Учасники Diba проводять кампанії проти опонентів КПК, в тому числі у західних соціальних мережах, під гаслом «коли Diba починає військову експедицію, пощади не буде для жодної травинки». Перед проведенням «експедиції» група оголошує дату початку кампанії та надає учасникам контент – фото, емодзі, гасла і повідомлення китайською та англійською мовами.

У січні 2016 року після обрання президентом Тайваню представника Демократичної прогресивної партії (ДПП) учасники Diba заполонили тисячами коментарів проти незалежності Тайваню акаунт новообраного президента у соціальній мережі Facebook та протайванські новинні видання Apple Daily і Sanlih News [59].

У відповідь на звинувачення з боку правозахисних організацій китайської влади у серйозних порушеннях прав і свобод уйгурів у квітні 2019 року китайські онлайн-коментатори заполонили зображеннями щасливих людей у Сіньцзяні Facebook-сторінки проуйгурських груп та Всесвітнього уйгурського конгресу. На світлинах були зображені усміхнені уйгури в національному одязі з підписами китайською та англійською мовами «Ми живемо дуже

добре». Інші дописи цитували промови президента Китаю Сі Цзіньпіна і державні документи про ситуацію у регіоні.

Влітку 2019 року об'єктами атаки групи Diba стали учасники масових протестів у Гонконгу проти законопроекту про екстрадицію, за яким місцева влада отримала право передавати підозрюваних у скоєнні злочину китайській владі для висунення звинувачень.

Учасники Diba розмістили тисячі коментарів на Facebook-сторінках двох гонконгських організацій – Громадянського фронту прав людини (головного організатора протестів) та Національного фронту Гонконгу (місцевої політичної партії). Типові коментарі були такого змісту: «бунтівники, які завдали шкоди батьківщині та Гонконгу, мають бути засуджені та суворо покарані»; «за гонконгськими порушниками спокою стоять західні господарі»; «їхні пропозиції не принесуть Гонконгу справжньої свободи та демократії, а лише катастрофу і руїну». Паралельно адміністратори Diba звернулись до своїх підписників з проханням поширювати повідомлення на підтримку поліції Гонконгу у соціальних мережах Facebook і Twitter. Крім того, на сторінці групи у Facebook були розміщені інструкції та технічні поради з використання іноземних соціальних медіа [60].

КПК також використовує розгалужену мережу з понад 20 мільйонів «добровольців мережевої цивілізації», які розміщують позитивні пости про Китай та збирають інформацію про громадську думку у мережі інтернет. Команди мережевих коментаторів складаються з членів Комуністичного союзу молоді Китаю (КСМ), студентів університетів і коледжів.

Волонтери мережевої цивілізації беруть участь у тематичних онлайн-заходах з нагоди важливих дат (День молоді, День заснування партії, День перемоги над Японією тощо), публікують дописи на підтримку партійної ідеології і політики (до 25 коментарів на місяць) та протидіють некоректним або шкідливим висловлюванням в інтернеті, що суперечать соціалістичним цінностям і становлять загрозу етнічній єдності.

Ці команди добровольців співпрацюють з іншими проурядовими онлайн-коментаторами, Комісіями з питань кіберпростору (організації КПК, відповідальні за моніторинг громадської думки у соціальних

мережах і протидію шкідливому контенту) та Бюро громадської безпеки (урядові структури, уповноважені відстежувати діяльність громадян на веб-платформах і видавати попередження правопорушникам) [61].

Ще одним інструментом, який використовує Китай для просування пропагандистських наративів у мережі інтернет та впливу на громадську думку, є контент-ферми. Це онлайн-платформи, які масово виробляють клікбейт-контент, аби отримати високий рейтинг у пошукових системах і прибуток від реклами. Для поширення своїх повідомлень контент-ферми використовують методи пошукової оптимізації, залучають окремих користувачів соціальних мереж або публікують свої посилання у популярних месенджерах.

Показовим прикладом діяльності контент-ферми Китаю на Тайвані є муніципальні вибори 2018 року у тайванському місті Гаосюн (2,8 млн. жителів), під час яких вперше за багато років здобув перемогу кандидат від Гоміньдану (Китайська націоналістична партія). За декілька місяців до виборів кандидат від Гоміньдану і опонент чинного на той час мера міста (представника ДПП Тайваня) був практично невідомим. Однак, його офіційна сторінка у Facebook менш ніж за місяць набрала 225 882 «лайків» і 235 038 підписників (середній показник по країні – близько 12 000 підписників). Наприкінці кампанії його акаунт у соціальній мережі мав близько півмільйона підписників – удвічі більше, ніж у його опонента від ДПП.

Важливу роль у виборчій кампанії пропекінського кандидата відіграла група його підтримки у Facebook, яка пропонувала інтернет-користувачам різноманітний контент – тези для розмови, меми та фейкові новини з критикою уряду ДПП. Пізніше було встановлено, що ця група не була створена справжніми шанувальниками кандидатів, а скоріше за все, контент-фермою з Китаю [62].

Китай через контент-ферми також намагався вплинути на громадську думку напередодні президентських виборів на Тайвані 2020 року. За кілька місяців до виборів у соціальній мережі Facebook почала працювати китайська контент-ферма mission-tw.com («Mission»), чиї публікації також поширювались тайванською контент-фермою nooho.net («Roar»).

«Mission» просувала наративи з критикою тайванського уряду, використовуючи інформацію, засновану на реальних фактах, але представлену в оманливий спосіб. Наприклад, в одній з публікацій стверджувалось, що Міністерство оборони Тайваню збиралося витратити гроші на стару модель винищувача (F-16A/B), хоча насправді це була нова модель F-16V.

Про зв'зок контент-ферми «Mission» з Китаєм свідчить часте згадування китайського веб-сайту China-Taiwan.net, створеного Управлінням у справах Тайваню. До того ж, деякі публікації «Mission» були репостами статей щоденної газети China Times [63].

Окрім вище згаданих груп онлайн-коментаторів, у 2019 році компанією Twitter було виявлено китайську мережу акаунтів з наративами, спрямованими на дискредитацію протестного руху у Гонконгу.

Проаналізувавши оприлюднені компанією близько 5000 найактивніших акаунтів, дослідники Австралійського інституту стратегічної політики виявили, що у мережі були задіяні спам-акаунти, які раніше публікували аполітичний контент, та «сплячі акаунти» з тривалим періодом бездіяльності і дописами різними мовами, які у 2018 році почали поширювати повідомлення китайською мовою. За три місяці 2019 року акаунти китайської мережі поширили 87 тисяч твітів і ретвітів. Основні наративи – засудження протестувальників Гонконгу, підтримка поліції Гонконгу і верховенства права, а також теорії змови про причетність західних країн до протестів [64].

Того ж року американська компанія з аналізу соціальних мереж Graphika також виявила китайську пропагандистську мережу, що використовувала зламані або фейкові акаунти на YouTube, Twitter і Facebook. Більшість створених акаунтів мали явні ознаки неавтентичності: імена з символами, відсутність особистої інформації, стокові або вкрадені світлини профілю тощо. Політичні повідомлення поширювались серед маси розважального контенту різної тематики.

У публікаціях, поширюваних через акаунти мережі впродовж 2019-2020 років, акцент робився на таких темах: протести у Гонконгу, досягнення КНР в економіці, політиці та боротьбі з COVID-19, невдачі США у політичній, економічній сферах та у боротьбі з пандемією,

суперництво між США і Китаєм. Усі поширювані наративи відповідали офіційній позиції КПК [65].

Акаунти мережі поширювали повідомлення однакового змісту, використовуючи відео з китайських державних медіа, меми і довгі тексти китайською та англійською мовами. Наприклад, на платформі Youtube акаунти репостили ідентичні відео про успішу боротьбу КНР з пандемією. Ці відео, у свою чергу, надходили з великої кількості акаунтів із західними іменами, які публікували проурядовий контент, змішаний зі спамом. Однак, справжніх інтернет-користувачів охопити не вдалось. Усі лайки, поширення та коментарі до публікацій мережі надходили від інших учасників мережі [66].

У другій половині 2020 року у мережі з'явились акаунти з персоналізованими профілями, які виглядали більш правдоподібно. Тематика повідомлень стала ширшою, і включала такі питання, як суперництво між США і Китаєм, контроль над озброєннями та економічний розвиток КНР. Збільшилась кількість відео, в яких США зображувались в негативному світлі, зокрема як країна-гегемон, як найбільша загроза миру у світі тощо.

Більше того, деяким акаунтам мережі вдалось вийти за межі ехо-камери й охопити реальних користувачів соціальних мереж. Наприклад, акаунт @jingrunhe зі світлиною молодої жінки у профілі поширював позитивний контент про Китай (зокрема, відео «Розвиток Китаю, подорож у часі») і критичні повідомлення про США англійською, мандаринською або кантонською мовами. Деякі дописи акаунту були оригінальними коментарями, що узгоджувались із наративами китайського уряду щодо Гонконгу, Тайваню, відносин із США та Австралією. Твітами цього акаунту поділились китайські посли, виконавчий директор Huawei Europe, чилійський і пакистанський політики, панамська телеведуча, мексиканський письменник тощо.

Крім того, фахівцями компанії Graphika було виявлено чотири YouTube-канали, які використовували персони відомих політичних оглядачів і поширювали власний контент у поєднанні з типовими відео мережі мандаринською або кантонською мовами.

Один Youtube-канал (Li Jian-nan Taiwan) поширював контент від імені коментатора тайванського походження і прихильника «об'єднання» Тайваню з Китаєм, другий канал (Zhang Zhaozhong) – дописи від імені відомого у Китаї військового аналітика і колишнього контр-адмірала НВАК (коментарі аналітика на теми від протиракетної оборони до 5G та типові відео мережі англійською і китайською мовами). Третій Youtube-канал (Chan Chi Ho) публікував контент від імені гонконгського політичного діяча з пропекінською позицією, а четвертий канал (Brother Shek Fong Yau) – коментарі колишнього офіцера поліції Гонконгу, противника протестів у Гонконга. Ці Youtube-канали набрали декілька тисяч підписників, а відео мали понад 2000 переглядів.

Ще одна мережа неавтентичних акаунтів, пов'язаних з китайським урядом, була виявлена і заблокована компанією Twitter у 2021 році. Фахівці Стенфордської інтернет-обсерваторії, які отримали доступ до цих даних, з'ясували, що 2016 акаунтів, створених у період з квітня 2019 року по лютий 2021 року, поширили 31 269 твітів. Акаунти здебільшого містили оригінальні твіти англійською мовою. Більше половини акаунтів (1459) не мали жодного підписника. Переважна більшість твітів CNHU (30 414) не отримали жодних лайків чи ретвітів. Лише 26 акаунтів мали описи профілю користувача.

У 2019 і 2020 роках акаунти поширювали неполітичний контент, а у 2021 році твіти сфокусувались на Сіньцзяні, аби представити політику КПК щодо уйгурів у більш сприятливому світлі. Часто твіти містили цитати зі статей китайських державних ЗМІ або скріншоти статей державних медіа без прямого посилання на публікації. До того ж, акаунти використовували англомовні хештеги, такі як #Xinjiang, #XinjiangOnline, #StopXinjiangRumors, #China, ймовірно, намагаючись витіснити негативні повідомлення по цій темі.

Через цю мережу акаунтів просувались такі наративи: уйгури Сіньцзяну живуть мирним і щасливим життям; Сіньцзянські «освітні та професійні центри» необхідні для запобігання тероризму; США навмисно поширюють дезінформацію про порушення прав у Сіньцзяні, переслідуючи політичні цілі [67].

У першій половині 2023 року американська технологічна компанія Meta (материнська компанія для Facebook, Instagram і WhatsApp) опублікувала звіт про ще одну китайську мережу, яка включала 7704 акаунтів, 954 сторінки і 15 груп у Facebook, а також 15 акаунтів в Instagram. Групи акаунтів ділились ідентичним контентом китайською та англійською мовами на понад 50 онлайн-платформах і форумах. Здебільшого це були позитивні коментарі про Китай і провінцію Сіньцзян, критика США, зовнішньої політики Заходу та опонентів китайського уряду. Дописи містили не лише посилання і цитати зі статей, але й короткі «особисті» коментарі, аби створити вигляд поширення оригінального і більш персонального контенту [68].

У звіті компанії Meta за листопад 2023 року йдеться про ще дві виявлені мережі неавтентичних акаунтів, пов'язаних з Китаєм. Одна мережа складалась з близько 4800 акаунтів у Facebook, які видавали себе за американців і писали про політику США та відносини між США і Китаєм. Використовуючи підроблені імена, вкрадені чи стокові світлини у профілях, акаунти репостили у Facebook твіти реальних інтернет-користувачів, а також ділились посиланнями на статті американських ЗМІ.

Інша мережа складалася з 13 акаунтів і 7 груп у Facebook, націлених на Тибет та Індію. Акаунти представлялися журналістами, юристами і правозахисниками. Деякі акаунти використовували однакові імена та фото профілів на Facebook і Twitter, а також публікували однаковий контент англійською мовою на цих платформах. Тематика публікацій була досить широкою: регіональні новини, спорт і культура, критика Далай-лами, звинувачення індійського уряду у корупції тощо. Декілька акаунтів видавали себе за американців і ділилися посиланнями на статті американських медіа, таких як HuffPost, Breitbart, Wall Street Journal і Fox News. Лише одній групі вдалось залучити 1400 фоловерів до її видалення фахівцями Meta [59].

Таким чином, астротурфінг у мережі інтернет є інструментом прихованого впливу на громадську думку. Досвід рф і Китаю показує, що ця технологія використовується з різними цілями, від захисту політики державного керівництва до втручання у політичні процеси в

інших країнах. Цілі можуть бути як короткостроковими, так і довгостроковими. Характерними рисами астротурфінгу є мімікрія під місцевих жителів або громадські організації, гнучкість і варіативність методів впливу на цільові аудиторії, різноплановість, провокативність (поширення повідомлень про актуальні і резонансні суспільні проблеми), багатопрофільність (ініціювання дискусій на різноманітні теми), децентралізоване поширення повідомлень з численних, нібито не пов’язаних між собою джерел тощо.

Питання для самоконтролю:

1. Що таке астротурфінг?
2. Для чого використовується астротурфінг у мережі інтернет?
3. Що таке інтернет-тролінг?
4. За якими ознаками можна розпізнати інтернет-троля?
5. Які тактики використовують інтернет-тролі для маніпулювання громадською думкою?
6. Як організована робота «фабрики тролів»?
7. Як рф використала технологію астротурфінгу під час президентських виборів у США 2016 року?
8. Які особливості використання астротурфінгу характерні для КНР?
9. Чим зумовлена різна ефективність використання астротурфінгу КНР і рф?
10. Які переваги і недоліки, на Вашу думку, має технологія астротурфінгу в контексті інформаційного протиборства?

Список використаних джерел:

1. Запорожець О.Ю. Кібервійна: концептуальний вимір. URL: http://journals.iir.kiev.ua/index.php/apmv/article/download/2378/2111
2. Добринская Д.Е. Киберпространство: территория современной жизни. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-territoriya-sovremennoy-zhizni/viewer
3. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. 328 с.
4. Плинер А.А. Киберпространство: информационный, языковой, технологический аспекты. URL: https://elar.urfu.ru/bitstream/10995/30971/1/episteme_2014_11.pdf
5. Тимошенко С.Г. Кибератака как современная форма совершения акта агрессии. URL: https://cyberleninka.ru/article/n/kiberataka-kak-sovremennaya-forma-soversheniya-akta-agressii/viewer
6. Закон України Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
7. Кандауров Д.Н. Война в киберпространстве: уроки и выводы для России. URL: https://nvo.ng.ru/concepts/2013-12-13/1_war.html
8. Зуйкова А. Десять самых громких кибератак XXI века. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e
9. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення. - https://cert.gov.ua/recommendation/2502
10. WannaCry (вирус-вымогатель). URL: https://www.tadviser.ru/index.php/Статья:WannaCry_(вирус-вымогатель)
11. WannaCry 2.0: наглядное подтверждение того, что вам обязательно нужно правильное решение для надежного бэкапа. URL: https://habr.com/ru/company/acronis/blog/328796/
12. Що таке фішинг і фішингова атака. URL: https://hostiq.ua/blog/ukr/internet-phishing/
13. Самые популярные виды кибератак в 2021. URL: https://10guards.com/ru/articles/the-most-common-types-of-cyber-attacks-in-2021/
14. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]. – К.: ДУТ, 2015. 288 с.
15. Google стала жертвой рекордной DDoS-атаки. 19.10.2020. URL: https://www.securitylab.ru/news/513144.php
16. Что такое DNS-туннелирование? Инструкция по обнаружению. URL: https://habr.com/ru/company/varonis/blog/513160/

17. Антонович П.И. О сущности и содержании кибервойны. URL: http://militaryarticle.ru/voennaya-mysl/2011-vm/10384-o-sushhnosti-i-soderzhanii-kibervojny
18. Baud M. Cyberguerre. En quete d'une strategie. URL: https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/cyberguerre-quete-dune-strategie
19. Грінберг Е. Піщаний хробак, або Sandworm/пер. з англ. В. Махонін. – Харків: Фоліо, 2020. 427 с.
20. Алешкевич Д. Особенности информационной войны против Ирана. URL: http://csef.ru/ru/oborona-i-bezopasnost/265/osobennosti-informaczionnoj-vojny-protiv-irana-2852
21. Кібератаки Російської Федерації. Хронологія. URL: https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html
22. Паганіні П. Крим: російська кіберстратегія війни. 27.03.2014. URL: https://day.kyiv.ua/uk/article/ekonomika/krim-rosiyska-kiberstrategiya-viyni
23. Сапитон М. Нерассказанная история NotPetya – самой разрушительной кибератаки в истории. URL: https://ain.ua/ru/2018/08/24/notpetya-istoriya/
24. Держспецзв'язку: 22 державних органи України постраждали від кібератаки. 25 січня 2022. URL: https://ms.detector.media/kiberbezpeka/post/28862/2022-01-25-derzhspetszvyazku-22-derzhavnykh-organy-ukrainy-postrazhdaly-vid-kiberataky/
25. Олиярнык М. Хакеры напали на ПриватБанк. Украина стала полем для тренировок кибератак на НАТО? URL: https://zaborona.com/ru/hakery-napali-na-privatbank-ukraina-stala-polem-dlya-trenirovok-kiberatak-na-nato/
26. Украинские сайты перестали работать из-за мощной DDoS-атаки, Европа активирует международную киберкоманду. 23.02.2022. URL: https://www.bbc.com/russian/news-60492316
27. Кібервійна: з 15 лютого було понад 3 тисячі DDoS-атак. 19.03.2022. URL: https://www.epravda.com.ua/news/2022/03/19/684330/
28. Дубов Д. Кіберфронт. Як РФ атакує Україну та чи готові ми захищатися. URL: https://biz.nv.ua/ukr/experts/kiberataki-rosiji-na-ukrajinu-yak-prohodyat-ta-chim-zagrozhuyut-ostanni-novini-50236927.html
29. Виловатых А.В. Меметика как инструмент современного информационного противоборства. Проблемы национальной стратегии. 2018. №5(50). С. 141-154.
30. Oxford Learner's Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/definition/english/meme

31. Шомова С.А. «Война мемов»: новые повороты информационного противостояния. URL: https://cyberleninka.ru/article/n/voyna-memov-novye-povoroty-informatsionnogo-protivostoyaniya/viewer
32. Броуди Р. Психические вирусы. Как программируют ваше сознание. URL: https://bookap.info/psywar/broudi_psihicheskie_virusy/#o
33. Катаев С.Л. Мем «бендеровец» как вирус ментальной эпидемии на Донбассе. URL: http://nbuv.gov.ua/UJRN/Mtpsa_2014_20_28
34. Смола Л. Мем як інструмент інформаційної війни // Вісник Київського національного університету імені Тараса Шевченка. Психологія. 2019. Вип. 1. С. 91-95.
35. Почепцов Г.Г. Меметическая война, или в поисках «арифметики» разума. URL: http://osvita.mediasapiens.ua/trends/1411978127/memeticheskaya_voyna_ili_v_poiskakh_arifmetiki_razuma/
36. Heylighen F. What makes a meme successful? Selection criteria for cultural evolution. URL: https://citeseerx.ist.psu.edu/viewdoc/download
37. Шомова С.А. Мемы как они есть. Аспект Пресс, 2018. 136 с.
38. Саидова З. Э. Мем как универсальный феномен интернет-культуры (на материале русского, английского и чеченского языков). URL: https://cyberleninka.ru/article/n/mem-kak-universalnyy-fenomen-internet-kultury-na-materiale-russkogo-angliyskogo-i-chechenskogo-yazykov
39. Giesea J. It's time to embrace memetic warfare. URL: https://stratcomcoe.org/publications/its-time-to-embrace-memetic-warfare/164
40. Zakem V., McBride M.K., Hammerberg K. Exploring the Utility of Memes for U.S. Government Influence Campaigns. URL: https://www.cna.org/cna_files/pdf/DRM-2018-U-017433-Final.pdf
41. Hancock B.J. Memetic Warfare: The Future of War. URL: https://www.academia.edu/43534914/Memetic_Warfare_The_Future_of_War
42. Haikarainen J. E. Astroturfing as a global phenomenon. URL: https://jyx.jyu.fi/bitstream/handle/123456789/44899/URN:NBN:fi:jyu-201412153512.pdf?sequence=1
43. Саморукова О. Деструктивна поведінка в соціальних мережах як інструмент інформаційної війни. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=5272
44. Hardaker C. Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. J. Politeness Res. Lang. Behav. Cult. URL: https://doi.org/10.1515/jplr.2010.011

45. Вовк Н. Явище тролінгу в Інтернеті як загроза інформаційному суспільству. URL: https://ena.lpnu.ua/bitstream/ntb/20753/1/45-104-105.pdf
46. Христенко В.Є. Маніпулювання свідомістю в умовах гібридної війни: психологічний аспект. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/5929/1/Khrystenko_monogr.pdf
47. Островська В.М., Войтович О.П. Тролінг як засіб інформаційної війни. URL:https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/20632/4071.pdf?sequence=3&isAllowed=y
48. Могилко С. Тролінг як спосіб психологічної маніпуляції в Інтернеті. Медіадослідження : збірник наукових праць студентів / наук. ред. Н. І. Зражевська. Черкаси: 2010. Вип.1. URL: http://eprints.cdu.edu.ua/231/1/Медіадослідження_1.pdf
49. Масленченко С.В. Троллинг как социально-политический феномен. URL: https://elib.bsu.by/bitstream/123456789/181902/1/127-132.pdf
50. Yle Kioski Investigated: This is How Pro-Russia Trolls Manipulate Finns Online. URL: https://kioski.yle.fi/omat/troll-piece-2-english
51. Русяева П., Захаров А. Расследование РБК: как «фабрика троллей» поработала на выборах в США. URL: https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1
52. Howard P.N., Ganesh B., Liotsiou D., Kelly J., François C. The IRA, Social Media and Political Polarization in the United States, 2012-2018. URL: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdfR.
53. DiResta R., Shaffer K., Ruppel B., Sullivan D., Matney R., Fox R., Albright J., Johnson B. The Tactics & Tropes of the Internet Research Agency. New Knowledge report. URL: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs
54. Nimmo B., Francois C. #TrollTracker: Glimpse Into a French Operation. Nov 28, 2018. URL: https://medium.com/dfrlab/trolltracker-glimpse-into-a-french-operation-f78dcae78924
55. Han R. Manufacturing Consent in Cyberspace: China's "Fifty-Cent Army". *Journal of Current Chinese Affairs*. 2015. Vol. 44, Issue. 2. P. 105–134. https://doi.org/10.1177/186810261504400205
56. King G., Pan J., Roberts M. E. How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument. *American Political Science Review*, 2017. Vol. 111, Issue. 3. P. 484-501. https://doi.org/10.1017/S0003055417000144

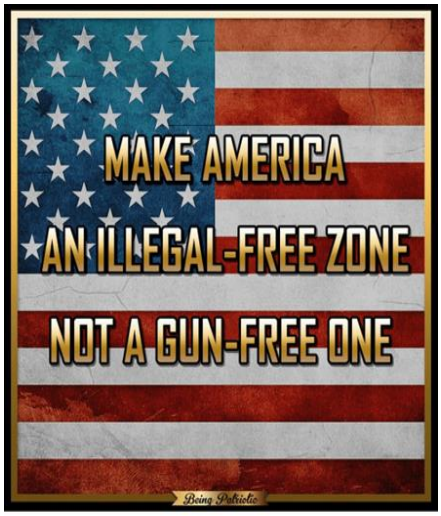
57. Han R. Defending the Authoritarian Regime Online: China's "Voluntary Fifty-Cent Army". *The China Quarterly*, 2015. Issue. 224. P. 1006 – 1025. https://doi.org/10.1017/S0305741015001216
58. Li J. An army of China's internet trolls has a message for Hong Kong protesters. *Quartz*, July 23, 2019. URL: https://qz.com/1672487/chinas-internet-trolls-target-hong-kong-protesters-
59. Запорожець О.Ю. Пропаганда КНР у соціальних медіа: інструменти прихованого впливу. *Міжнародні та політичні дослідження*. 2025. №39. С. 35-47. https://doi.org/10.32782/2707-5206.2025.39.3
60. Chen L. China troll army's battle expeditions leap Great Firewall to target Hong Kong anti-government protests. 7 August 2019. URL: https://www.scmp.com/news/china/society/article/3021798/china-troll-armys-battle-expeditions-leap-great-firewall
61. Fedasiuk R. Buying Silence: The Price of Internet Censorship in China. January 12, 2021. URL: https://cset.georgetown.edu/article/buying-silence-the-price-of-internet-censorship-in-china/
62. Charon P., Vilmer J-B. J. Chinese Influence Operations: A Machiavellian Moment. October 2021. URL: https://www.irsem.fr/report.html
63. Diresta R., Miller C., Molter V., Pomfret J., Tiffert G. Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives. July 20, 2020. URL: https://stacks.stanford.edu/file/druid:pf306sw8941/sio-china_story_white_paper-final.pdf
64. Uren T., Thomas E., Wallis J. Tweeting through the Great Firewall. 03 September 2019. URL: https://www.aspi.org.au/report/tweeting-through-great-firewall
65. Nimmo B., Eib C.S., Tamora L. Cross-Platform Spam Network Targeted Hong Kong Protests. 09.2019. URL: https://graphika.com/reports/spamouflage
66. Nimmo B., Francois C., Eib C. S., Ronzaud L. Return of the (Spamouflage) Dragon. 04.2020. URL: https://public-assets.graphika.com/reports/Graphika_Report_Spamouflage_Returns.pdf
67. DiResta R., Goldstein J.A., Miller C., Wang H. One Topic, Two Networks: Evaluating Two Chinese Influence Operations on Twitter Related to Xinjiang. December 2, 2021. URL: https://stacks.stanford.edu/file/druid:sn407zm8237/20211202-china-twitter-takedown.pdf
68. Nimmo B., Torrey M., Franklin M., Agranovich D., Milam M., Hundley L., Flaim R. Adversarial Threat Report. August 2023. URL: https://transparency.meta.com/uk-ua/metasecurity/threat-reporting/

ДОДАТОК А

Приклади пропагандистських повідомлень російської «фабрики тролів» під час президентських виборів у США 2016 року

Being Patriotic

How can we even speak about helping and even sheltering some foreigners while our own veterans are dying in the streets? That's simply unfair to our veterans, they deserve better lives, and they deserve all the assistance our government can give them!



Our government should end the liberal hysteria and turn all their efforts to another direction. The government's first duty is to protect its citizens. Taking away our guns won't enforce our security. Deporting all criminal illegals will. patriots

Via Being Patriotic~CajunSpice

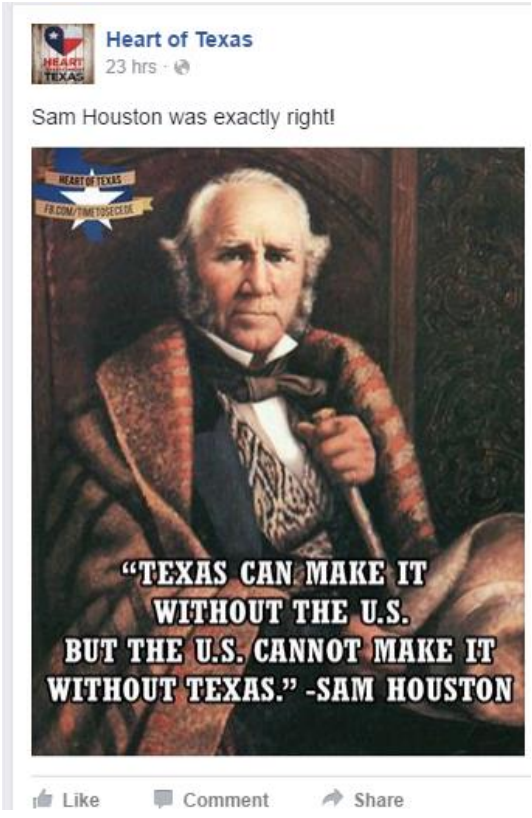
Stop All Invaders

@stop_all_invaders has a point.

Let's help Donald Trump to make our country truly great again! stopallinvaders stopimmigration noillegals stopterrorism nojihad immigrationreform illegalimmigration America USA securetheborder buildthewall Trump Trump2016

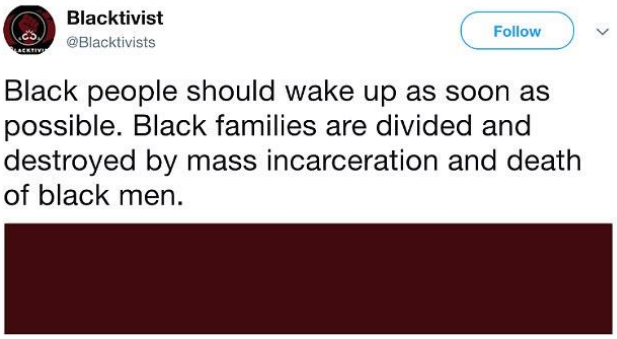
Джерело інформації: https://ushadrons.medium.com/stop-the-invasion-f8c93d774f97

Heart of Texas



Джерело інформації: Casey Michel How Russia Created the Most Popular Texas Secession Page on Facebook. - https://extranewsfeed.com/how-russia-created-the-most-popular-texas-secession-page-on-facebook-fd4dfd05ee5c

Blacktivist



Джерело інформації: Geoff Earle 'Blacktivist' pages on Facebook and Twitter stoked racial tensions during presidential campaign. - https://www.dailymail.co.uk/news/article-4934148/Russia-linked-Blacktivist-pages-stoked-racial-tensions.html

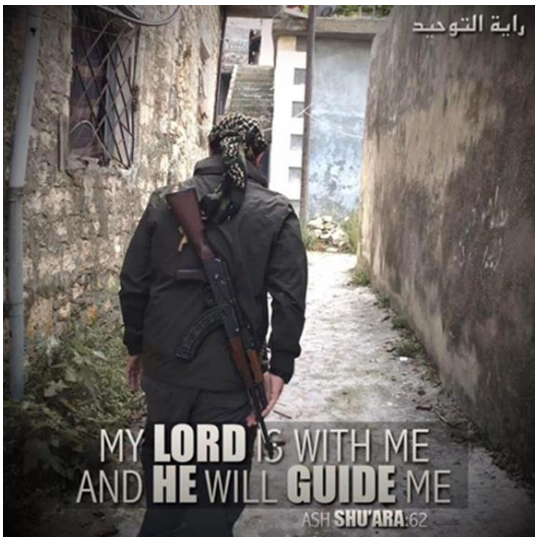
Army of Jesus

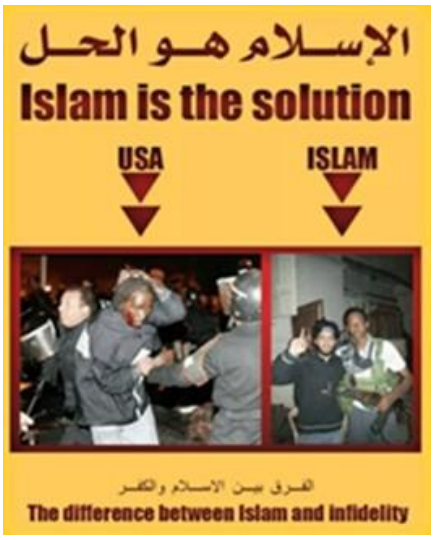
Black matters

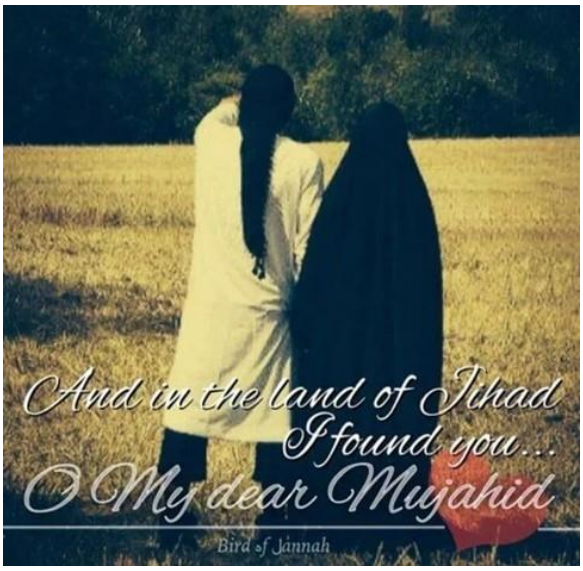
Джерело інформації: https://ushadrons.medium.com/this-space-is-a-repository-for-content-from-the-russian-social-media-group-army-of-jesus-553c6aa74fea; https://ushadrons.medium.com/this-space-is-a-repository-for-ads-from-the-russian-social-media-group-black-matters-us-da81a3d5902

ДОДАТОК Б

Приклади пропагандистської продукції терористичної організації «Ісламська держава»







Джерело інформації:
Speckhard A. The Hypnotic Power of ISIS Imagery in Recruiting Western Youth. https://www.academia.edu/17120997/The_Hypnotic_Power_of_ISIS_Imagery_in_Recruiting_Western_Youth

Навчальне видання

ЗАПОРОЖЕЦЬ Оксана Юріївна

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Навчальний посібник
2-е видання

Друкується за авторською редакцією

ISBN 978-966-972-128-0

Підписано до друку 16.06.2025 р.
Формат 60x84/16. Гарнітура Times New Roman. Папір офсетний.
Ум. друк. арк. 9,72. Тираж 300 пр.
Зам. № 016/25

Видавець ТОВ «ВАДЕКС»
04074, м. Київ, вул. Бережанська 9
тел. 067 502-22-42
сайт: http://vadex.com.ua/
Свідоцтво про внесення до Державного реєстру України
суб'єктів видавничої справи ДК № 4285 від 27.03.2012 р.