КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
Військовий інститут
Військовий гуманітарно-лінгвістичний факультет
Кафедра військової журналістики

Курбан О.В.

СУЧАСНІ ІНФОРМАЦІЙНІ ВІЙНИ У МЕРЕЖЕВОМУ ОН-ЛАЙН ПРОСТОРІ

Навчальний посібник

Київ - 2016

УДК 316.6:659.9]:004.7
ББК 60.56
К 93

Рекомендовано до друку Вченою радою Військового інституту
Київського національного університету імені Тараса Шевченка
(протокол № 8 від 17 грудня 2015 року)

Рецензенти:

СОКОЛОВ КОСТЯНТИН ОЛЕКСАНДРОВИЧ – полковник, начальник Управління інформаційних технологій Міністерства оборони України.

ІВАНОВ ВАЛЕРІЙ ФЕЛІКСОВИЧ – доктор філологічних наук, професор, завідувач кафедри реклами та зв'язків з громадськістю Інституту журналістики Київського Національного університету імені Тараса Шевченка.

Курбан О.В.
Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с.

У посібнику представлено методологічні, методичні та практичні аспекти сучасних інформаційних війн у мережевому он-лайн просторі. Методологічною основою посібника є алгоритмізація управлінських процесів під час планування, реалізації та оцінки результативності здійснених інформаційно-психологічних операцій у соціальних он-лайн мережах.

Навчальний посібник розрахований на курсантів Військового інституту Київського національного університету імені Тараса Шевченка, фахівців з питань інформаційної війни, науковців, викладачів, аспірантів, студентів профільних спеціальностей цивільних ВНЗ та всіх тих, хто цікавиться питаннями розвитку сучасних інформаційно-комунікаційних процесів.

ББК 60.56
УДК 316.6:659.9]:004.7

ЗМІСТ

ВСТУП

Сучасне суспільство формується в контексті трьох технологічних напрямків – хай-х'юм (високі гуманітарні), хай-тек (високі технічні) та хай-сенсоро (високі сенсорно-технологічні). Вони формують характер людської спільноти початку ІІІ-го тисячоліття, що визначається як постіндустріальна, постмодерністська та цифрова.

Цифровий характер сучасних технічних комунікацій формує принципово нову модель взаємовідносин між індивідуумами на персональному, внутрішньогруповому та міжгруповому рівнях. З моменту народження, у середині ХХ ст., цифрові технології пройшли три етапи технологічного оновлення, які визначаються форматами web 1.0, web 2.0, web 3.0. Сьогодні ми знаходимося на етапі коли працюють технології web 2.0 та 3.0 та народжується 4.0. Цей етап розпочався із створення першої соціальної мережі (1995 р.) і визначається як час домінування он-лайн мережевих суспільств, деякі з них, зокрема, мають глобальний планетарний характер. Зсув значної частини життєвих процесів у віртуальний простір призвів до формування нових філософських постулатів, морально-етичних концепцій соціально-економічних та політичних управлінських систем. А також до напрацювання нових підходів та засобів ведення військових дій.

У контексті зазначених вище тенденцій військова справа набуває сьогодні принципово нових рис, порівняно з усією минулою історією локальних та світових війн. Система управління віртуалізується, значна частина функцій людини перекладається на штучний інтелект та машини. Бойові роботи – андроїди, безпілотні літальні апарати, системи наведення та корегування вогню, розвідувальні пристрої поступово переходять зі сторінок фантастичних творів у реальний театр бойових дій. В цих інноваціях особливе значення відіграють інтернет-технології, як засіб передачі даних та технічна підтримка базового інформаційного процесу.

Розвиток он-лайн соціальних мереж і глобалізація світового співтовариства активно використовуються у військовій галузі не тільки з метою здійснення управлінських процесів, але й для ведення віртуальних бойових дій, які забезпечують реальні військові протистояння.

Технології 2.0 органічно вписалися в інформаційно-психологічний формат ведення так званої гібридної війни, а їх значення зростає з кожним наступним міжнародним військовим конфліктом в арифметичній прогресії.

Актуальність процесів формування системної практики ведення віртуальних інформаційних війн викликала необхідність комплексної підготовки профільних фахівців як важливої стратегічної ***мети*** для вітчизняних закладів освіти та центрів перепідготовки військових кадрів. Особливо гостро це питання постало в контексті останніх подій на Півдні та Сході України. Саме на досягнення зазначеної мети орієнтований даний навчальний посібник. Основні ***завдання***, які вирішує видання, – це надання системного розуміння теорії, методології та методики ведення сучасних мережевих інформаційно-комунікаційних протистоянь у соціальних он-лайн мережах, а також практична підготовка майбутніх фахівців із питань інформаційної безпеки.

В основі навчання та прикладних тренувань закладено принцип алгоритмічності інформаційних процесів, що складаються з окремих інструментів, які компонуються відповідно до комунікаційної ситуації, специфіки цільових груп та характеристик інформаційного поля.

Структурно навчальний посібник складається з трьох розділів. У першому розглядається історія розвитку та становлення практики ведення інформаційних війн від давніх часів до сьогодення. Другий розділ присвячений засвоєнню принципів та правил розробки стратегії, тактики та ситуативного планування інформаційно-психологічних операцій в он-лайн соціальних мережах. У третьому представлені методи та засоби моніторингу, пошуку інформації та

оцінюванню ефективності інформаційних процесів у рамках мережевих протистоянь.

Усі запозичені матеріали текстового, графічного або іншого ілюстративного характеру використовуються виключно в навчальних (некомерційних) цілях, автор не має на меті одержати з них будь-яку фінансову винагороду чи прибуток під час або після видання, тиражування, розповсюдження цього видання.

Навчальний посібник підготовлений для курсантів спеціальності «журналістика» і «реклама та зв'язки з громадськістю» Військового інституту Київського національного університету імені Тараса Шевченка та для забезпечення навчальних курсів: «ЗМІ в сучасних інформаційних війнах» і «Мас-медіа в сучасних мережевих війнах».

РОЗДІЛ 1. Історія, методологія та методика дослідження та розвитку інформаційних конфліктів

1.1. Розвиток інформаційно-комунікаційних технологій у форматі історії інформаційних конфліктів

1.1.1. Інформаційно-комунікаційні технології в первісному суспільстві (3,5 млн – IV тис. рр. до н.е.)

Перші люди - Homo erectus з'явилися близько 3,5 млн років до н.е., і вже на той момент мали певні інформаційно-комунікаційні технології, які допомагали первісному стаду організовувати полювання, займатися збиральництвом та захищати свої групи. Це були переважно жести, міміка, тактильна комунікація та вигуки. Саме на основі вигуків відбулася подальша трансформація первісних комунікаційних технологій людства, перетворивши їх з часом на **мову** (у форматі мовлення) [366, с. 14].

За своїм визначенням **мовлення** – це система звукових знаків, що має соціальне призначення [366, с. 14].

Мовлення стало першою універсальною інформаційно-комунікаційною технологією, винайденою людством, яка докорінно змінила та прискорила подальшу еволюцію людства. Ця технологія із відповідними змінами та вдосконаленнями проіснувала до теперішнього часу і має подальші перспективи.

Визначається кілька базових функцій мови [366, с.15]:

1. **Інформаційна функція** полягає в тому, що мова є засобом пізнання, збирання й оформлення всіх тих знань, які накопичені людьми в процесі їх свідомої діяльності. Різновидами цієї функції є функція збереження інформації, контактна функція, функція оформлення культурних цінностей.

2. **Комунікативна функція** реалізується у спілкуванні, розмовах, діалогах, полеміці. Вона створює суспільство як соціум. Комунікативна функція може виступати як самовираження особистості.

1. **Виражальна (експресивна, емотивна, модальна) функція** охоплює величезний діапазон у мовленнєвій поведінці людини. Ця функція мови реалізується в художній літературі, ораторському мистецтві, у дискусійному мовленні — суперечці, полеміці, пісні, опері тощо.
2. **Когнітивна функція**. Це спогади, роздуми у хвилини відпочинку, підготовка до усних висловлювань і формування письмового тексту, творча діяльність та ін.

Для первісної людини мовлення було важливим інструментом, за допомогою якого здійснювалося:

1. Передання досвіду та навчання.

2. Координація спільних дій під час полювання, війни, господарчої діяльності.

3. Пізнання навколишнього середовища та міжособистісні контакти.

Протягом X-V тис. до н.е. первісні мови почали формувати мовні родини, яких зараз налічується по світу 25 [366, с.12].

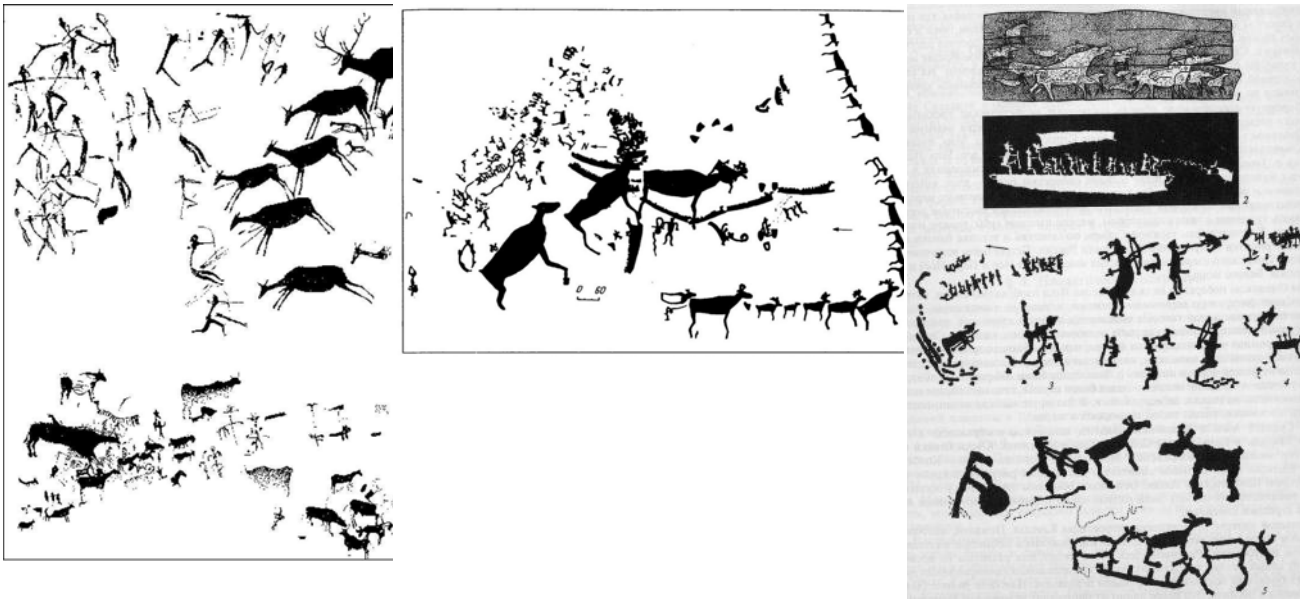
Другим за значенням винаходом щодо розвитку інформаційно-комунікаційних технологій у первісному суспільстві стало народження **мистецтва**, яке стало графічним образно-символьним засобом передання інформації та здійснення комунікацій.

Доісторичне мистецтво можна простежити тільки за збереженими знахідкам кам'яної доби. Відомості про музичну культуру первісних людей можна отримати на основі збережених первісних музичних інструментів, а дані про образотворче мистецтво — на основі наскельного живопису, до якого належать петрогліфи і наскельні розписи (мал. 1.1) [366, с. 115].

Табл. 1.1. Мовні родини сучасного світу

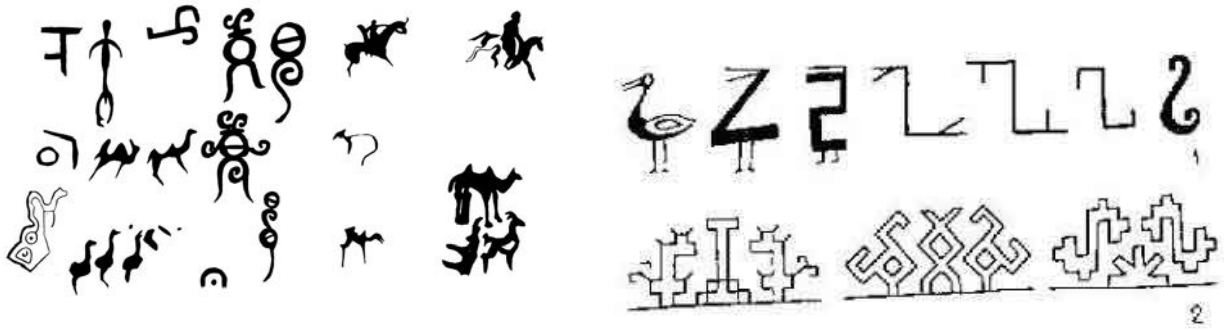
Ранг	Мовна сім'я	Всього мов	Живих мов	Мільйонів мовців	Регіон поширення
1	**Індоєвропейська**	280	220	2675	Європа, Південно-західна та Південна Азія; нині по всьому світу
2	**Сино-тибетська**	343	335	1288	Китай, Гімалаї, Південно-східна Азія
3	**Нігеро-кордофанська**	1386	1364	354	Західна, Центральна та Південна Африка
4	**Афразійська**	354	311	347	Північна Африка, Близький Схід
5	**Австронезійська**	1144	1119	296	Філіппіни, Індонезія, Мадагаскар
6	**Дравідійська**	27	27	220	Південна, Центральна та Північна Індія; Пакистан
7	**Тюркська**	41	37	160	Західна та Центральна Азія, Східна Європа, Північно-східний Сибір
8	**Японсько-рюкюська**	4	4	126	Японія, Окінава
9	**Австроазійська**	157	156	95	Північно-східна Індія, Південно-східна Азія
10	**Тай-кадайська**	69	68	83	Південний Китай, Південно-східна Азія
11	**Корейська**	1	1	78	Корея
12	**Ніло-сахарська**	196	188	34	Південна Сахара, Судан
13	**Уральська**	31	28	24	Південно-східна Європа, Угорщина, Урал, Західний Сибір
14	**Кечуа**	39	38	10	Перу, Еквадор, Колумбія, Болівія, Аргентина
15	**Монгольська**	14	14	7,5	Монголія, Північний Китай; Бурятія, Калмикія
16	**Мяо-яо** (Miao-Yao)	21	21	6,3	Південний Китай, Південно-східна Азія
17	**Тупійська**	74	60	5,3	Парагвай, Болівія, Бразилія
18	**Картвельська**	4	4	8	Грузія; Туреччина
19	**Майя**	33	31	4,2	Мексика, Гватемала, Беліз
20	**Трансновогвінейська**	533	530	3,2	Нова Гвінея; Тимор, Алор, Пантар
21	**Нахсько-дагестанська**	29	29	3,0	Росія: Чечня, Інгушетія, Дагестан
22	**Аймара**	3	3	2,2	Болівія, Перу, Чилі, Аргентина
23	**Ото-мангська**	21	19	2,0	Мексика, Нікарагуа, Коста-Ріка
24	**Юто-ацтекська**	32	22	1,6	Захід США, Південно-східна та Центральна Мексика
25	**Абхазо-адигська**	5	4	1,1	Грузія, Абхазія, Росія: Адигея, Кабардино-Балкарія

Мал.1.1. Перші графічні зображення



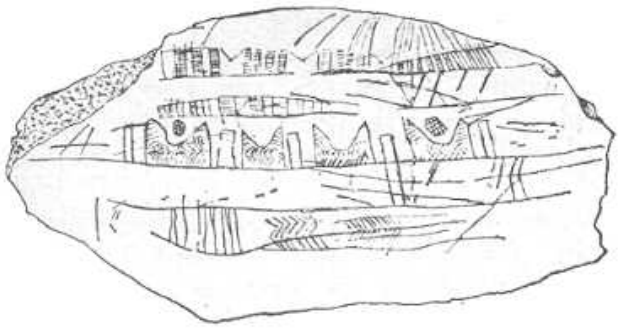
Поступовий розвиток образотворчого мистецтва – від перших печерних розписів та первісної пластики призвів до трансформації певних образів у символи, які несли в собі певні обсяги інформації і передавалися як у просторовому, так і в часовому вимірі (див. мал. 1.2) [366, с. 100].

Мал.1.2. Образи та знаки первісності



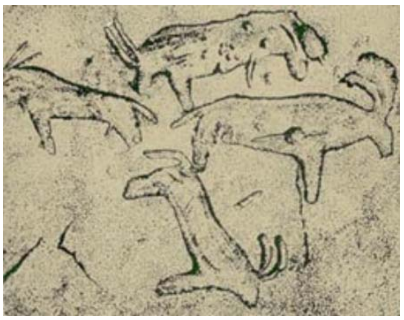
З часом образні малюнки перетворювалися на певні символи (мал. 1.3). При цьому один символ міг нести інформацію як про окремий об’єкт (тварина, людина, камінь, зброя та ін.), так і про певне явище (смерть, народження, життя) або подію (полювання, свято, обряд та ін.).

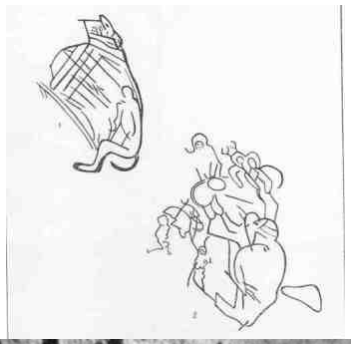
Мал. 1.3. Малюнок на кістках мамонта з Межиріччя

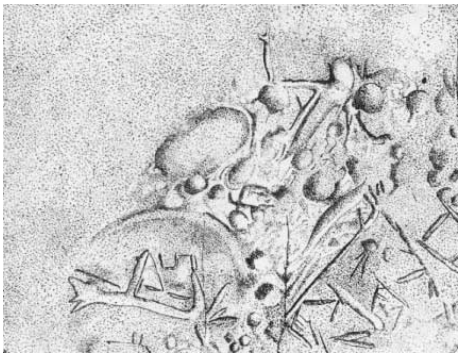


На теренах сучасної України прикладами народження та розвитку первісних інформаційно-комунікаційних технологій слід вважати знахідки зразків образотворчого мистецтва на стоянці Межиріччі (мал. 1.3.), наскельних малюнків та графіті Кам'яної Могили (мал. 1.4.), а також система знаків та символів на кераміці трипільської культури (мал. 1.5.) [366, с. 123].

Мал. 1.4.Зображення Кам'яної Могили

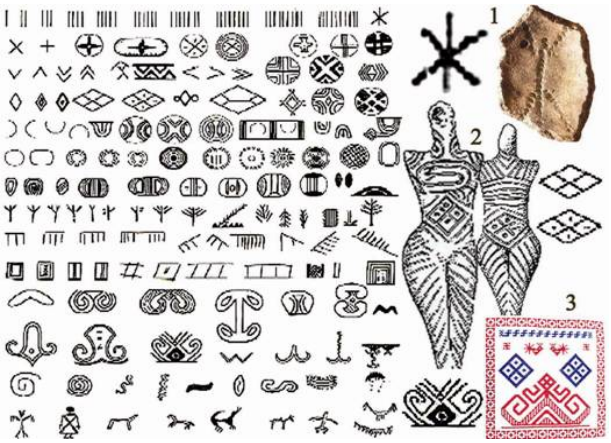


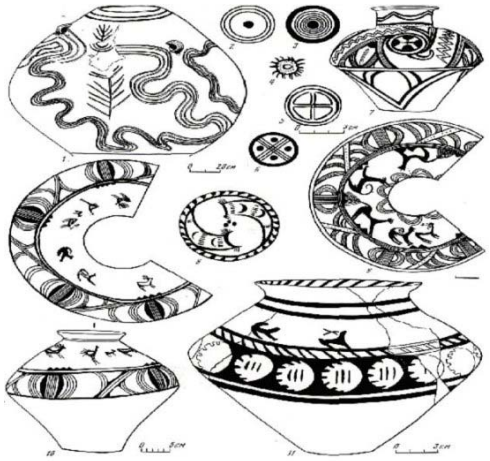




Особливо важливою та показовою, в контексті порушеної проблематики, стала система протописемності, яку дослідники зафіксували у представників Трипільської спільноти. Фактично це можна вважати писемністю, яка поки що не розшифрована. Втім певні смислові образи та символи трипільців все ж таки були розкриті радянським археологом Б.А.Рибаковим (мал. 1.5.) [366, с.154-155].

Мал.1.5. Символи на трипільській кераміці





Наприкінці кам’яної доби, у так звану епоху неоліту, з’являються перші протоміста, основи виробничої економіки (землеробство та тваринництво) а також певні потужні соціальні об’єднання, які потребували певних символьно-образних систем для здійснення класичного інформаційного процесу – створення, накопичення, збереження та поширення інформації. Остаточно зазначені системи сформувалися вже на наступному етапі.

Підсумовуючи інформаційно-комунікаційні здобутки первісної епохи, слід окреслити її найбільш характерні ознаки.

Основними типовими прикладами первісних *інформаційних війн* можна вважати сакральну боротьбу (первісна магія) із силами природи та тваринами, а також на рівні внутрішньоплеменних та міжплеменних конфліктів. Останні супроводжувалися не тільки магічними обрядами, але й першими

інформаційними атаками у вигляді залякування, дезінформації, приховування та інших типових для базового рівня інструментів.

Базовий *інформаційний процес* у первісному суспільстві відбувався шляхом створення (дослідження навколишнього світу), фіксації (мистецтво, образно-символьна система) та передання (мовлення, мистецтво, образно-символьна система) інформації.

Головними *інформаційними носіями* для первісної людини слугували побутові речі, твори мистецтва, зброя та прикраси з кістки та шкіри тварин, дерев'яні речі, посуд (глина та дерево), каміння (окремі вироби, валуни, стіни печер).

Як таких центрів або чітко визначених виробників інформації виокремити важко. Знання та досвід, що передавалися з покоління в покоління, накопичувалися колективно. Можливо твори первісного мистецтва були прерогативою шаманів, утім чітких підтверджень цьому немає.

1.1.2. Інформаційно-комунікаційні технології в ранніх державах Сходу та Європи епохи Античності (III тис. рр. до н.е. – III ст. н.е.)

Поява великих соціальних об'єднань (протоміста та ранні міста, іноді налічували 10-15 тис. мешканців) призвела до необхідності формування певних регламентуючих систем, згідно з якими відбувався чіткий розподіл праці, повноважень, прав та обов'язків. Так сформувалися перші міста держави у долинах річок Інд (Мохенджодаро), міжріччі Тигру і Єфрату (Месопотамія) та Нілу (Давньоєгипетська держава).

Важливою складовою частиною державного устрою зазначених утворень є певні універсальні управлінські системи, що базувалися на конкретних інформаційно-комунікаційних технологіях. Це призвело до остаточної трансформації малюнкової образно-знакової системи передання відомостей та даних на перші, **ієрогліфічні писемні системи.** Цю подію можна

ідентифікувати як типову інформаційну революцію з усіма її відповідними ознаками.

У різних місцях зазначеного ареалу сформувалися власні системи писемності, втім базовий принцип був однаковий для усіх. Малюнок трансформувався у абстрактній образний символ, а потім набував ознак чіткого символу з чітким змістом (мал.1.6) [160].

Мал.1.6. Трансформація малюнка в писемність

IV тысяче-летие до н.э.	III тысяче-летие до н.э.	II-I тысячелет. до н.э. Скоропись Вавилон-ская	Ассирий-ская	Что изобра-жено	Словесное значение: что означает	по-шумерски	по-аккадски	Слоговое значение
				Нога	„Ходить" „Стоять" „Приносить"	Ду, Гин, Ара Губ Тум	Алáку Узýззу Вабáлу	Ду, Гин Губ, Гуп Ра, Тум
				Левая рука	„Левый"	Каб, Куб, Губ	Шумéлу	Каб, Кап Губ, Гуп Хуб, Хуп
				Колышек для крепления цыновки	Колышек" „Строить"	Гаг Ду	Сúккату Бану́	Гаг, Кан Ду
				Пучок лука	„Дуку́чеснок" „Отдавать"	Сум Сум, Си(м)	Карáшу Надану	Сум, Шум Се
				Звезда	„Небо" „Бог"	Ан Дингир	Шамý И́лу	Ан
						Значок перед именами богов		
				Рыба	„Рыба"	Куа, Ха	Нýну	Ха
						Значок после названий рыб		
				Горы	„Гора" „Страна"	Кур, Гин Кур	Шадý Мáту	Кур, Гин Шад, Шат Мад, Мат Над, Нат Лад, Лат
1	2			1 Дикий бык 2 Домашний бык + знак „Горы"	„Дикий бык"	Ам	Рéму	Ам
				Оросительный канал	„Канал"	Э	Йку	Э
				Колос	„Ячмень"	Ше	Шéу	Ше
				Плуг	„Плуг" „Земледе-лец" „Пахать"	Апин Энгар Уру	Эпи́нну Йккару Эрéшу	Пин

Начальное рисуночное письмо из Ура	Рисуночное письмо, приближающееся к поздней-шей клинописи	Ранневави-лонское	Ассирийское	Начальное или производное значение
				Птица
				Рыба
				Осел
				Вол (Бык)
				Солнце, День
				Хлеб; Зерно
				Сад
				Пахать, Возделывать
				Бумеранг, бросать, сбрасывать
				Стоять, итти

Подальша трансформація первинних письмових систем призвела до виникнення його еволюційного продовження – **абеткової писемності**. Останню винайшли фінікійці, як більш надійний та ефективний засіб обрахунку та фіксації інформації, пов'язаної з торгівлею та мореплавством. На відміну від ієрогліфічної писемності, яку складало іноді до кількох тисяч знаків, у першій абетці було 22 (мал. 1.8.) [160]. Ця система була більш гнучкою та універсальною і вже від неї походять всі письмові системи епохи Античності.

Писемність надала інформаційному процесу конкретність, чіткість та змістовність. З'явилась можливість для надійного збереження та ефективного поширення інформації.

На цьому етапі в Давньому Єгипті було винайдено більш універсальний, порівняно з традиційними, інформаційний носій – папірус з чорнилами (мал. 1.7) [160]. Така форма фіксації інформації не вимагала значних зусиль, її було простіше зберігати, вона була більш мобільною.

Мал.1.7. Давньоєгипетська писемність

Найбільш поширеним інформаційним носієм для міст-держав Месопотамії були глиняні таблички - на сиру поверхню наносили записи, потім їх фіксували і зберігали у відповідних архівах (мал. 1.8) [160]. Зазначена форма фіксації

зберігалася краще ніж папірус чи пергамент (шкіра тварин), утім її суттєвим недоліком була незручність при транспортуванні та крихкість застиглої глини.

Мал.1.8. Писемність ранніх держав Месопотамії

Також залишається практика різьблення написів на камені. Останні набувають ознак сакральності та офіційності. Офіційні повідомлення про перемоги царів, природні явища та історичні події фіксувалися на скелях (храми, культові місця) та окремих каменях, наприклад, стела законів царя Хамурапі, Розетський камінь та ін. (мал.1.9) [160].

Мал.1.9. Ієрогліфічні тексти на камені (стела Хамурапі та Розетський камінь)

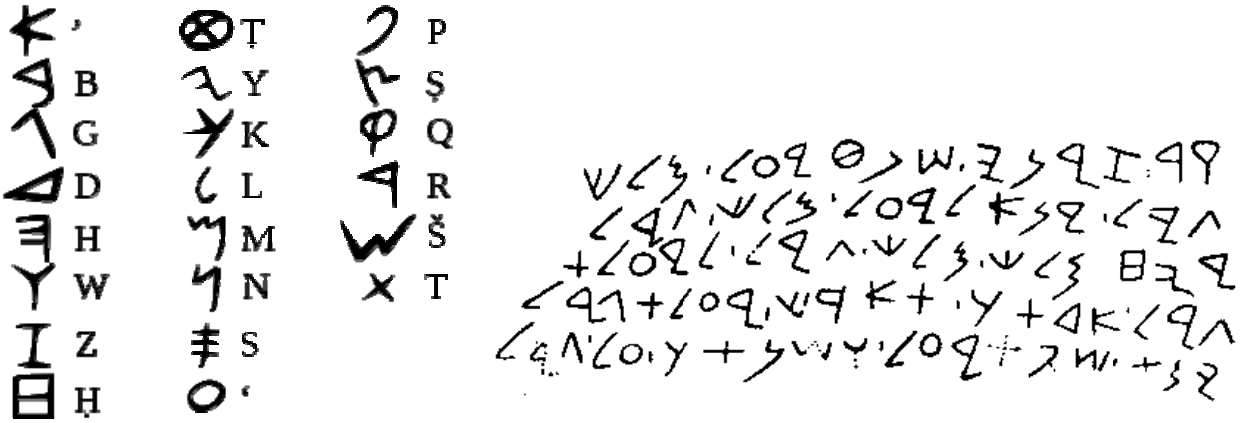
Інформаційні протистояння ранніх держав Сходу носили різноманітний характер. Вони супроводжували військові дії, політичні, економічні та релігійні процеси. Саме в цей час людина здійснює перші спроби системного застосування інформаційно-комунікаційних технологій. Цього потребувала державна політика, економіка, військова справа та торгівля.

Під час військових дій вожді та полководці застосовували практику залякування, психологічного тиску, дезінформації, спрямовані проти ворогів, а також методи стимулювання, підбадьорювання власних воїнів.

У політичному житті владна верхівка активно використовувала методи маніпулювання свідомістю мас населення з метою підтримання ідеї божественного походження влади царя, жерців та знаті.

У сфері економіки особливої потреби в застосуванні таких технологій не помітно. Втім історія знає певні факти використання конкретних інформаційно-комунікаційних методів у боротьбі за джерела сировини, ринки збуту та торгівельні шляхи.

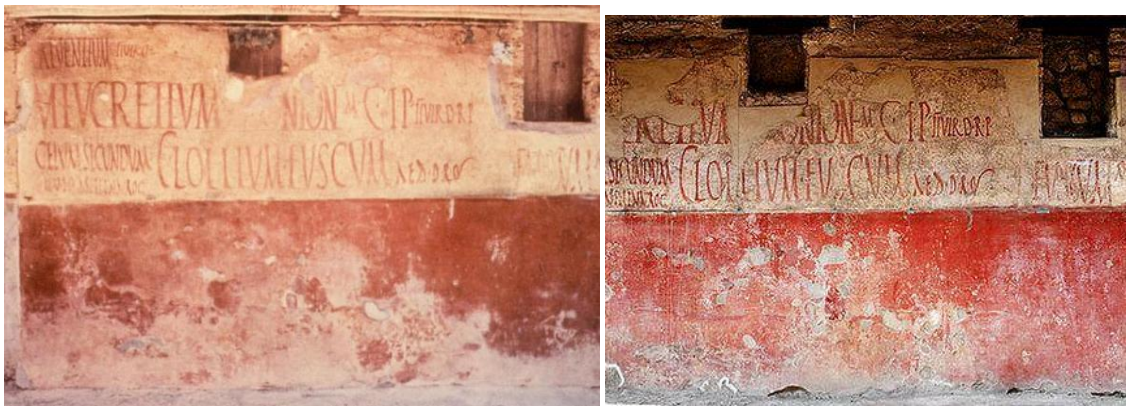
Мал. 1.10. Фінікійська абетка та текст



Суспільно-політичне та економічне життя античних держав Греції та Риму викликало потребу винайдення поліпшених варіацій наявних інформаційно-комунікаційних технологій, які в цілому не мали революційного характеру, втім деякі з них несуть в собі риси інформаційних вибухів.

Одним із нових інструментів, що з’явився саме за часів античності, є **реклама**. Первинна реклама функціонувала у вигляді системи аудіо та текстових оголошень – перші здійснювалися за допомогою глашатаїв, іноді у вигляді тематичних пісень та віршів, другі наносилися на стіни будинків (на спеціально побілених для цього стінах «амбусах»). У цілому така комунікація носила достатньо мирний характер – у вигляді оголошень про продажі, збори, гладіаторські бої, повідомлення особистого характеру (мал.1.11) [160].

Мал.1.11. Рекламні написи у Помпеях



Втім іноді такі повідомлення виконували функцію інформаційної зброї. Зокрема в місті Помпеї були зафіксовані написи, котрі можна трактувати як дискредитацію, компромати або позитивні відгуки на певних персон, які обиралися на посади в міські магістрати. Також глашатаї могли вигукувати заклики до певних дій або звинувачення проти певних осіб.

Інформаційне супроводження міжнародних подій – військових конфліктів, дипломатичних стосунків, міжнародної торгівлі здійснювалося за допомогою певних демаршів, надання дезінформації шляхом шантажування ворожих лідерів.

На жаль, серйозних напрацювань, які б систематизували мистецтво ведення інформаційної війни в цю епоху, немає. Частково цю проблематику в своїх роботах згадував давньогрецький філософ Аристотель (мал. 1.12) [197, с. 47].

Мал.1.12. Аристотель та його твори

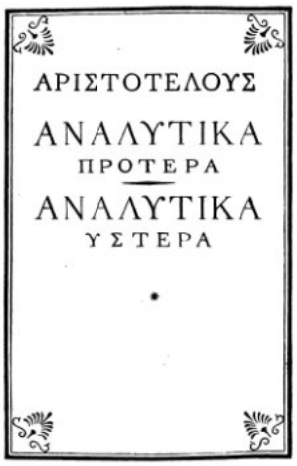

ΑΡΙΣΤΟΤΕΛΟΥΣ ΚΑΤΗΓΟΡΙΑΙ.

ΠΕΡΙ ΟΜΩΝΥΜΩΝ.

ΠΕΡΙ ΣΥΝΩΝΥΜΩΝ.

ΠΕΡΙ ΠΑΡΩΝΥΜΩΝ.

ΠΕΡΙ ΤΩΝ ΛΕΓΟΜΕΝΩΝ.



Приблизно в цей час (500 рр. до н.е.) в Китаї, військовий стратег Сунь Цзи написав книгу «Мистецтво війни», в який згадував необхідність застосування певних елементів інформаційної війни для забезпечення переваг у реальних військових та міжнародних протистояннях (мал. 1.13). Певні його рекомендації взагалі можна віднести до прийомів гібридної війни. Зокрема він радив [152, с.37]:

1. Висміювати та дискредитувати все цінне і добре, що є в країні ворога.
2. Втягувати видатних представників противника у злочини.
3. Підривати імідж національних лідерів та виставляти їх на загальний осуд.
4. Залучати до співпраці підлих та мерзотних людей.
5. Розпалювати сварки та провокувати конфлікти у населення ворожої країни.
6. Підбурювати молодь проти старих.
7. Заважати діяльності влади.
8. Підривати міць війська.
9. Знецінювати традиції та національні цінності.
10. Розбещувати населення.
11. Застосовувати підкуп, стимулювати корупцію.

Мал.1.13. Сунь Цзи та його «Мистецтво війни» (на бамбукових дощечках)

У плані супроводження військових дій Сунь Цзи радив активно застосовувати дезінформацію, залякування, психологічний тиск та інші традиційні методи.

Тогочасні інформаційно-комунікаційні технології активно застосовували античні політики. Зокрема в Давній Греції їх активно практикував оратор Демосфен у процесі боротьби з македонським царем Філіпом, який завоював грецькі міста-держави. За допомогою публічних виступів, дискусій, діалогів досягали своїх цілей афінські політики Солон, Фемістокл, Перикл.

Саме в Давній Греції виникла нова професія - софістика, представники якої спеціалізувалися у публічних виступах та вмінні переконувати. Це можна вважати еволюцією традиційних глашатаїв [197, с.47].

У Давньому Римі політики та полководці Юлій Цезар, Марк Цицерон, Марк Аврелій успішно застосовували інформаційні технології проти своїх політичних противників та зовнішніх ворогів. Наприклад, Сципіон Африканський, активний прибічник війни з Карфагенською державою, кожний свій виступ в Сенаті закінчував фразою: «Втім, Карфаген має бути знищений». Цей прийом – багатократне повторення певної тези й сьогодні активно використовується [197, с.48].

Література, зокрема сатиричні твори, також використовувалися в якості інформаційної зброї, спрямованої проти конкретних персон або для впливу на колективну свідомість.

У Давньому Римі з'явився прообраз першої газети. Це були свитки новин «*Acta diurna populi romani*» («Актуальні справи населення Риму») - записи подій, що вивішувалися у людних місцях та доставлялися відомим громадянам (мал. 1.14) [197, с.48].

Мал.1.14. Давньоримський часопис «Acta diurna populi romani»

Підсумовуючи інформаційно-комунікаційні здобутки епохи ранніх держав та Античності, слід окреслити її найбільш характерні ознаки.

Базовий *інформаційний процес* у первісному суспільстві відбувався шляхом створення (дослідження навколишнього світу, наукового пізнання та перетворення умов зовнішнього середовища), фіксації (мистецтво, архітектура, реклама, писемність) та передання (мовлення, мистецтво, реклама, писемність) інформації.

Головними *інформаційними носіями* для первісної людини слугували кістки та шкіра тварин, дерев'яні речі, посуд (глина, дерево, метал, скло),

каміння (окремі вироби, статуї, скелі), з'являється і набуває значного поширення папірус. Основними типовими прикладами *інформаційних війн* епохи ранніх держав Сходу та Античності можна вважати класичні, в сучасному розумінні, інформаційно-психологічні операції. Останні супроводжували військові конфлікти, політичні та економічні, а також релігійні процеси.

В епоху ранніх держав та античності виробництво контенту поступово виокремлюється в окремий напрям діяльності, який охоплює мистецтво, релігію, військову справу, державне управління, а також науку, яка народжується в ці часи. Тепер створенням, накопиченням та поширенням інформації займаються чітко визначені соціальні групи. Саме жерці та вчені були в переважній більшості виробниками інформації.

Храми та світські школи стають своєрідними *фабриками контенту*, який продукується відповідно до специфіки та тематики діяльності її виробників. Значні обсяги інформації накопичуються у перших бібліотеках (Шумер, Вавилон, Олександрійська в Єгипті та ін.). Також в якості центрів створення інформації були адміністративні структури – царські канцелярії, муніципальні управління, військові структури, торгові об'єднання.

1.1.3. Розвиток інформаційно-комунікаційних технології в часи Середньовіччя та епоху Відродження (IV - XVI ст.)

У часи Середньовіччя та Відродження розвиток усіх аспектів суспільства відбувається під безпосереднім контролем та за участі церкви. Саме цей соціальний інститут, більш ніж на тисячоліття стає провідним споживачем та розробником інформаційно-комунікаційних технологій, а також активним учасником тогочасних інформаційних війн.

Медіа технології цього часу базуються на таких традиційних інструментах, як: мова, мистецтво, писемність, реклама, література. Разом з тим з'являються нові, як то: **пропаганда** та **психологічна війна**.

Зазначені інструменти активно використовували очільники Ватикану. Зокрема папа Урбан II (1095 р.) задля підготовки до Хрестових походів, спрямованих на звільнення Ієрусалиму, застосовував мережеве (через єпископів, кардиналів, священиків) поширення закликів до священної війни (мал. 1.15) [197, с.49].

У часи боротьби католицької церкви з Реформацією при Ватикані було створено «Конгрегацію пропаганди віри» (1622 р.), яка була фактично першим історично зафіксованим центром підготовки та проведення інформаційно-психологічних спецоперацій [197, с.49].

Мал.1.15. Папа Римський Урбан II та його «Конгрегація пропаганди віри»

Боротьба Ватикану із Реформацією стала також одним з ключових моментів в історії інформаційних війн Середньовіччя (мал. 1.16). Цей конфлікт мав дуже важливу інформаційну складову, бо боротьба велася саме за свідомість, духовні цінності та соціально-політичні настрої населення.

Мал.1.16. Документи та акції часів Реформації.

Провідні діячі реформаторського руху – Мартін Лютер, Томас Мюнстер, Жан Кальвін головною своєю зброєю в боротьбі із засиллям католицької церкви вважали слово і тексти. Їх інформаційні атаки базувалися на публічних звинувачувальних промовах, друкованих памфлетах, теологічних диспутах з опонентами. Базові меседжі спиралися на факти корупції та розкошів у церковному середовищі, а також на пропозиціях оптимізації витрат на потреби церкви та зміни системи служіння. В якості системних каналів комунікації формувалися контактні соціальні мережі – таємні та відкриті товариства.

Церква воювала з Реформацією традиційними та відпрацьованими століттями інструментами – використовували мережу храмів, монастирів та церковних орденів, непорушний авторитет «Біблії», папського престолу, авторитет єпископів, архієпископів, кардиналів, настоятелів монастирів. Активно залучалися всілякі божественні дива, маніпуляція історичними та науковими фактами. В цій боротьбі дуже активно себе проявила «Конгрегація пропаганди віри».

Доволі значний внесок у практику ведення інформаційних війн внесла Візантійська імперія. Зокрема ми знаємо багато історичних фактів, коли візантійські імператори перемагали свої ворогів не силою зброї, а шляхом дезінформації, психологічного тиску, підкупу. Особливо активно велися такі

війни у протистояннях із князями Київської Русі, ісламськими державами, кочовими племенами давніх тюрків та ін.

Серед визначних теоретиків та практиків інформаційних війн можна виділити Маврикія та його твір «Стратегікон», Костянтина Багрянородного, а також окремий анонімний документ «Риторика мелітаріс» (збірка військових промов та настанов) [197, с.50].

Мал.1.17. Костянтин Багрянородний та його «Стратегікон».

Певні прийоми та засоби ведення інформаційної війни від візантійців запозичили керманичі Київської Русі, додав до цього аналогічний досвід варягів, створивши таким чином свою систему. Зокрема інформаційно-комунікаційні технології в Давньоруській державі застосовувалися як у внутрішньополітичних процесах, так і під час збройних конфліктів. Звичайно активну участь у цьому брала православна церква.

Серед відомих київських князів практикували такі технології під час військових походів та при вирішенні внутрішньополітичних проблем - Святослав, Ольга, Володимир Великий, Ярослав Мудрий та Володимир Мономах.

В епоху Середньовіччя головними центрами із виробництва контенту стали монастирі та релігійні організації – духовні ордени.

Зокрема значний внесок у створення інформаційного продукту, його зберігання, популяризацію та поширення – тобто підтримку інформаційного процесу, вносили монастирі. Протягом тривалого часу вони виконували функції видавництва книжок, розробку ідеологічних постулатів, напрацювання методології та методик інформаційно-комунікаційних процесів. Також вони відігравали роль певних центрів науки та мистецтва. З часом їх естафету перехопили міста із цивільними школами, університетами, адміністративними центрами та королівські адміністрації.

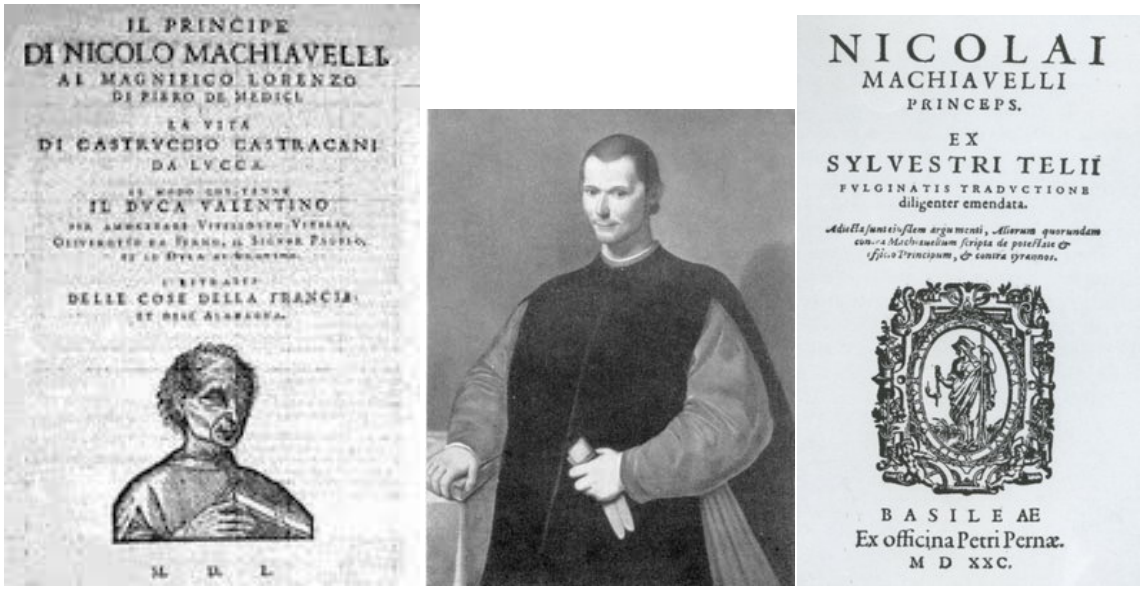
Наприкінці Середньовіччя в епоху Відродження в Європі з'являється новий спосіб поширення інформації – **друкарство**, яке з часом стало **першою глобальною мас-медіа технологією**. Перша книга була надрукована Іоганом Гутенбергом у 1452 році, це була «Біблія» [160]. Слід зазначити, що Гутенберг був не першим, хто почав застосовувати друкарську технологію (мал. 1.18). Перед ним у VI ст. цю технологію застосовували у Китаї [160]. Втім там вона не набула значного поширення і тому європейський винахідник вважається першим, хто почав системну роботу в цьому напрямку.

Мал.1.18. І.Гутенберг та його друкарський верстат

Значний внесок у розвиток інформаційно-комунікаційних технологій зробили вчені епохи Відродження, зокрема так звані гуманісти. Центром інтересів гуманістів була «словесність» - філологія та риторика. Наприклад, Лоренцо Валла акцентував увагу на необхідності активізації комунікації між лідерами громадської думки та широкими колами публіки. П'єтро Паоло Верджеріо, Гуаріно Веронезе, Вітторіно да Фельтре та багато інших гуманістів наполягали на необхідності розвитку соціальних комунікацій з метою поширення знань, передання досвіду.

Ближче всіх до проблематики проведення інформаційних війн були роботи Ніколо Макіавеллі (мал. 1.19). В своєму творі «Государ» (1532 р.) він сформулював поради для політичних та військових лідерів, як необхідно здійснювати ефективну інформаційну політику для здійснення успішних війн та управління державою [197, с.50]. Розглядаючи специфіку розвитку монархічної та республіканської форми правління, автор надає поради, як потрібно вибудовувати комунікацію між народом та правлячою елітою, а також як вибудовувати міждержавні стосунки.

Мал.1.19. Ніколо Макіавеллі та його твори



Підсумовуючи інформаційно-комунікаційні здобутки епохи Середньовіччя та Відродження, можемо визначити найбільш характерні ознаки.

Базовий *інформаційний процес* у Середньовіччі та Відродженні відбувався шляхом створення (дослідження навколишнього світу, наукового пізнання та перетворення умов зовнішнього середовища), фіксації (наука, мистецтво, архітектура, реклама, писемність) та передання (мовлення, мистецтво, реклама, писемність) інформації.

Головними *інформаційними носіями* для цього періоду слугували друковані тексти – книги, офіційні документи, твори мистецтва. Матеріал на якому фіксувалася інформація – пергамент, папір, тканина, глина, камінь, метал.

Основними типовими прикладами *інформаційних війн* зазначених часів можна вважати типові, в сучасному розумінні, інформаційно-психологічні операції, що супроводжували військові конфлікти, політичні та економічні, а також релігійні процеси.

Виробництво контенту виокремлюється в окремий напрям діяльності, який охоплює релігію, військову справу, державне управління, мистецтво, а також науку. Накопиченням та поширенням інформації займаються представники церкви та окремих соціальних груп.

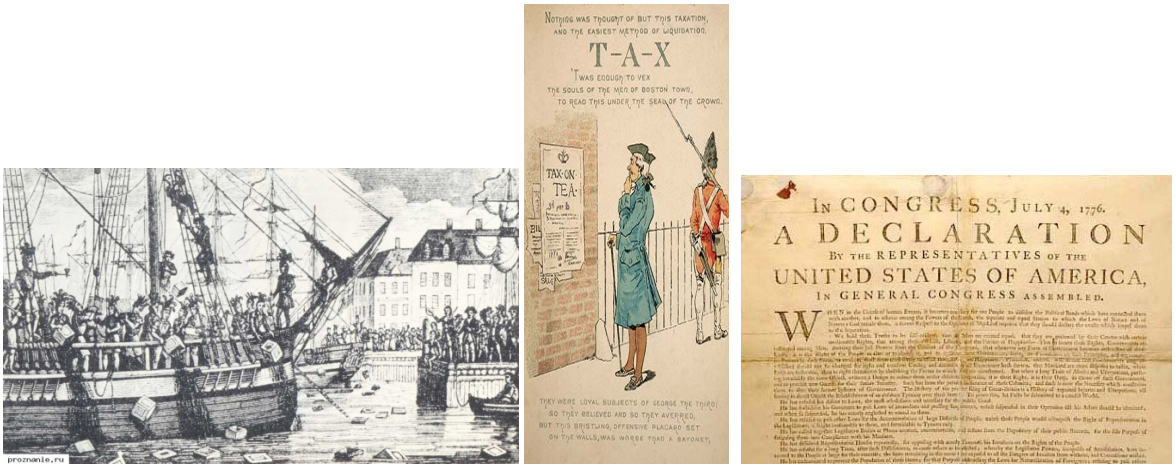
Храми з часом поступаються містом університетам, адміністративним та науковим центрам своїм статусом головного *виробника контенту*, який продукується відповідно до специфіки та тематики діяльності ї виробників. Значні обсяги інформації накопичуються в університетах, державних адміністративних структурах, наукових та мистецьких центрах, а також торговельно-економічних структурах (цехи, гільдії, торгові союзи та ін.).

1.1.4. Народження системної практики застосування інформаційно-комунікаційні технології в епоху раннього капіталізму (XVII –XIX ст.)

В епоху формування та первинного розвитку ринкових капіталістичних відносин інформаційні війни виконували функцію допоміжної технології із супроводження збройних конфліктів та економічних війн. Завдяки запровадженню європейцями нових технологій та поширення їхнього впливу на інші континенти, центри розвитку інформаційно-комунікаційних технологій формуються далеко за межами Європи. Зокрема одним з провідних стала колоніальна, а потім незалежна Північна Америка.

Історія США розпочиналася із війни за незалежність низки Північно-Американських колоній проти Англії (1775—1783 рр.). Саме під час цього протистояння сформувалися базові технології та розвинулися інформаційно-комунікаційні технології, які набули системних обрисів (мал. 1.20) [197, с. 51].

Мал.1.20. Події та зразки преси війни за незалежність США

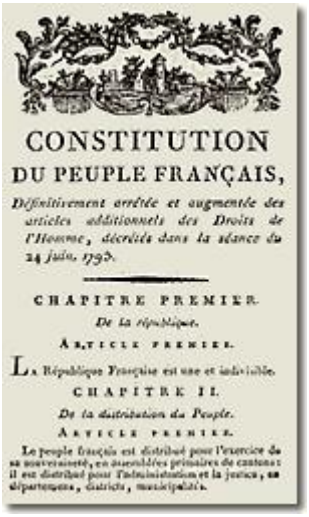


У своїй боротьбі колоністи використовували соціальні мережі (товариства «Сини свободи», «Кореспондентські комітети»), застосовували образні символи («Дерево свободи»), стереотипи та лозунги («Воля або смерть»). Вони дуже активно застосовували дієві акції, тогочасні медіа, чутки, маніпуляцію.

Остання, зокрема, яскраво втілилися у події, що отримала назву «Бостонське чаювання» (1773 р.), коли купа перевдягнених в індіанців колоністів знищила вантаж чаю, що прибув на кораблях з Англії (висипали у бухту) [197, с. 52]. Окрім інформаційної діяльності безпосередньо в театрі військових дій, агенти колоністів проводили в Європі активну пропагандистку роботу щодо пояснення Старому світу того, що відбувається в Новому світі. Зокрема завдяки такій агітації вдалося перетягнути на свій бік Францію і отримати симпатії та підтримку від Російської імперії.

Невдовзі після війни за незалежність у Північній Америці, в Європі відбулися події, які також стали важливою віхою в історії розвитку інформаційних війн – це була Французька революція (1789 р.) та наполеонівські війни (1799-1815 рр.). Ці непересічні події залишили значний слід як в суспільно-політичній історії, так і в історії інформаційних війн (мал. 1.21).

Мал.1.21. Преса та агітаційні матеріали часів Французької революції


CONSTITUTION
DU PEUPLE FRANÇAIS,
Définitivement arrêtée et augmentée des articles additionnels des Droits de l'Homme, décrétés dans la séance du 24 juin. 1793.
CHAPITRE PREMIER.
De la république.
ARTICLE PREMIER.
La République Française est une et indivisible.
CHAPITRE II.
De la distribution du Peuple.
ARTICLE PREMIER.
Le peuple français est distribué pour l'exercice de sa souveraineté, en assemblées primaires de cantons; il est distribué pour l'administration et la justice, en départemens, districts, municipalités.


LE DESPOTISME TERRASSÉ

Французька революція та подальша її трансформація у наполеонівську імперію була підготовлена розробками так званих вчених-енциклопедистів, зокрема таких, як: Д.Дідро, Ж.Д'Аламбер, Ж.-Ж.Русо, Вольтер, Монтеск'є та ін. Саме вони, досліджуючи специфіку розвитку суспільства та взаємовідносин між людьми, сформували ідеї та технології, які революція принесла народу Франції та сусіднім народам.

Головним інструментом ведення інформаційних війн перша французька республіка та Наполеон вважали соціально привабливі ідеї свободи, рівності економічного та політичного прогресу, що розповсюджували у суспільствах монархічних країн, з якими вони вели війни. Французькі емісари підривали внутрішню міць та єдність противника, формували мережі агентів впливу, підбурювали до спротиву та створення опозиційних організацій і медіа.

Усі провідні світові конфлікти XIX ст. обов'язково супроводжувалися інформаційними протистояннями із застосуванням такого інструменту, як **преса,** що стала **другою глобальною мас-медіа технологією**. Сам цей термін походить від назви першої масової газети «La Presse», що почала видаватися у 1831 р. (мал. 1.22) [197, с. 63]. З цього моменту специфіка та особливості ведення інформаційних війн набувають специфічного характеру. Преса стає інструментом масового впливу на свідомість суспільства, а відповідно засобом маніпуляції, дезінформації, залякування, стимулювання, заклику та інших засобів ведення інформаційних війн.

Мал.1.22. Перші французькі та італійські газети


LA PRESSE

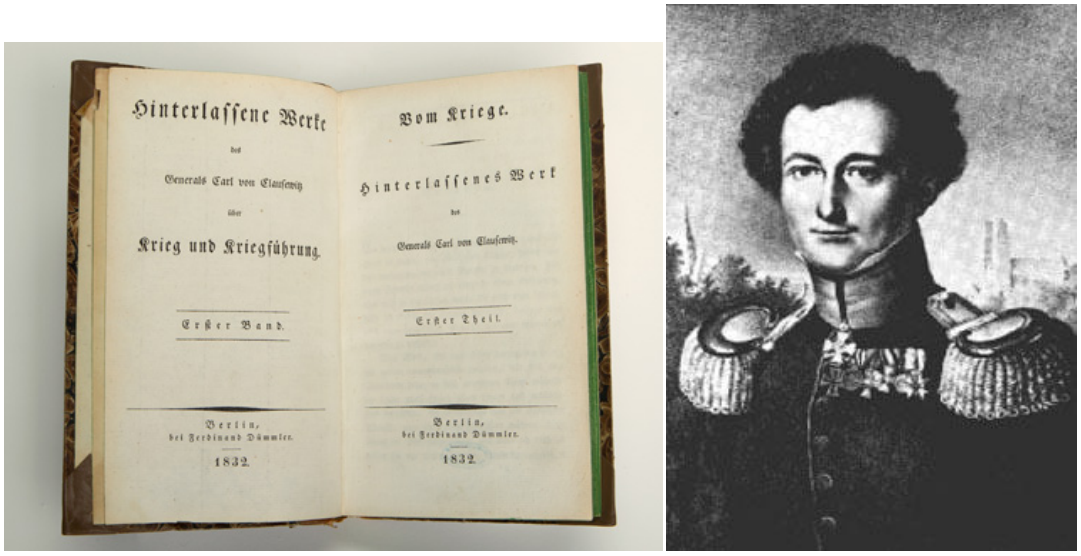
La Fête de la Reconnaissance nationale - La Chute de Bela Kuhn


RECVEIL DES
GAZETTES
de l'année 1631.
DEDIE' AV ROY.
AVEC VNE PREFACE SERVANT
M. D C. XXXII.

Наприкінці XIX століття з’являється нова інформаційно-комунікаційна технологія – **радіо** (Марконі, Попов, 1895), яка з часом перетворилася на потужну **третю глобальну мас-медійну технологію.**

Серед теоретиків та практиків інформаційних війн зазначеного періоду важливе значення мали розробки прусського генерала Карла Фон Клаузевіца, викладені в його книзі «Про війну» (1832 р.). На його думку, однією з головних складових успіху будь-якої армії є «відчуття перемоги», тобто переможна психологія, дух, мораль. Вони є головною мішенню та об’єктами, по відношенню до яких діють інформаційно-комунікаційні атаки противника (мал. 1.23) [152, с. 37].

Мал.1.23. Генерал К.Клаузевіц та його книга «Про війну»



У форматі нашої тематики особливе значення мають такі його постулати, які можуть бути трактовані й навіть як базові для гібридної війни:

1. Битва - це не тільки знищення живої сили ворога, а й знищення його мужності.

2. Заколот у суспільному та державному устрої набагато легше відбувається в умовах загального потрясіння та прискореного розвитку, які приносить війна.

3. Ті, хто не пам’ятають власного минулого, приречені на його повторення.

Узагальнюючи інформаційно-комунікаційні здобутки епохи раннього капіталізму, визначаємо наступні характерні ознаки.

Базовий *інформаційний процес* у XVII-XIX ст. відбувався шляхом створення (дослідження навколишнього світу суспільних процесів, наукового пізнання та перетворення умов зовнішнього середовища), фіксації (наука, мистецтво, архітектура, реклама, писемність) та передання (мовлення, мистецтво, реклама, писемність, ранні медіа) інформації.

Головними *інформаційними носіями* для людини в ці століття були передусім книжки, офіційна документація, листи – на основі паперу, твори мистецтва – папір, тканина та інші, характерні минулим епохам. Основними прикладами *інформаційних війн* цього періоду можна вважати типові, в сучасному розумінні, інформаційно-психологічні операції (залякування, дезінформація, психологічний тиск та ін.). Останні супроводжували військові конфлікти, політичні та економічні процеси.

Виробництво контенту є окремою спеціальністю, яка забезпечує необхідними даними економічні процеси, мистецтво, військову справу, державне управління, науку, релігію. Створенням, накопиченням та поширенням інформації займаються чітко визначені фахівці.

Фабриками контенту стають навчальні заклади, наукові центри, адміністративні структури, безпосередньо медіа.

1.1.5. Інформаційні війни XX - поч. XXI ст.

На початку XX ст. більш-менш сталий світовий порядок, який формувався століттями, було порушено. Відбулася низка потужних революцій (Росія, Німеччина, Австрія, Латинська Америка, Далекий Схід та Південна Азія), а

також дві світові війни. Потім майже до кінця століття світ знаходився у форматі двополярного протистояння (США-СРСР).

Першим прикладом найбільш успішного застосування технологій інформаційної війни в XX ст. стало виведення з числа активних учасників Першої світової війни Росії та розвал Російської імперії (мал. 1.24).

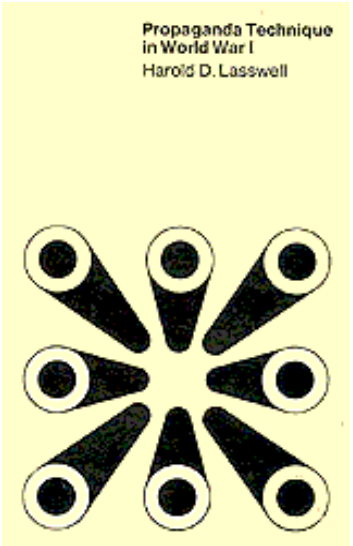
Розуміючи міць Антанти (союз Англії, Росії, Франці та США та в цілому 34 держави) і неможливість прямої перемоги Німеччини та її союзників (Австро-Угорщина, Болгарія, Туреччина), уряд Кайзера Вільгельма почав стимулювати революційні рухи в Росії та, зокрема, допоміг здійснити заколот і прийти до влади Леніну та очолюваній ним партії більшовиків. У результаті цієї спецоперації один з найпотужніших учасників Антанти – Росія вийшла з війни та розпочала боротьбу із своїми колишніми союзниками.

Мал.1.24.Агітаційні плакати часів І-ї Світової війни

Проте, значної переваги Німеччині ця перемога не дала. Антанта таки перемогла, в Німеччині, а також у її союзника Австро-Угорщини відбулися революції, які призвели до розвалу цих імперій і утворення республік з більш-менш демократичними режимами.

Одним з перших питання розвитку інформаційно-комунікаційних технологій та інформаційної війни в XX ст. почав системно досліджувати Г.Д.Лассуел (1902-1978). Він активно залучав методи соціальної психології, психоаналізу, психіатрії для дослідження політичної поведінки та пропаганди, виокремлюючи роль масових комунікацій в процесі ведення інформаційних протистоянь між провідними країнами світу. Саме Лассуел першим провів аналіз здійснення пропаганди під час Першої світової війни. Свої розробки він узагальнив у роботі «Техніка пропаганди у світовій війні» (1927 р.), де вперше було виділено інформаційно-психологічну сферу війни, а пропаганду подано як особливий вид зброї, що впливає на моральний стан ворога (мал. 1.25) [152, с.35].

Мал. 1.25. Г.Лассуєл та перше видання «Техніка пропаганди у світовій війні»



Народжена в горнилі Першої світової війни Радянська Росія, що з часом перетворилася на неоімперську державу СРСР, з перших днів свого існування

активно застосовувала інформаційно-комунікаційні технології ведення внутрішніх та зовнішніх війн (мал. 1.26).

Внутрішня інформаційна війна велася в СРСР проти політичної опозиції (Троцький, Зинов'єв, Каменєв, Бухарін), широких незалежних соціальних верств населення (заможні селяни, інтелігенція, духовенство), національних об'єднань. У цьому контексті застосовувалися агітація, дискредитація, маніпулювання, залякування, впровадження певних психологічних установок. Жертвами цієї війни стали мільйони невинних громадян, її наслідками - створення великого державного концтабору, який охопив 1/6 світу.

Мал.1.26.Агітаційні плакати перших десятиліть СРСР

Зовнішню інформаційну війну очільники СРСР проводили проти іншого цивілізованого світу, і в першу чергу проти своїх політичних та економічних

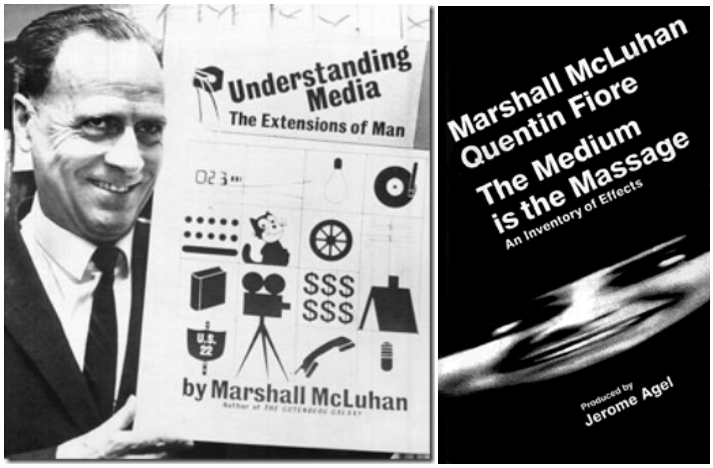
конкурентів, якими в різні часи були Німеччина, США, а також міжнародні торговельно-економічні (СОТ, ЄС) та військові (НАТО) союзи. Інформаційні атаки супроводжували відкриті та приховані конфлікти, в яких брала участь СРСР (мал. 1.26). Серед них війна з Польщею (1920 р.), Фінляндією (1939-1940 рр.) гітлерівською Німеччиною (1941-1945 рр.), участь у Корейському конфлікті (1950-1953 рр.), війні у В'єтнамі (1973-1975) Афганської війни (1979-1989 рр.), багатьох збройних конфліктах у Африці та Латинський Америці (мал. 1.27; 1.29).

Мал.1.27. Агітаційні матеріали епохи радянського соціалізму

Фактично весь час свого існування СРСР перебувала в стані інформаційної війни, що дозволило відповідним структурам – КДБ, ЗМІ, партійним та радянським громадським організаціям напрацювати величезний досвід та сформувати дієвий інструмент ведення не тільки інформаційної, але й гібридної війни.

У плані розвитку теорії та методології ведення інформаційних війн в середині XX ст. важливе значення мали наукові розробки канадського соціолога Г.М.Мак-Люена, який досліджував роль і значення медіа в сучасному світі та історичній ретроспективі (мал. 1.28). В контексті останнього він класифікував історію розвитку людства в залежності від типів медіа, якими воно володіло у певний час. Зокрема він визначає дописемний період, писемну культуру та сучасний період. Основними ознаками сучасності він вважає такі категорії, як «електронне суспільство» та «глобальне село». Останнє він розуміє як сучасний світ, який завдяки цифровим технологіям знаходиться в єдиному інформаційному полі. Також він впровадив класифікацію медіа за функціями та можливостями на «гарячі» (інформативні) та «холодні» (емоційні) [249, с.138].

Мал.1.28. Г.М.Мак-Люєн та його твори



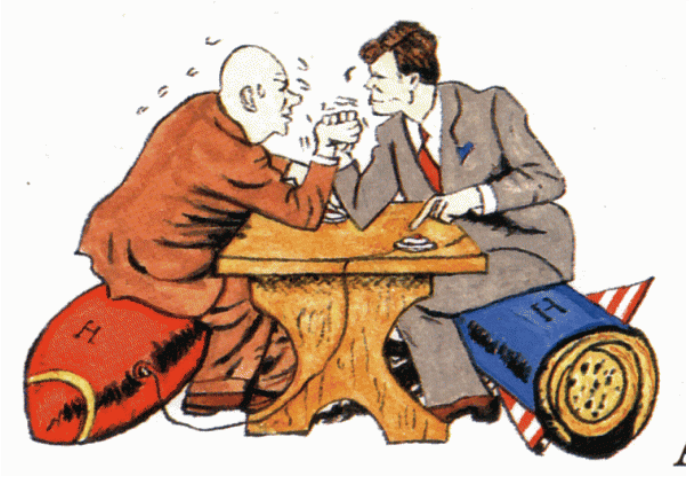
Найбільш потужним суперником СРСР та його союзників (так званий соціалістичний табір – військовий «Варшавський союз», економічний СЕВ) були США та його союзники (СОТ, НАТО та ін.).

Пройшовши Першу та Другу світові війни, оволодівши ядерною зброєю, Америка стала потужним центром геополітичного впливу і поділила весь світ з СРСР на власні зони впливу. Це протистояння отримало назву «Холодна війна» (1946-1991 рр.). Остання полягала у постійних інформаційних протистояннях,

гонці озброєнь та економічному протистоянні в боротьбі за джерела сировини та ринки збуту (мал. 1.29).

Захищаючи власні військові, політичні та економічні інтереси, США протягом XX ст. брала участь в усіх значних регіональних конфліктах у Латинській Америці, на Близькому Сході, в Європі, Південній та Східній Азії, Африці. В переважній більшості випадків головним опонентом був СРСР. Жорстке протистояння двох геополітичних гігантів не одноразово ставило світ на край реальної гарячої війни.

Мал.1.29. «Холодна війна» в агітаційних плакатах



Такими були Карибська криза (1962 р.), Берлінська криза (1961 р.), а також низка менш відомих конфліктів.

Основними центрами планування та ведення інформаційних війн у США стали Державний департамент (дипломатичне прикриття операцій), ЦРУ (планування та реалізація спецоперацій), Пентагон (військово-політичні

операції) та низка різноманітних профільних дослідницьких центрів та громадських об’єднань.

Найбільш успішною інформаційною кампанією для США стало фінальне протистояння «Холодної війни», яке прискорило процеси, що призвели до розвалу СРСР. Головною діючою особою цього протистояння став 40-й американський президент Рональд Рейган (1981-1989 рр.). Останній оголосив ще в 1979 р. хрестовий похід проти «Імперії Зла» і розпочав безкомпромісну економічну та інформаційно-психологічну війну з СРСР та його союзниками (мал. 1.30).

Головними складовими частинами боротьби Рейгана стала економічна складова – зниження світових цін на нафту, продаж якої був на той час чи не найголовнішою статтею прибутку СРСР, та низка економічних санкцій. Разом з тим було активізовано гонку озброєння, яка суттєво спустошила економічний потенціал Радянського Союзу [56, с.214].

Мал.1.30. «Імперія зла» та «Зоряні війни» Р.Рейгана

Активно використовувалася й ідеологічна складова. В 1983 році Рейган оголосив запуск програми «Стратегічна оборонна ініціатива», сутність якої полягала в тому, що американські супутники за допомогою лазерних пристроїв мали можливість знищувати будь-які ядерні ракети, націлені на Америку та її союзників ще на старті. Навколо цього проекту було багато галасу,

дезінформації, відвертих маніпуляцій. Долучився до цього навіть Голівуд, де зняли блокбастер «Зоряні війни» (1970-80-ті рр.). Також багато інформації було навколо так званої кліматичної зброї (мал. 1.30).

Загнавши шляхом економічного та інформаційно-психологічного тиску нового радянського лідера Михайла Горбачова в глухий кут, Америка змусила його розпочати перебудову та підписати низку мирних угод із Заходом, що дорівнювалося до капітуляції. Так було знищено пресловуту «Імперію Зла».

Починаючи з 1991 р. США стає фактично гегемоном у плані світової геополітики та перебудовує світову систему безпеки та економічних відносин під свої потреби та потреби своїх союзників.

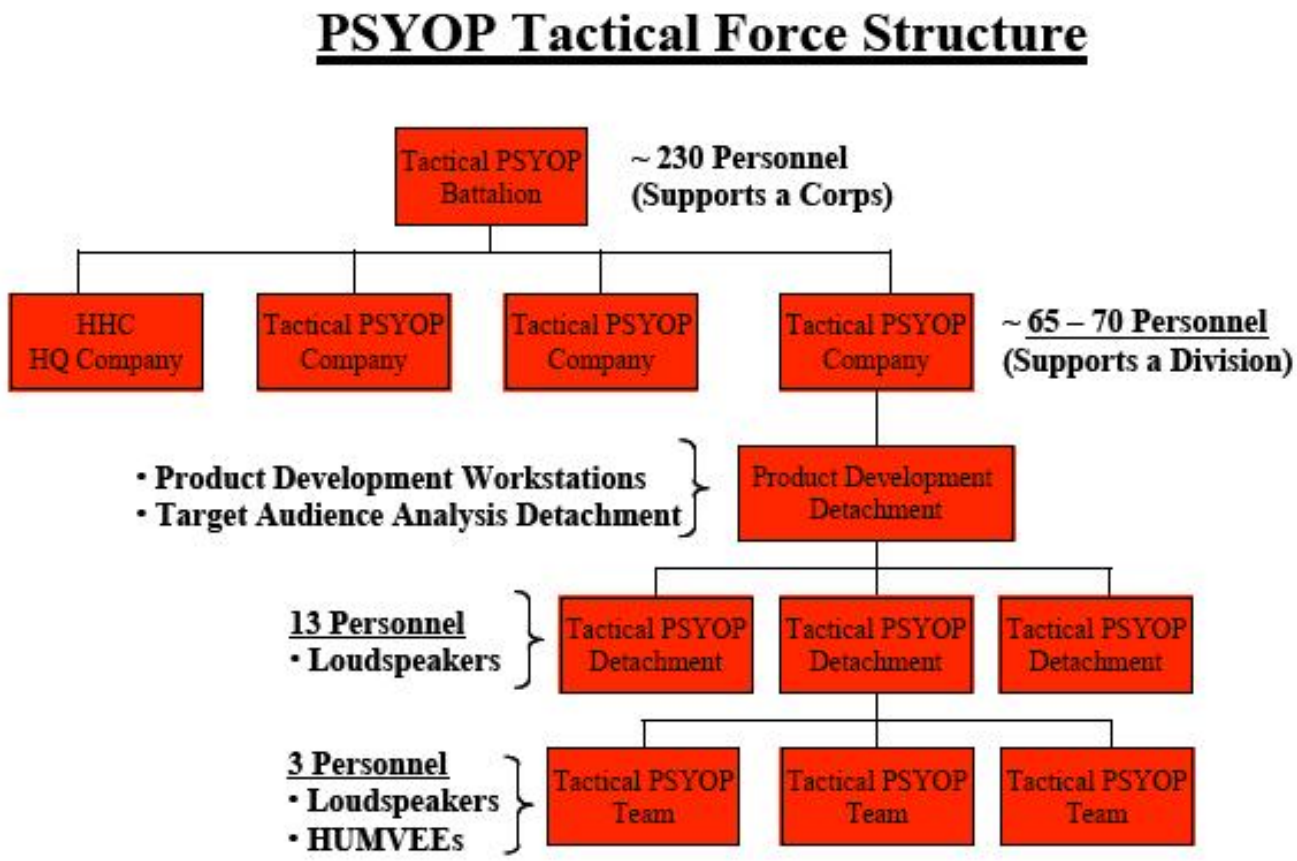
Без особливих складнощів США вирішують конфлікти під час війни в Перській затоці (1990-1991 р.), війни на Балканах (1991-1999 рр.), що призвела до розпаду Югославії. Потім була війни в Іраку (2003 р.).

Під час цих конфліктів остаточно сформувалася сучасна базова американська доктрина ведення інформаційно-психологічної війни другого покоління, з’явилися спеціалізовані стратегії, методики, інструменти. Було створено окремі військові підрозділи психологічних операцій PSYOPS (Psychological Operations) або з 2010 р. – центри інформаційного забезпечення MISO (Military Information Support Operation). Сам термін «інформаційна війна» почав офіційно вживатися з 1992 р., а у 1993 р. було надане розширене тлумачення цього терміна [90, с. 40-41].

Мал.1.31. Знаки підрозділів, що ведуть інформаційно-психологічні операції

Базовим документом для регулювання питань проведення інформаційної війни стали Польовий Статут армії США FM-106 «Інформаційні операції» і Доктрина спільних інформаційних операцій (мал. 1.32).

Мал.1.32. Структура типового підрозділу із інформаційно-психологічних операцій



Інформаційні війни XX ст. в якості базових інструментів роботи використовували як традиційні медіа, що було напрацьовано у попередні часи (друк, преса, радіо), так і нові: **кіно, телебачення**, **Інтернет**. Ці комунікаційні інструменти суттєво підвищили ефективність інформаційно-комунікаційної діяльності в рамках військових конфліктів. А два з них – телебачення та Інтернет перетворилися, відповідно, на **четверту** та **п'яту глобальні мас-медіа технології**.

Розробки Мак-Люена, що з'явилися в середині XX ст., значною мірою вплинули на формування сучасного розуміння ролі та значення цифрових медіа в контексті інформаційних конфліктів. Серед тих, хто формував теоретичні та методологічні основи сучасних інформаційних війн, особливої уваги заслуговують розробки американського політолога та соціолога З. Бжезінського «Велика шахівниця», що вийшла в 1997 р. на стала підручником для сучасних політологів (мал. 1.33) [56].

Мал. 1.33. З.Бжезінський та його бачення сучасної геополітичної стратегії

Аналізуючи сучасний світ, його глобальні тренди та регіональні особливості розвитку, він спрогнозував та сформулював роль і значення США на глобальному просторі, місце і перспективи Росії, Китаю та інших провідних гравців світу. Зокрема щодо ролі і місця на світовій геополітичній мапі України він зазначив: «Україна - новий і важливий простір на євразійській шахівниці, вона є важливим геополітичним центром, тому що саме її існування як незалежної держави допомагає трансформувати Росію. Без України Росія втратить статус євразійської імперії. Без України Росія ще може поборотися за імперський статус, утім тоді вона буде азійською імперською державою» [56, с.346].

Наприкінці XX ст. на початку XXI ст. людство переходить у цифрову епоху, значна частина життя віртуалізується. Разом з тим інформаційні протистояння переносяться в мережу Інтернет. Особливого значення набуває

такий формат як **кібервійна**. Остання стає важливою частиною «гарячої» війни, виконуючи функцію забезпечення та надання суттєвих переваг в реальному протистоянні.

Народження та впровадження нових технологій ведення інформаційної війни не впливає на її традиційні складові частини та цілі. Так само, як і у XX та XIX ст. або в попередні віки, головним завданням є отримання суттєвих переваг у забезпеченні військових, економічних та політичних конфліктів. Незмінність цих постулатів продемонстрували останні міжнародні конфлікти, ініціаторами яких стала Російська федерація.

Ліберальна єльцинська епоха в Росії закінчилася приходом до влади ставленика олігархічно-кланових та колишніх структур КДБ – Володимира Путіна. Почали лунати реваншистські заяви, розпочалася мілітаризація суспільства, збільшення виробництва зброї та активізація зовнішньополітичної агресії.

Ще з минулих часів у спадок путінській Росії залишилися конфлікти в Абхазії, Чечні та Придністров'ї. До цього додали війну з Грузією, анексію Південної Осетії (2008 р.) та війну с Україною (2014-2015 р.) з анексією Криму та створенням в Донбасі терористичних об'єднань так званих «Донецької народної республіки» та «Луганської народної республіки». Крім того РФ втрутилася в конфлікт на території Сирії, де урядові війська Асада Башара воюють із військовими угрупованнями ІДІЛ («Ісламська держава Іраку та Леванту») та місцевих повстанців.

У зазначених конфліктах Росія застосувала останній досвід вдалих інформаційно-психологічних війн, що велися США та найбільш сучасні інформаційно-комунікаційні технології. Останнє дало режиму Путіна певну тактичну перевагу та тимчасові перемоги, але в стратегічній перспективі затягло його в таку ж саму геополітичну пастку, в яку свого часу затягнув Рейган СРСР.

Слід зазначити, що інформаційній складовій у зовнішній та особливо внутрішній політиці Росія приділяє чи не головну увагу та фінансує медіа проекти по першій категорії.

Важливим здобутком XX-XXI ст. у плані розвитку інформаційно-комунікаційних технологій стало народження мережевих он-лайн та оф-лайн структур. Особливо важливе значення мали он-лайн структури – соціальні мережі формату WEB 2.0.

Виникнення Інтернету (1957 р. – прототип, 1991 р. - глобалізація) надало поняттю «соціальна мережа» нового значення та відкрило перед людством великі перспективи. Вже у 1995 р. Ренді Конрадс створює перший віртуальний соціальний мережевий ресурс і дає йому назву - **Classmates.com** - (охоплює переважно США та Канаду). Головною метою цього проекту Конрадс вбачав надання зареєстрованим користувачам допомоги у встановленні та підтримці зв'язків з друзями та знайомими, з якими вони перетиналися протягом всього життя. Через певний час з'явилися нові мережі - **Friendster** (2002 р.), **Linked ln** (2003 р.), **MySpace** (2003 р.), **Tribe** (2003 р.), **Hi5** (2003 р.).

У 2004 р. з'являються такі соціальні мережі як: **Orkut**, **Bebo**, **Yahoo 360**. У цьому ж році студент Гарвардського університету Марк Цукерберг створив **Facebook**, мережу, яка зараз є безумовним лідером (в середньому кожен сьомий мешканець планети є її користувачем). На території країн СНД першими були такі соціальні мережі, як: **Мой круг (**2005 р.) **Odnoklassniki.ru (**2006 р.**)** и **VKontakte.ru (**2006 р.).

Узагальнюючи інформаційно-комунікаційні здобутки XX-XXI ст., в плані розвитку інформаційних війн визначаємо наступні характерні ознаки.

Базовий *інформаційний процес* у цей період та наш час відбувався шляхом створення (дослідження навколишнього світу суспільних процесів, наукового пізнання та перетворення умов зовнішнього середовища), фіксації (наука,

мистецтво, архітектура, реклама, писемність) та передання (мовлення, медіа, мистецтво, реклама, писемність) інформації.

Головними *інформаційними носіями* для людини сьогодні є цифрові пристрої, друковані книжки, офіційна документація, персональні листи – на основі паперу, твори мистецтва – віртуальні площини, папір, тканина та інші, характерні ще минулим епохам.

Основними типовими прикладами *інформаційних війн* цього періоду можна вважати цифрові віртуальні конфлікти та реальні інформаційно-психологічні операції. Вони супроводжують військові конфлікти, політичні та економічні процеси.

Виробництво контенту стає чи не найголовнішою функцією суспільства, що забезпечує необхідними матеріалами економічні процеси, мистецтво, військову справу, державне управління, науку, релігію тощо. Створенням, накопиченням та поширенням інформації займаються практично всі, хто бере участь у соціальних процесах.

Фабриками контенту стають наукові центри, військові структури, навчальні заклади, адміністративні структури, безпосередньо медіа.

1.2. Теорія інформаційної війни: методологія та понятійний апарат

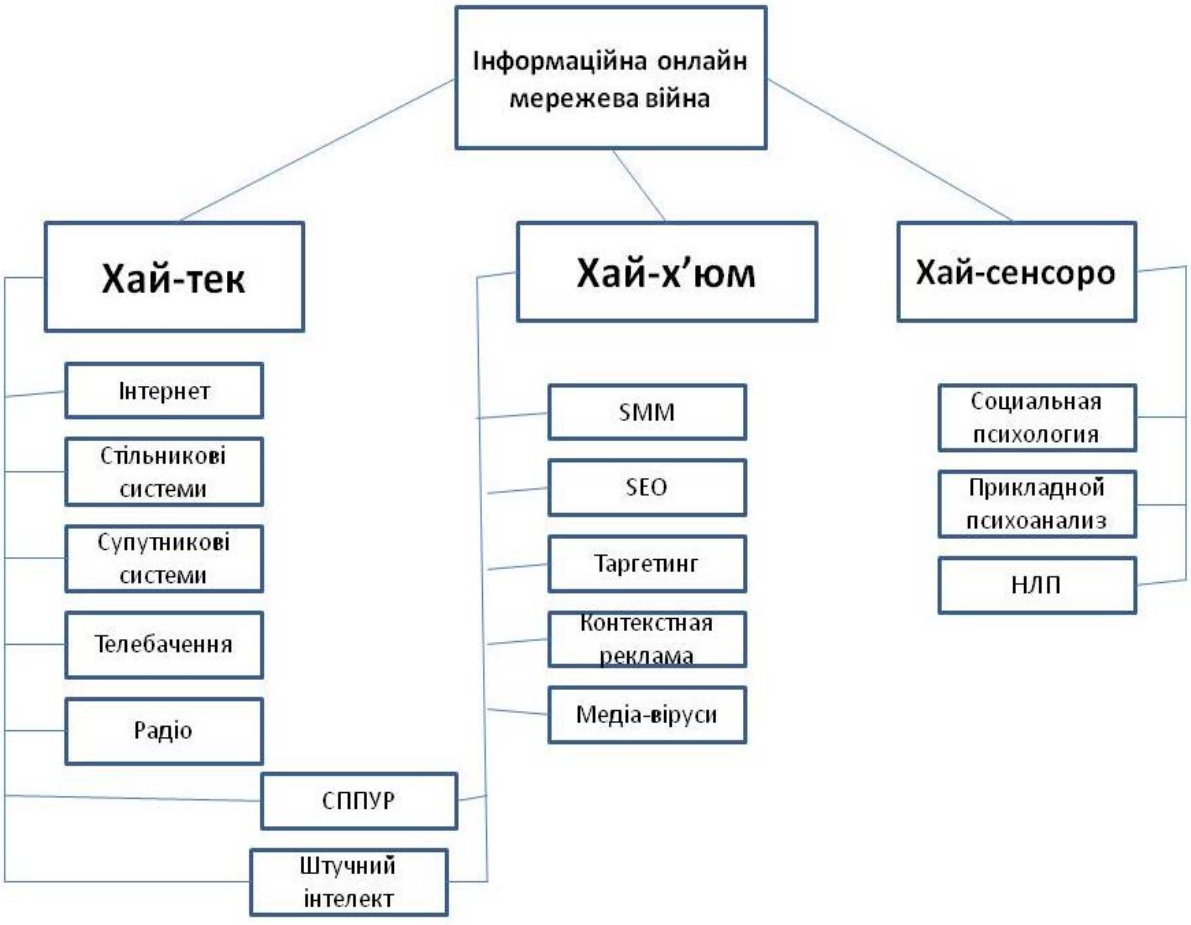
1.2.1.Базова модель теорії сучасної інформаційної війни у соціальних он-лайн мережах

Ключовим елементом у теоретичній моделі є поняття **інформаційна он-лайн мережева війна** (ІОМВ)**,** що визначається, як комплекс інформаційних впливів між соціальними системами (групами), що орієнтовані на отримання певних перваг у економічних, військових, політичних, культурних та громадських протистояннях.

В своїй основі ІОМВ має три ключові технологічні аспекти: хай-тек, хай-х’юм та хай-сенсоро. Кожен з цих аспектів має власні технології, які формують профільні напрямки дослідження та практичної роботи (див. мал. 1.34.).

Хай-тек в ІОМВ – сучасні високі техногії цифрових комунікацій, що в основі мають системи телебачення, радіо, Інтернет, месенджерів, стільникової, супутникової та інших видів сучасного зв’язку та базуються на таких гаджетах, як стаціонарні комп’ютерні пристрої, планшети, смартфони, пристрої індивідуального та групового зв’язку.

Мал.1.34. Модель інформаційної онлайн мережевої війни



До цього аспекту відноситься класичне *телебачення*, в ефірному та цифровому форматах. Останне визначають, як технологію трансляції

телевізійного зображення та звуку за допомогою кодування відеосингалу та сигналу звуку із використанням цифрових каналів за стандартом MPEG.

Радіо, як класичне електронне ЗМІ, розглядається у традиційному аналоговому (AM, FM) та цифровому форматах. Останній визначається, як технологія трансляції сигналів радіостанцій в цифровій формі за допомогою електромагнітних хвиль радіодіапазона.

Інтернет, в контексті досліджуваної теми розглядається, як всесвітня система об'єднаних комп'ютерних мереж для зберігання та транслювання інформації. На основі цієї мережі, як комунікаційної платформи формуються типові поштові сервіси, сервери зберігання даних, а також нові формати мережевого телебачення та радіо.

При цьому *інтернет-телебачення* визначається, як телебачення міжмережевого протоколу (on-line TV) — система, що базується на двустороньому цифровому переданні телевізійного сигналу через інтернет-з'єднання за допомогою широкополосного підключення.

Інтернет-радіо або веб-радіо, визначають як групу технологій трансляції потокових аудіоданих через мережу Інтернет для здійснення широкої трансляції програм. Також, в якості терміна інтернет-радіо визначається радіостанція, що використовує для трансляції технологію потокового віщання у глобальній мережі Інтернет.

Месенджери – мережі миттєвого з'єднання. Типовими прикладами таких технологій є WhatsApp, Facebook Chat, Hangouts (Google), Skype, LINE, WeChat, Viber, Kik, Snapchat, ICQ, Telegram.

Стільниковий звязок – один з різновидів мобільного зв'язку, в основі якого закладено стільникову мережу. Ключова особливість полягає в тому, що спільна зона покриття поділяється на ланки (соти), що визначаються зонами покриття окремих базових станцій. Соти частково перекриваються створюючи мережу.

Супутниковий зв'язок (радіо та телебачення) - один з різновидів космічного радіозв'зку, що базується на використанні штучних супутників в якості ретрансляторів. Цей зв'язок здійснюється між наземними станціями, що є стаціонарними або мобільними. Супутниковий зв'язок є продовженням розвитку традиційного радіорелейного зв'язку шляхом винесення ретранслятора на велику висоту.

Хай-х'юм в ІОМВ – сучасні високі соціально-гуманітарні технології створення, зберігання, розповсюдження та пошуку інформації. До них відноситься SMM, SEO, таргетинг, контекстна реклама, медіа-віруси та ін.

SEO (Search Engine Optimization) – комплекс заходів із пошукової оптимізації, орієнтований на підвищення позиції веб-сайту у пошукових системах.

SMM (Social Media Marketing) – комплекс заходів із просування персонального акаунта або окремого контенту в соціальних мережах.

Таргетинг – рекламний механізм, що дає можливість виокремити з наявної аудиторії лише певну її частину, яка відповідає потрібним критеріям, і показати саме їй рекламне повідомлення.

Контекстна реклама – метод розміщення інформації, що орієнтована на зміст інтернет-ресурсу, представлена у вигляді банеру чи текстового повідомлення.

Медіа-віруси – інформаційні носії (події, скандали, чутки, діяльність організацій та окремих осіб), що несуть в прихованому вигляді завуальовані ідеї та меседжі.

Хай-сенсоро в ІОМВ - сучасні високі психотехнології, що дають можливість регулювати та керувати соціальними комунікаційними процесами на рівні соціальних груп та окремих індивідуумів. Типовими в цьому аспекті є соціальна психологія, прикладний психоаналіз та НЛП.

Соціальна психологія – галузь в психології, що орієнтована на вивчення принципів та закономірностей діяльності людини в умовах взаємодії в соціальних групах. Основні проблеми соціальної психології: закономірності спілкування та взаємодії людей, діяльність великих (нації, класи) і малих соціальних груп, соціалізація особистості та розвиток соціальних установок.

Прикладний психоаналіз – напрямок знань в психології, що досліджує практику використання ідей та концепцій орієнтованих на досягнення глибокого розуміння різноманітних аспектів людської природи, культури та суспільства. Найбільша кількість досліджень, в цьому плані припадає на галузі історії, біографії, літератури, мистецтва, релігії, міфології та антропології.

Нейро-лінгвістичне програмування – технологія моделювання вербальної та невербальної поведінки людей за допомогою поєднання форм мовлення, руху очей, тіла та пам'яті.

В структурі зазначеної моделі існують елементи, що мають ознаки двох аспектів. Це Системи підтримки прийняття управлінський рішень (СППУР) та Системи штучного інтелекту. Вони мають характерні ознаки хай-тек та хай-х'юм.

Кожен з зазначених аспектних напрямків має свої методологічні складові та прикладні інструменти, що в комплексі формують сучасну систему управління інформаційно-комунікаційними процесами, в форматі економічних, політичних, військових, культурних та громадських конфліктів.

1.2.2.Методологічна основа сучасної інформаційної війни у соціальних он-лайн мережах

Основою будь-якого інформаційного протистояння є **інформаційний процес**, ***що визначається як діяльність із створення, накопичення, зберігання, пошуку та розповсюдження відомостей або даних певного тематичного характеру*** [218, с.26].

Базовими поняттями для вивчення сучасних мережевих інформаційних протистоянь є **інформація** та **комунікація**, які формують основу всього того, що в подальшому розглядається як інформаційна війна.

Інформацію розуміють ***як відомості або дані про навколишнє середовище, що оточує людину*** [218, с.24]. А ***комунікація - це процес передання або обміну інформацією*** [218, с. 25].

У різні епохи інформаційні процеси носили в собі відбитки тих технологій, які було винайдено на певному етапі. Це позначалося на особливостях проведення відповідних інформаційних протистоять.

Кожен з таких винаходів за історичною значущістю та технічними характеристиками можна визначити або як **інформаційний вибух,** або як **інформаційну революцію**.

Під поняттям ***інформаційна революція*** ми розуміємо ***докорінну зміну методів створення, накопичення, зберігання, пошуку та поширення інформації*** [218, с.25]. До таких явищ можна віднести появу мовлення, писемності, комп'ютерної техніки. Всі ці винаходи були початком принципово нового напрямку розвитку інформаційно-комунікаційних технологій.

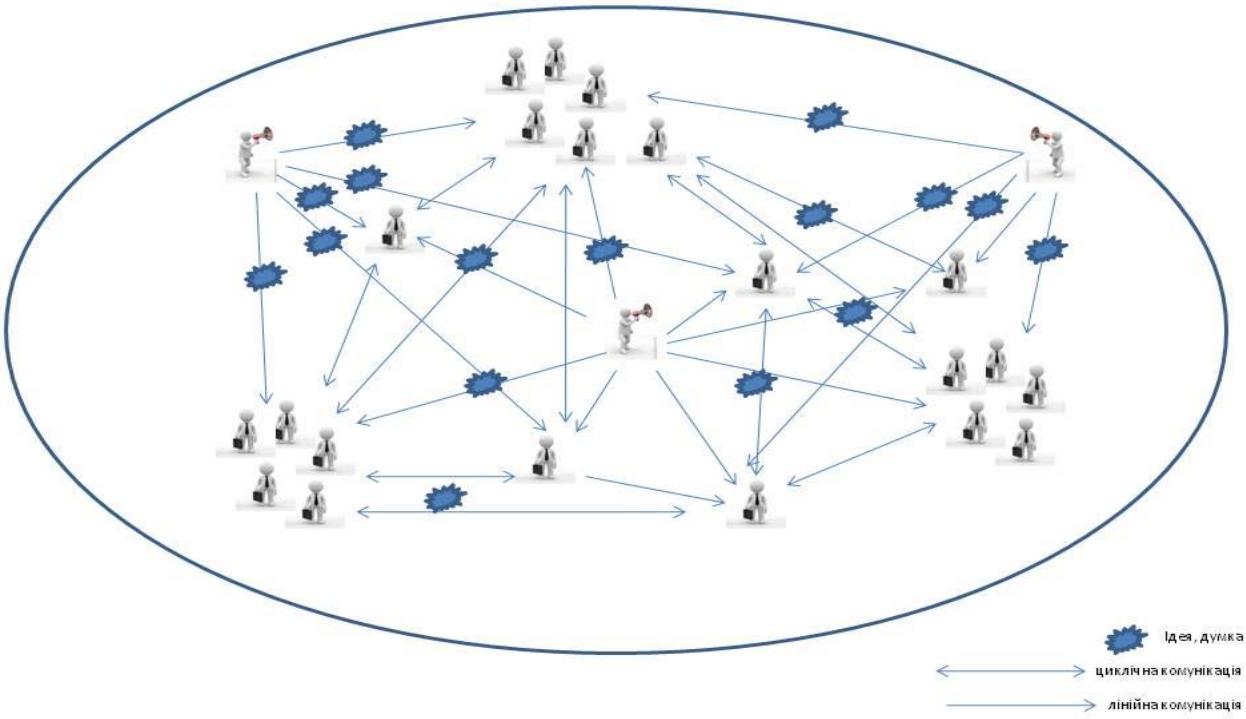
За визначенням, ***інформаційний вибух*** – це ***суттєве прискорення процесів створення, накопичення, пошуку та поширення інформації*** [218, с.26]. Типовим прикладом останнього є винайдення абеткової писемності (як модернізація системи писемності), друкарства (оптимізація писемних процесів), Інтернету (еволюція комп'ютерних технологій).

Будь-які інформаційні процеси відбуваються в певних площинах або теренах, які можна узагальнити в рамках поняття **інформаційне поле**. Останнє визначається, як ***соціальний або географічний простір, у межах якого відбуваються типові комунікаційні процеси, які охоплюють їх учасників (суб'єкти) на основі обміну інформацією (об'єкт)*** (мал. 1.35).

Складовими частинами інформаційного поля є **суб'єкти інформаційних процесів** – ***учасники комунікацій, індивідууми, соціальні групи, організації (ЗМІ, громадські, державні, комерційні структури)***. Також важливою складовою частиною інформаційного поля є **об'єкти інформаційних процесів** - ***інформація або ті, хто отримують цю інформацію в процесі спрямованої комунікації***.

Суб'єкти та об'єкти інформаційних процесів поєднуються між собою за допомогою **лінійної** або **діалогової моделей** соціальних комунікативних процесів (мал.1.36.).

Мал. 1.35. Інформаційне поле



Лінійна модель комунікації передбачає однобічний, цілеспрямований процес передання інформації від автора повідомлення до отримувача. На першому етапі у свідомості автора з'являється певна ідея (думка) яку він, на другому етапі, перетворює на інформацію шляхом кодування – матеріалізації

ідеї у вигляді слова, тексту, малюнка, звука. Сформована таким чином інформація (контент) на третьому етапі транслюється через посередника (технічні засоби комунікації або інша особа) або особисто автором (артикуляція або демонстрація). На четвертому етапі повідомлення досягає отримувача, який його декодує (читає, переглядає, прослуховує) для того, щоб зрозуміти базову ідею (думку), яка була закладена автором повідомлення. Надіслану ідею отримувач обробляє та формує власне судження з цього приводу у вигляді певної ідеї. На цьому процес лінійної комунікації закінчується.

У разі, якщо отримувач інформації має намір відреагувати на повідомлення, він спрямовую свою думку, на основі отриманої ідеї автору, застосовуючи той же самий механізм. Він кодує свою думку, транслює її, потім відбувається її декодування та сприйняття. Це ***циклічна модель комунікації***, ***яка передбачає взаємний обмін інформацією, в процесі якого учасники комунікації поступово змінюють ролі автора та отримувача повідомлення*** (мал. 1.36)**.**

Мал. 1.36. Базовий комунікаційний процес

Базовими сферами застосування сучасної інформаційної війни є: політична, дипломатична, військова, фінансово-економічна. Інформаційні протистояння в цих сферах, за структурою, виглядають як ***циклічний або лінійний обмін інформацію, яка може/має спричинити певну шкоду***

отримувачу, а автору надати певну перевагу. Саме в цьому і полягає сутність **сучасної інформаційної війни**.

Базовою методологічної основою сучасних інформаційних протистоянь є **маніпуляція** - ***засіб психологічного впливу, що застосовується задля прихованого проникнення в психіку жертв із метою занесення цілей, бажань, намірів, відносин або установок маніпулятора*** [152, с.59]. Фактично це приховане управління людьми та їх поведінкою.

Головним форматом здійснення інформаційних протистоять є поняття **інформаційна зброя** або **інформаційна атака**. Останні розуміють як ***здійснення тимчасового або остаточного виведення з ладу систем та підрозділів противника, що відповідають за процеси управління та інформування*** [152, с.35].

Головною метою інформаційної атаки є ***отримання суттєвих переваг в реальному військовому, економічному або політичному протистояннях*** [152, с.36].

Традиційним базовим інструментом інформаційного протистояння є **медіа**, які здійснюють посередницьку функцію із трансляції ідей та думок у вигляді конкретних меседжів, між автором повідомлення та отримувачем. Медіа ***розуміють як канали та засоби зберігання, передачі і подання інформації або даних*** [217, с.168]. Фактично до медіа можна віднести будь-який інформаційний носій, що виконує означені функції. Разом з тим існує ще таке поняття як **мас-медіа**, яке іноді ототожнюють із поняттям медіа. Втім мас-медіа мають дещо конкретніші обриси і визначається як: ***технології та засоби трансляції інформації від конкретного джерела на широку аудиторію, яка обмежується рамками певного інформаційного поля в якому ці мас-медіа діють*** [48, с. 126].

Типові мас-медіа поділяються на три групи, за специфікою функціонування [217, с.168].

- друкована преса (газети, журнали, бюлетені та ін.);

- аудіовізуальні (радіо, телебачення, Інтернет);
- інформаційні служби (агенції, прес-служби, прес-бюро, центри громадських зв'язків тощо);
- рекламно-інформаційні носії (зовнішня реклама, візуальна реклама та ін.);
- засоби маскультури (кіно, театри, концерти та ін.)

За регіональним розповсюдженням мас-медіа поділяються на [217, с.168]:

- транснаціональні (на міждержавному рівні);
- національні (в кордонах певного державного утворення);
- регіональні (окрема територіально-адміністративна зона);
- місцеві (прив'язані до конкретної місцевості – місто, район, село або окрема організація).

Здобутком XX ст. стало народження нового формату інформаційно-комунікаційних протистоянь, який отримав назву **кібервійна**. Останню розуміють як ***боротьбу сторін на рівні програмного забезпечення шляхом видобування закритої інформації та виведення з ладу програмно-апаратних засобів противника з метою отримання суттєвих переваг у економічних, політичних та військових протистояннях*** [152, с. 38]**.**

Головними діючими особами в такій війні є спеціальні фахівці: **хакери** (ті, що видобувають інформацію) та **кракери** (ті, що псують програмно-апаратні засоби).

У форматі кібервійни визначаються наступні види [152, с. 38]:

- вандалізм – псування інтернет-сторінок, зміна змісту негативними або пропагандистськими матеріалами;

- пропаганда – поширення звернень, що закликають до певних дій, або розміщення відповідної інформації на чужих інтернет-майданчиках;
- збирання інформації – зламування сторінок приватних осіб або окремих організацій для отримання закритої інформації
- від втручання в роботу програмно-апаратного забезпечення – dDoss атаки на комп'ютери, що виконують адміністративно-контрольні функції в державних, громадських, військових та комерційних організаціях;
- атаки на мережеву інфраструктуру – напад на комп'ютери, що контролюють життєдіяльність міст, зокрема телефонних ліній, водопостачання, електропостачання, пожежної безпеки, транспортного сполучення та ін.

З народженням інтернет-технологій web 2.0 формується новий напрямок інформаційних конфліктів – **мережева війна**. Це поняття містить таке визначення, як: ***інформаційно-комунікаційне протистояння у форматі оф-лайн та он-лайн мережевих структур.***

Типовими **оф-лайн мережевими структурами** вважаються ***організації або тимчасові/ситуативні об'єднання індивідуумів на основі спільної діяльності або загальних інтересів***.

До **он-лайн мережевих структур** відносяться ***інтернет-ресурси формату WEB 2.0-3.0 – віртуальні соціальні мережі*** (VKontakte, Facebook та ін.).

Провідне значення в теорії, методології та методиці ведення сучасних інформаційних війн посідає поняття **гібридна війна**. Таку війну розуміють, як: ***засіб протистояння, який поєднує в собі комплекс різноманітних інструментів політичного, економічного, військового та ідеологічного характеру***. Іноді для визначення цього явища застосовують такий термін, як:

асиметрична війна. Це визначення підкреслює та визначає нетрадиційний специфічний креативний характер протистояння, що відбувається за допомогою нестандартних комбінованих стратегії та тактики ведення конфлікту. Під час такої війни ресурси та характер дій противників відрізняються один від одного. Головна мета – шляхом певної концентрації компенсувати недостатність ресурсів і можливостей однієї із сторін або отримання суттєвої переваги по конкретному напрямку в рамках конфлікту.

Полем застосування інструментів гібридної/асиметричної війни є: населення конфліктної зони, тилове населення, міжнародна спільнота.

Формат ведення такого виду війни:

- громадські заворушення – акції громадської непокори, демонстрації, блокування, вуличні зіткнення;
- повстання – відкритий військовий виступ проти офіційної влади;
- партизанський рух – прихований збройний опір офіційній владі;
- тероризм – організація та здійснення гучних вбивств, підривання транспортних засобів, споруд, місць масових соціальних контактів (он-лайн та оф-лайн);
- громадянська війна – військові дії між прихильниками різних ідеологічних, територіальних або національних груп у межах однієї держави.

1.3. Українське законодавство в галузі інформаційної політики та безпеки

1.3.1. Нормативно-правові акти, що прямо регулюють питання інформаційної безпеки

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». Зазначений нормативно-правовий акт визначає правові

основи організації та діяльності Державної служби спеціального зв’язку та захисту інформації в Україні [14]. В Законі встановлюються правила, принципи підготовки повідомлення, зберігання передання інформації, системи доступу до певних типів інформації та умови зберігання пов’язаною з цим державної таємниці.

Закон України «Про державну таємницю». Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України [11].

Закон України «Про доступ до публічної інформації». Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [13].

Закон України «Про електронні документи та електронний документообіг». Цей Закон встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів [16].

Закон України «Про засади державної мовної політики». Зазначений нормативно-правовий акт регулює основи мовної політики в Україні, специфіку та особливості використання української мови як державної та мов національних меншин у територіальному та культурному аспектах [17].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [12].

Закон України «Про захист персональних даних». Зазначений Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав та свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з

обробкою персональних даних. Поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться в картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [9].

Закон України «Про інформацію». Базовими положеннями цього нормативно-правового акту закріплюється право громадян на інформацію, закладаються правові основи інформаційної діяльності. Ґрунтуючись на Декларації про державний суверенітет України та Акті проголошення незалежності, Закон стверджує інформаційний суверенітет України і визначає правові норми міжнародного співробітництва в галузі інформації [2].

Закон України «Про наукову і науково-технічну експертизу». Закон визначає правові, організаційні і фінансові основи експертної діяльності в науково-технічній сфері, а також загальні основи і принципи регулювання суспільних відносин у галузі організації та проведення наукової та науково-технічної експертизи з метою забезпечення наукового обґрунтування структури і змісту пріоритетних напрямів розвитку науки і техніки, наукових, науково-технічних, соціально-економічних, екологічних програм і проектів, визначення напрямів науково-технічної діяльності, аналізу та оцінки ефективності використання науково-технічного потенціалу, результатів досліджень [15].

Закон України «Про Національну систему конфіденційного зв'язку». Зазначений нормативно-правовий акт регулює суспільні відносини, пов'язані із створенням, функціонуванням, розвитком та використанням Національної системи конфіденційного зв'язку [18].

Закон України «Про основи національної безпеки України». Цей Закон відповідно до пункту 17 частини першої статті 92 Конституції України визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності [19].

Закон України «Про підтвердження відповідності». В Законі визначаються правові та організаційні засади підтвердження відповідності продукції, систем якості, систем управління якістю, систем екологічного управління, персоналу та спрямований на забезпечення єдиної державної технічної політики у сфері підтвердження відповідності [20].

Закон України «Про радіочастотний ресурс України». Цей Закон встановлює правову основу користування радіочастотним ресурсом України, визначає повноваження держави щодо умов користування радіочастотним ресурсом України, права, обов'язки і відповідальність органів державної влади, що здійснюють управління і регулювання в цій сфері, та фізичних і юридичних осіб, які користуються та/або мають намір користуватися радіочастотним ресурсом України [21].

Закон України «Про телекомунікації». Закон встановлює правову основу діяльності в сфері телекомунікацій. Визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних та юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами [7].

1.3.2. Нормативно-правові акти, що опосередковано регулюють питання інформаційної безпеки

Конституція України. В ст. 10, 17, 31, 32, 34, 40, 50 регулюються загальні положення щодо свободи слова та висловлення думки, можливості отримання та розповсюдження інформації, міжособистого та міжгрупового спілкування та ін. [1].

Закон України «Про друковані засоби масової інформації (пресу) в Україні». Закон створює правові основи діяльності друкованих засобів масової інформації в Україні, встановлює державні гарантії їх свободи відповідно до Конституції України, Закону України «Про інформацію» та інших актів

чинного законодавства і визнаних Україною міжнародно-правових документів [3].

Закон України «Про телебачення та радіомовлення». Закон регулює діяльність телерадіоорганізацій та території України, визначає правові, економічні, соціальні, організаційні умови їх функціонування, спрямовані на реалізацію свободи слова, права громадян на отримання повної, достовірної та оперативної інформації, на відкрите і вільне обговорення суспільних питань [4].

Закон України «Про систему Суспільного телебачення і радіомовлення України». Нормативно-правовий акт, що регулює питання створення та діяльності суспільних засобів масової інформації – телебачення та радіомовлення. Зазначені ЗМІ мають статус незалежних структур, діяльність яких контролюється Громадською радою, до її складу залучаються відомі та незалежні громадські діячі та профільні фахівці [22].

Закон України «Про інформаційні агентства». Закон регулює порядок реєстрації, формування та практичної діяльності національних інформаційних агенцій та представництв іноземних агенцій. Також визначаються формати та порядок розповсюдження інформаційної продукції в Україні (національна та іноземні агенції) та закордоном (національних агенцій) [5].

Закон України «Про науково-технічну інформацію». Закон визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу. Мета цього нормативно-правового акту - створення в Україні правової бази для одержання та використання науково-технічної інформації [23].

Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації». Закон відповідно до Конституції України визначає порядок всебічного і об’єктивного висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації і захисту їх від

монопольного впливу органів тієї чи іншої гілки органів державної влади або органів місцевого самоврядування, є складовою частиною законодавства України про інформацію [8].

Закон України «Про рекламу». Закон визначає засади рекламної діяльності в Україні, регулює відносини, що виникають у процесі виробництва, розповсюдження та споживання реклами. Особливої уваги заслуговує ст. 12, присвячена соціальній рекламі, правилам її використання та тематичному наповненню соціальних інформаційних послань [6].

Закон України «Про видавничу справу». Закон визначає загальні засади видавничої справи, регулює порядок організації та провадження видавничої діяльності, розповсюдження видавничої продукції, умови взаємовідносин і функціонування суб'єктів видавничої справи. Відповідно до Конституції України цей Закон покликаний сприяти розвитку національної культури, захисту прав та інтересів авторів, видавців, виробників, розповсюджувачів і споживачів видавничої продукції [10].

Закони України «Про Національну програму інформатизації» та «Про Концепцію Національної програми інформатизації». Закони визначають загальні засади формування, виконання та корегування Національної програми інформатизації. Остання в свою чергу передбачає створення в Україні сучасного інформаційного суспільства, заснованого на організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесах, що спрямовані на створення умов для задоволення інформаційних потреб, реалізації прав громадян і суспільства на основі створення, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, створених на основі застосування сучасної обчислюваної та комунікаційної технік [24].

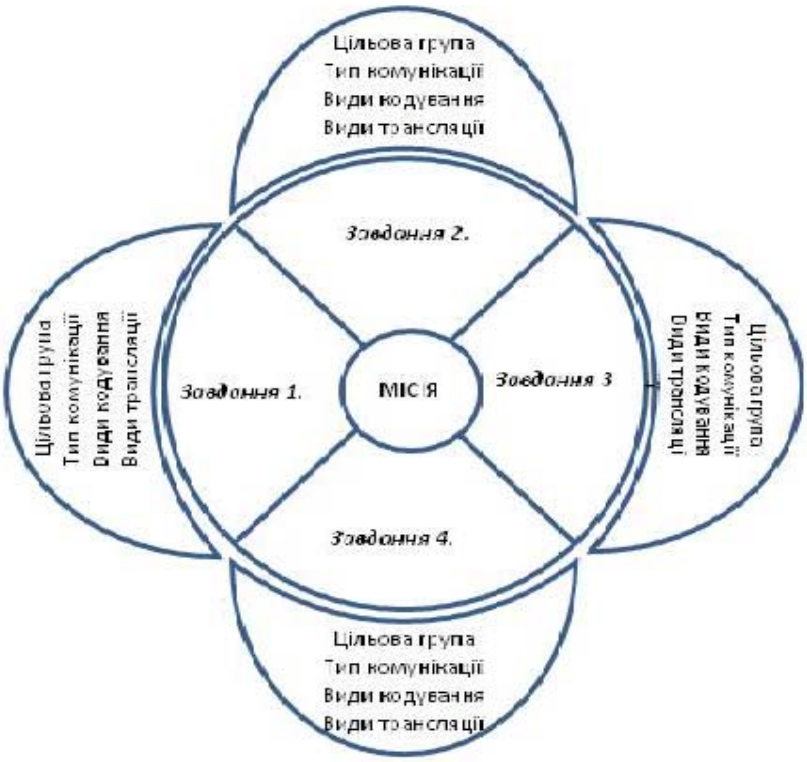
РОЗДІЛ 2. Стратегія та тактика інформаційної війни

2.1. Стратегічне та тактичне планування інформаційних протистоянь

2.1.1. Стратегічний рівень планування інформаційні процесів

Перший рівень – **СТРАТЕГІЯ.** Цей рівень позначає базові напрямки та орієнтири, а також певні умови і характеристики комунікаційних процесів (табл. 2.1).

Мал.2.1. Алгоритм стратегії



Перший крок - визначення **мети**, що може висловлюватися в таких варіантах, як [214, с. 43]:

1. ***Консолідація*** – необхідність сприяння об'єднанню представників цільових груп задля вирішення певних завдань. Така мета може мати місце у ситуації, коли потрібно мобілізувати суспільство в умовах військової агресії,

протидії певним обставинам або силам внутрішнього характеру для вирішення екологічних, соціальних або економічних проблем.

Практичні приклади.

Класичним прикладом ситуації, коли необхідно застосовувати консолідаційний підхід – боротьба із російською агресією (2014-2015 рр.) При цьому слід зазначити, що у випадку з цими подіями консолідаційна стратегія України формувалася переважно стихійно через механізми самоорганізації суспільства, його найбільш активної частини. Громадськість одразу визначила свої пріоритети та висловила їх у соціальних мережах. Замість розгубленості сформувався активний волонтерський рух. Відбулося згуртування навколо традиційних українських цінностей, національна символіка набула шаленої популярності, а гімн став чи не найбільшим хітом. Ініціаторами такого руху в соцмережах стали окремі користувачі та відомі блогери, що дуже швидко об'єдналися у тематичні групи, в яких оперативно обмінювалися інформацією щодо волонтерських справ, розвінчання фейкової та поширення об'єктивної інформації про події на фронті.

2. ***Заспокоєння*** - потреба в зниженні суспільного напруження, агресії, незадоволення представників певних цільових груп або суспільства в цілому. Зазначена мета виникає у разі виникнення внутрішніх несприятливих умов соціально-економічного або політичного розвитку, а також за умови зовнішнього намагання підбурення населення до проявів незадоволення.

Практичні приклади.

Унаслідок внутрішньополітичної економічної кризи та зовнішньої агресії протягом 20014-2015 рр. суттєво зросли настрої протесту в українському суспільстві. Цією обставиною дуже активно намагалися скористуватися зовнішні противники, які за алгоритмами гібридної війни створювали штучні кризові ситуації, що призводили до напруження в

суспільстві та виникнення громадських протистоянь. Головна теза опонентів – в Україні відбувається громадянська війна. Натомість українське мережеве суспільство інстинктивно, а певні профільні державні структури, громадські об'єднання та окремі блогери цілеспрямовано поширювали матеріали, що вказували на перспективи, створювали позитивний заспокійливий вірусний контент, сприяли формуванню національної свідомості та патріотизму, а також актуалізували демократичні цінності з акцентом на європейську інтеграцію.

3. ***Залякування*** – необхідність викликати невпевненість чи острах серед певних соціальних груп, у суспільстві в цілому, по відношенню до певних викликів або загроз. До такого підходу вдаються в разі необхідності припинення розвитку процесів сталого соціально-економічного або політичного розвитку. Це є, в переважній більшості випадків, ознакою прихованої інформаційно-психологічної агресії. Рідше ця мета може мати стримуючий характер або при необхідності дезорієнтації суспільства.

Практичні приклади.

Саме таку стратегію – на залякування російськомовного населення Криму та Сходу України перед загрозою націоналістичної агресії з боку політичних організацій «Правий сектор» та «Свобода» застосувала Росія в 2014 р., на початку і впродовж перших етапів агресії. Такий підхід дозволив атакуючій стороні отримати максимально можливу підтримку місцевого населення та формальний привід для введення військового контингенту і надання усіх видів підтримки озброєним бандформуванням, так званих ДНР та ЛНР.

4. ***Невдоволення*** – необхідність виведення із стану рівноваги окремі соціальні групи або суспільство в цілому для формування настроїв протесту. У

такому випадку намагаються викликати відчуття дискомфорту щодо існуючих обставин або умов розвитку соціально-економічних чи політичних процесів, стимулюючи громадське невдоволення.

Практичні приклади.

Стратегія на викликання незадоволення в суспільстві українською владою впродовж 2014-2015 рр. була головною для сил, які здійснювали інформаційну агресію проти України. Критика рішень влади, поширення інформації про гіперболізовані факти корупції та порушення закону представниками політичної еліти мали на меті формування настроїв протесту в суспільстві та спонукання до реальних акцій громадської непокори.

5. ***Протести*** – публічні дії представників певних соціальних груп або найбільш активної частини суспільства спрямовані проти певних ситуацій, структур або окремих осіб. У такому разі відбуваються дії організовані конкретно або самоорганізовані, внаслідок яких може відбуватися зміна, трансформація або цілковите знищення певних соціальних інститутів, зміна ситуації, усунення певних осіб від керівництва соціально-економічними або політичними процесами.

Практичні приклади.

Стратегія орієнтована на підбурення певного контингенту до акцій протесту, громадських заворушень, терористичних актів. Класичним прикладом прояву успішної реалізації такої стратегії є хода 300-ти нацгвардійців військової частини, дислокованої в с. Нові Петрівці, на Київ 13 жовтня 2014 року. Останнє стало наслідком здійснення активної підривної роботи з боку російських спецслужб через соціальні мережі, зокрема через мережу «ВКонтакті». Через лідерів та найбільш активну частину згаданого підрозділу поширювалися настрої та інформація, що

викликала невдоволення військовослужбовців, і, зокрема, була поширена ідея про здійснення ходи протесту.

До першого стратегічного рівня також відноситься другий крок загального алгоритму – **завдання**, які конкретизують та уточнюють шляхи досягнення базової мети. Найбільш типовими завданнями, в рамках SMM-комунікацій, можуть бути наступні [203, с. 44]:

1. ***Підготовка контенту*** – створення інформаційного повідомлення, що має певну тематичну цільність та цінність. У такому разі контент може бути у вигляді графічного зображення, фото, відео, аудіо або текстового матеріалу, який може бути переданий за допомогою соціальних он-лайн мереж.

2. ***Поширення контенту*** – дії спрямовані на якомога широке розповсюдження певної інформації в середовищі конкретних соціальних груп або адресно – на конкретні персоналії.

3. ***Збирання контенту*** – процедура пошуку систематизації та аналізу певної цільової інформації з метою отримання певного бачення ситуації або передбачення певних ситуацій, що можуть мати місце за певних обставин.

Після визначення завдання, наступним логічним кроком є визначення **цільових груп**, по відношенню до яких передбачається вчинення певних комунікаційних дій. Серед них визначаються такі категорії визначення, як [214, с. 44]:

1. ***Стать*** – соціальна група, що формується за принципом статевої приналежності.

2. ***Вік*** – соціальна група, що формується за принципом вікової приналежності.

3. ***Соціальне положення*** – соціальна група, що об’єднує осіб за подібним соціальним положенням, як то: певний рівень прибутків, рід діяльності,

фізіологічні особливості (люди з особливими потребами), расові або етнічні чинники та ін.

4. ***Ситуативні соціальні групи*** – соціальні групи, що формуються за принципом тимчасового об'єднання навколо певної проблеми, ідеї, завдання і не враховують соціальні, вікові та статеві характеристики.

5. ***Персоналії*** – соціальні групи, які формуються з конкретних персон, що викликають зацікавленість у певних комунікаційних ситуаціях.

Четвертим рівнем є характер та зміст **меседжів**, що спрямовуються на визначені на попередньому етапі цільові групи. За своїм характером меседжі можуть:

1. ***Закликати*** - змушувати, спонукати їх отримувачів до певних дій або рішень.

2. ***Констатувати*** – фіксувати певний стан речей, ситуації або факти, що мають місце в певний момент часу.

2.1.2. Основи тактики планування інформаційних процесів

Другий рівень – **ТАКТИКА**. На цьому рівні визначаються конкретні інструменти та шляхи досягнення головної мети і вирішення завдань (табл.2.1). При цьому загальна алгоритмічна послідовність не переривається, а продовжується, зокрема у вигляді п'ятого кроку, який передбачає визначення **каналів комунікацій**.

У випадку роботи із соціальними мережами це, в першу чергу: Facbook, VKontakte, Odnoklassniki, Instagram, Linked In та ін.

Шостий крок передбачає визначення базових **засобів роботи**, серед останніх [214, с. 43]:

1. ***Робота на чужих майданчиках*** – розміщення власного контенту або збирання необхідної інформації на чужих інформаційних майданчиках. Такий

Табл. 2.1. Базовий алгоритм планування в SMM

СТРАТЕГІЯ		**МЕТА**
1	- консолідувати - заспокоїти - налякати - викликати невдоволення/гнів - закликати до протесту	
2	- створити контент - поширити контент - зібрати контент	**ЗАВДАННЯ**
3	- стать - вік - соціальна страта - ситуативне об'єднання - персоналії -	**ЦІЛЬОВІ ГРУПИ**
4	- закликати - констатувати	
ТАКТИКА		**МЕСЕДЖИ**
5	- Facbook - VKontakte - Odnoklassniki - Instagram - Linked In - Ін.	**КАНАЛИ КОМУНІКАЦІЇ**
6	- на чужих майданчиках - на власних майданчиках - симбіоз власні/чужі	**ЗАСОБИ РОБОТИ**
7	- Створення та промоція співтовариств бренду - Промоція у нишевих соціальних мережах - Створення та розвиток власних інформаційних майданчиків - Промоція контенту - Промоція інтерактивних акцій - Створення та промоція інтерактивних елементів - Робота з лідерами думок - Вірусний маркетинг - Персональний брендинг - Інструменти без категорій - Комунікативна активність - Рейтинги та ТОПи	**ІНСТРУМЕНТИ**
8	- моніторинг - SMM-аудит - опитування	**МЕТОДИ КОНТРОЛЮ**

підхід застосовується у разі, коли необхідно приховати джерело розповсюдження контенту або непомітно для об'єкта дослідження отримати корисну інформацію. Іноді розповсюдження контенту на чужих майданчиках здійснюється із зазначенням адресата – так званий «партизанський маркетинг».

2. ***Робота на власних майданчиках*** – розміщення власного контенту та залучення до співпраці певної цільової групи або персоналій на власних інтернет-ресурсах. У такому разі в певних соціальних мережах створюються тематичні інформаційні майданчики (сторінки, групи, акаунти, події та ін.) відповідно до інтересів, потреб та запитів цільових груп або окремих персоналій, увагу яких необхідно привернути.

3. ***Поєднання роботи на своїх та чужих майданчиках*** – комплексне суміщення роботи на власних та чужих майданчиках, що передбачає проведення складних комунікаційних кампаній, орієнтованих на широке коло цільових груп та персоналій.

Сьомий крок – визначення найбільш типових базових інструментів комунікаційної діяльності у Web 2.0-3.0.

2.2. Ідеологічні аспекти та психологія сучасної інформаційної он-лайн мережевої війни

2.2.1. Ідеологія та процеси створення меседжів в інформаційних кампаніях

Базовою складовою частиною процесів інформаційних протистоянь є ідеологія, яка втілюється у вигляді певних меседжів і реалізується за допомогою прикладних методів агітації та пропаганди.

Для успішної реалізації коротких та довготривалих планів у рамках інформаційної війни важливе значення має системність формування

ідеологічних складових. Інакше кажучи, потрібно розробити чітку ієрархію в ідеологічному контексті, яка буде складатися із **місії**, **візії** та ситуаційних ідеологічних установок [217, с.83-84].

При цьому ***місію*** розуміють ***як головну мету, в якій закладається сенс існування та соціальної активності конкретного об'єкта або суб'єкта комунікації*** [217, с.83]**.** Вона є одним з складових елементів стратегічного управління. Саме на основі місії визначається стратегія та позначаються базові основи інформаційно-комунікаційних процесів, що мають застосовуватися в рамках роботи. Місія орієнтується на чітко визначені цільові групи та враховує характери та специфіку інформаційного поля, в межах якого вона буде діяти.

Конкретизація місії здійснюється у вигляді візії або головних завдань, які стоять перед комунікатором або комунікантом. У такому разі візія визначається ***як добірка ідеологічних орієнтирів та напрямків комунікаційних процесів, які використовуються для досягнення мети, сформульованої у місії*** [217, с.83]**.**

Вже на основі місії та візії розробляється система оперативних ідеологічних постулатів, що складається з базового меседжа (адаптований варіант місії) та тематичних меседжів (візія, головні завдання) [217, с.84].

При цьому, в плані управління меседжами встановлюється певна чітка ієрархія. Головний меседж несе в собі ключовий інформаційний посил, який розкривається тематично або в розрізі конкретних цільових груп. У такому разі спрямованість меседжів на цільові групи або на теми є ситуативним рішенням, яке залежить від певної комунікаційної ситуації, або конкретних завдань, які необхідно виконати.

Під час розроблення відповідних агітаційних матеріалів активно використовуються зрозумілі для цільової аудиторії образи, символи, цінності, що виступають в якості обгортки, під якою подаються головні меседжі. При підготовці до здійснення прихованої інформаційної атаки до зазначених дій додається ще завдання із маскування цих меседжів.

Для того, щоб ідеї, образи, інформаційні посили чітко відпрацьовували на досягнення поставлених завдань, необхідно враховувати специфіку та особливості соціально-психологічного портрету цільових груп.

Важливим чинником успіху роботи із цільовими групами є відповідь на ключові питання, які дадуть можливість скласти відповідні характеристики [217, с.84-85]:

- Які конкретно соціальні групи є важливими для реалізації завдань (розставити за рівнем пріоритетності)?
- Яким є типовий портрет представника конкретної цільової групи?
- Які уподобання мають представники конкретних цільових груп?
- Яка мотивація спрацьовує по відношенню до представників конкретних цільових груп?
- Хто є безумовними або відносними (по ситуації) авторитетами для представників конкретних цільових груп?
- Які образи, символи, аудіо-візуальні інструменти будуть дієвими в роботі з конкретними цільовими групами?
- Де і на яких комунікаційних майданчиках можна знайти представників конкретних цільових груп (портали, сайти, блоги, соцмережі та ін.)?

Відпрацювавши зазначені питання із комплексної ідентифікації цільових груп та їх представників, можна переходити до вибору символів та образів (свідомі та підсвідомі), що стане основою для відповідного контенту та характеру інформаційних повідомлень. У подальшому до процесу роботи підключають специфічні психотехнології.

2.2.2. Сучасні психотехнології в он-лайн інформаційних війнах

Чітке формулювання ідей, меседжів та кодування їх у відповідному форматі (текст, відео, графіка, фото) стає вістрям, своєрідним проникаючим елементом інформаційного тарану, який б'є по свідомості конкретних цільових груп. У цьому контексті важливим компонентом є психологічні методики програмування, маніпулювання та блокування людської свідомості, серед яких особливе місце посідають такі, як: наприклад, **бойове НЛП**.

НЛП визначається ***як техніка моделювання вербальної та невербальної поведінки людей за допомогою поєднання форм мовлення, руху очей, тіла та пам'яті*** [152, с. 29]. Відповідно бойове НЛП застосовує ці методи з метою нанесення максимальної шкоди протилежній стороні.

З точки зору теорії і практики НЛП базовим інструментом в досліджуваній темі є **інформаційна зброя**. Останню визначають, як ***сукупність засобів, методів, способів та технологій інформаційно-психологічного впливу, спеціально створених для прихованого та явного управління інформаційним середовищем противника, процесами й системами, що функціонують на основі інформації, а також для нанесення їм невиправної шкоди*** [152, с.17].

Основним управлінським процесом визначається **інформаційний вплив** – ***цілеспрямоване виробництво і розповсюдження спеціальної інформації, яка здійснює безпосередній вплив (позитивний чи негативний) на функціонування та розвиток інформаційно-психологічного середовища держави, психіку та поведінку політичної еліти, населення*** [152, с.33].

На думку профільних фахівців у форматі інформаційної війни, в тому числі формату web 2.0, можуть бути застосовані такі технології НЛП, як [152, с. 157]:

- якоріння, мета моделювання (відновлення мапи реальності);
- субмодальності (перефарбування дійсності);

- шкалювання (порівняння по принципу «більше-менше», «занадто-замало»);
- структуризація результату (хто, що, куди, як);
- переривання ланцюга громадської думки (техніка «замаху» та спіндокторінг);
- подолання/створення фобій;
- вирішення/актуалізація інформаційного конфлікту;
- створення майбутнього (ймовірного та неймовірного);
- внесення змін у минуле (пам'ять про небувальщину);
- реімпринтинг формату (переформатування минулих травм);
- перекодування міфів (швидка зміна переконань);
- побудова системи цінностей (ідеологічне щеплення та перекодування);
- подолання/створення внутрішнього конфлікту.

Особливе місце в практиці бойового НЛП відводиться технологіям гіпнотичного характеру, тобто таким, що впливають на підсвідомість і мають більш серйозні наслідки ніж звичайні форми агітації та пропаганди.

За своєю сутністю, **гіпнотичні методи** – ***технології зміни стану свідомості, що поєднують у собі ознаки одночасно неспання, сну і сну із сновидіннями.*** Гіпнотичний транс дозволяє співіснувати одночасно взаємовиключним станам свідомості [152, с.285].

Для здійснення масового гіпнотичного трансу традиційно застосовуються ритмізовані дії, світлові та шумові ефекти, колективне співання. Це можуть бути масові театралізовані заходи, мітинги, масштабні ходи, народні віче та ін. [152, с.285].

Застосування таких технологій в інтернет-просторі дає можливість масового трансу фактично у планетарних масштабах, не кажучи про те,

наскільки легко таким чином охоплювати окремі країни чи території [152, с.286].

Наслідком застосування таких методів є спалахування серед широких мас населення стану **масового психозу**. Останній визначається ***як своєрідна психічна епідемія, в основі якої лежать наслідування та навіювання.***

Масовий психоз вражає соціальні групи або ситуативно сформований натовп. У наслідок цього люди втрачають свідому можливість і здатність до раціонального мислення та нормального оцінювання ситуації. Це робить людину одержимою і керованою з боку того, хто застосовує зазначені методи [152, с.286].

Важливою складовою частиною роботи із масової підсвідомістю є таке явище, як **троп** – ***риторичний образ, слово або вислів, що використовується у переносному значенні з метою підсилення контенту***. Тропи активно використовуються у літературних творах, публічних виступах, повсякденному спілкуванні, в матеріалах ЗМІ. Основними різновидами троп є: *метафора, метонімія, синекдоха, фразеологізм, гіпербола, дисфемізм, каламбур, літота, порівняння, перифразування, алегорія, уособлення, іронія, пафос, сарказм, евфемізм, мейозис* [152, с.288].

Приміром, для сучасної Росії такими тропами є: «ведмідь», «орда», «русский мир». В Україні до традиційних троп можна віднести такі речі, як: «козак», «воля», «Дніпро». Нещодавно для нас цей список розширився за рахунок таких, як: «Майдан», «АТО», «Правий Сектор».

При застосуванні у соціальних мережах такі тропи вставляються у тексти та іноді використовуються у вигляді хештегів. Найбільш популярними хештегами, в рамках україно-російської інформаційної війни, сьогодні стали такі, як: **#КрымНаш**, **#НяшМяш**, **#ВизиткаЯроша, #RussiaInvadedUkraine, #Снегири, #Двараба, #РаспятыйМальчик** та ін.

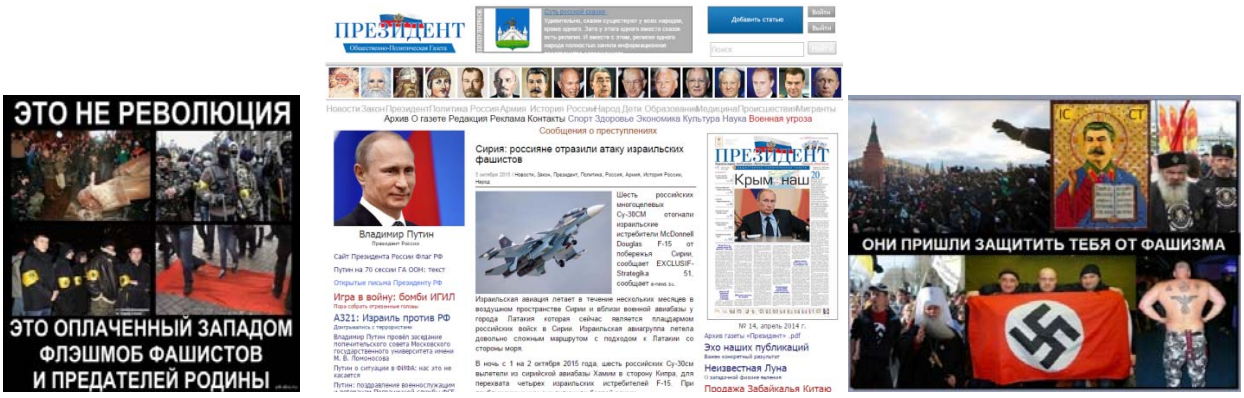
Найбільш активно зазначені вище технології застосовують сьогодні в полі діяльності **пропаганди**. Професійна пропаганда, в форматі інформаційної

війни, може бути визначена як ***практика застосування спеціальних форматів, видів, засобів, каналів та технологій соціально-психологічного впливу для перебудови чи укріплення існуючої системи суспільно-політичних поглядів, світогляду людей*** [152, с.34].

Серед основних методів пропагандистської роботи визначають:

Навішування ярликів (Name-calling) - застосування при згадуванні противника негативних епітетів («фашисти», «каратели», «нацисти», «кати»).

Мал.2.2. Пропагандистські ярлики



http://www.prezidentpress.ru/news/3482-siriya-rossiyane-otrazili-ataku-izrailskih-fashistov.html

Узагальнення (Glittering generalities) – асоціювання інформаційного повідомлення із певними типовими цінностями. Зазначені цінності мають бути універсальними та актуальними для різноманітних соціальних груп. В якості прикладу можна розглянути той факт, що путінські ЗМІ подають інформацію про те, що російські бойовики в Донбасі – це інтернаціоналісти, захисники «русского мира» та ін.).

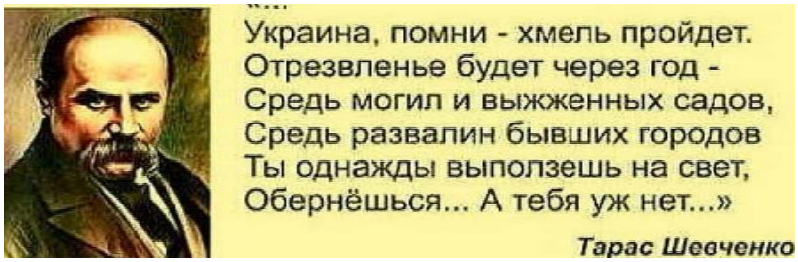
Мал.2.3. Узагальнення в агітаційному процесі

Перенесення (Transfer device) – позиціонування власного повідомлення на фоні широко відомої події, явища, особи. В такому разі розбудовується чіткий асоціативний ряд, який дозволяє авторам повідомлення посилювати власні позиції та меседжі, паразитуючи на більш відомих достовірних або історичних явищах. Класичний приклад такої технології меседжі-слогани типу: «діди перемогли фашистів, ми переможемо націоналістів» та ін.

Мал.2.4. Технології узагальнення

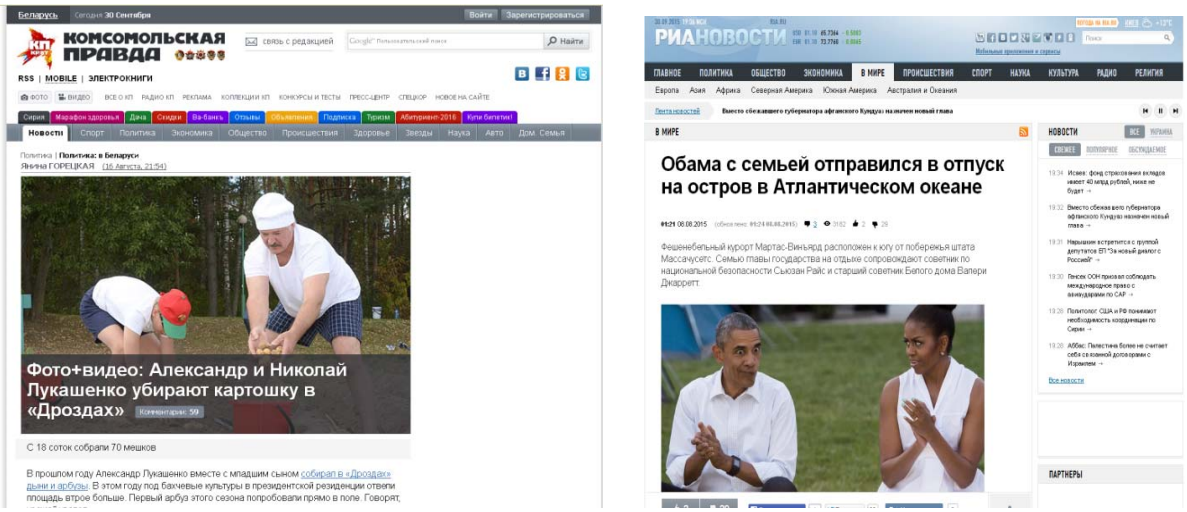
Засвідчення (Testimonial) – посилання на думку, свідоцтво або коментарі особи, що є лідером громадської думки для певних цільових аудиторій. Таким чином, інформаційне повідомлення паразитує на іміджі конкретної особи. При цьому маємо зазначити, що доволі часто позиція або думка такої особи виявляється фейковою.

Мал.2.5.Метод засвідчення



Вирівнювання (Plain folks) – представлення лідерів у розрізі звичайних понять, «він з народу», «він читає такі ж газети, як і ми», «він працює на городі» та ін. Останній прийом доволі активно використовується в країнах із напівдемократичними режимами, де певний політичний лідер ще не отримав статус недоторканого і має завойовувати прихильність електорату кожного разу під час перевиборів.

Мал.2.6. Метод вирівнювання



Як варіант цього прийому існує практика підвищення статусу лідера та перетворення його у супергерої. В такому разі образи керманичів у ЗМІ подаються у вигляді пілотів, мисливців, міцних чоловіків, розумних керівників та ін.

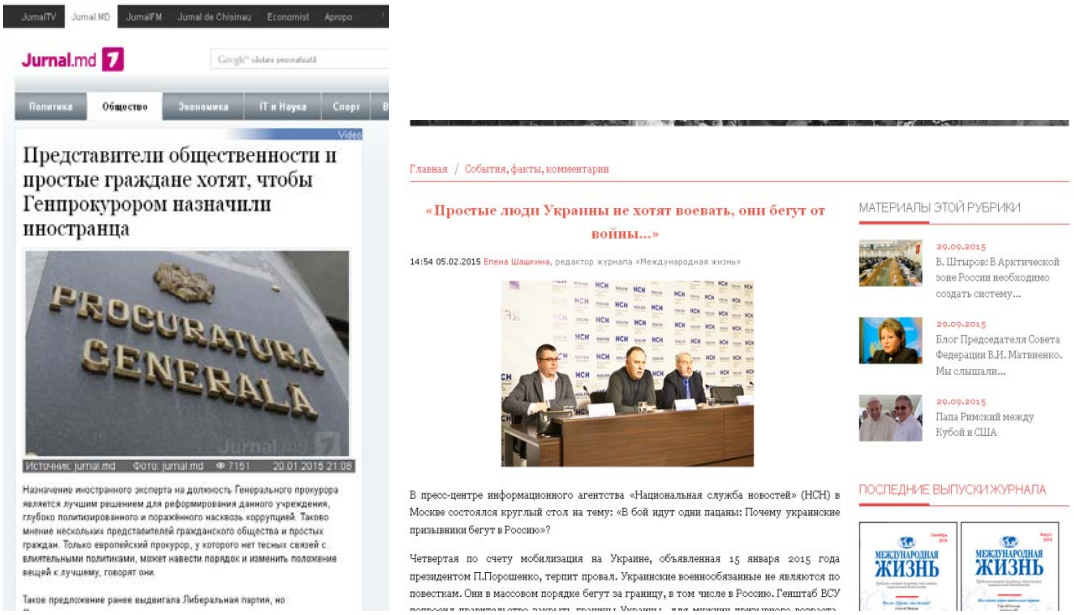
Мал.2.7. Метод підвищення

Несподіванка (Card stacking) – використання фактів, символів та образів, що є несподіванкою для певної ситуації або цільових груп. Такий прийом є характерною ознакою інформаційно-психологічної війни другого покоління та відноситься до категорії асиметричних дій. Доволі часто такі несподіванки будуються на алогічних рішеннях та діях.

Мал.2.8.Застосування несподіваних повідомлень

«Заскакування на воза» (Bandwagon) – апеляція або звернення до думки загальної маси, поглядів та переконань широких верств суспільства. Такий прийом є класичною ознакою інформаційної війни другого покоління і реалізується на принципах симулякрів – гри в демократичний процес або його імітацію. Він застосовується для виправдання певних дій та рішень представників політичних еліт або керівництва держави, трактуючи їх як реалізацію народного волевиявлення. Таким було обґрунтування кремлівською владою рішення про анексію Криму або надання допомоги фейковим республікам «ДНР» та «ЛНР».

Мал.2.9. «Заскакування на воза» в агітаційних матеріалах



Висміювання **–** висвітлення в комічному аспекті національних лідерів або певних історичних подій, що є знаковими для противника. В основі цього прийому лежить принцип висміювання проблеми, що призводить або до нивілювання загрози або до приниження противника. Таким чином, реалізується класичний принцип – те, що комічне, не лякає. Саме за таким принципом формувалась протягом 2014-2015 рр. система інформаційного захисту в соціальних он-лайн мережах в Україні проти російської агресії.

Мал.2.10. Висміювання національного лідера

Практичний приклад

Класичним прикладом ефективності використання таких технологій є результат застосування Росією інформаційно-психологічних методів для обробки населення Півдня та Сходу України з метою забезпечення умов для здійснення результативної військово-політичної агресії та захоплення зазначених територій.

Фактично інформаційно-психологічна війна Росії проти України на Сході та Півдні нашої країни розпочалася з перших днів незалежності. То затихаючи, то активізуючись, вона безсистемно продовжувалася фактично до серпня 2008 р. (п'ятиденна війна в Грузії). Саме з цього моменту починається комплексна, системна підготовка до майбутньої агресії з розробкою конкретних кроків, створення відповідних організаційних структур [413].

Одним з ключових напрямків роботи, яка здійснювалася російською стороною, є закладання певних психологічних установок, активізація яких мала привести до соціального вибуху, в межах певних територіальних груп. Серед таких установок були:

- *захист права на використання російської мови;*
- *загроза українського національного радикалізму;*
- *нерозривність культурних зв'язків з Росією;*
- *економічна необхідність співпраці з Росією;*
- *зазіхання країн ЄС та США на цілісність України.*

Згідно з попереднім задумом, після досягнення необхідного психологічного ефекту (впровадження установок), у потрібний час, передбачалася активація закладених «психологічних мін» шляхом запуску в ЗМІ та на рівні чуток певних тем. Останнє викликає суспільний резонанс та спонукає до певних дій, на які розраховує атакуюча сторона.

Зазначені установки протягом багатьох років закладалися на свідомому та підсвідомому рівнях у мешканців Сходу та Півдня України, за допомогою

всього спектру інструментів інформаційного впливу (ЗМІ, література, кіно, неформальні комунікації та ін.). У 2004 р. пройшла перша обкатка та випробування – ініціювання створення так званої Південно-Східної Української автономної республіки (Донецька та Луганська обл.) та території самоврядування «Новороссийский край» (Одесская обл.).Тоді довести до завершення атак не вдалося через певну неготовність російської сторони та недостатню глибину ситуації протесту. В 2014 р. готовність російської сторони була більш високою, а ситуація більш сприятливою для розв'язання повномасштабної інформаційно-психологічної.

2.3. Ситуативне планування інформаційних он-лайн процесів

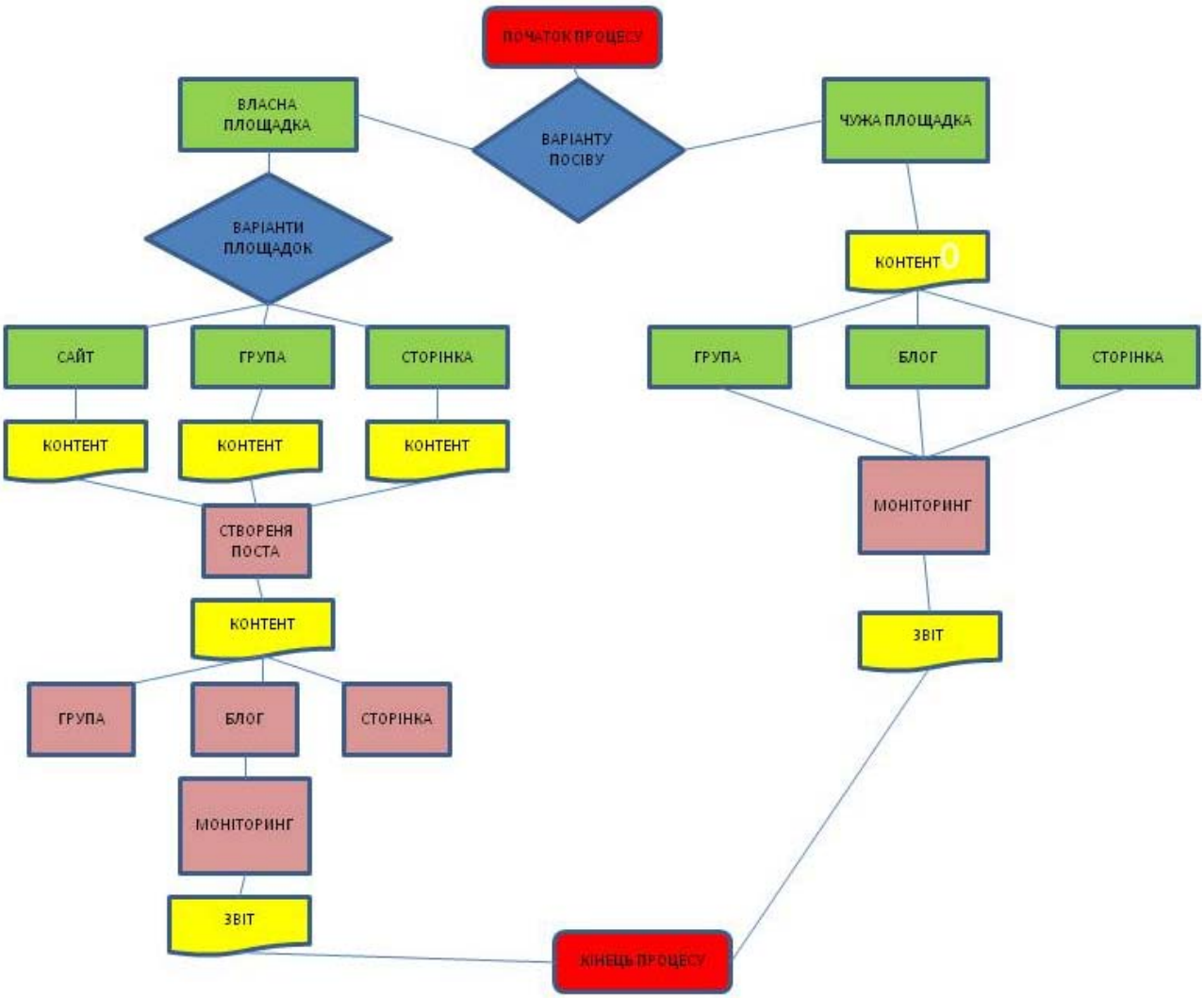
2.3.1. Алгоритмізація та формалізація процесів

Для систематизації та оптимізації процесів створення і поширення інформації в форматі віртуальних інформаційно-психологічних конфліктів, найбільш ефективним засобом є стандартизація інформаційно-комунікаційних процесів шляхом **алгоритмізації** процедур прийняття відповідних рішень та їх реалізації.

Базовим алгоритмом у такому разі може бути схема, що складається з двох варіантів рішень та відповідних до них етапів реалізації (мал. 2.11).

Перший варіант рішення – обрання варіанта поширення контенту з власного майданчика. В такому разі контент розміщується на власному сайті, в групі або на сторінці у соціальній мережі, де автор є модератором. Розміщений на такому майданчику контент складає основу для постів, що потім розміщуються вже на чужих площадках – групах (пост або в коментарях), блогах (у коментарях), сторінках (пост або в коментарях). Після розміщення зазначеного контенту здійснюється моніторинг результатів та складається звіт.

Мал. 2.11. Базовий алгоритм поширення контенту



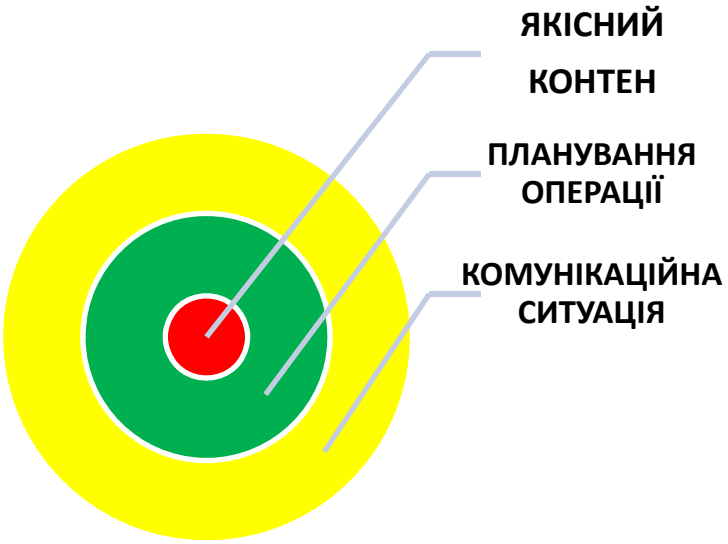
Другий варіант рішення – передбачений для поширення контент розміщується одного разу на чужих майданчиках. У такому разі, це в групах (пост або в коментарях), блогах (в коментарях), сторінках (пост або в коментарях). Після розміщення зазначеного контенту здійснюється моніторинг результатів та складається звіт.

Зазначена схема в цілому спрощена і розкривається у подальшому в конкретних рішеннях та кроках.

2.3.2. Структура та ключові умови реалізації інформаційних операцій

Головними складовими частинами успішної інформаційної операції або кампанії є: **комунікаційна ситуація**, **планування** та **контент** [206, с. 152].

Мал.2.12. Базові умови інформаційної операції



Оцінюючи комунікативну ситуацію, під час планування операції необхідно врахувати такі аспекти:

- інформація має бути актуальною та профільною для цільових груп, на які вона спрямовується;
- інформація має подаватися саме в той час, коли вона отримає максимального поширення, який не погасить інший більш потужний інформаційний привід або подія;
- для спрощення комунікації, інформація має бути викладена зрозумілою для цільових груп мовою (стиль, ключові слова, поняття, образи, символи).

Мал.2.13. Алгоритм інформаційної операції 2.0-3.0

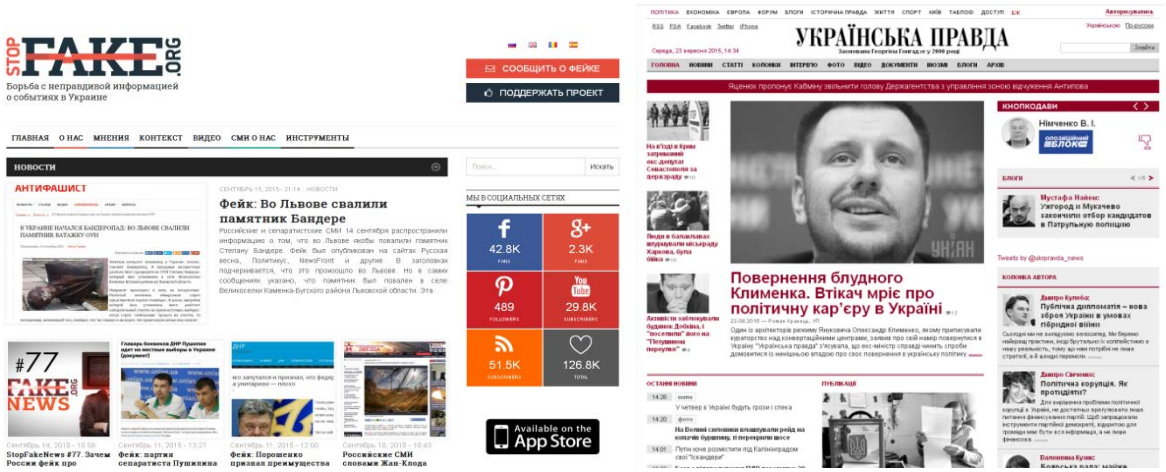
Базовий алгоритм проведення операції або планування передбачає п’ять послідовних етапів:

1. Підготовка майданчика. Зазвичай пост для розміщення в соціальних мережах базується або на унікальному контенті (власні фото, відео, текст) або на посиланні на інший ресурс (сайт, чужий акаунт та ін.). У першому випадку це доцільно давати на розкручених акаунтах або в групах за авторства розкрученого блогера.

За потреби анонімності або при недостатній популярності автора в основу краще всього закласти посилання на контент з розкрученого інтернет-майданчика. До таких можна віднести:

Сайти інтернет-видань – веб-сторінки інформ-агенцій, друкованих видань, радіо або телевізійних каналів.

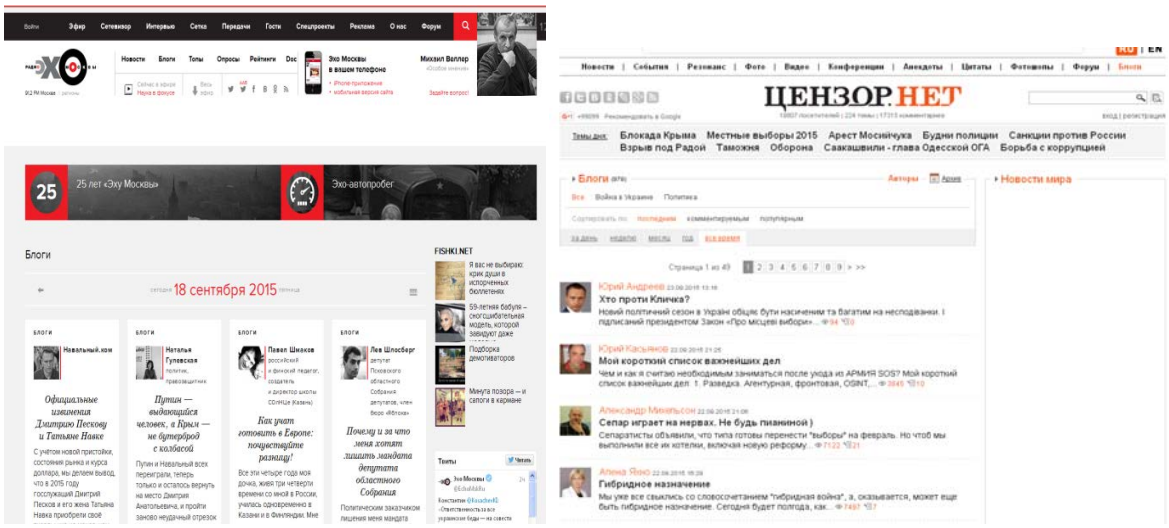
Мал.2.14. Тематичні сайти



http://www.stopfake.org http://www.pravda.com.ua/

Блоги – авторські сторінки на інтернет-порталах.

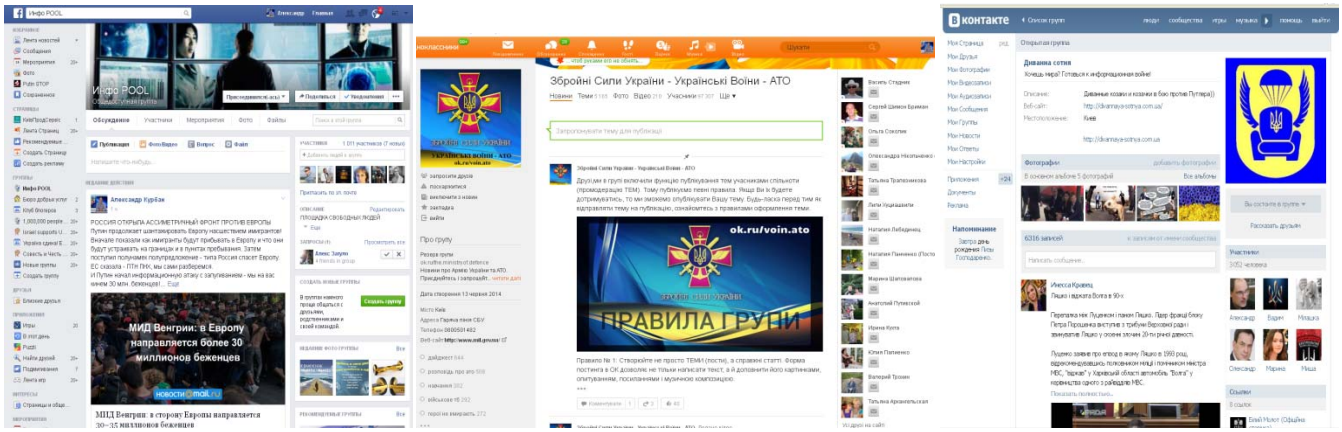
Мал. 2.15. Блоги



http://echo.msk.ru/blog/ http://censor.net.ua/blogs/all

Групи в соцмережах – локальні спільноти, що об'єднуються за тематичним принципом для спілкування та обміну інформацією (у коментарях та шляхом розміщення постів).

Мал. 2.16. Групи в соцмережах



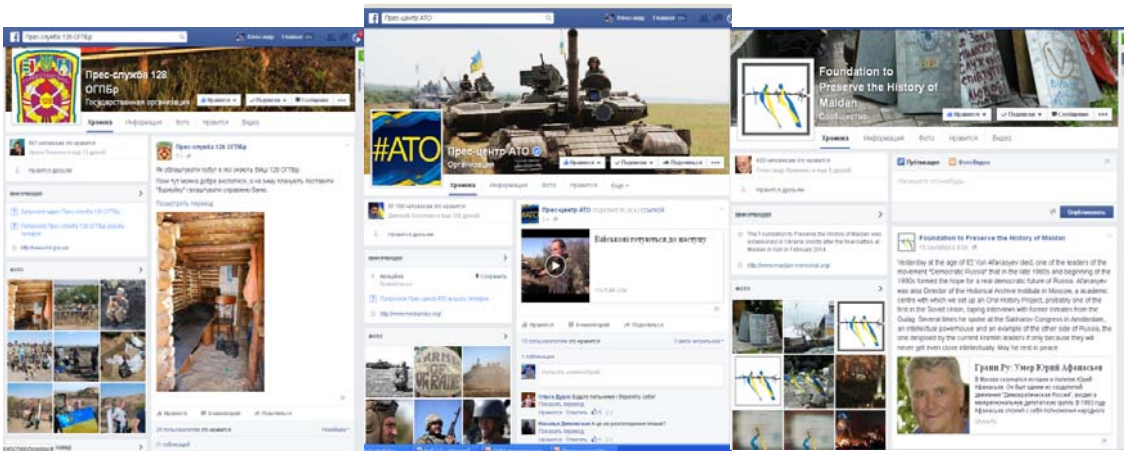
https://www.facebook.com/groups/349777181858648/

http://ok.ru/voin.ato

http://vk.com/dyvannasotnja

Сторінки в соцмережах – мережевий варіант тематичного сайту та обмеженою можливістю спілкування (лише у коментарях).

Мал. 2.17.Сторінки в соцмережах



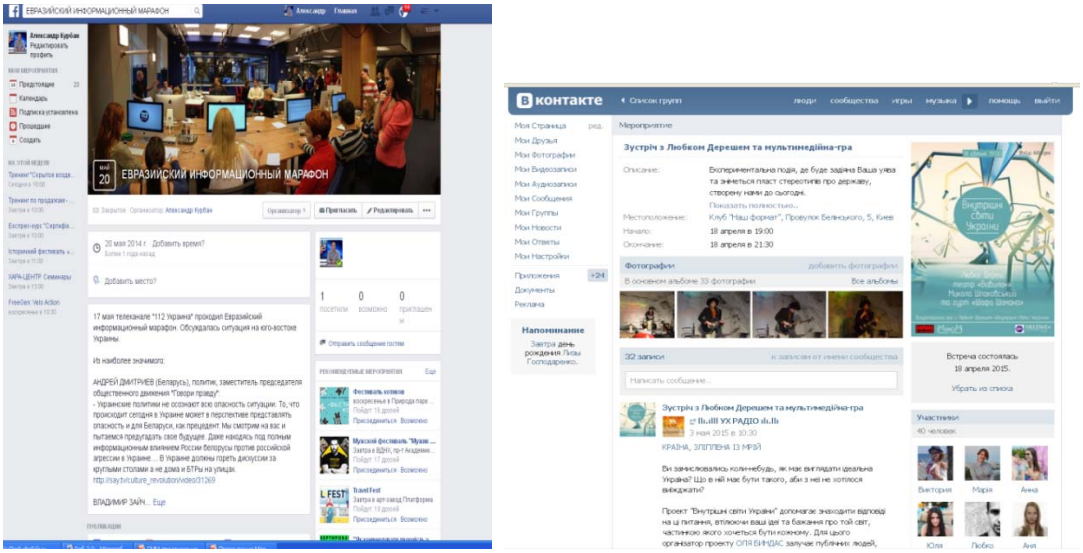
https://www.facebook.com/%D0%9F%D1%80%D0%B5%D1%81-%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0-128-%D0%9E%D0%93%D0%9F%D0%91%D1%80-1491000804527968/timeline/?ref=profile

https://www.facebook.com/ato.news

https://www.facebook.com/Foundation-to-Preserve-the-History-of-Maidan-917719314909539/timeline/

Розділи «подія» на акаунтах у соцмережах – мережева сторінка, яка містить інформацію анонсуючого характеру по конкретному заходу.

Мал. 2.18. Розділи «Подія» в соцмережах



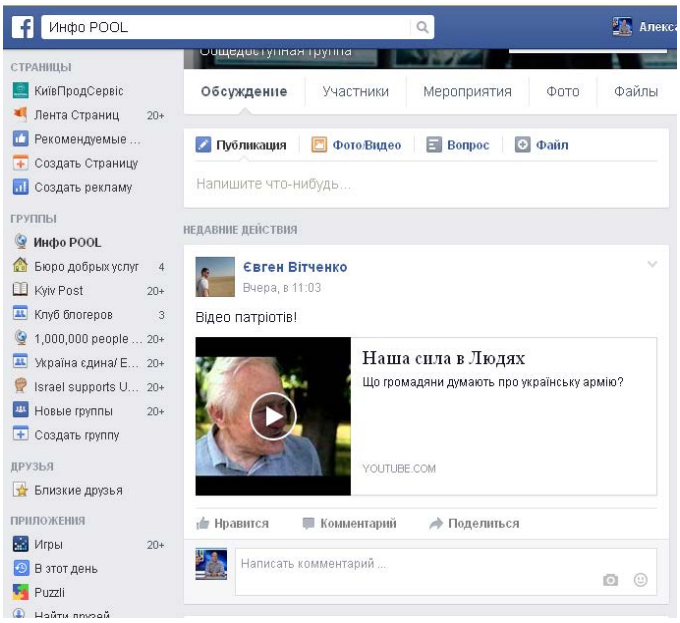
https://www.facebook.com/events/1487926221436686/

http://vk.com/event91546412

2. Підготовка контенту. Важливою складовою інформаційної операції є якість контенту – інформаційного повідомлення. Останнє може бути у вигляді:

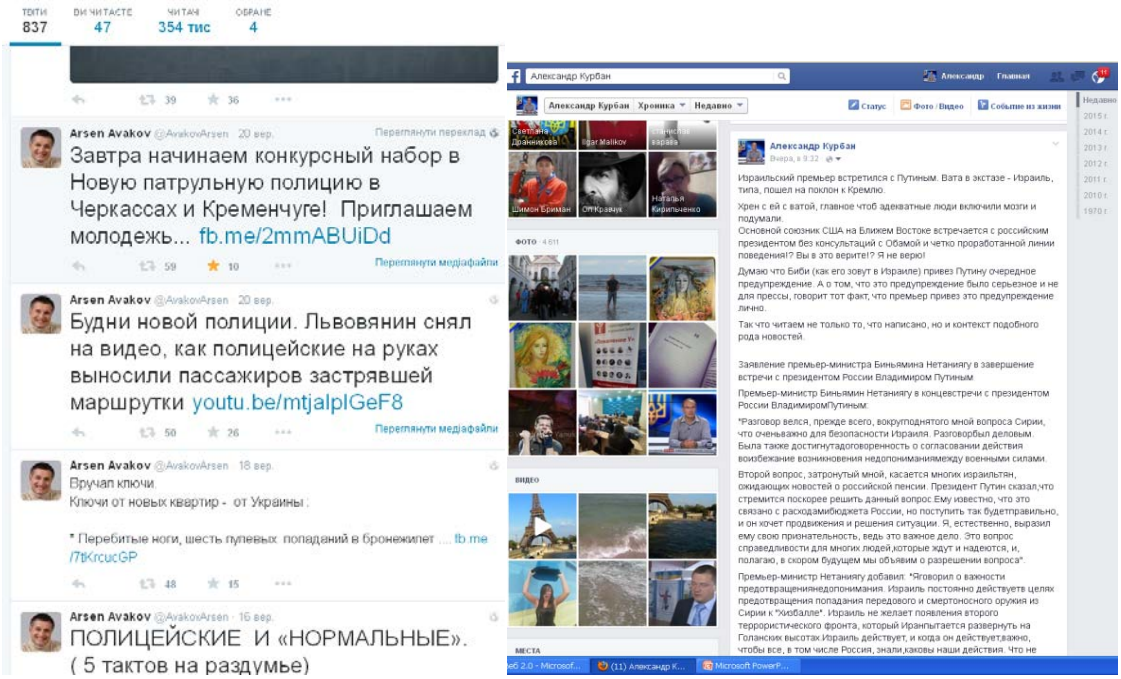
Відео або аудіо ролика – звукового або відеоряду помірного обсягу, зручного для розкриття формату, загальною тривалістю до 1 хв.

Мал. 2.19. Пост з роликом



Текстові повідомлення – контент із середнім текстовим обсягом 2-10 абзаців (для Facbook, Odnoklassniki та VKontakte) або короткого повідомлення (Twitter – 140 знаків).

Мал. 2.20. Текстові пости

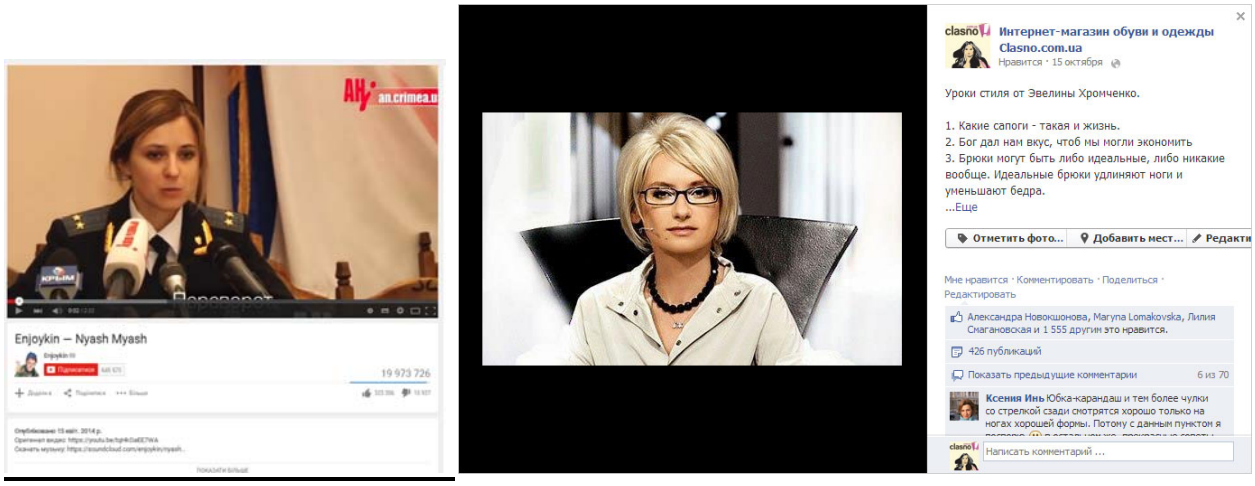


Графіка – фото, малюнки, інфографіка, меми.

Мал. 2.21. Пости з графічними зображеннями

Найбільш якісний контент може перетворитися на вірусний, тобто поширюватися самими користувачами соцмереж за рахунок унікальності або цікавості. Головною умовою «вірусності» є: емоційна складова, корисність та можливість здивувати (мал. 2.22). Контент стає вірусним, якщо отримує від кількох десятків до мільйонів «лайків» та репостів.

Мал.2.22. Вірусний контент, приклади



https://www.youtube.com/watch?v=TBKN7_vx2xo

http://www.masterskayafanstranic.com.ua/37-primerov-virusnyh-publikacij-na-facebook/

Необхідно пам’ятати, що додатковими правилами, які забезпечують успіх при створенні інформаційного повідомлення є:

- гумор та сарказм;
- невеликі обсяги тексту (2-3 абзаци);
- простий та зрозумілий стиль повідомлення (мовою цільових груп);
- використання хештегів **(#крымнаш, #четамухохлов** та ін.) та ріплі (@Posttrans, @VolonretTsentr та ін.);
- широке використання інфографіки.

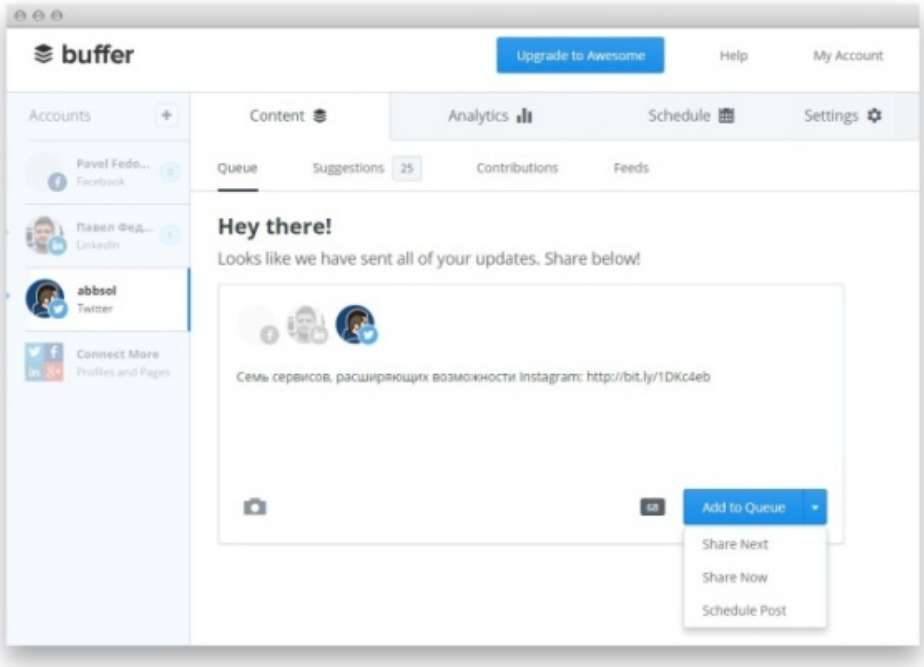
3. Поширення контенту. Розповсюдження контенту («розшарування» або «посів») здійснюється в режимі ручного постінгу чи за допомогою окремих програм (сервіси автопостінгу).

Постінг у ручному режимі здійснюється шляхом створення постів у тематичних відкритих групах або на акаунтах. В якості прийомів, які не дуже підтримуються, можна використовувати розміщення власного контенту в коментарях під чужим популярним постом або на чужому акаунті, якщо він є відкритим.

Автопостінг поширює контент у межах заданого простору за визначеними параметрами. Найбільш популярними на сьогодні є такі, як:

BUFFER – дає можливість розміщувати матеріали у Facebook, Twitter, LinkedIn, App.net и Google+ (мал. 2.13). Разом з тим Buffer є не тільки автопостером, але й аналітичною системою, яка досліджує соціальні медіа.

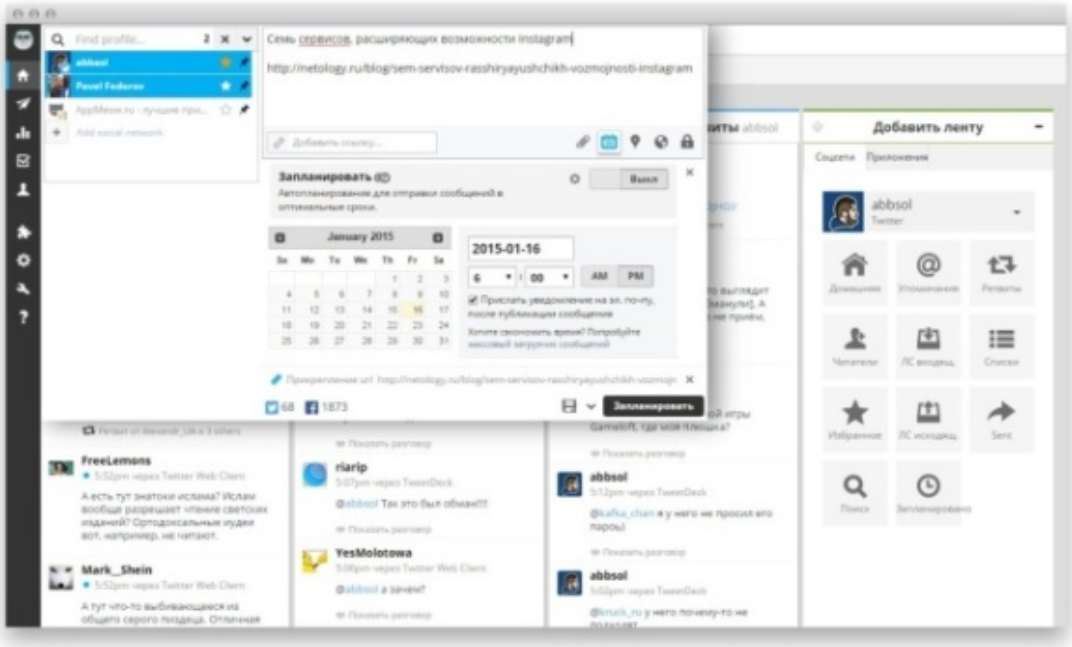
Мал. 2.23.Інтерфейс Buffer



HOOTSUITE – програма для роботи з Twitter, ВКонтакте, Facebook, Google+, LinkedIn, Foursquare и WordPress у браузері або на мобільних гаджетах (мал. 2.14). Через Hootsuite можна не тільки читати стрічки у соціальних мережах, але й публікувати контент. У Pro-версії є масовий

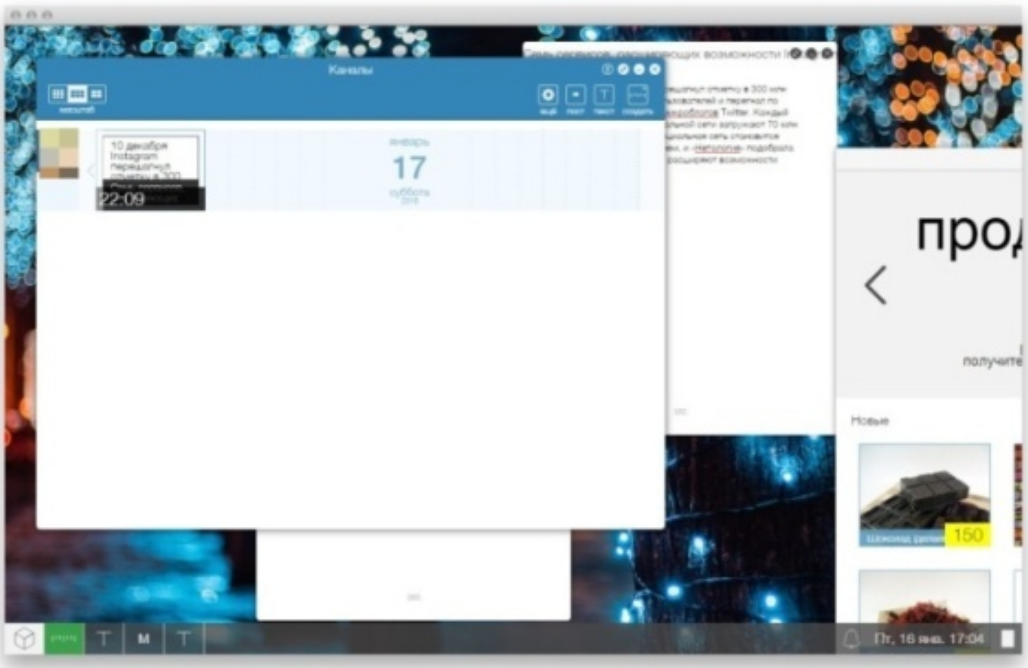
завантажувач інформації, що дозволяє працювати з кількома постами одночасно.

Мал. 2.24. Інтерфейс Hootsuite



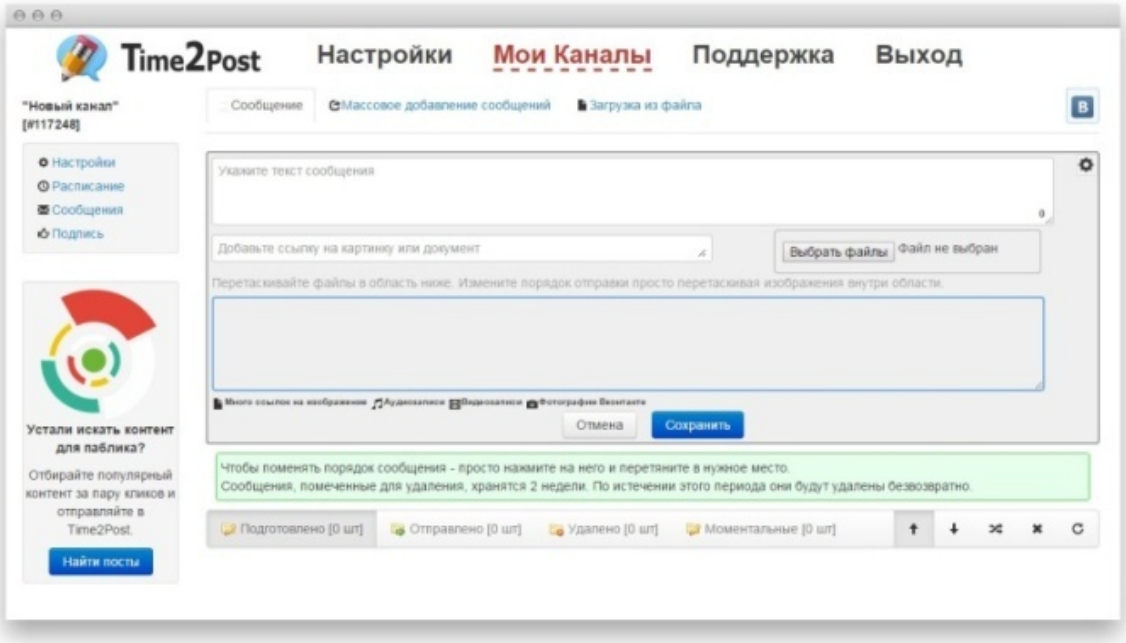
BUZZLIKE – система дозволяє розміщувати пости у VKontakte, Facebook та Odnoklassniki (мал. 2.15). Пости налаштовуються за часовою стрілкою. В сервісі є шаблони – текстові та з медіа файлами.

Мал. 2.25.Інтерфейс Buzzlike



TIME2POST – програма дає можливість працювати з VKontakte, Facebook, Twitter та LinkedIn (мал. 2.16). Ця система вміє імпортувати повідомлення з RSS, а також створювати водяний знак на зображення. В наявності також є масовий завантажувач зображень. Пости можна планувати за часом або в хаотичному порядку.

Мал. 2.26. Інтерфейс Time2post



4. Моніторинг результатів. За результатами розповсюдження контенту необхідно відстежити результати щодо складання звіту (див. наступний пункт). Також важливою функцією моніторингу є спостерігання за певним акаунтом, групою, сторінкою або окремим інформаційним полем, що містяться у певних соціальних мережах. В останньому випадку застосовуються спеціалізовані методики та використовуються відповідні сервіси.

5. Звіт за результатами. Збирання даних щодо результатів поширення контенту та узагальнення їх у форматі звіту є важливою складовою частиною процесу поширення у соціальних он-лайн мережах. Формат та зміст таких звітів

поки що не стандартизовано, він може мати будь-яку зручну конфігурацію. Головною умовою є подання перш за все кількісних показників. Серед критеріїв оцінювання є (мал. 2.27):

- ***кількість репостів*** – скільки разів цей контент розмістили на власних акаунтах інші користувачі;
- ***кількість «лайків»*** - скільки користувачів висловили своє позитивне відношення до контенту;
- ***кількість коментарів*** – скільки користувачів та скільки разів долучалися до дискусії або обговорення контенту;
- ***кількість контактів*** – кількість учасників груп, сторінок та фоловерів, акаунтів, на яких було розміщено контент.

Представлені вище алгоритми є варіативними, бо відповідно до певних комунікаційних ситуацій або особливостей завдань, на які орієнтуються певні інформаційні процеси, вони можуть корегуватися навіть у момент реалізації.

Такий гнучкий підхід дозволяє оперативно реагувати на певні непередбачувані обставини або перешкоди, які виникають у ході процесу. Постійна динаміка та оцінка перспектив подальшого руху з певних точок біфуркації також дозволяє вишукувати найбільш оптимальні шляхи досягнення поставлених цілей.

У форматі інформаційно-психологічної війни, як складової сучасних гібридних конфліктів, зазначена складова визначається як головна ознака асиметричності процесів.

Разом з тим маємо зазначити, що така гнучкість та варіативність стосується розгортання процесів на окремих етапах. Послідовність цих етапів та їх взаємозв’язок є константним явищем і не передбачає змін.

Мал. 2.27. Звіт про інформаційну операцію

ОТЧЕТ
по результатам проведения акции «Ссора»

Посев: 27-28.10.2014
Мониторинг: 29.10.2014
Базовый тезис: «Сепаратиское быдло на службе русского мира»
Дополнительные (раскрывающие) тезисы:
«На Донбассе местное быдло умеет только грабить и бухать» (для России)
«Российская сторона нас держит за быдло и использует нас в своих целях» (для жителей Донбасса)

Сети: Facebook, Vkontakte, Odnoklassniki
Общие количественные итоги:
Контакты - 1 272 323
Лайки – 406
Репосты – 32
Комментарии – 320

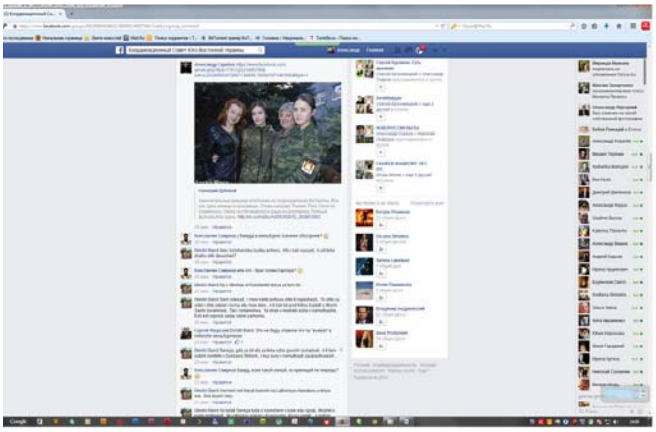
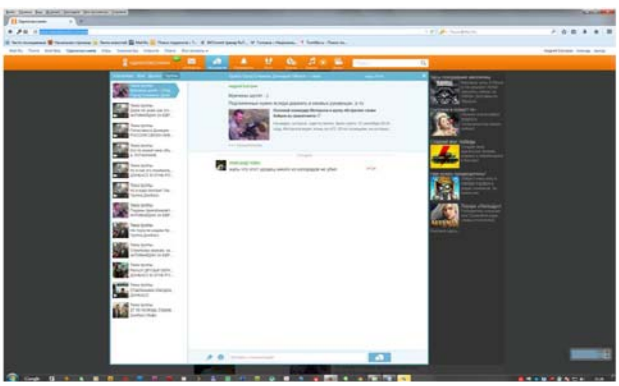
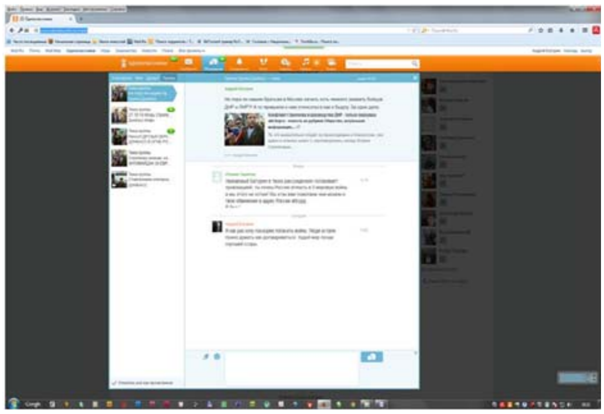
Материалы размещенные в Facbook.com
Пост 1.
Пацаны развлекаются :-)
Полевой командир армии ДНР - "Моторолла" лупит из гранатомета по своим, проверяет как они окопались.
Вояка, блин. Пол года топчется перед Донецким аэропортом, ни как не может его зачистить окончательно.
Вот так бывает, когда гопника ставят начальником, сколько пацанов положил под аэропортом ...
http://slon.ru/fast/world/polevoy-komandir-motorola-v-shutku-obstrelyal-svoikh-boytsov-iz-granatometa-1174060.xhtml
Видео: http://www.youtube.com/watch?v=8SloarndHlk

Пост2.
Блин, эти местные аППатченцы, только орать могут "Россия [illegible]". А как реально воевать - в кусты!
Прав был Стрелков, с этой быдлотой русский мир в Донбассе не построишь!
То ли дело в Крыму было!
http://newsland.com/news/detail/id/1450396/

Материалы размещенные на Odnoklassniki.ru
Пост1.
Стрелкова уважаю, как гениального военного и талантливого писателя!
Но, блин, его отношение к ополченцам ЛНР и ДНР, оставляет желать лучшего!
Господин, Стрелков, мы не быдло и не пушечное мясо!
Мы кровь за Русский мир проливаем! Имейте совесть уважать нас и считаться с нами!
http://newsland.com/news/detail/id/1450396/
Пост2.
Не пора ли нашим братьям в Москве начать хоть немного уважать бойцов ДНР и ЛНР?!
А то привыкли к нам относиться как к быдлу. За одно дело кровь проливаем, господа хорошие!
На сейчас нужно остановить укров и защитить Новороссию, а не понты столичные гонять. Стрелков, конечно авторитетный товарищ, но уважительнее нужно относиться к своим соратникам.
http://newsland.com/news/detail/id/1450396/
Пост3.
Стрелкова уважаю, как гениального военного! Но, блин, его отношение к ополченцам ЛНР и ДНР, оставляет желать лучшего!
Господин, Стрелков, мы не быдло и не пушечное мясо!
Мы кровь за Русский мир проливаем!
Имейте совесть уважать нас и считаться с нами!
http://newsland.com/news/detail/id/1450396/
Пост4.
Уважаю Игоря Ивановича, но палку перегибает!
Надо бы уважать своих соратников!
Мы не быдло и не пушечное мясо! Донецкие и Луганские ополченцы воюют хорошо, жизни не жалеют.
И не надо к нам так с высока!
http://newsland.com/news/detail/id/1450396/
Пост5.
Пора бы нашим российским братьям понять, что и на Донбассе есть русские патриоты, которые кровью своей готовы оплатить создание Русского мира.
А то, иногда просто как к быдлу относятся. Пора бы эти понты московские забыть. За одно дело кровь проливаем.
Несмотря на весь авторитет Стрелкова, хотелось бы больше уважение со стороны первопрестольной получать.
http://newsland.com/news/detail/id/1450396/

МАТЕРИАЛЫ
https://www.facebook.com/groups/491209804248832/560091144027364/?notif_t=group_comment



РОЗДІЛ 3. Базові прийоми та інструменти ведення інформаційної війни в соціальних он-лайн мережах

3.1. Загальна характеристика сучасного інтернет-простору

3.1.1. Основи формату web 1.0, 2.0 та 3.0

Основним **об'єктом** інтернет-комунікацій є *контент* (від англ., «content» - зміст) у вигляді тексту, відео, графіки, який створюють, просувають та використовують **суб'єкти** – учасники віртуальних комунікаційних процесів. У залежності від того, які механізми створення та просування контенту застосовуються, інтернет-технології класифікуються за форматами **WEB 1.0, WEB 2.0** и **WEB 3.0** [217, с. 144].

WEB 1.0 (тип «монолог» - 1:99) – технології, що формують віртуальну систему, в якій автори (1%) створюють та розміщають на власних веб-ресурсах контент, що споживає інша частина користувачів (99%). Базовим елементом комунікації є корпоративний або тематичний веб-сайт, який містить відповідну інформацію.

WEB 2.0 (тип «діалог» - 50:50) – технології, що створюють віртуальне поле, в якому автори ґатунку формату Web 1.0 перетворюються на модераторів, створюючи окремі мережеві майданчики, на яких усі інші учасники комунікаційних процесів мають можливість бути як авторами, так і споживачами контенту.

WEB 3.0 (тип «співпраця» - 100:100) – технології, що об'єднають усі мережеві майданчики в єдиний віртуальний простір, формуючи нову реальність, в якій суспільство та кожний окремий його представник проходить процес аватарізації. На цьому етапі формуються основи для майбутнього формату (4.0), основу якого складатимуть штучний інтелект у вигляді www-ботів та штучних нейронних мереж.

Пануючим форматом інтернет-технологій на сьогодні в практичному аспекті є web 2.0, також доволі активно використовуються і технології web 3.0. Безумовно має місце і web 1.0, але в меншій мірі. Також певні дослідники та практики вважають, що саме зараз, у вигляді тестових програм та прототипів інформаційних процесів починає формуватися основа для подальшого розвитку технологій web 4.0 (боти, штучні нейронні мережі, агрегатори новин, біржі контенту, програми автоматичного управління роботи з контентом, ройовий штучний інтелект та ін.)

Уперше це поняття формату web, зокрема 2.0, запропонували фахівці компанії «O'Reilly Media», що спеціалізується на інформаційних технологіях. Згідно з опублікованою у вересні 2005 року статтею Тіма О'Райлі, засновника компанії O'Reilly Media, «Що таке Веб 2.0?» ця концепція з'явилася в результаті «мозкового штурму» між компаніями O'Reilly Media та MediaLive International [194].

Автори ідеї визначили чотири базові принципи web 2.0, серед яких [194]:

- ***Веб, як платформа***, без посередницьких програм, що дозволяє запускати програми прямо в мережі Інтернет;
- ***Можливість синдикації контенту;***
- ***Співпраця розробників та користувачів*** у відкритій інформаційній інфраструктурі;
- ***Соціальні мережі та блогосфера,*** багатовекторне інтерактивне спілкування користувачів мережі.

У форматах web 2.0 та 3.0 мережа Інтернет визначається, як засіб комунікації, при цьому його об'єктами є медіа-сервіси, блоги, агрегат ори новин, соціальні мережі, а суб'єктами – співучасники. Робота в цих форматах передбачає активну участь користувачів у створенні контенту для інтернет-ресурсів, у тому числі й чужих. Це робить ресурси web 2.0 та 3.0 більш інтерактивними і надає користувачам свободу самовираження.

Серед найбільш відомих, типових прикладів інтернет-майданчиків цих форматів є:

1. ***Вікіпедія*** — вільна багатомовна енциклопедія
2. ***Google Maps*** — Google-карти
3. ***Flickr*** — он-лайн-фотоальбом
4. ***del.icio.us*** — он-лайн служба закладок
5. ***Netvibes*** — персональний десктоп
6. ***Digg.com*** — ресурс новин
7. ***Pligg*** — web 2.0 CMS
8. ***Quintura*** — візуальна пошукова система з інтуїтивною картою підказок
9. ***Live Journal*** — сервіс для ведення блогів
10. ***Youtube*** — відео сервіс
11. ***MySpace*** — Сайт мережевих співтовариств
12. ***Last.fm*** — музичне співтовариство
13. ***Ucoz*** — web-сервіс для створення сайтів

Найбільш відомими, серед ресурсів зазначеного формату сьогодні, є он-лайн соціальні мережі (або соціальні медіа). Вони є найрезультативнішими інструментами серед тих, що можуть бути використані сучасними фахівцями із інформаційних війн. У разі правильного використання ці технології дають максимальний комунікаційний ефект. При цьому їх базовими якісними перевагами є [217, с.143]:

- *Оперативність та гнучкість* – інформаційні повідомлення (графіка, відео, текст) доходять дуже швидко, разом з тим зберігається можливість у будь-який момент вносити зміни (виходячи з реакції отримувача);

- *Персональне таргетування* – трансляція інформаційного повідомлення на конкретного представника цільової групи, при цьому враховуються особисті моменти та уподобання;
- *Мала витратна складова* – вартість прямої промоції у соцмережах складає невеличкий відсоток у порівнянні із класичними інструментами (ТБ, радіо, преса, зовнішня реклама), а промоція з майданчика акаунта приватної особи взагалі офіційно не тарифікується.

У контексті зазначених вище базових характеристик, соціальні медіа дедалі все більш активно відтягують на себе основні ресурси, що виділяються для фінансування інформаційних конфліктів. Така тенденція носить загальний характер, що особливо яскраво позначилося внаслідок глобальної економічної та політичної кризи.

Практичними інструментами роботи із соціальними медіа, що мають бути визначені окремо, є технології **SEO, SMO и SMM** [217, с. 145].

SEO (Search Engine Optimization) – комплекс заходів із пошукової оптимізації, орієнтований на підвищення позиції веб-сайту в пошукових системах.

SMO (Social Media Optimization) – комплекс заходів із просування веб-ресурсів у мережі Інтернет.

SMM (Social Media Marketing) – комплекс заходів із просування персонального акаунту або окремого контенту в соціальних мережах.

За цільовим призначенням та змістовними характеристиками сучасні соціальні медіа поділяються на [217, с. 145]:

1. ***Соціальні контактні мережі*** (Facebook, ВКонтакте.ru, Одноклассники.ru та ін.) – віртуальна платформа або он-лайн сервіс для розбудови соціальних взаємовідносин.
2. ***Блоги*** (LiveJournal, Корреспондент.net, Blog.Liga.net) – персональні, групові або корпоративні мережеві майданчики для розміщення, в

режимі щоденника, інформації профільної для авторів із можливістю залучення до обговорення сторонніх користувачів.

3. ***Мікроблоги*** (Twitter, Writemore.ru) – видозмінена версія блогу, метою якої є формування оперативних комунікаційних зв'язків за допомогою коротких повідомлень та спрощеної процедури комунікації.
4. ***Файлообмінники*** (YouTube, Flickr) – он-лайн сервіс із надання майданчика під розміщення, пошук та обмін контентом.
5. ***Соціальні мережі новин*** (Reddit) – он-лайн майданчики із розміщення та оперативного поширення новин.
6. ***Вікі-проекти*** (WikipediA) – он-лайн проекти із створення та накопичення довідково-інформаційного контенту із можливістю групового співавторства.
7. ***Сайти закладок*** (Google.Bookmarks, BlogMarks.net) – он-лайн сервіс із зберігання та накопичення інтернет-посилань.
8. ***Віртуальні світи*** (Second.Life.ru, Habbo.com) – інтернет-співтовариство із певним чином модельованою реальністю.
9. ***Підкастінг*** (накопичувачі цифрових медіа-файлів) – он-лайн ресурс із створення, накопичення та поширення медіа-файлів у стилі радіо або телебачення.
10. ***Мультиінструментальні ЗМІ*** (SAY.TV) – інтернет-ресурси, що містять мультиінструментальні можливості із створення, накопичення та поширення контенту в межах певних тематичних завдань.

3.1.2. Сучасні он-лайн соціальні мережі

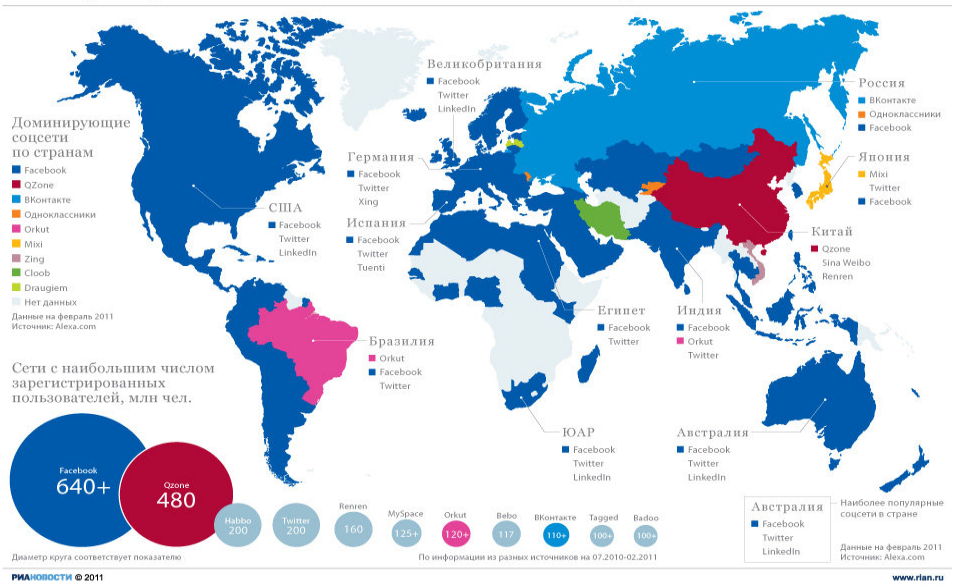
За великим рахунком, базові принципи, що лежать в основі будь-якої соціальної мережі, однакові. Головними складовими є аватарізація користувача шляхом створення його віртуального «Я», інструменти здійснення комунікації

та певні механізми пошуку і розповсюдження контенту. Різниця полягає лише у цільовому призначенні та якості програмного забезпечення.

Для фахівця із ведення інформаційної війни, при виборі певної соціальної мережі або кількох з них, в якості поля бою, необхідно звертати увагу на дві позиції. Перш за все, які цільові групи є найбільш активними користувачами певної соціальної мережі та яку їх кількість вона охоплює. Також необхідно чітко розуміти, які комунікаційні механізми ця соціальна мережа може запропонувати.

Виходячи з цього, розглянемо найбільш поширені соціальні мережі щодо доцільності, зручності їх використання та тих завдань, які вони дозволяють вирішувати.

Мал. 3.1. Розповсюдження соціальних мереж у світі

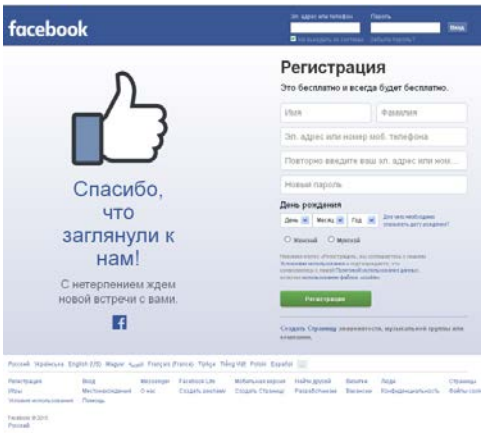


http://ria.ru/infografika/20110225/338976030.html

Facebook.com – *промоція об'єктів, ідей, персоналій, організаційних структур*. Сьогодні кількість користувачів перейшла за 1,32 млрд осіб, при середньодобовій активності 890 млн осіб 810 млн осіб на місяць відвідують цю мережу з мобільних пристроїв. Щоденно відвідувачі залишають у мережі 3,2 млрд «лайків» та коментарів, близько 300 млн фото. В мережі існує понад 125

млрд дружніх зв’язків, кількість переглянутих сторінок – 1млрд на місяць [217, с. 147].

Мал. 3.2. Базові складові Facbook.com



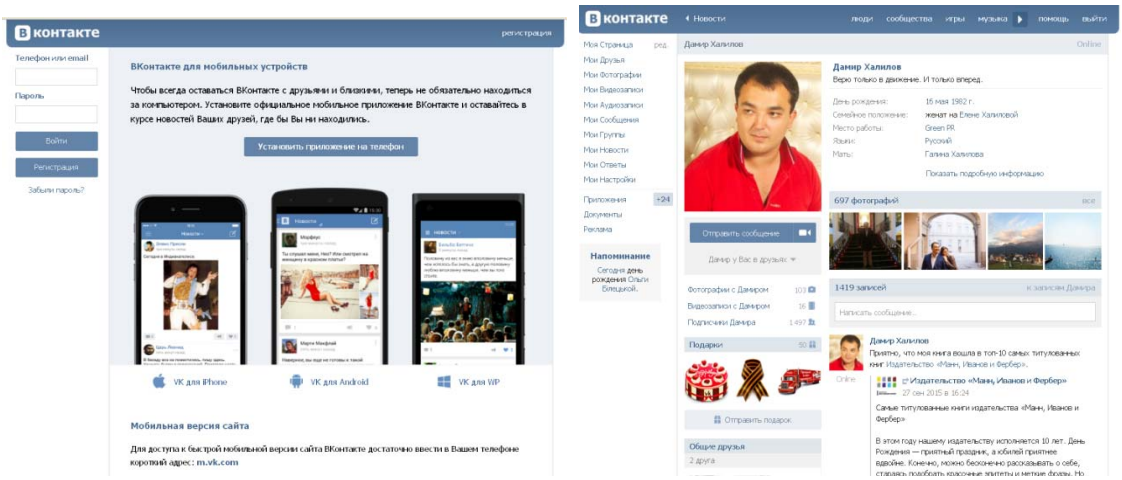
Прибутки Facebook у 2013 році становили $2,804 млрд Зазначена соціальна мережа є найбільш зручною для роботи фахівця із інформаційних протистоянь, бо дає можливість здійснювати промоцію шляхом персональної рекомендації, адресно, на конкретних представників конкретної цільової групи. В інструментарії досвідченого фахівця ця мережа може бути найефективнішою та найточнішою зброєю. Базовими елементами Facebook є: персональні профілі (акаунти користувачів), групи (співтовариства за інтересами), фанатські сторінки (тематичні сторінки) та заходи (анонсування та підбиття підсумків реальних подій).

У цілому користувачі Facebook на 50% використовують мережу для спілкування, підтримки стосунків, пошуку нових знайомих, на 25% для здійснення власної промоції та на 25% для вирішення тематичних завдань.

VKontakte.com - *промоція об’єктів, ідей, персоналій, організаційних структур.* Зараз ця мережа нараховує більше 219 млн користувачів, переважно у країнах СНД. Річний прибуток від діяльності мережі складає близько $ 25 млн Мережа дає можливість створювати особисті та корпоративні сторінки, групи,

промотіювати контент, відслідковувати зворотну реакцію, впливати на споживацьку думку [217, с. 148].

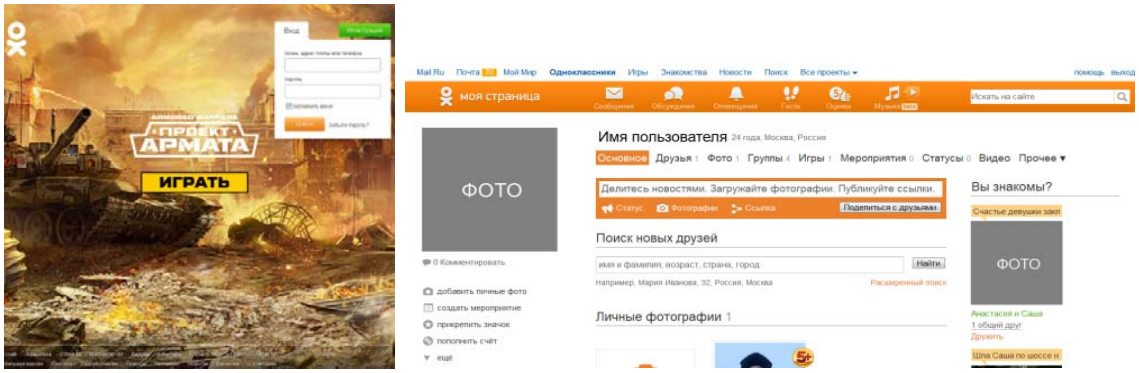
Мал. 3.3. Базові складові VKontakte.com



Користувачі VKontakte.com на 70 % використовують мережу для дозвілля – спілкування, знайомства, розваги, 20 % здійснюють власну промоцію та 10% - для вирішення тематичних завдань.

Odnoklassniki.ru - промоція об'єктів, ідей, персоналій, організаційних структур. Мережа нараховує понад 205 млн користувачів (відвідування - 44 млн за добу), переважно з країн СНД. Дає можливість створити персональну сторінку, групу, розповсюджувати контент, слідкувати за реакцією представників цільових груп та певним чином здійснювати на них вплив. Odnoklassniki.ru не така універсальна мережа в справі вирішення тематичних завдань, утім функціонально, принципово від двох попередніх не відрізняється [217, с. 148].

Мал. 3.4. Базові складові Odnoklassniki.ru

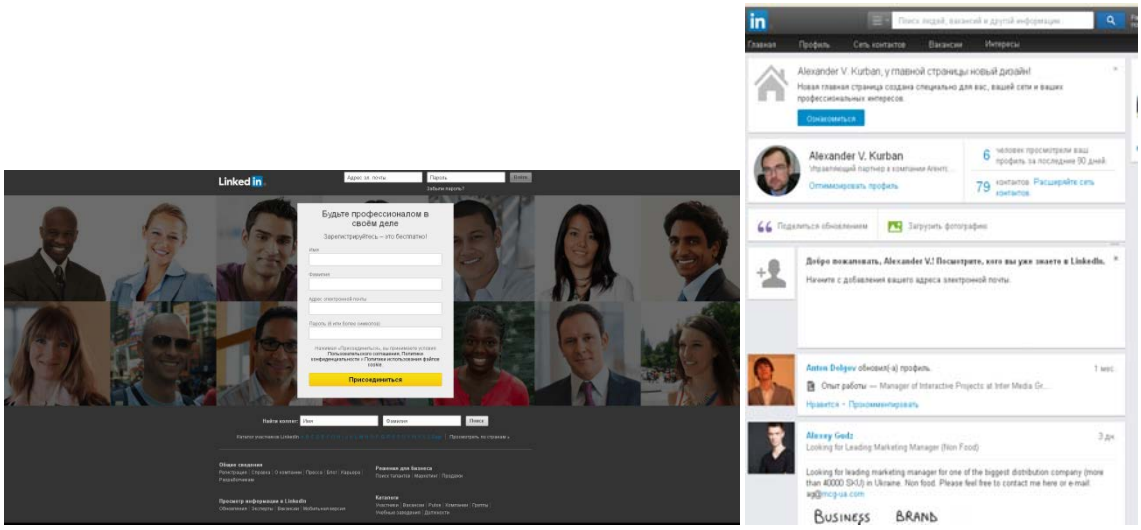


Користувачі цієї мережі приблизно на 70-80 % використовують її для спілкування та розваг, близько 20% - для власної промоції і десь на 10% для вирішення тематичних завдань.

LinkedIn – промоція бізнес-проектів та персоналій. В мережі сьогодні зареєстровано більше 225 млн користувачів, що презентують понад 150 галузей бізнесу 200 країн. Мережа надає можливість зареєстрованим користувачам створювати та підтримувати ділові контакти. Контакти можуть формуватися як з кола фоловерів, так і ззовні, втім Linked In вимагає попереднього знайомства з контактами. У випадку, якщо користувач не має прямого зв'язку з контактом, він може бути представленим через інший контакт. Linked In також дозволяє розміщати інформацію про ділові відрядження, майбутні конференції, прочитані книги [217, с. 149].

Користувачі Linked In можуть використовувати список контактів для того, щоб бути представленими через існуючи контакти та розширювати зв'язки; здійснювати пошук компаній, людей, груп за інтересами; розміщувати професіональні резюме та здійснювати пошук роботи; рекомендувати та бути рекомендованими; оголошувати вакансії; створювати групи за інтересами.

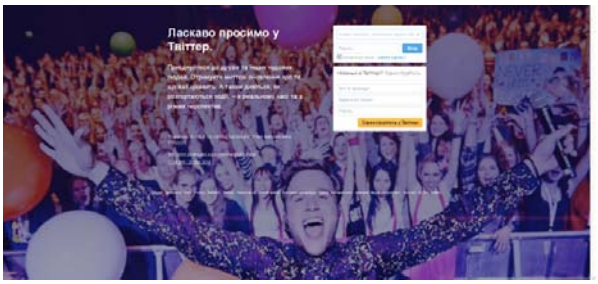
Мал. 3.5. Базові складові Linked In.com



За прямим призначенням – промоція бізнесу зазначену мережу використовують 80%, 20% - персональна промоція.

Twitter – промоція персоналій та тематичних проектів. Мережа нараховує близько 500 млн активних користувачів, при цьому близько 100 млн з них відвідують мережу щоденно. Прибуток мережі складає понад $168,6 млн [217, с. 149].

Мал. 3.6. Базові складові Twitter.com



За змістом унікальних повідомлень: 41 % - бесіда; 38 % - розмови; 9 % - ретвіти (повідомлення, що повторюються); 6 % - самореклама; 4 % - спам; 4 % - новини. Базовим інструментом роботи в мережі Twitter є твіт – інформаційне повідомлення до 140 символів (від англ. «twitt» - чирикати), в якому можна закласти рекламне оголошення, дати коментарі відносно об’єкта або ідеї, поділитися корпоративною новиною, анонсувати подію. Мережа дає можливість оперативно та об’єктивно оцінювати реакцію представників цільових груп та керувати комунікаційними процесами.

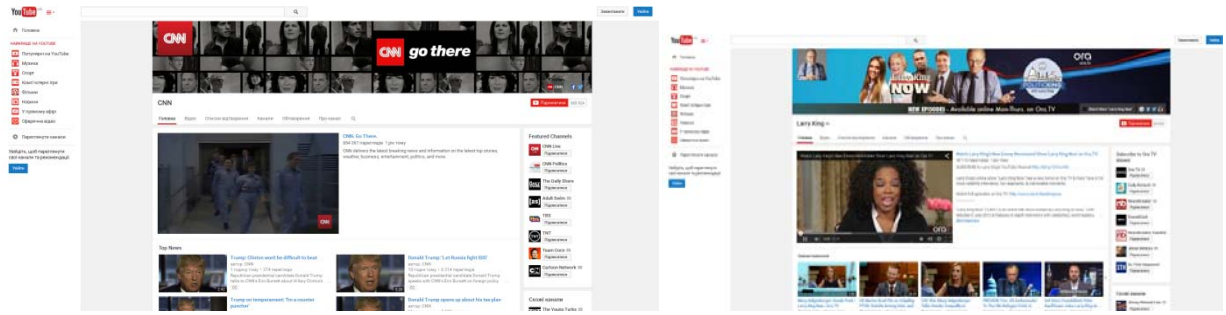
У практичному аспекті зазначена соціальна мережа використовується для спілкування – 50%, промоції персоналій – 25% та промоції проектів – 25%.

YouTube – промоція об’єктів, ідей, персоналій, організаційних структур. На теперішній момент на портал щоденно завантажується близько 2 млрд роликів на день. Загальна аудиторія складає понад 250 млн осіб. Головним

носієм інформації в цьому випадку є відеоролики, що можуть містити рекламну, розважальну новину та інші види інформації. Ролики розміщуються безпосередньо на сайті, для бажаючих може бути створено окремий канал (персональний або корпоративний) [217, с. 150].

Користувачі мають можливість залишати власні коментарі, оцінювати чужі, додавати анотації та титри до відео, виставляти рейтинги.

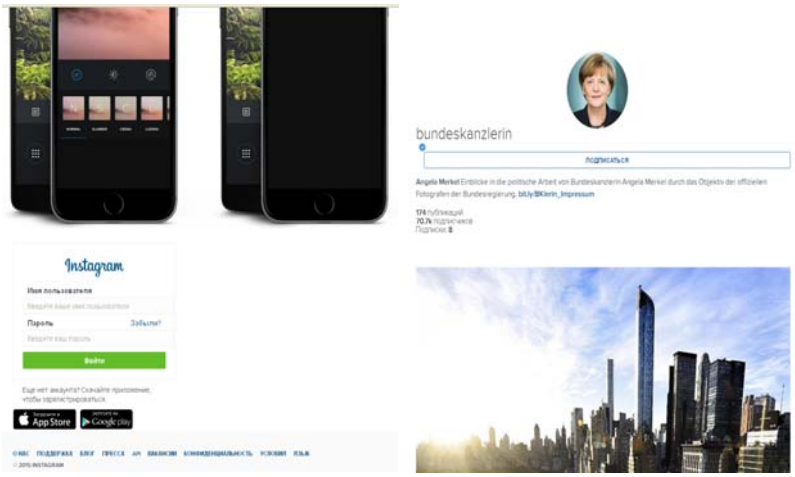
Мал.3.7. Базові складові YouTub.com



У практичному аспекті на YouTube можна робити промоцію новинам, іміджевим, ігровим роликам з можливістю відстеження реакції представників цільових груп.

Instagram.com – промоція об'єктів, ідей, персоналій, організаційних структур. Соціальна мережа орієнтована на розміщення та обмін фото та відеоматеріалів.

Мал. 3.8. Базові складові Instagram.com

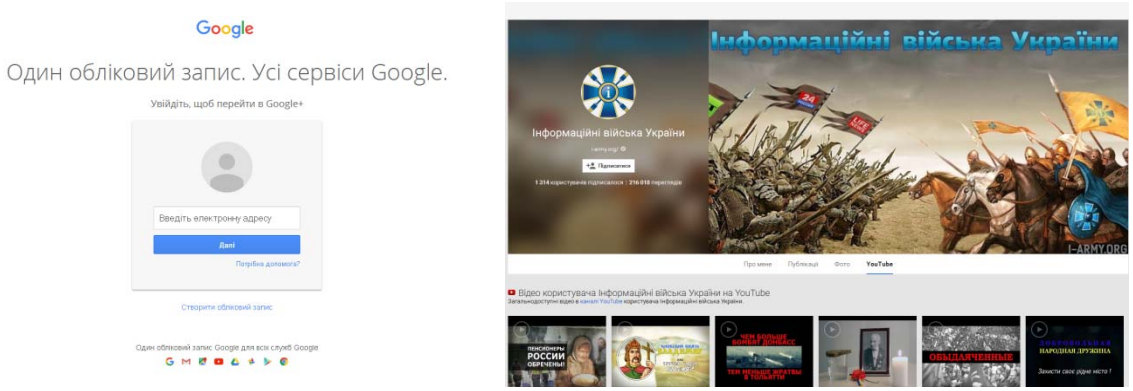


Загальна кількість акаунтів – понад 200 млн осіб. Дає можливість записувати відео (15 сек.), визначати на фото персоналії, бренди, розсилати повідомлення та ін. У 2012 році компанія Facebook придбала цю мережу за $ 300 млн. Мережа Instsgrsm є однією з найтехнологічніших. Профільні софти дозволяють швидко робити, обробляти, роздруковувати та запускати у мережу зображення та відео. Втім слід зазначити, що такий технологізм не дозволяє поки що в повній мірі використовувати мережу при вирішенні маркетингових завдань. У разі подальшого розвитку саме в напрямку забезпечення комунікаційної складової мережа матиме успіх [217, с. 150].

Google + – *промоція громадських проектів, ідей, персональне спілкування.*

Багатомовна соціальна мережа та ідентифікаційна служба. Створено у 2011 р., має понад 359 млн активних користувачів, у цілому має понад 500 млн. Замість звичного, для користувачів інших соціальних мереж, єдиного списку «друзів», який можна ділити на групи, Google+ пропонує розподіляти контакти за «колами»: родичі, колеги, гурток крою та шиття тощо [217, с. 150].

Мал. 3.9. Базові складові Googl+

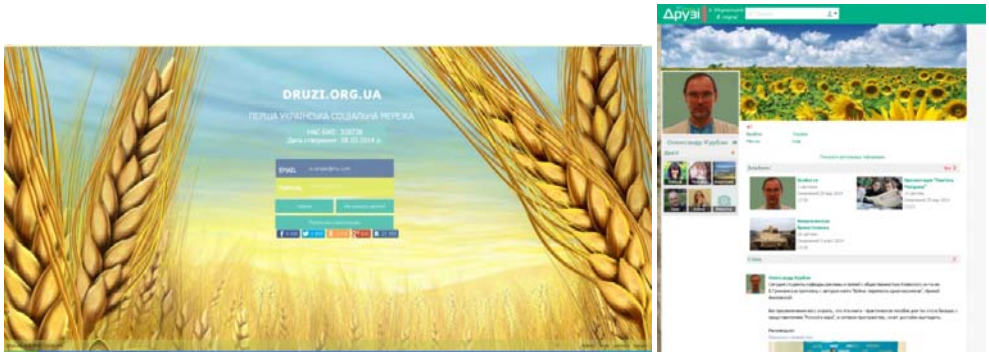


Дає можливість завантажувати відео та фотографії з мобільного телефону за допомогою сервісу «миттєвого завантаження» (Instant Upload). Для цього використовується спеціальна програма що доступна для смартфонів, працюючих як на операційній системі Android, так і на iOS. Також до особливостей Google+ належить можливість влаштовувати відеочати з друзями і навіть проводити відеоконференції з декількома учасниками.

За прямим призначенням – промоція проектів та ідей, зазначену мережу використовують 60%, 40% - персональна промоція.

Druzi.org – *промоція об'єктів, ідей, персоналій, організаційних структур.* Альтернативна соціальна українська мережа, в якій на сьогодні зареєстровано понад 318 тис. користувачів, працює з 18 березня 2014. Виборює першість серед повноцінних українських соціальних мереж.

Мал. 3.10. Базові складові Druzi.org



За прямим призначенням – промоція проектів та ідей, зазначену мережу використовують 80%, 20% - персональна промоція.

QirimTatar-Portali.ru та Selyam.com (національні кримськотатарські соціальні мережі) – *промоція громадських проектів, ідей, персональне спілкування.*

Зокрема соціальна мережа *QirimTatar-Portali* почала працювати з 1 червня 2015 р. та за короткий термін стала популярною серед кримськотатарських користувачів. У середньому на добу в мережі реєструється 75-80 користувачів, у цілому має 600 унікальних відвідувачів. *Selyam.com* існує вже кілька років і є не досить розвинутою.

Мал. 3.11. Базові складові QirimTatar-Portali.ru та Selyam.com

За прямим призначенням – промоція проектів та ідей, зазначені мережі використовують 50%, 50% - персональна промоція.

Серед українських соціальних мереж є також Connect.ua (1,5 млн) та Weua.info (понад 250 тис. користувачів).

Мал. 3.12. Базові складові Connect.ua та Weua.info

Перша себе позиціонує як сайт знайомств та спілкування, друга – як соціальна мережа для молоді, об'єднаної ідеєю створення якісного, адекватного, інформативного та безпечного місця для спілкування. На теперішній момент динаміка їхнього розвитку повільна, та особливого впливу і популярності вони не мають.

Кожна із зазначених он-лайн мереж має свої переваги та недоліки. Останні компенсуються користувачами або розробниками додаткових програмних сервісів, які покращують ці характеристики або надають їм нових особливих рис.

3.1.3. Базові інструменти просування контенту в соціальних мережах

Так само, як подібні базові принципи всіх провідних соціальних мереж, подібні й їх базові комунікаційні інструменти. Серед таких визначаються: **пост** (медіа-реліз), **подія, коментар**.

Кожен з них є базовою одиницею, з яких складаються алгоритми інформаційно-комунікаційних процесів, що будуються в он-лайн мережах відповідно до тих чи інших завдань.

Медіа-реліз. Зазначений інструмент представляє собою модифікований та адаптований варіант класичного н'юс-релізу. В практиці Web 2.0 та 3.0 медіа-реліз частіш за все визначають поняттям «пост» (від англ. «post» - повідомлення, інформація, оголошення) [217, с. 151].

Головними конструктивними особливостями медіа-релізу є такі характеристики, як:

- *Розмір* – 1-2 абзаци, кожен на 2-3 речення
- *Зміст* – один базовий меседж
- *Стилістика* – коротко, яскраво, емоційно (т.з. «телевізійний стиль»)

Зазначені якості виходять з базового принципу поведінки інтернет-користувачів – *серфінгу* (від англ. «surf» - займатися серфінгом, ковзати по хвилях), читання «по діагоналі» з концентрацією уваги на ключових фразах, словах, назвах, іменах. Для «якоріння» уваги читача медіа-реліз бажано доповнювати графічними або відеоматеріалами, смайликами та ін. При необхідності акцентувати увагу на ключових словах використовую такі позначення, як хештегі (# - передсловом) або ріпли (@ - перед ім'ям).

Подія. Інструмент має вигляд окремого розділу персонального акаунта, який містить інформацію про захід – анонсуючого або постфактум характеру. У форматі «події» автор розсилає своїм мережевим друзям запрошення та посилання на розділ, в якому знаходиться уточнююча інформація (що, де,

коли), а також після його проведення розміщує інформацію про результати. Інформація може подаватися в текстовому, графічному та відео форматах [217, с. 152].

Коментар. Цей інструмент є у вигляді, як правило, короткої замітки або відгуку на медіа-реліз/пост або супроводжує розміщений на власному акаунті чужий матеріал («перепост» або «репост»). Коментар може бути оцінений як одиниця виміру результативності інформаційного повідомлення (кількість та зміст відгуків). Також він може бути використаний і як засіб промоції власного контенту в стилі «партизанського маркетингу». Останнє передбачає розміщення у коментарях рекламної інформації, посилань, суб'єктивних (позитивних або негативних) оцінок [217, с. 152].

3.1.4. Засоби промоції контенту в соціальних мережах

Використовуючи технології Web 2.0 та 3.0, сучасний фахівець із інформаційно-комунікаційних технологій має чітко зрозуміти, що в цьому плані стрижньовим елементом процесу є **контент**. Контент може бути ***об'єктом комунікаційного процесу***, тоді він являє собою те, що шукають, вивчають, оцінюють, тобто ціллю.

Також контент може бути ***суб'єктом комунікаційного процесу*** – інформацією, через яку здійснюється промоція об'єктів, ідей, персоналій або корпоративних структур. У такому разі він стає інструментом.

Головна риса контенту – варіативність та гнучка, ситуативна зміна цільового призначення, що є також типовою рисою формату web 2.0 та 3.0. В цьому плані слід зазначити, що, за певних обставин, контент може стати навіть незалежним (від автора) учасником інформаційних мережевих процесів, перетворившись на так званий вірусний контент (ролик, графічне зображення, текст, звуковий трек).

Набуття певним інформаційним повідомленням статусу вірусного є найвищою ознакою успішності контента та ефективності його як інструмента інформаційного процесу. В залежності від ситуації та мети вірусний контент може бути адресним або анонімним. В інформаційних війнах частіш за все прагнуть створювати такі вуси на основі анонімності.

Як інструмент комунікаційного процесу, контент є важливим чинником в роботі фахівця із інформаційних війн. І від того, наскільки професійно підібрані методи просування контенту, залежить успіх роботи і порозуміння із відповідними представниками цільової аудиторії.

Прийоми та засоби просування контенту в соцмережах доволі варіативні та залежать від характеру ситуації, умов, постановки завдання та комунікаційних можливостей системи. Відомий російський фахівець у галузі інтернет-маркетингу Дамір Халілов визначає 100 базових інструментів 1 форматі 12-ти категорій [429, с. 124-126]:

Категорія 1. Створення та просування співтовариств бренду

1. Створення та просування співтовариств компанії у соціальних мережах
2. Створення та просування зустрічей/заходів
3. Купівля існуючих співтовариств
4. Product Placement в існуючих співтовариствах
5. Спонсорство тематичних співтовариств
6. Створення та просування Fan Page (сторінок фанатів)
7. Підтримка співтовариств «громадських маркетологів»
8. Підтримка співтовариств співробітників компанії
9. Створення мережі співтовариств для кожного товару/послуги

Категорія 2. Просування у нишевих соціальних мережах

10. Просування у закритих соціальних мережах (leprosorium та ін.)
11. Просування контенту у вузько тематичних соціальних мережах (Habrahabr, Dirty.ru та ін.)
12. Просування новин на сервісах соціальних новин (News2, Newsland та ін.)

13. Створення власної соціальної мережі

14. Прив’язка бренду до географічної позиції на гео-сервісах (GoogleMaps, Foursquare та ін.)

15. Просування через Google Buzz

16. Просування через FriendFeed

17. Просування через мобільні соціальні мережі (Vstrecher та ін.)

18. Просування через рекомендовані соціальні мережі (Imhonet, Reputacia.ru)

Категорія 3. Створення та розвиток власних інформаційних майданчиків

19. Створення та просування корпоративного блогу

20. SMO-оптимізація блогу

21. Інтеграція корпоративного сайту із соціальними мережами

22. Створення брендованих фонів для оформлення власних співтовариств та блогів (Твиттер, YouTube та ін.)

23. Написання гостьових постів для близьких по тематиці блогів

24. Кроспостінг ключових постів блогу в соціальні мережі

25. Ініціація розміщення закладок на сайті у сервісах соціальних закладок

26. Лінкбайтінг

27. RSS-маркетинг

28. Введення та просування корпоративного Твіттера

29. Розвиток власного хеш-тега в Твіттері

30. Організація промо-акцій в Твіттері

31. Створення та пром list Твіттер-каналів, пов’язаних з брендом

32. Публікація статусів на Facebook

33. Запис та просування підкастів на підкаст-директоріях

34. Введення та просування відеоблога

35. Створення он-лайн ТВ

36. Створення системи продажів через соціальні мережі

37. Розбудова партнерської системи в соціальних мережах

38. Генерація лідів через співтовариства компанії

Категорія 4. Просування контенту

39. Написання статей для Wikipedia
40. Впровадження тематичних посилань у наявні статті на Wikipedia
41. Створення лінз на Squidoo та компасів на МойКомпас
42. Просування відео на відеоагрегаторах
43. Просування фото на фотоагрегаторах
44. Просування аудіоконтенту
45. Просування презентацій у соціальних мережах (SlideShare та ін.)
46. Написання та розповсюдження соціальних релізів
47. Розміщення на сайті (в блозі) унікального безкоштовного контенту (наприклад, плагіна або електронної книги)
48. Позначення користувачів на промо-контенті

Категорія 5. Проведення інтерактивних акцій

49. Проведення вебінарів
50. Проведення віртуальних флешмобів
51. Участь у естафетах, конкурсах та флешмобах у блогосфері
52. Проведення опитувань, пов'язаних брендом
53. Надання ексклюзивних умов використання продукту для учасників співтовариства або передплатників блогу (знижки, безкоштовні заняття та ін.)
54. Стимулювання користувачів до створення контент, пов'язаного з брендом
55. Проведення у співтоваристві консалтингової акції з експертом
56. Проведення відкритої акції тестування для учасників тематичних ком'юніті
57. Організація та проведення гри в соціальних мережах

Категорія 6. Створення та просування інтерактивних елементів

58. Створення та розвиток промо-додатків
59. Product Placement у промо-додатках
60. Створення «філіалів» інтернет-магазинів у додатках для соціальних мереж
61. Розповсюдження віджетів

Категорія 7. Робота з лідерами думок

62. Взаємодія з комунікаційними хабами у соціальних мережах
63. Організація оф-лайн подій для блогерів
64. Проведення акцій тестування для блогерів
65. Ініціювання регульованого витоку інформації в соціальні мережі та блогосферу
66. Ініціювання публікації промо-постів
67. Залучення ВІП-персон до співтовариства/корпоративного блогу
68. Створення закритих ком'юніті для комунікації з лідерами думок

Категорія 8. Вірусний маркетинг

69. Створення та розповсюдження мемів
70. Створення та розповсюдження вірусних інфоприводів
71. Створення та розповсюдження вірусного контенту
72. Створення вірусних сайтів

Категорія 9. Персональний брендінг

73. Створення та просування персонального профайлу
74. Створення та просування промо-персонажу
75. Брендування аватарів користувачів
76. Просування профайлів працівників компанії
77. Просування персонального блога керівника компанії
78. Ведення рольового блогу від особи яку промотіюють
79. Просування через сервіси професійних зв'язків (МойКруг, LinkedIn)
80. Збирання «прихильників» у соціальних мереж «VКонтакте»
81. Участь представника компанії в адмініструванні популярного колективного блогу

Категорія 10. Інструменти позакатегоріальні

82. Таргетована реклама в соціальних мережах
83. Медіа реклама в соціальних мережах
84. Розміщення об'яв у соціальних мережах

85. Застосування бірж платних постів у блогах (наприклад, Блогун)

86. Використання бірж агентів у соціальних мережах (наприклад, BeAgent)

Категорія 11. Комунікативна активність

87. Спілкування з аудиторією на форумах

88. Організація гарячих ліній на тематичних ком'юніті

89. Нейтралізація негативу на комунікаційних майданчиках

90. Організація консалтингових акцій на комунікаційних майданчиках

91. Прихований (партизанський) маркетинг

92. Просування на сервісах питань-відповідей

93. Публікація статей на комунікаційних майданчиках

94. Створення системи клієнтської підтримки в соціальних мережах

95. Постійне представництво співробітника або секретаря бренду на популярному тематичному ком'юніті

Категорія 12. Рейтинги та ТОПи

96. Винесення інформації у ТОП «Головні теми дня» Яндекс. Блогов

97. Винесення посту в ТОП Livejournal

98. Підвищення блогу в рейтингу Яндекс. Блогов

99. Виведення посилання на сайт на сервісах соціальних закладок

100. Виведення посту в незалежні ТОПи популярних записів на основі API Яндекс. Блогов.

3.2. Типологія та класифікація інформаційних операцій формату web 2.0 та 3.0

Як вже було зазначено у попередніх розділах, сучасна інформаційно-психологічна війна вимагає гнучкості та інтегрованих підходів. Останнє, в свою чергу, передбачає високий рівень варіабельності при обранні інструментів та засобів роботи. Інакше кажучи, кожна кампанія або окрема акція має мозаїчний формат, який складається відповідно до ситуації та поточних завдань. Разом з

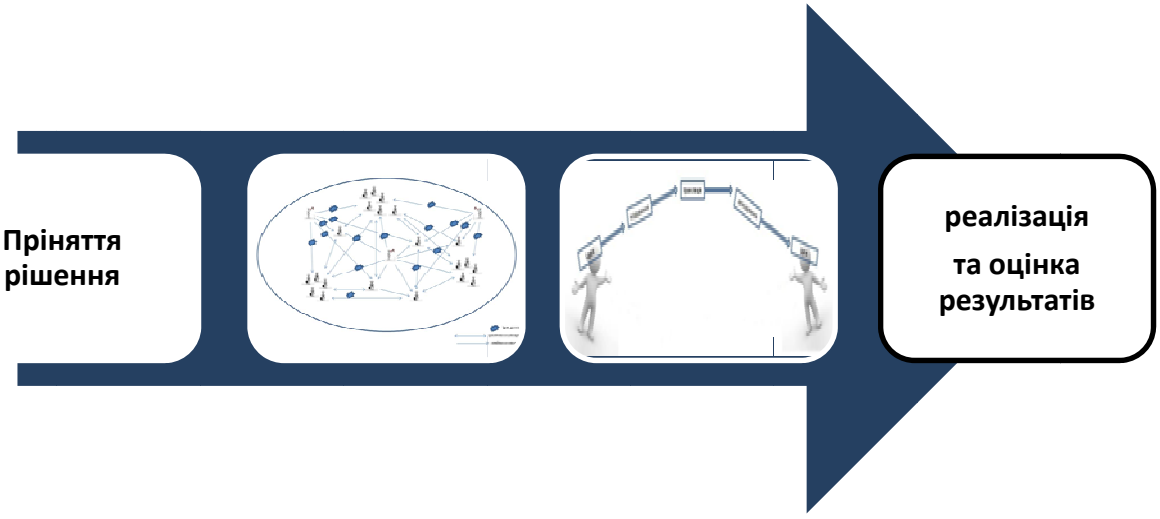
тим слід зазначити, що існують певні константні позиції, які не змінюються і є базовими ланками в кожному інформаційному процесі в незалежності від того, де, як і за яких обставин він реалізується. До таких можна віднести алгоритмічні схеми реалізації інформаційних процесів на оперативному рівні.

Операції формату web 2.0 та 3.0 є складовою частиною більш широких, в розумінні та реалізації, **інформаційно-психологічних операцій** (Psychological Operations, PSYOP). Останні визначають, як ***засіб впливу на свідомість цільових груп з метою зміни психологічних установок та стимулювання до певних дій.***

Операції формату web 2.0 та 3.0 здійснюють супроводжувальні або забезпечувальні функції по відношенню до базової інформаційно-психологічної операції, маючи свій сектор роботи та чітко визначені завдання. Інакше кажучи, вони реалізують весь спектр та комплекс завдань, що відноситься до певної оф-лайн інформаційно-психологічної операції.

За змістом, завданнями та термінами реалізації такі операції можна поділити на два види: **інформаційні акції** та **інформаційні кампанії**.

Мал.3.13. Алгоритм інформаційної акції



Інформаційні акції мають одну, чітко визначену задачу, та обмежені хронологічні рамки. Такі акції є моно цільові й зазвичай тривають від одного дня до тижня. Їх застосовують з метою розвідки («прокачки» ситуації), коли необхідно відпрацювати на випередження або вирішити локальну комунікаційну проблему.

Алгоритм підготовки та реалізації такої операції будується на основі моделі типового лінійного інформаційно-комунікаційного процесу та врахуванні особливостей інформаційного поля, в рамках якого відбуватиметься операція.

Підготовка та реалізація інформаційної акції web 2.0-3.0 складається з таких етапів:

1. **Прийняття рішення** – формулювання завдання, уточнення цільових груп, виділення ресурсів та визначення очікуваних результатів у вигляді певного комунікаційного ефекту від поширення або збирання контенту.

2. Розробка **тактичного плану** операції – уточнення меж інформаційного поля, визначення реакцій, які ми очікуємо від цільових груп, визначення інформаційних посилів/меседжів, оцінка характеру зв’язків між соціальними групами та окремими об’єктами, вибір інструментів, які мають бути використані в роботі.

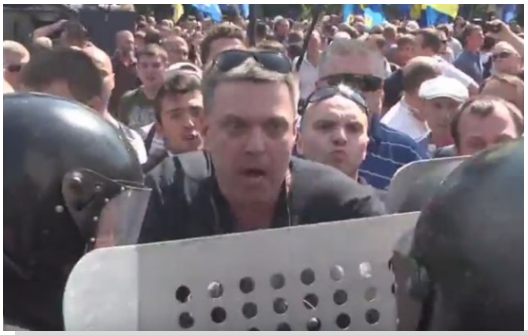
3. **Ситуативне планування** – уточнення меседжів (1), кодування у вигляді текстів, аудіо, відео, мультимедіа (2), транслювання через ЗМІ (3), декодування – ознайомлення (4), формування власної думки (5).

4. **Реалізація** операції відповідно до розробленого та узгодженого плану.

5. **Підбиття підсумків**, складання звіту та оцінка результатів.

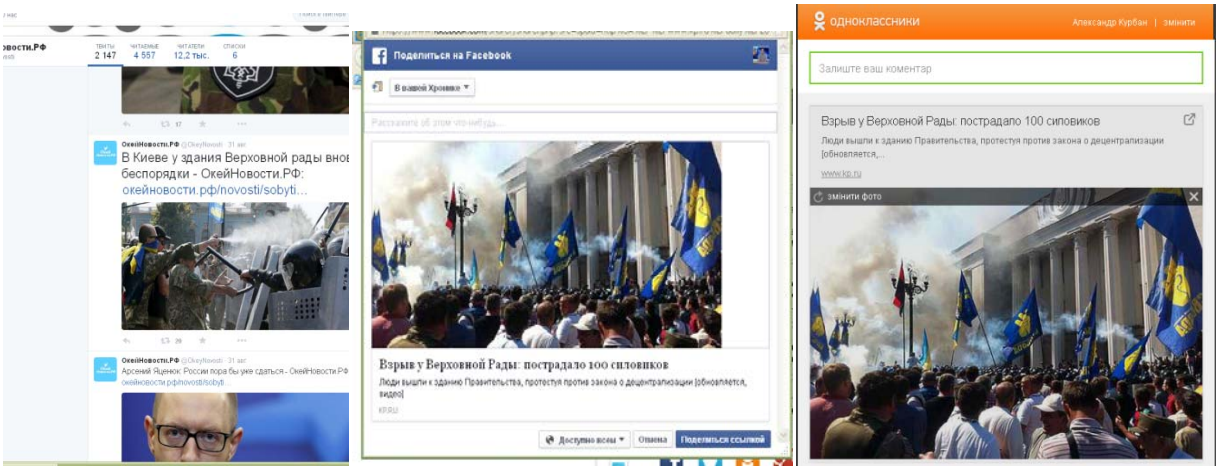
Практичний приклад

31 серпня 2015 р. під Верховною Радою сталися сутички між правоохоронцями та радикально налаштованими прибічниками кількох політичних сил, що виступали проти внесення змін до Конституції України відповідно до Мінських угод.



Під час сутичок перед приміщенням Верховної Ради з'явилося багато російських журналістів, які цю акцію подали у відповідному світлі та запустили в медіа і соцмережах із відповідними акцентами.

Події було активно поширено в соціальних мережах. Зокрема таких, як Twitter, Facebook, Odnoklassniki, VKontakte із відповідними коментарями та висновками.

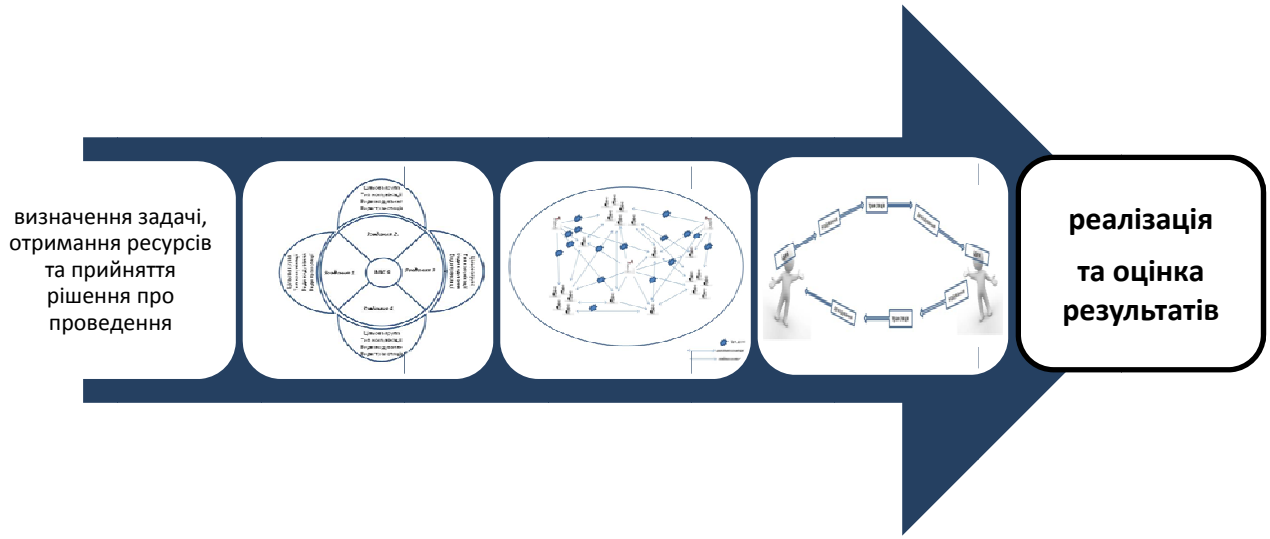


Інформаційні кампанії зазвичай мають одну стратегічну мету та кілька тематичних завдань. Такі операції є тривалими – від кількох тижнів до року і більше та є поліцільовими.

Протягом тривалого часу (XX ст.) такі операції носили лінійний характер і здійснювалися від початку до кінця за чітко визначеною схемою, яка була характерною ознакою першого покоління інформаційно-психологічних війн.

Сьогодні, за умови застосування принципів інформаційно-психологічної війни другого покоління, по ходу реалізації операції завдання можуть коригуватися і навіть змінюватися, при цьому мета залишається незмінною. Це надає таким операціям певної асиметричності, гнучкості, непередбачуваності. Фінал кожного етапу операції перетворюється на точку біфуркації, в який розробляється та приймається певне управлінське рішення, яке відповідає певній комунікаційній ситуації та обставинам, що її формують та впливають на її подальший перебіг.

Мал.3.14. Алгоритм інформаційної кампанії



Підготовка та реалізація інформаційної кампанії web 2.0 та 3.0 складається з таких етапів:

1. **Прийняття рішення** – визначення завдання, уточнення цільових груп, виділення ресурсів та визначення очікуваних результатів.

2. Розробка **стратегічного плану** – визначення мети, завдань, цільових груп, ресурсів, напрямків реалізації.

3. Розробка **тактичного плану** операції – уточнення меж інформаційного поля, визначення бажаної реакції цільових груп, визначення інформаційних посилів/меседжів, оцінка характеру зв'язків між соціальними групами та окремими об'єктами, вибір інструментів, які мають бути використані в роботі.

4. **Ситуативне планування** – уточнення базових меседжів (1), кодування у вигляді текстів, аудіо, відео, мультимедіа (2), транслювання через ЗМІ (3), декодування – ознайомлення (4), формування власної думки (5) з подальшим циклічним продовженням.

5. **Реалізація** операції відповідно до розробленого та узгодженого плану.

6. **Підбиття підсумків**, складання звіту та оцінка результатів.

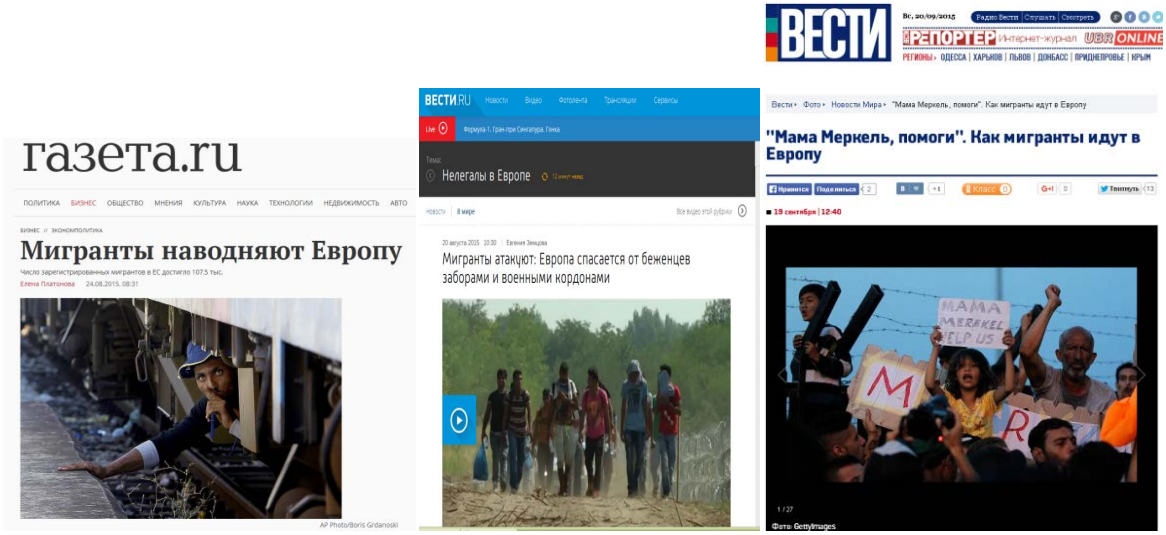
Практичний приклад

Найбільш гучною та потужною інформаційною кампанією у 2015 р. стала атака біженцями з країн Близького Сходу (Сирія, Ліван та ін.) спрямована на країни ЄС. Ця кампанія, відповідно до стратегічного задуму її організаторів, мала на меті послаблення одного з надпотужних учасників антипутінської коаліції та розхитування єдності самої коаліції. Основними завданням кампанії були:

- *дестабілізація внутрішньополітичної ситуації в країнах ЄС;*
- *викликання недовіри громадян до національних урядів та керівництва ЄС у цілому;*
- *стимулювання руху протестів та заворушень;*
- *здійснення тиску на керівництво країн ЄС щодо необхідності зближення із РФ та зняття санкцій.*

Кампанія розгорталася по класичній схемі – створити проблему, роздмухати її, а згодом запропонувати рішення/допомогу, яке є вигідним для «автора» кризи.

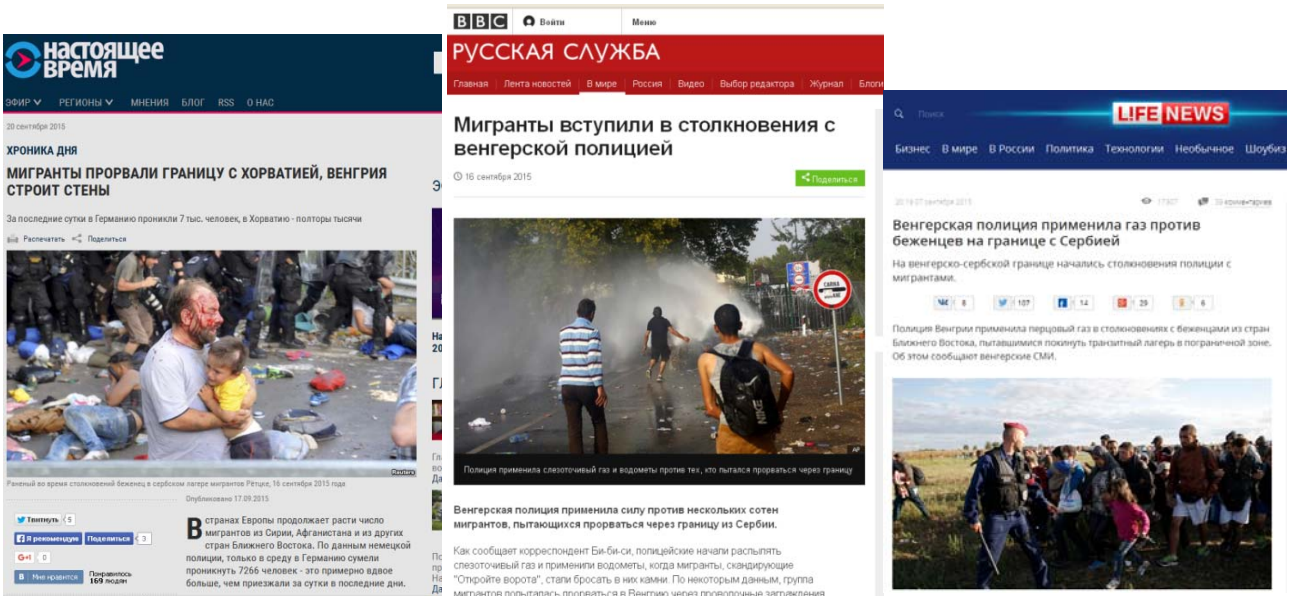
Спочатку було актуалізовано проблему в ЗМІ:



Головною тезою стало збільшення в рази потоків біженців, які спрямовуються в країни ЄС. З метою посилення ефекту залякування було повідомлено, що серед мігрантів дуже багато чоловіків молодого та середнього

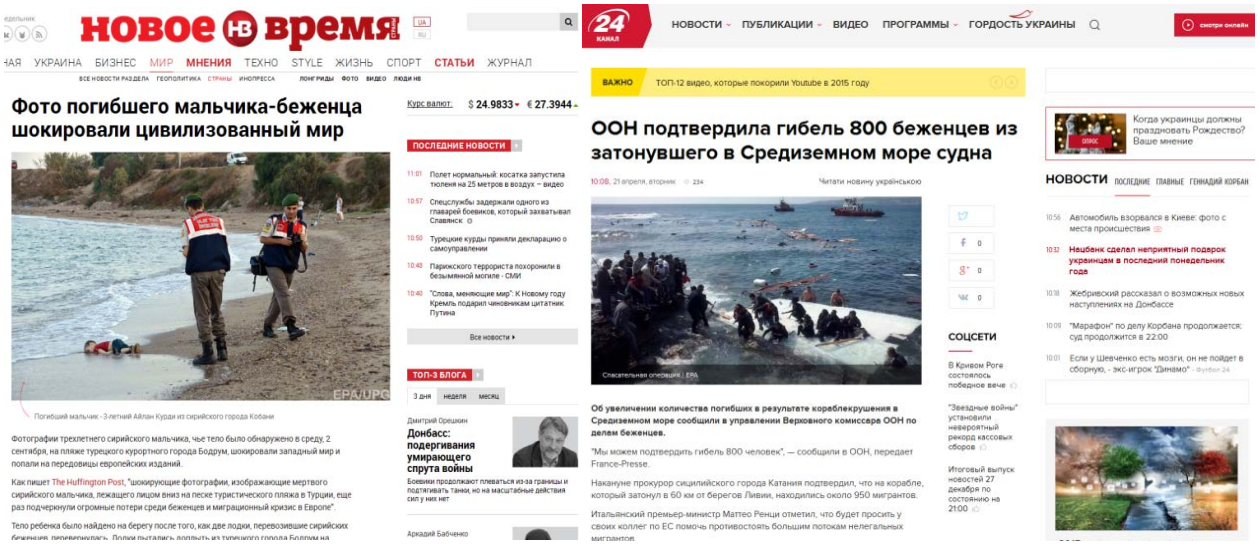
віку, які є агентами впливу та бойовиками ІДІЛУ. При цьому надавалися персональні фото осіб, які є «відомими терористами» з лав ІДІЛу:

Далі відбулися події у вигляді масового напливу та сутичок на кордонах ЄС, що набули максимального розголосу в європейських та світових ЗМІ. Масштабна медіа-атака була здійснена у російських ЗМІ:

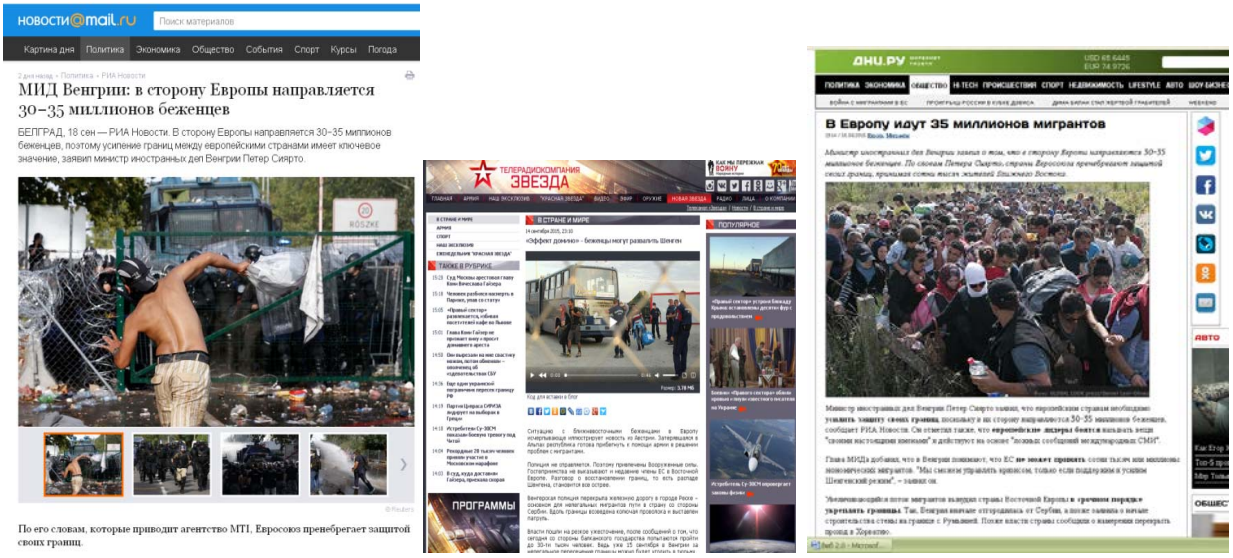


Особливо активно поширювалися фото та відео, де було видно, як біженці агресивно атакують прикордонні пункти, нападають на прикордонників та

вчиняють інші протиправні дії. При цьому окремий акцент здійснювався на факті гуманітарної катастрофи та порушенні базових прав людини.



З метою максимального накалу ситуації з'явилися повідомлення про можливість збільшення чисельності мігрантів до 30-35 млн., що призведе до колапсу Шенгенської системи та розвалу ЄС:



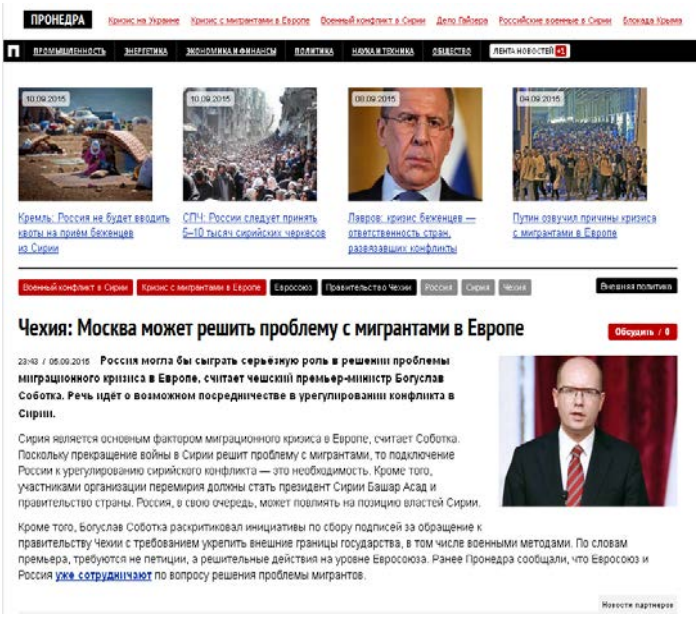
Слід зазначити, що на цьому етапі інформаційна кампанія досягла максимального результату. Переважна частина населення ЄС була дійсно налякана і схилялася до ідеї зміни формату ЄС, Шенгенської угоди та ін.

Також здійснювалися спроби інформаційного залякування щодо перспективи впливу мусульманської громади на традиції та принципи європейців.

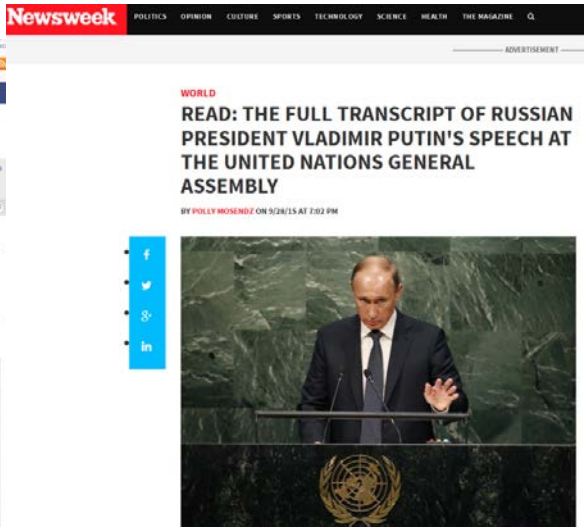
http://pikabu.ru/story/musulmane_germanii_trebuyut_otmenit_nemusulmanskiy_pivnoy_festival_oktoberfest_v_myunkhene_3659467

І після того, як ситуацію було доведено до точки кипіння, через ЗМІ та соціальні мережі пройшла теза про те, що Росія готова допомогти ЄС вирішити проблему з мігрантами, з натяком, що за це Путін чекає на зняття санкцій.

Слід зазначити, що саме на цей момент припадає максимальна активність кремлівських тролів у національних групах у соціальних мережах та в коментарях до ТОПових тематичних статей. Головною метою такої атаки було створення фейкової громадської думки - панічних настроїв, що створюють стан масового когнітивного дисонансу та спонукатимуть до думки або рішення, яке працюватиме на користь атакуючої сторони.



Фінальним акордом кампанії став виступ президента Путіна на 70-й сесії Генеральної Асамблеї ООН, де він цю проблему зазначив як глобальну, та намагався запропонувати власний варіант її вирішення. Фактично його виступ остаточно розкрив усі карти та намалював загальну картину інформаційно-психологічної атаки, яку здійснювали відповідні структури керівництва РФ.



3.3. Базові прийоми в інформаційних війнах

3.3.1. Прийоми захисту від інформаційних атак в он-лайн мережах

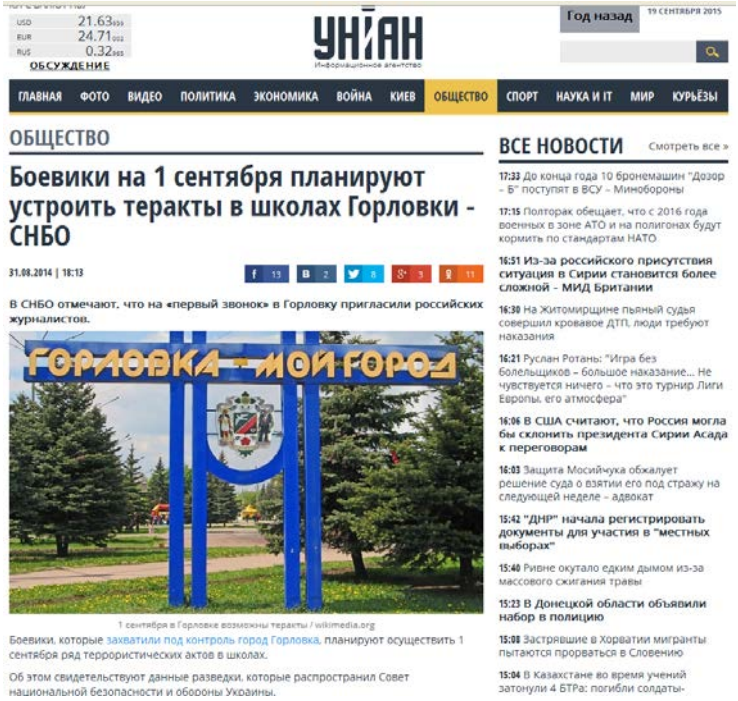
У цілому слід зазначити, що застосування інформаційної зброї та ефект від її дії може бути подібний до застосування зброї масового знищення. Глобалізація медіа процесів перетворює окремі інформаційно-психологічні акції на події планетарного масштабу. Саме так це було приміром із терористичною атакою Аль-Каїди на вежі Всесвітнього торговельного центру (Нью-Йорк) та будівлю Пентагону (Вашингтон) 11 вересня 2001 р., яку в усьому світі спостерігали навіть у режимі реального часу.

Зважаючи на зазначені вище обставини, проти інформаційної атаки краще всього діяти або **на випередження**, шляхом **оперативного реагування,** або створивши потужний **ментальний бар'єр** у свідомості тих, хто має стати ціллю такої атаки. В усіх трьох випадках основний формат дій – **розвінчання** неправдивої інформації.

Серед засобів захисту від інформаційної атаки найбільш ефективним є ***робота на випередження*** шляхом поширення у певному інформаційному полі (де станеться атака) інформації, яка може бути інструментом атаки із відповідними поясненнями або застосовуючи сарказм чи гумор. Таким чином, потенційні отримувачі небезпечної інформації – представники конкретної цільової групи або кількох груп будуть готові до прийому такого повідомлення та сприйматимуть його критично.

У цьому разі створюється малий, тимчасовий ментальний бар'єр, що стає свого роду тимчасовим щепленням від інформаційного вірусу, який вкидає супротивник у наше інформаційне середовище.

Практичний приклад



http://www.unian.net/society/957452-boeviki-na-1-sentyabrya-planiruyut-ustroit-teraktyi-v-shkolah-gorlovki-snbo.html

Спрацювавши на випередження, розмістивши відповідні матеріали у власних ЗМІ (преса, інтернет-видання, радіо та телебачення), українській стороні вдалося випередити, в плані інформаційної атаки, провокації з боку терористичних угруповань ДНР-ЛНР. Втративши ефект несподіванки та можливість звинуватити в обстрілах українську сторону,провокатори відмовилися від своїх планів.

Оперативне реагування є антикризовим інструментом ситуативного характеру. Він застосовується в разі, коли інформаційна атака застала атаковану сторону зненацька, а її наслідки не можна ігнорувати через потенційно небезпечні наслідки. В такому разі, через попередньо сформовану інформаційну мережу (ЗМІ, постінг у групах, інформація на акаунтах відомих блогерів) надається інформація спростовуючого та роз'яснювального

характеру. В цьому плані результативність захисту напряму залежить від якості обгортки контенту. Особливо цінними у такому разі є вірусні матеріали.

Найбільш результативно в таких випадках працює так зване «сарафанне радіо», яке по ефективності впливу на широкі маси є важливішим іноді за класичні ЗМІ, бо транслюється у неформальному середовищі від знайомих джерел. Саме тому повідомлення в ЗМІ та соціальних мережах потрібно формувати під стандарти чуток – проста форма, зрозумілі ідеї, сенсаційний характер. Для виконання таких завдань краще всього використовувати блоги та мікроблоги, а також підключати відомих блогерів із широкою власною мережею контактів.

Типовими для інформаційної війни в цілому, а також дієвими для інформаційної війни у соціальних он-лайн мережах є такі методи нейтралізації інформаційних атак, як [317, с. 50]:

1. ***Парасолька*** – обмеження технічним шляхом (блокування доступу до окремих порталів, сайтів, соціальних мереж);
2. ***Воронка*** – нейтралізація певного повідомлення шляхом поглинання на фоні великої кількості інших;
3. ***Колесо*** – заміна певного повідомлення іншим, як більш важливим та статусним
4. ***Заміна*** – спростування певної інформації шляхом викликання недовіри до джерела розповсюдження повідомлення.

Практичний приклад

У період захоплення російськими військами АР Крим в українських ЗМІ з'явилася інформація про те, що через Чонгар у бік Запоріжжя висувається колона російських танків. Інформація спричинила значну паніку в соціальних мережах та призвела до певних негативних наслідків у системі державного та військового управління. Зусиллями блогерів-активістів ця інформація була

оперативно перевірена та відповідне спростування було поширено в українській частині он-лайн соцмереж.


ВЕСТИ

РЕПОРТЕР Интернет-журнал UBR ONLINE

СМИ сообщили о проходе российских войск через Запорожскую область

Колонна военных якобы была замечена в районе Чонгарского полуострова

Российских солдат видели из Азова? Фото: mil.ru

Дочь Яроша служит в батальоне отца

Шустер дал ответ "1+1": Я не ваш раб и не дерьмо в ваших руках

ООН: Доказательства по пожару в Доме профсоюзов уничтожены

Выходные готовят украинцам 33 градуса жары

Как Мосийчук с "Азовом" ставил на колени сотрудников ГАИ

НБУ объявил о ликвидации банка "Столичный"

Порошенко повысил прожиточный минимум и минимальную зарплату

СК обвинила силовиков в мукачевской стрельбе

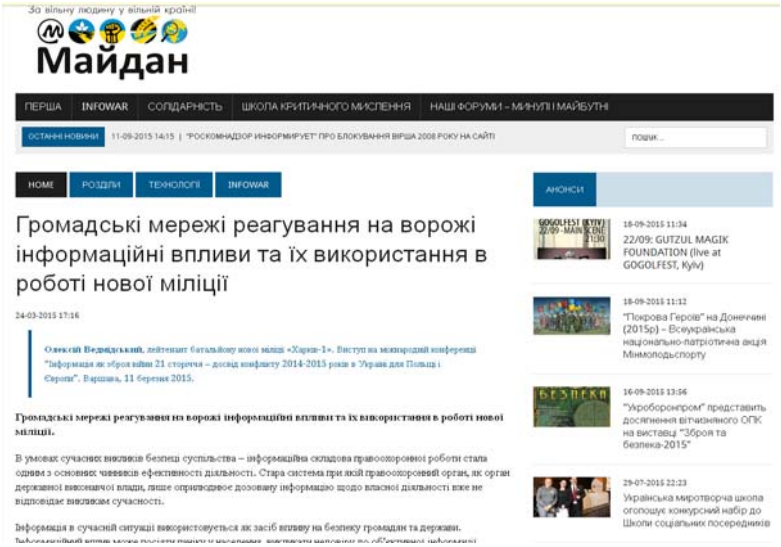
http://vesti-ukr.com/strana/40325-smi-soobwili-o-prohode-rossijskih-vojsk-cherez-zaporozhskuju-oblast

Такий прийом неодноразово використовувався російською стороною з максимально разючим ефектом. Згодом українська сторона навчилась відповідним чином реагувати на такі інформаційні провокації. Зокрема найбільш ефективним засобом стала робота на випередження.

Найбільш надійним засобом боротьби із інформаційними атаками є ***створення тотального ментального бар'єру***, який може витримати будь-які несподіванки. При цьому отримувачі інформації будуть знаходитися на певних ідеологічних позиціях, що дозволить їм критично сприймати або взагалі не сприймати шкідливу інформацію. Створення такого механізму є довготривалим процесом та передбачає налагодження системного інформування на основі мультимедійного ефекту та багатократного повторення певних попереджень, розкриття механізмів можливих маніпуляцій та типових фейків, з якими можуть стикнутися основна маса населення.

Формування такого роду захисту є комплексною роботою, до якої необхідно залучати зусилля та ресурси суспільства, держави та окремих громадських лідерів.

Практичний приклад



http://maidan.org.ua/2015/03/hromadski-merezhy-reahuvannya-na-vorozhi-informatsijni-vplyvy-ta-jih-vykorystannya-v-roboti-novoji-militsiji/

Багато громадських об'єднань та рухів сьогодні займаються просвітницькою роботою, підготовкою певних соціальних груп, потенційно вразливих щодо можливих інформаційних атак.

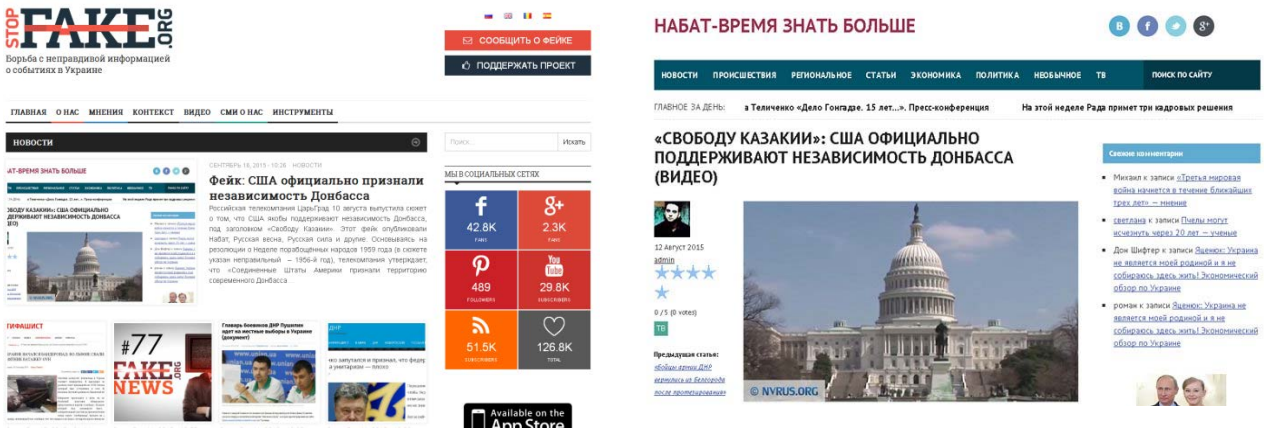
Найкращим форматом боротьби із інформаційними атаками є **розвінчання фейку** із тлумаченням характеру та реального змісту повідомлення.

Зважаючи на той факт, що переважна більшість інформаційних атак у форматі сьогочасних інформаційно-психологічних війн є анонімними, одним з ключових механізмів розвінчання є з'ясування та доведення до відома широкої громадськості авторів агресії або тих, на чию користь вона працює.

У залежності від характеру та специфіки інформаційної атаки до справи розвінчання необхідно залучати різного роду ресурси. Найбільш ефективними в цьому плані є неформальні або такі, що є авторитетними для відповідних

цільових груп. У разі масштабності нападу до процесу розвінчання мають залучатися всі можливі ресурси – державні, громадські, індивідуальні.

Практичний приклад



http://www.stopfake.org/fejk-ssha-ofitsialno-priznali-nezavisimost-donbassa/

Перекрутивши зміст резолюції про «Тиждень поневолених народів» (1956 р), російські ЗМІ поширили інформацію про визнання з боку США країни «Казакії» (Донбас, Кубань, Ростовська обл.). Цей фейк було спростовано шляхом надання повного тексту резолюції та відповідних роз'яснень.

3.3.2. Прийоми здійснення інформаційних атак у он-лайн мережах

В основі будь-якої інформаційної атаки лежить базовий алгоритм інформаційного процесу web 2.0 та 3.0. Основними його етапами є:

- створення контенту;
- розміщення на певному віртуальному майданчику;
- поширення;
- моніторинг та аналіз результатів операції.

Найбільш ефективними прийомами інформаційних атак є: **дезінформація**, **залякування**, **схематизм**, **глузування**, **вклинювання**, **фальшування**.

З метою введення противника або цільові групи, що визначені як мішень для атаки, застосовується ***дезінформація – надання хибної інформації***.

Практичний приклад

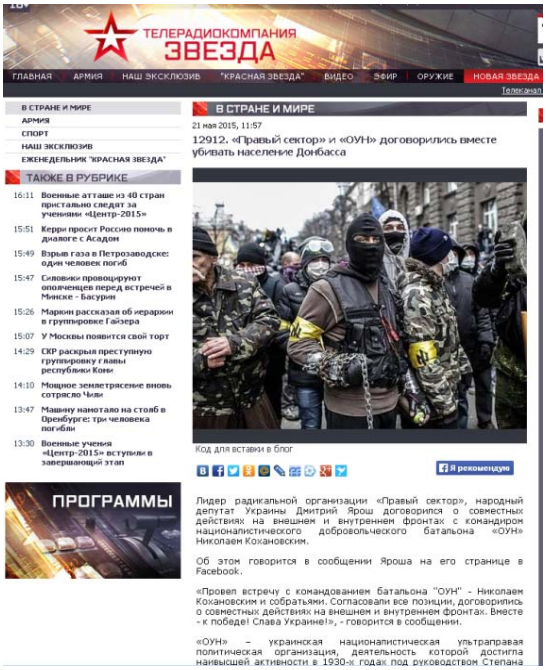
http://www.kp.ru/daily/26205/3091200/

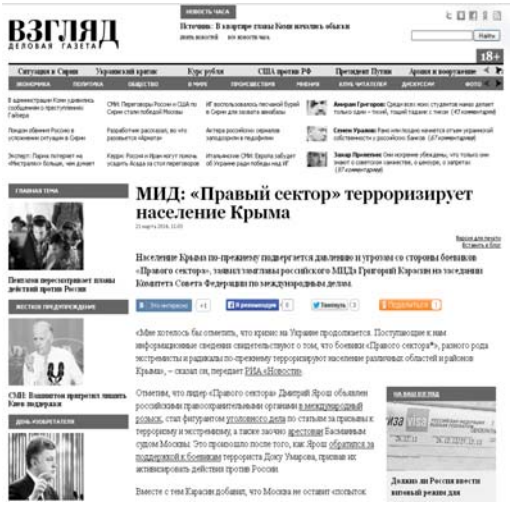
Перші тижні після перемоги Євромайдану в східних та південних регіонах України поширювалися на рівні місцевих офіційних ЗМІ (преса та інтернет-видання окремих політичних структур) неправдиві повідомлення дискредитуючого характеру.

Приміром абсолютно серйозно говорилося про відрахування грошей з зарплат шахтарів та металургів на відновлення Майдану. Останнє окрім політичного подразника (бендерівський Майдан) мало ще й економічний. Ця інформація з часом набула формату медіа-вірусу та через неформальні канали комунікації отримала максимального поширення.

Для відволікання уваги від реальних цілей та намірів противника й представників цільових груп-мішеней частіш за все застосовують ***залякування - трансляція інформації, що має на меті порушення рівноваги та формування тривожних або панічних настроїв.***

Практичний приклад



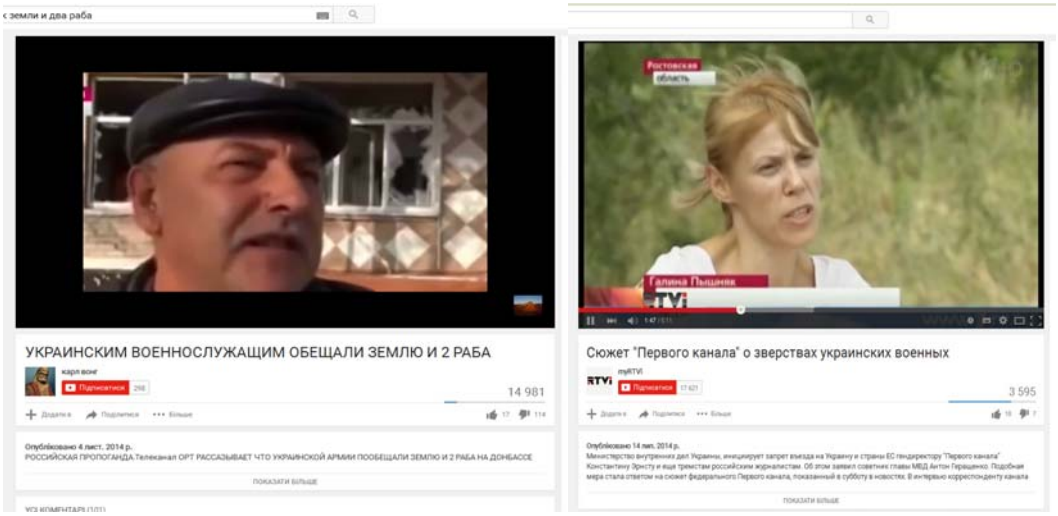


http://tvzvezda.ru/news/vstrane_i_mire/content/201505211157-s4p6.htm http://vz.ru/news/2014/3/21/678285.html

На початку російської агресії на Сході України та в Криму активно поширювалися повідомлення про те, як українські радикальні націоналістичні організації готуються тероризувати російськомовне населення. Останнє викликало панічні настрої, а під це в свідомість місцевих мешканців закладалися ідеї про необхідність створення загонів самооборони та відокремлення територій від України.

Окрім матеріалів у друкованих ЗМІ та повідомленнях з інтернет-видань було запущено в якості вірусних роликів відео з постановочними кадрами вуличних зіткнень, під час яких молодики з українською націоналістичною символікою підпалюють авто, тероризують пересічних громадян. Особливою популярністю користувалися виступи фейкових свідків злочинів Нацгвардії або бойовиків «Правого сектору», як то: Галини Пишняк про розіп'ятого хлопчика,

свідків, що розповідали про винагороду «українським карателям» за участь в АТО у вигляді клаптика землі і двох рабів та інші.

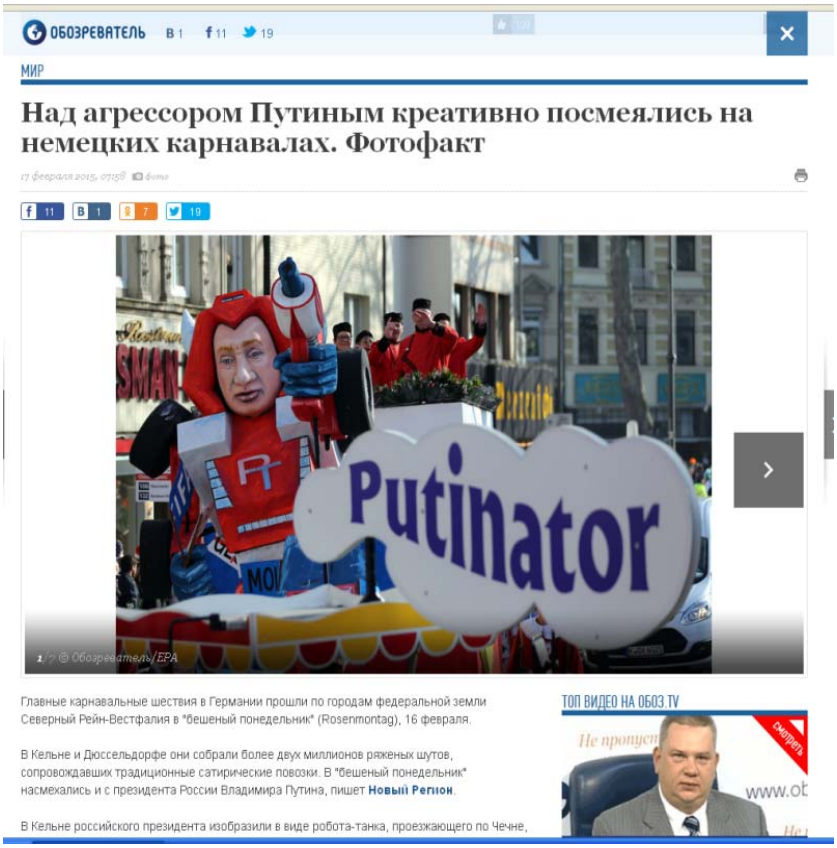


Для спрощення та прискорення сприйняття інформації її отримувачами застосовується ***схематизування – графічно-кількісна подача даних у доступному для представників цільової групи форматі.*** Представлена в такому вигляді інформація використовує принцип образно-символьного сприйняття, яке вважається найбільш ефективним для промоції певних ідей або ідеологічних концепцій.

Практичний приклад

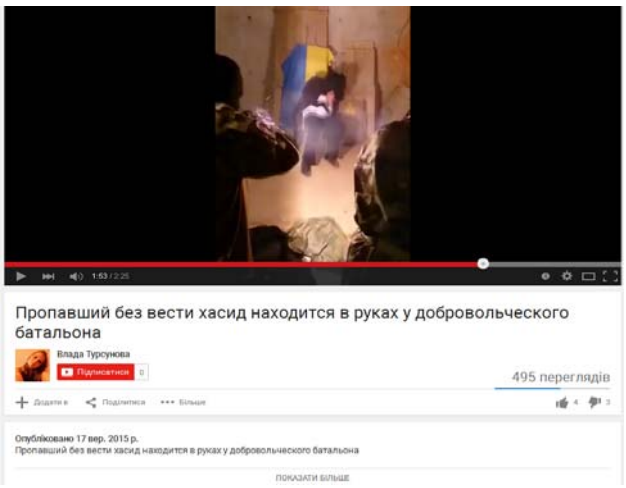
Під час підготовки до ведення активних дій в оф-лайн форматі та в якості нейтралізації передбачень щодо потенційних можливостей противника використовують метод ***глузування – виставлення противника та його можливостей в комічному світлі.*** В такому разі спрацьовує психологічний принцип те, що комічне, не викликає страху або опасінь.

Практичний приклад



http://obozrevatel.com/abroad/97542-nad-agressorom-putinyim-kreativno-posmeyalis-na-nemetskih-karnavalah--fotofakt.htm

В якості своєрідного інформаційного айкідо для посилення ефективності та атакуючого потенціалу можливо застосувати ***вклинювання - використання інформаційних повідомлень противника шляхом додавання до них певної інформації і корекції повідомлення в потрібному руслі.***



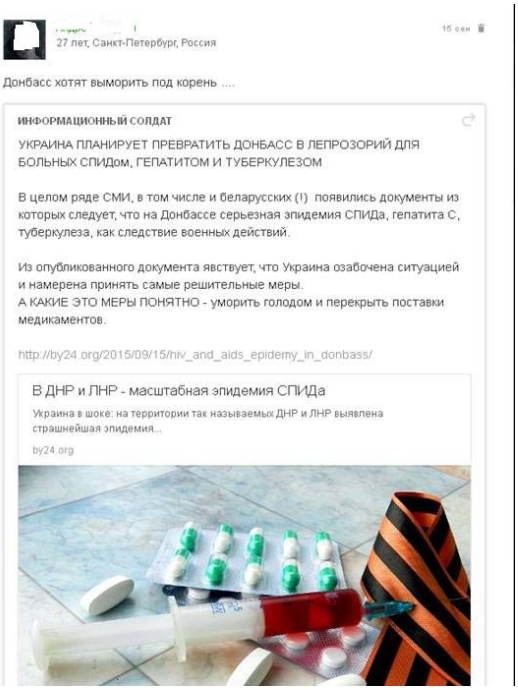
http://izrus.co.il/dvuhstoronka/article/2015-09-17/28853.html https://www.youtube.com/watch?v=rz3SSM99p6w

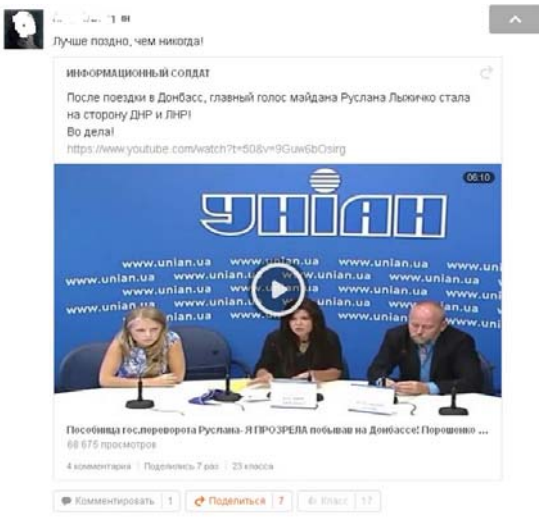
Скориставшись повідомленням про зникнення хасіда, що прибув до Умані на святкування нового року, група прибічників Росії зняла відео, на якому начебто представники добровольчих батальонів катують викраденого громодянина Ізраілю.

У соціальних мережах цей прийом зазвичай використовують для того, щоб на фоні повідомлення ЗМІ, яке не викликає сумніву, подати приховані меседжі або психологічні установки. Для цього, в якості базової основи для повідомлення, обирається потрібний матеріал (посилання, фото, відео), а на додаток до нього у ліді (анотація або підводка до матеріалу) концентрується те, що є основним змістом. Для загальної маси фоловерів, яка не має критичного сприйняття мережевої інформації, такий прийом є досить результативний.

Практичний приклад

Так, українськими інформаційними бійцями на основі матеріалу білоруського інтернет-видання http://by24.org про масштабну епідемію в ДНР-ЛНР було створено пост, що мав на меті поширення панічних настроїв серед так званих ополченців та місцевого населення, яке підтримує Росію.





Також можна навести приклад застосування аналогічного прийому з протилежного боку, коли за основу для атакуючого повідомлення було взято ролик з емоційним виступом української співачки та громадського діяча Р.Лижичко про ситуацію на окупованих територіях Донбасу. Головна мета мережевого повідомлення в цьому випадку – використання авторитету лідера громадської думки для посилення тези та приховання реальних намірів.

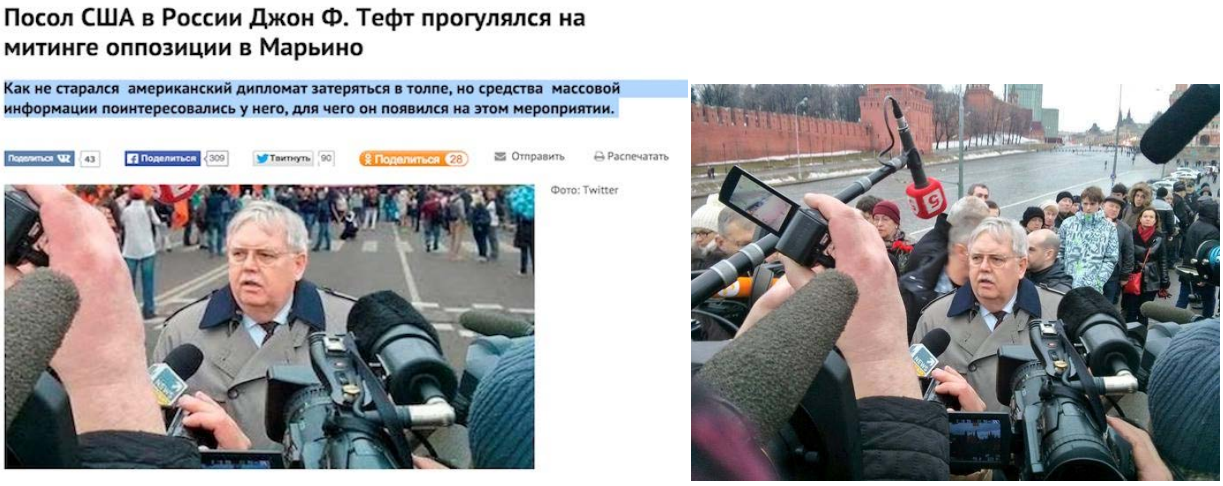
Фактично впродовж усього періоду інформаційної війни, яку веде Росія проти України, через брак візуальних матеріалів ***використовується контент з іншими подіями, що є класичним методом фальшування***.

Практичний приклад

Прибічник «ДНР» у своєму блозі видав фото подій в Ізраілі за події в Донецьку. Представники ЗМІ фейкових республік доволі часто використовують задля ілюстрації власних меседжів спотворені або перекручені матеріали, в тому числі відео для підкріплення власних позицій.

http://www.ipukr.com/?p=39845

Приклад застосування інтегрованого маніпулювання з позиціонуванням на фоні відомого інформаційного бренду (телеканал «1+1») та заголовка-якоря, який гіперболізує зміст самої статті.



Типовий приклад маніпуляції в газеті «Комсомольская правда» (ліве фото). Інформація про те, що посол США начебто відвідав у Москві акцію протесту опозиції, ставши її духовним лідером. Для ілюстрації цієї інформації дали змонтоване фото посла на фоні акції. В реальності це фото зроблене в іншому місці (праве фото.)

3.3. 3. Прийоми та засоби маскування і демаскування в інформаційних протистояннях

Однією з важливих складових частин діяльності в будь-яких військових протистояннях є вміння маскуватися або розкривати замаскованого противника. Це мистецтво особливо актуальне і в протистояннях у соціальних он-лайн мережах.

Зважаючи на те, що головним засобом боротьби у соціальних мережах є обмін інформацією та спілкування, успішною буде комунікація між тими, хто має однакові погляди або належить до близьких соціальних груп. Саме тому дуже важливо, щоб майданчик, з якого відбувається трансляція інформаційного послання або персональний акаунт мали відповідний вигляд.

Обкладинка та інше оформлення в групах, на сторінках та акаунтах має відповідати образам та символам, характерним тим групам, на які вони

орієнтовані. Аватарки на блогах та акаунтах повинні виглядати також відповідним чином. Це все аксіома, яка не потребує деталізації та обґрунтування.

Більш складним та специфічним є питання функціонування так званих ботів та тролів – фейкових акаунтів, які застосовуються в якості атакуючих одиниць у класичній війні формату web 2.0 та 3.0. Загально відоме негативне ставлення інтернет-спільноти до таких суб'єктів. Ідентифікація в якості троля автоматично викликає недовіру до трансльованої інформації, робить марними всі зусилля та навіть може допомогти зрозуміти плани противника. Тому, особливо важливо мати навички маскування власних фейкових акаунтів та вміння вираховувати ворожі.

Для надання власним акаунтам більшої правдивості необхідно:

1. ***Обирати реальне ім'я***, яке є типовим для представників відповідних цільових груп;

2. Ставити на аватарку реальне фото – обирати фотографію будь-якої людини;

3. Робити акаунт реальним - створювати персоніфіковані альбоми, підписуватися на різнопланові (не тільки за призначенням троля) сторінки і групи, ставити разом з тематичними пости, що мають розважальний або персональний характер.

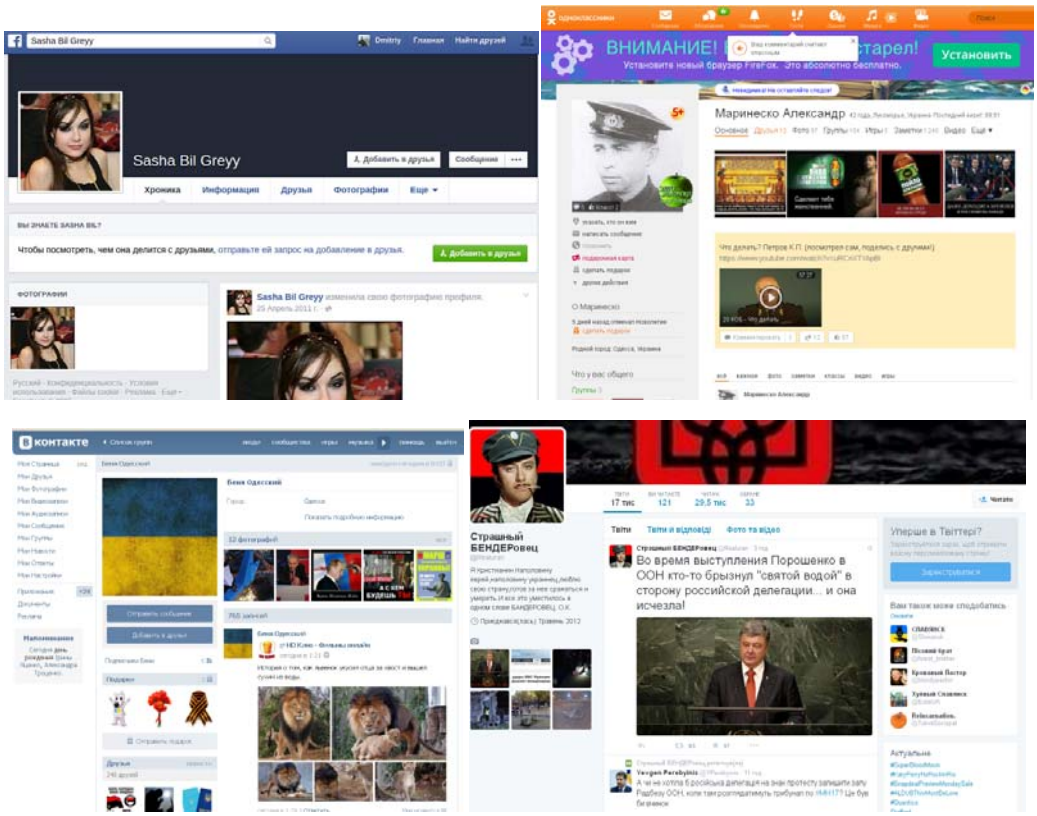
Загальне правило – такі акаунти не мають сильно виокремлюватися на фоні інших, вони мають бути типовими, стандартними на фоні відповідних представників цільових груп.

Реєструючи такі акаунти в тематичних групах, необхідно проявляти життєву активність – лайкати чужі пости, ставити нейтральні коментарі.

Життєва активність фейкових акаунтів, крім маскування, має ще одне завдання – налагодження корисних контактів, видобування важливої інформації та вербування прибічників (напряму або «втемну»)

Демаскування фейкових акаунтів, відповідно, відбувається за такими ж трьома ознаками, але в такому разі фіксується їх відсутність або не повна відповідність.

Мал. 3.15. Типові фейкові аканти

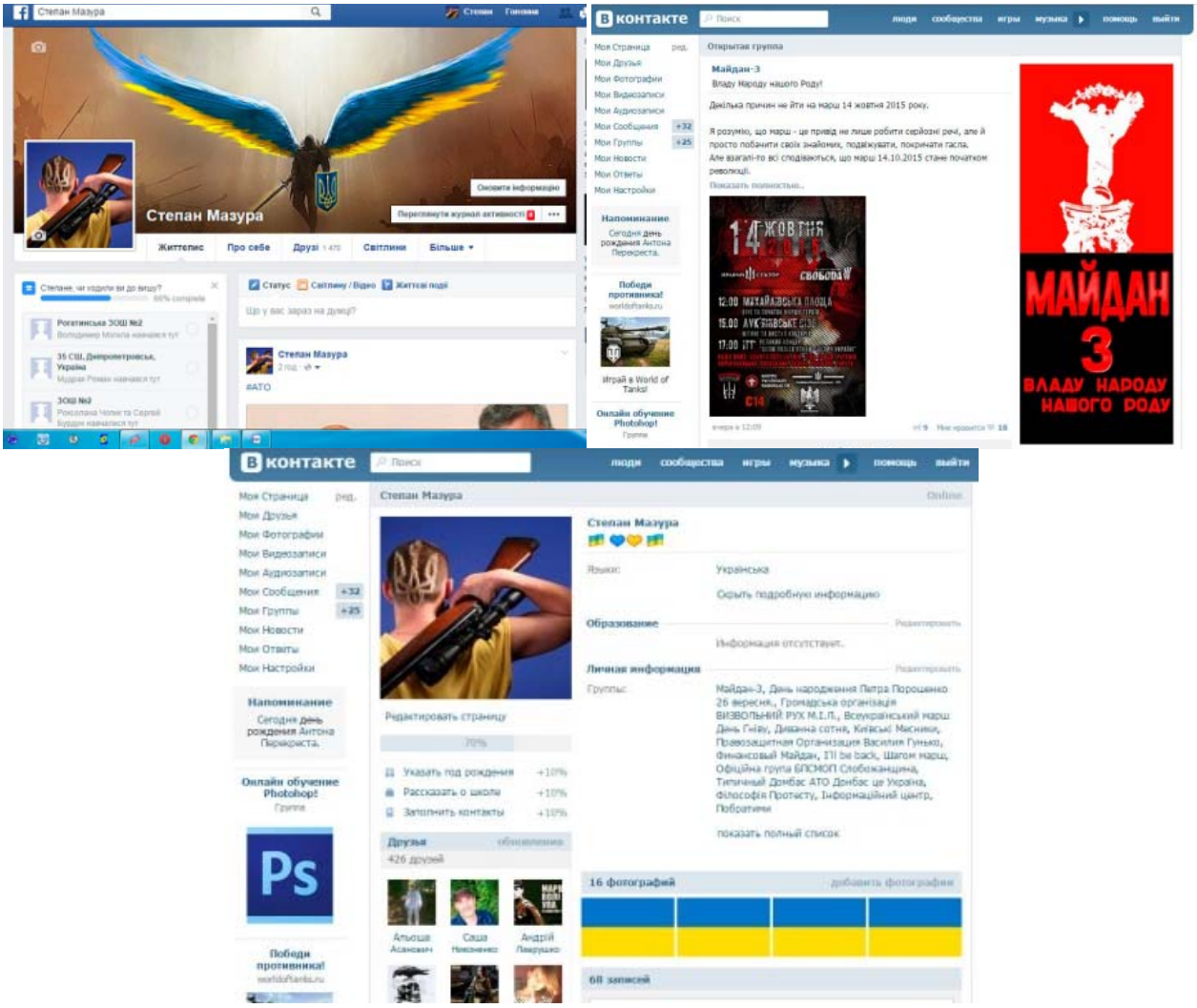


Серед класичних ознак, за якими можна ідентифікувати типового троля, можна визначити такі, як:

- шаблонність формулювань та висловлювань, що виникає внаслідок використання кількох варіацій на один меседж;
- демонстративна лояльність по відношенню до головної теми, занадто палка підтримка офіційної влади, окремих персоналій;
- висока агресивність, використання ненормативної лексики, персональні образи, знущання, погрози.

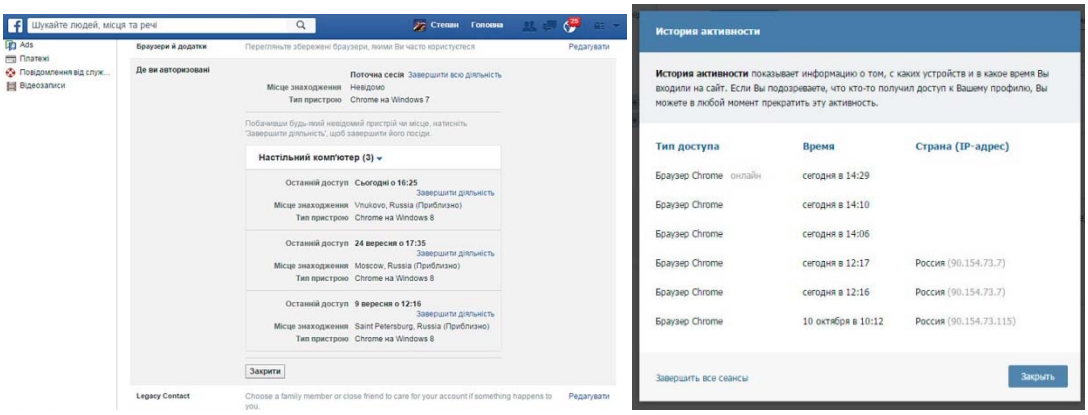
Практичний приклад.

Типовим прикладом вдалого маскування та доволі успішного виконання завдань із інформаційно-психологічної диверсії може слугувати діяльність групи, очолюваної мережевим активістом, колишнім бойовиком ДНР Сергієм Жуком, що діяв як медіа-активіст під ніком «Степан Мазур» і позиціонував себе у провідних соціальних мережах під виглядом українського націоналіста.

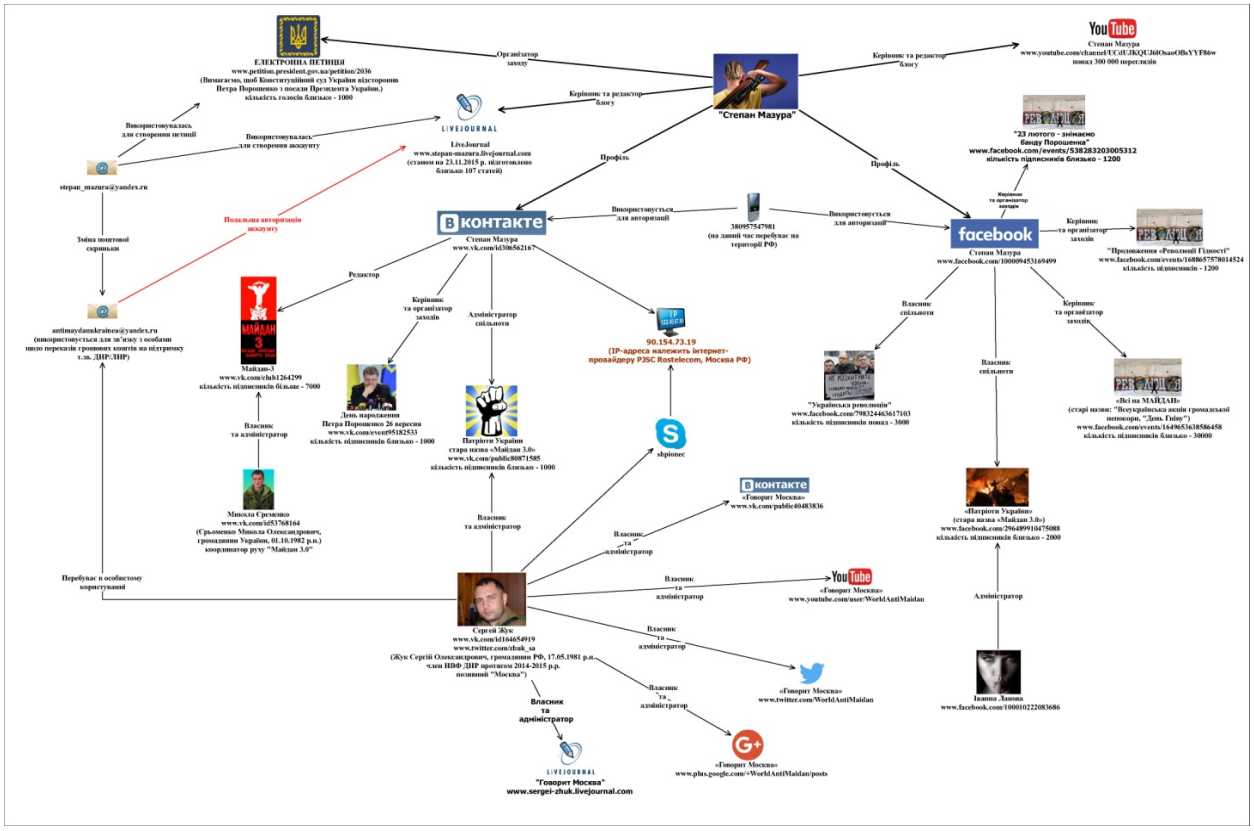


Головним завданням цього агента впливу було підбурення населення проти влади. Для цього було створено групи «Майдан-3» в провідних соціальних мережах. Головним меседжем стали заклики до організації нового Майдану.

«Степана Мазура» доволі швидко вирахували за IP-адресою і встановили місце його базування. Цим місцем виявилася Москва.



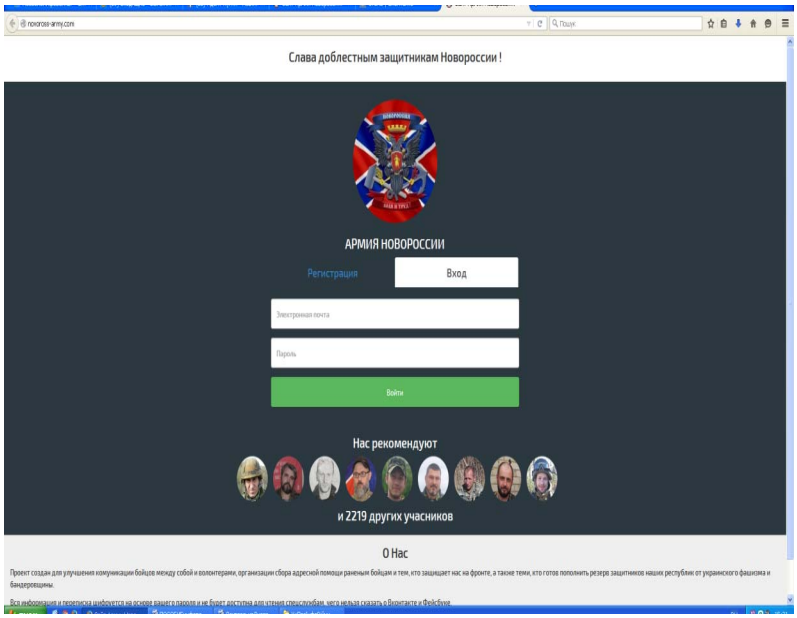
Сергій Жук та його команда створили доволі потужну систему, яка протягом певного періоду успішно працювала, виконуючи завдання із здійснення інформаційно-психологічного тиску на користувачів українського сегменту соціальних мереж.



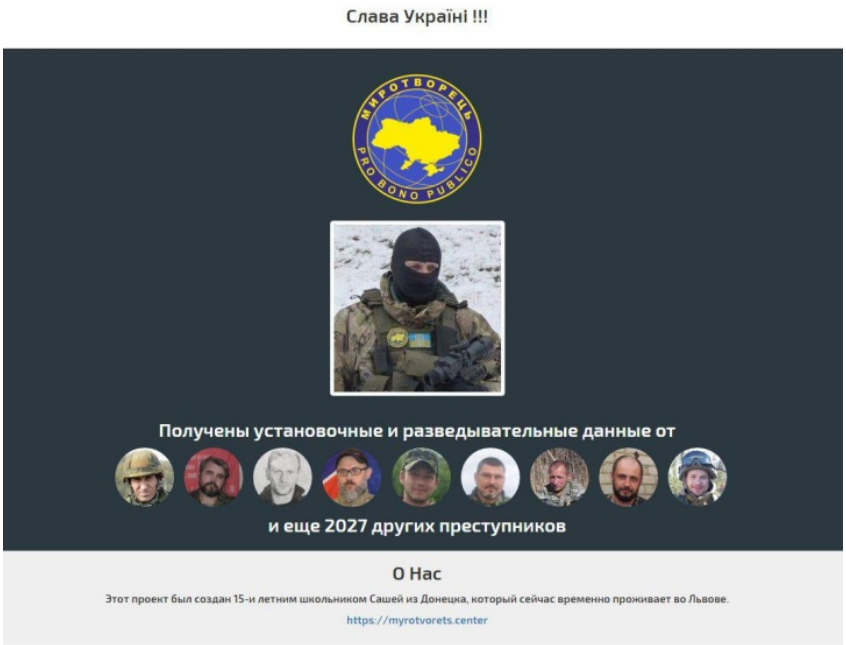
В якості фейкових, добре замаскованих, можуть бути не тільки персональні акаунти, але й окремі інтернет-проекти. В такому разі потрібно буде застосувати більше зусиль та часу для промоції, втім результати можуть бути набагато цікавішими.

Практичний приклад

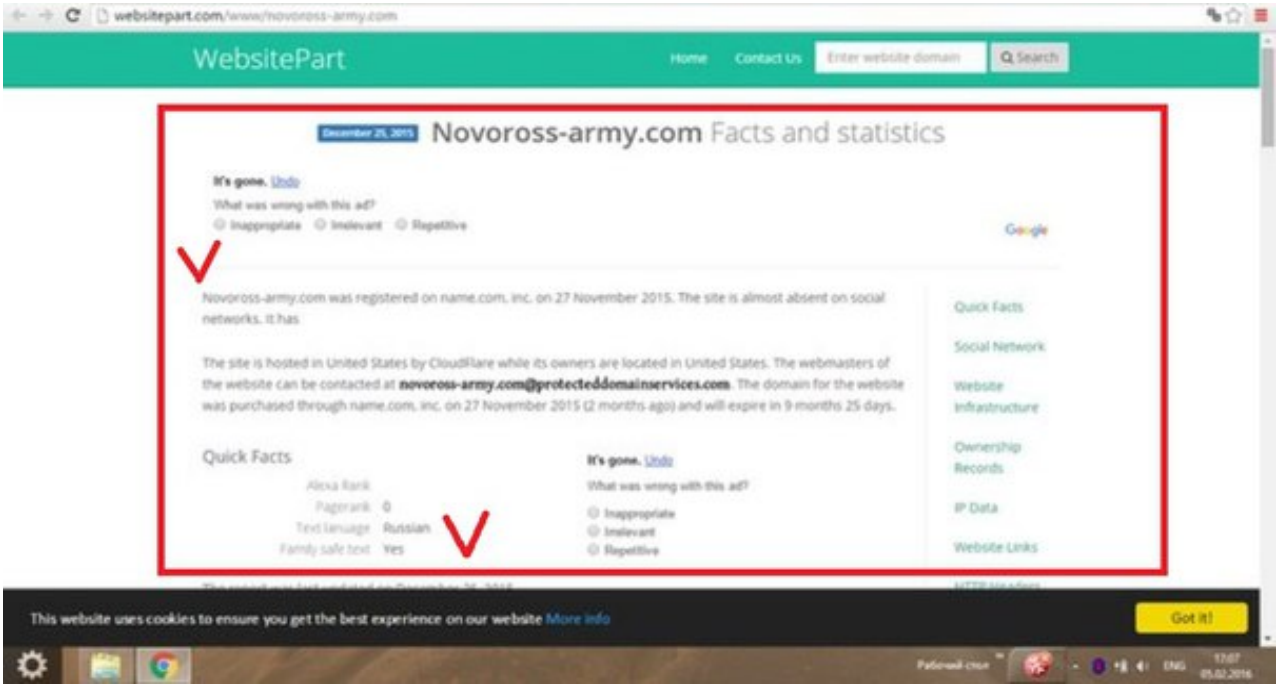
З метою збирання інформації про учасників незаконних збройних формувань було створено інтернет-портал «Армия Новороссии» (http://novoross-army.com). Проект було створено для «поліпшення комунікації між бійцями та волонтерами, організації збирання адресної допомоги пораненим бійцям…».



Слід зазначити, що автором проекту був 15-ти річний хлопчина, який разом з родиною втік до Львова від окупації з Донецьку.



Адміністратори проекту запевнювали всіх, хто долучався, в тому, що вся інформація шифрується та захищається надійними паролями, а це унеможливлює доступ сторонніх осіб.



Система управління проекту була дуже проста та невибаглива. А його аргументація та промоція дозволили вже протягом першої години отримати кілька десятків зареєстрованих, які залишили повну інформацію про себе, включаючи контакти.

Сайт пропрацював кілька місяців, генеруючи до 3 Гбайт інформації на день. Уцілому вдалось зібрати понад 2,5 тис контактів серед найманців ДНР та ЛНР. І тільки тоді російські фахівці розкрили проект.

Окрім візуальних засобів ідентифікації фейкових акаунтів існує низка технічних інструментів та сервісів, що дають можливість отримувати більш конкретну інформацію:

- знайти сторінку конкретної людини одразу в усіх соцмережах (Yandex);

- знайти останні дописи людини одразу в усіх соцмережах (Facebook, Instagram, Flickr, Tumblr, Vimeo, Reddit);
- дізнатися, що конкретна людина писала на своєму акаунті в конкретний день (Twitter);
- дізнатися тематику та зміст постів мешканців конкретного населеного пункту (Twitter);
- дізнатися, що про конкретну людину пишуть у соцмережах (Social Mention);
- отримати інформацію про нещодавно розміщені та відзняті фото в конкретному місці (Yomapic);
- отримати інформацію про відеоматеріали, в яких фігурує конкретна людина (YouTube);
- ідентифікувати людей на фото (Google);
- визначати, в якому районі придбано сім-карту мобільного зв'язку (gsm-inform.ru);
- вирахувати місцезнаходження через IP (ipfingerprints.com);

Окреме питання, в процесі інформаційної війни web 2.0 – технології пошуку друзів та залучення їх до кола власних інтересів, а також використання на дружній основі чужих ресурсів. Мовою професійної розвідки це називається **вербування** – процес залучення до співпраці на добровільній основі або за певну винагороду (матеріальну чи нематеріальну) персони, яка володіє цінною інформацією або корисними організаційними ресурсами.

Процес вербування в соціальних мережах в основі має класичну схему, але з певною корекцією на специфіку середовища. Зокрема визначаються такі етапи:

1. ***Пошук*** – моніторинг у тематичних групах активних та авторитетних блогерів, що мають максимальну кількість друзів та фоловерів.

2. ***Встановлення первинного контакту*** – лайки під авторськими постами, розміщення улесливих коментарів під авторськими постами, згадування при розміщенні цікавих постів (вказати назву акаунта в статусі та в тексті поста).

3. ***Встановлення дружніх стосунків*** – спілкування в коментарях з поступовим переходом на особисте листування в «лічку».

4. ***Залучення до спільних дій*** – запрошення до власних груп та сторінок, віртуальних заходів або до чатів, створених у «лічку». Як варіант можна надати людині статус модератора у власній групі.

5. ***Стимулювання*** – надання цікавої інформації, корисних посилань, порад за потребою.

6. ***Утримання*** – підтримка постійного інформаційного контакту із цікавим об'єктом, привітання із святами персональними, загальними та професіональними. Звернення за порадами та консультаціями.

Головним полем для роботи із вербування в соцмережах є пости та коментарі під ними у групах, пабліках та на тематичних сторінках.

Базовими засобами, що використовуються при вербуванні, є:

- прояв зацікавленості до конкретної персони та того, чим вона цікавиться;
- «безкорисливе» надання певних власних інформаційних ресурсів;
- промоція об'єкта вербування за рахунок власних ресурсів.

3.4. Інтернет-реклама та її застосування в інформаційній війні

3.4.1. Таргетована реклама в соціальних он-лайн мережах

Реклама, як засіб поширення інформації, може використовуватися не тільки в комерційних цілях, але й як інформаційна зброя при відповідному її застосуванні.

Зокрема за допомогою стандартних рекламних інструментів, типових для багатьох глобальних он-лайн соцмереж, можна:

- Пересувати та промотіювати пости та публікації;
- Промотіювати акаунт або тематичну сторінку;
- Створювати та спрямовувати трафік користувачів на веб-сайт;
- Збільшувати кількість конверсій на веб-сайті;
- Отримувати установки програмних додатків;
- Збільшувати залученість для додатку;
- Промотіювати заходи.

Однією з найважливих функцій є застосування цільової реклами або, так званий, **таргетинг**. Останній розуміють як ***рекламний механізм, що дає можливість виокремити з наявної аудиторії лише певну її частину, яка відповідає потрібним критеріям, і показати саме їй рекламне повідомлення*** [217, с. 170].

Виходячи з потенційних можливостей сучасних соціальних он-лайн мереж, маємо визначити такі види таргетингу:

1. Підбір інформаційно-рекламних майданчиків – пошук та використання віртуальних майданчиків (сайти, портали, блоги, групи), на яких рекламодавець може знайти необхідну цільову аудиторію;

2. ***Тематичний таргетинг –*** показ реклами на віртуальних майданчиках (сайти, портали, блоги, групи), що відповідають певній тематиці;

3. Таргетинг за інтересами – показ реклами у відповідності до інтересів відвідувачів віртуальнго майданчика (сайти, портали, блоги, групи);

4. Геотаргетинг – показ реклами за географічним принципом (країна, регіон, місто та ін.) у відповідності до замовлення рекламодавця;

5. Гіперлокальний таргетинг – показ реклами на всіх пристроях у радіусі від 1 до 15 км від точки трансляції;

6. Таргетинг за часом показу – демонстрація реклами в певний час дня або день тижня, місяця, року;

7. Соціально-демографічний маркетинг – показ реклами відповідно до вікових, статевих, соціальних та інших персональних характеристик користувачів;

8. Обмеження кількості показів – регулювання кількості демонстрації реклами одному користувачеві через банерну рекламу;

9. Поведінковий маркетинг – збирання інформації про діяльність конкретного користувача за допомогою cookie-файлів – через акаунт користувача (переглянуті сайти, пошукові запити, закупки в інтернет-магазинах та ін.) з метою отримання портрета конкретного представника цільової групи;

10. Геоповедінковий маркетинг – вивчення поведінки та уподобань користувача за допомогою геосервісів у процесі його переміщення.

Серед окреслених вище видів таргетингу для здійснення безпосереднього інформаційного контакту із представниками цільових груп, у плані поширення інформації можна застосовувати практично всі. Разом з тим деякі із зазначених інструментів можуть виступати в якості доволі серйозної зброї в рамках не тільки інформаційної, але й реальної війни.

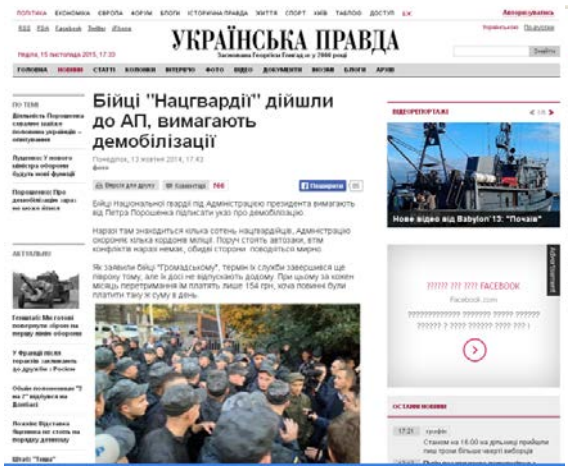
Зокрема, як свідчить практика АТО на сході України 20014-2015 рр., російські підрозділи спеціальних операцій застосовували гіперлокальний таргетинг, що дозволяло певним чином впливати на психологічний стан українських військовослужбовців, особливо в критичних моментах, коли доступ до об’єктивної інформації був обмежений. Зокрема подавалася інформація, що спонукала до панічних настроїв та капітуляції. Особливо активно такі методи застосовувалися під час боїв за Дебальцево.

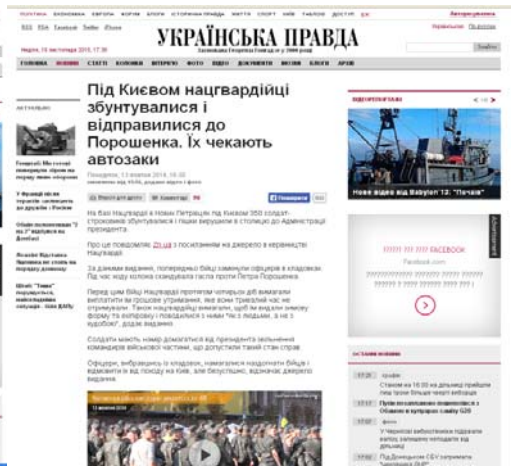
За допомогою поведінкового та геоповедінкового маркетинга можна здійснювати стеження за певними персоналіями, які є ключовими особами у процесах прийняття та реалізації управлінських рішень. А це вже є фактично виконанням шпигунських функцій стеження. Інші види таргетингу є менш небезпечними, втім не менш дієвими для роботи із конкретними цільовими аудиторіями, стеження за їхніми реакціями, поведінкою в певних ситуаціях. Зокрема тематичний таргетинг, таргетинг за інтересами, а також геотаргетинг дає можливість працювати з окремими цільовими групами на безпечній відстані, здійснюючи цільову агітацію та пропаганду.

За допомогою зазначених інструментів досвідчені фахівці спецслужб мають можливість дистанційно організовувати та координувати не тільки он-лайн, але й оф-лайн події.

Практичний приклад

Класичним прикладом практичної реалізації таких можливостей стали події 13.10.14 р., коли на базі Нацгвардії в с. Нові Петрівці під Києвом 350 солдат-строковиків збунтувалися і пішки вирушили в столицю до Адміністрації Президента вимагати поліпшення умов служби та негайної демобілізації. В цьому випадку робота російських спецслужб здійснювалася через лідерів громадської думки в середовищі рядового складу підрозділу, шляхом налагодження контактів та здійснення впливу через соціальну он-лайн мережу VKontakte.



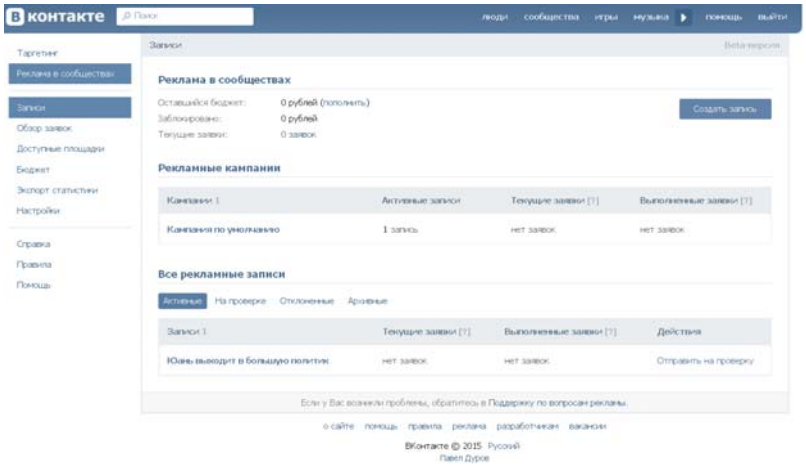


http://www.pravda.com.ua/news/2014/10/13/7040648/ http://www.pravda.com.ua/news/2014/10/13/7040631/

Механізми використання таргетованої реклами прості та максимально автоматизовані. Рекламодавцю або замовнику не потрібно складати технічне завдання. Складання заявки здійснюється безпосередньо з персонального акаунту в режимі трьох кроків.

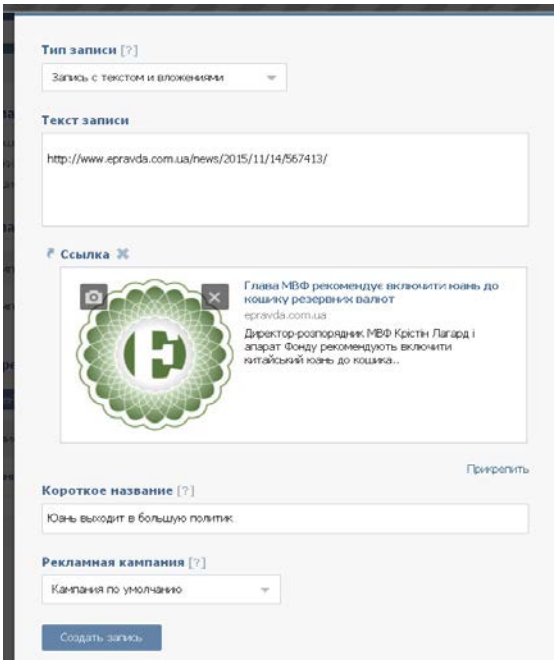
Переший крок – створення персонального кабінету, в якому формуються та зберігаються замовлення на рекламу (мал. 3.16.).

Мал. 3.16. Персональний кабінет рекламодавця



За відповідними параметрами користувач визначає характер та специфіку рекламної кампанії. Вказує зміст рекламного повідомлення та додатковий контент, який потрібно додати до повідомлення (мал.3.17.).

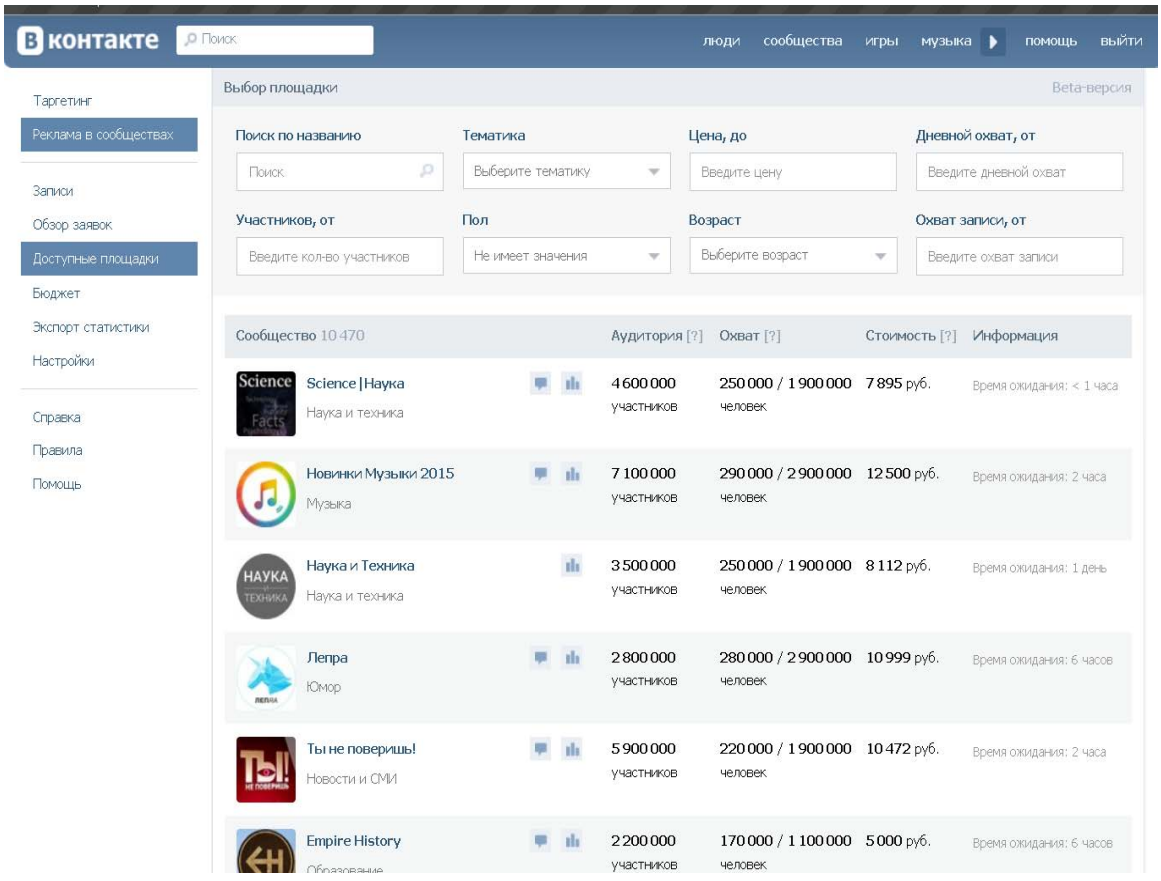
Мал. 3.17. Визначення змісту рекламної кампанії



Далі користувач, відповідно до параметрів цільових груп (вік, стать та ін.) та умов кампанії (охоплення, кількість, часові параметри та ін.), уточнює вимоги, отримуючи варіанти майданчиків, на яких може бути поширена інформація (мал. 3.18.).

Кожна з соціальних он-лайн мереж має певні особливості та специфіку процедури складання параметрів рекламної кампанії або дослідження, втім принципові положення подібні і відбуваються за єдиним, представленим вище, механізмом.

Мал. 3.18. Визначення змісту рекламної кампанії



3.4.2. Контекстна інтернет-реклама

Окремий маркетинговий інструмент, що може бути задіяний в сучасній інформаційній війни, це **контекстна реклама**.

Контекстну рекламу визначають, ***як принцип розміщення інформації, коли вона орієнтована на зміст інтернет-ресурсу, представлена у вигляді банеру чи текстового повідомлення*** [31, с. 18].

Наприклад, на веб-сайті, присвяченому продуктам харчування, контекстна реклама пов'язуватиметься із поварами, споживачами або працівниками супермаркетів.

Однією із переваг контекстної реклами є геотаргетинг, що дає можливість обирати географію показу сторінок. Також застосовуються рамкові обмеження для часу показу. Ефективність контекстної реклами визначається рейтингом кліків (CTR) і вимірюється у відсотках [42, с. 22].

Специфічним видом контекстної реклами є пошукова реклама, яка розміщується в пошукових системах. Закладаючи ключове слово або словосполучення, користувач разом з необхідними матеріалами отримує посилання на рекламні оголошення або сайти, де певні товари або послуги рекламуються опосередковано. При цьому рекламне оголошення може з’явитися поруч із результатами пошуку (по боках або над даними). У випадку з текстовою рекламою, контекстна реклама розміщується блоками.

Головними провайдерами контекстної реклами є системи Google AdWords, Yahoo! Publisher Network та Microsoft adCenter.

Головною специфікою та особливістю контекстної реклами є принцип прив’язування інформаційного повідомлення до тематичних запитів користувача. В такому разі, при правильному складанні рекламного повідомлення, меседжі, закладені в посланні, легко досягатимуть свідомості користувачів. При цьому деструктивна або маніпулятивна складова вуалюється під виглядом реклами.

Ефективність застосування контекстної реклами визначається за рейтингом кліків або клікабельністю – CTR (Clik-through rate). Останнє розраховується як співвідношення кількості кліків на оголошення відповідно до кількості його показів. Одиниці виміру – відсотки.

Формула розрахунку – CTR = (число кліків / число показів) х 100%. Наприклад, якщо рекламне оголошення було показано 100 разів, а клікнули по ньому лише один раз, то показник CTR дорівнюватиме 1%. Таким чином, чим більше відсотковий показник розрахунку, тим точніше відпрацьовує рекламне повідомлення.

Необхідно зазначити, що використання інтернет-реклами в будь-якому її варіанті в якості інформаційної зброї в інформаційно-психологічних війнах, є досить специфічним, але доволі ефективним інструментом.

Головний принцип – здійснення інформаційної атаки там, де її користувач очікує менш за все (контекстна реклама) та вихід на персональний рівень стосунків (таргетована реклама).

У разі вдалого застосування таких інструментів навіть досвідчені фахівці не одразу можуть вирахувати наявність та спрямування атакуючих дій і своєчасно відреагувати. Крім того, така атака може сягати підсвідомого ментального рівня, що робить її ще більш небезпечною, ніж традиційні агітація та пропаганда.

Зважаючи на те, що серед провідних тем, навколо яких точаться інформаційні протистояння, є побутові питання, питання харчового забезпечення, послуг та товарів широкого вжитку, саме інтернет реклама може дати можливість належним чином замаскувати та максимально наблизити до актуальних потреб цільових груп, дії атакуючої сторони.

3.5. Використання мобільних засобів зв'язку як інструмента інформаційної атаки

Ще одним специфічним мережевим інструментом у сучасних комунікаціях можуть бути мобільні засоби зв'язку. В якості гаджетів використовуються класичні стільникові системи зв’язку, а також різноманітні месенджери та інші сервіси, що розмивають чітку лінію розмежування між Інтернетом та класичним стільниковим зв’язком.

У такому разі засоби комунікації можуть застосовуватися як в класичному варіанті (телефонна розмова), так із залученням до мережі Інтернет. Цей напрямок має назву – **мобільний маркетинг** - ***комплекс заходів, спрямованих на промоцію товарів або послуг із використанням засобів стільникового зв’язку*** [217, с. 157]**.**

Мобільній маркетинг є одним з самих дешевих та, разом з тим, найбільш таргетованих засобів комунікаційного просування. В його основі - ***послуги SMS-розсилки*** та деякі інтернет-технології (Viber, WhatsApp, Skype, Telegram, Line, Facebook Messenger, ICG та ін).

Останнім часом дедалі більшої популярності набувають **месенджери** - програми для швидкого обміну повідомленнями, розроблені для спілкування за допомогою мережі Інтернет. Відповідне програмне забезпечення встановлюється на персональних комп’ютерах або мобільних пристроях (смартфони, планшети). Сучасні месенджери дають можливість не тільки обмінюватися текстовими файлами, але й надають можливість голосового і відео зв’язку. При цьому, сучасні соціальні мережі можуть забезпечити достатньо високий рівень конфіденційності спілкування та передання даних.

Зазначений інструмент дає можливість донести комунікаційне повідомлення персонально, привернути увагу та налаштувати на певну дію конкретну особу.

Важливим аспектом класичної SMS-розсилки є її масовість – переважна частина користувачів є власниками мобільних телефонів.

Для розповсюдження інформації зазначеним засобом використовують бази телефонних номерів. Останні можна отримати різними шляхами. *Офіційним* - адресат дає згоду на отримання рекламно-інформаційних SMS-повідомлень. *Не офіційним* – розсилка спам-повідомлень. У цивілізованому світі існують певні законодавчі бар'єри, що блокують нав'язливу персональну рекламу, аж до кримінального переслідування.

Зазвичай, адресні бази формуються в процесі здійснення купівлі (комерційна сфера) або при складанні баз даних по конкретним організаціям (державним, громадським, військовим структурам та ін.).

В умовах ведення військових конфліктів сучасні засоби радіоелектронної боротьби можуть забезпечити доступ до стільникового зв'язку, накриваючи окремі території.

Серед провідних технологій, що використовуються в мобільному маркетингу, визначають [217, с. 158]:

• голосові повідомлення;

• SMS-розсилки;

• MMS-розсилки (текстові або мультимедійні повідомлення, з можливістю використовувати фото, відео, музику, посилання та ін.);

• wap, gprs, edge та інші технології, що доступні для отримання інформації з мережі Інтернет за допомогою мобільного телефону;

• голосове меню (дозволяє тому, хто телефонує, спілкуючись із автоінформатором, отримати інформацію за потрібними темами, зробити замовлення, дізнатися про акції, знижки, промо-заходи та ін.);

• технології для створення додатків під відповідні мобільні платформи (Android, iPhone, Windows Mobile та ін.);

- системи обміну миттєвими повідомленнями (спілкування, конференція, чат).

У форматі сучасної інформаційної війни використання всього спектру мобільних засобів комунікації – від стільникового зв’язку до різноманітних месенджерів набуває особливого значення. Зокрема використання звичайного розсилання SMS-повідомлень може застосовуватися як інструмент прямого або опосередкованого психологічного тиску на військовослужбовців.

Зокрема застосування такого інструмента ведення інформаційно-психологічної війни можна було спостерігати під час активної фази війни 2014-2015 рр. в Донбасі. За допомогою відповідних електронних пристроїв, російська сторона робила розсилання повідомлень панічного характеру на мобільні пристрої українських військовослужбовців, що знаходилися безпосередньо в зоні бойових дій.

<u>РОЗДІЛ 4.</u> Пошук, моніторинг та оцінка ефективності інформаційних процесів

4.1. Сучасні методи та засоби аналізу

За базовими принципами щодо пошуку та опрацювання інформації аналітичні дослідження в соціальних комунікаціях умовно можна поділити на два рівні – **первинна та поглиблена аналітика**.

До **первинної аналітики** відносяться методи та інструменти збору даних, які дають швидкі результати та не потребують значних матеріально-технічних витрат. Найбільш поширеними в цьому плані є ***моніторинг ЗМІ*** та різноманітні ***експрес-опитування***, ***вивчення громадської думки*** та ін. Такі дослідження дозволяють отримувати інформацію та робити відповідні висновки, не виходячи з офісу, максимум протягом кількох годин або одного робочого дня.

Поглиблена аналітика здійснюється за допомогою ***багаторівневих дослідницьких процесів*** або шляхом застосування комплексних ***інтегрованих методик***. Типовим дослідницьким ланцюгом є послідовність: польовий збір інформації – систематизування – опрацювання – аналітична оцінка.

Умовно, аналітичні дослідження, які застосовуються в інформаційних процесах, можна поділити на три групи:

1.Маркетингові:

- огляд ринків та їх окремих сегментів (поглиблена аналітика);
- вивчення споживацького попиту (первинна аналітика);
- експертне опитування (поглиблена аналітика);
- фокус-група (поглиблена аналітика).

2. Соціологічні:

- дискрептивні (поглиблена аналітика);
- «омнібус» (поглиблена аналітика);
- фокус-групи (поглиблена аналітика).

3. Інтегровані та спеціальні:

- Комунікаційний аудит (поглиблена аналітика);
- Моніторинг ЗМІ (первинна аналітика);
- Розвідка (поглиблена аналітика).

Найбільш активно використовуються в інформаційних протистояннях дослідження, які презентують дані, що подаються в абсолютних показниках – грошах, відсотках, виробничих показниках, електоральних голосах та інших профільних одиницях виміру. Матеріали цих досліджень дають підстави робити більш-менш точні аналітичні прогнози та висновки, що дозволяє вірно інтерпретувати факти та планувати конкретні кроки. Водночас, здійснення розвідок у цьому форматі вимагає значних часових та матеріальних затрат. У цілому цей напрямок роботи можна визначити як поглиблену аналітику.

У контексті загального вивчення інформаційних процесів **маркетингові дослідження** є доволі ефективним діагностичним інструментом. Серед усього різноманіття засобів для вивчення комунікаційних процесів частіше використовуються такі, як: ***огляди профільних ринків*** та їх окремих сегментів, ***тематичні***, ***експертні опитування*** та ***вивчення споживацького попиту***.

Огляди ринків та їх окремих сегментів зазвичай супроводжують розробку корпоративних стратегій та тактичних схем у рамках загального інформаційно-комунікаційного процесу.

Експертне опитування передбачає вивчення думки профільних спеціалістів щодо певної маркетингової задачі або ситуації. Інформація в цьому випадку збирається шляхом індивідуального інтерв'ювання відповідних фахівців. Таке дослідження знаходить застосування в діагностиці соціальних комунікативних процесів у тих випадках, коли мова йде про вирішення питань, пов'язаних з промоцією окремих брендів, торгових марок, окремих груп товарів або вирішення певних критичних ситуацій.

Вивчення споживацького попиту спрямоване на дослідження реакції громадян на ті чи інші товари, або послуги, коли вони запускаються на ринок, корегуються їхні якісно-вартістні характеристики або вирішуються питання, пов'язані з кризовими ситуаціями навколо них. Збір інформації відбувається або шляхом бліц-інтерв'ювання споживачів на території торгових точок, або через фокус-групове дослідження. Місце та призначення матеріалів вивчення споживацького попиту в контексті соціокомунікативного процесу є подібним до того, яке відводиться експертному опитуванню.

Найбільш поширеними видами **соціологічних досліджень**, що супроводжують інформаційно-комунікаційні процеси, є: ***дескриптивні дослідження*** та ***фокус-групове опитування***.

Інтегровані та **спеціальні дослідження** застосовуються на індивідуальному рівні відповідно до певної комунікаційної ситуації або завдання. Класичним прикладом таких є ***комунікаційний аудит.***

За структурою комунікаційний аудит є складним комплексним процесом, який передбачає певну кількість процедур та допоміжних методик. Зокрема в процесі такого аудиту можуть бути застосовані:

- аудит інформаційних потоків (карти інформаційного поля)
- оцінка вартості нематеріальних активів
- імідж-аудит
- структурний аудит внутрішньо корпоративних комунікацій
- SMM-аудит

Моніторинг ЗМІ є інструментом поточного спостереження та первинної аналітики. *Розвідка* – комплексний аналітично-оперативний збір інформації про опонентів.

Слід зауважити, що всі, зазначені вище, методи дослідження є рамковими, а їх практичне використання має базуватися на індивідуально налаштованому алгоритмі. Зазначена аксіома базується на тому, що кожна комунікативна

ситуація, яка досліджується, є специфічною. Виходячи з цього, підхід до кожного випадку має бути також специфічний та індивідуальний.

Складність поєднання алгоритмічності дослідницьких процедур та індивідуальності підходу може бути вирішено шляхом поміркованого застосування базових непорушних шаблонів на макрорівні та гнучкого їх поєднання на макрорівні. Таким чином, виникає мозаїчний підхід, що є найбільш адекватним варіантом вирішення досліджуваних питань.

4.2. Базові методи та засоби оцінки ефективності інформаційних процесів в інтернет-просторі

Базовими маркерами оцінки ефективності акаунту, сайту, блогу або будь-якого іншого інтернет-ресурсу є:

- відвідування інтернет-ресурсу;
- час перебування на сторінках інтернет-ресурсу;
- сторінки, з яких користувачі йдуть з ресурсу;
- кількість відвідувачів, що завітали на ресурс за рекламою;
- середні показники зростання ресурсу.

Для правильної оцінки реальних показників роботи інтернет-ресурсу необхідно чітко уявляти, які завдання віршуються за його допомогою та яка очікується віддача щодо витрачених на його створення коштів. Важливо розуміти, що недостовірність або неактуальність наданої інформації може звести нанівець усі зусилля, які докладалися для створення та промоції ресурсу.

Заходи з якісної оцінки ефективності інтернет-ресурсу:

- визначення першочергових завдань інтернет-проекту та вивчення відповідності сайту цім завданням;
- перевірка достовірності та актуальності наданої на сайті інформації;

- аналіз оперативності доступу до сайту;
- запити до пошукових сайтів та каталогів Інтернет для пошуку інформації про сайт та приблизного визначення рівня його складності;
- дослідження системи обліку відвідувань сайту з використанням ресурсів Інтернету та з допомогою власних рахівників;
- проведення досліджень про коло відвідувачів, частоти відвідування сайту та їх уподобання;
- отримання відгуків від відвідувачів сайту за допомогою форуму або анкетування;
- дослідження динаміки збільшення або зменшення кількості передплатників розсилок;
- виявлення найбільш та найменш цікавої інформації;
- аналіз ефективності банерів;
- дослідження динаміки продажів (для інтернет-магазинів);
- оцінка прибутку від продажів за допомогою систем замовлення on-line (для інтернет-магазинів);
- динаміка змін чисельності відвідувачів сайту в цілому та окремих його сторінок;
- збір даних про швидкість функціонування системи;
- кореляція чисельності відвідувачів та реальних економічних показників діяльності компанії.

Для здійснення кількісного аналізу ефективності функціонування інтернет-ресурсу застосовуються такі методи оцінки результативності просування контенту, як: **PageRanke** (в системі Google) та **тИЦ** (у системі Yandex).

PageRanke. Алгоритм виміру популярності інтернет-ресурсу за 10-ти бальною шкалою. Оцінює «важливість» та «авторитетність» за кількістю

посилань. Використовується системою Google для ранжування сайтів при видачі результатів пошуку за запитами користувачів.

***тИЦ (тематичний індекс цитування*).** Технологія оцінки авторитетності інтернет-ресурсів з врахуванням якісної характеристики – посилань на інших сайтах. Даний показник розраховується як сумарна вага посилань через систему апдейтів (рахівників показників) з оновленням два рази на місяць.

У системі Web 2.0-3.0 оцінка ефективності комунікації здійснюється переважно за принципом оцінки рейтингу акаунту (кількість лайків, коментарів, перепостів). У принципі такий підхід є доволі адекватний та репрезентативний, втім дещо обмежений, бо виводить за межі дослідження інформацію, що знаходиться поза зоною діяльності досліджуваного ресурсу.

Під час вирішення таких важливих завдань, як: оцінка споживацького попиту, реакції покупців на товари і послуги та інше, потрібен більш масштабний, багаторівневий підхід. У такому разі можливим є застосування методики SMM-аудита.

4.3. Методи та засоби моніторингу ситуації в інтернет-просторі

4.3.1.Методи базового моніторингу

Моніторинг засобів масової інформації найбільш швидкий та найменш затратний засіб вивчення громадської думки та відстеження зворотного зв’язку в рамках комунікаційного процесу. Здійснюючи силами профільного структурного підрозділу або сторонніх фахівців регулярний аналіз мас-медійних матеріалів, можна виявляти певні тенденції ретроспективного та перспективного спрямування. Це дозволяє або передбачати майбутні наслідки певних сьогоднішніх дій, або виявляти причинно-наслідкові тенденції, що призвели до тих, чи інших ситуацій або фактів, які мають місце нині. Цей

напрямок роботи можна вважати первинною аналітикою**,** матеріали якої дають можливість зрозуміти певні процеси в цілому, виявити окремі загрозливі або позитивні тенденції**.**

Для здійснення регулярних вимірів громадської думки, яка найбільш системно висвітлюється в засобах масової інформації, можна використовувати процедуру моніторингу і контент-аналізу в рамках трьох етапів.

I етап – збір наявних матеріалів. Окрема особа або профільна аналітична група не частіше одного разу на день, але не рідше ніж один раз на тиждень, збирає та формує, у вигляді зведеного звіту, дані моніторингу профільних та загально тематичних ЗМІ та мережевих майданчиків (групи, пабліки, сторінки, акаунти, форуми, блоги). Зазначений звіт може складатися у вигляді ***моніторингу-копії*** або ***моніторингу-конспекту***.

Моніторинг-копія – комплектується зі скопійованих версій друкованих видань, роздрукованих фрагментів інформаційних стрічок, матеріалів інтернет-видань, теле- та радіо сюжетів. При цьому на кожній роздруківці дається посилання на видання, з якого цей матеріал взято, дату, номер, сторінку, або інтернет-адреси зазначених матеріалів.

Моніторинг-конспект **–** матеріали подаються в тезово-описовому варіанті з усіма необхідними посиланнями. Для форматування моніторингу в такому вигляді робиться трьохсекційна таблиця (табл. 4.1.).

Таблиця 4.1. Шаблона структура звіту «Моніторинг-конспект»

№ з/п	НАЗВА СТАТТІ, АВТОР, ДЖЕРЕЛА	СТИСЛИЙ ВИКЛАД	ЗАБАРВЛЕННЯ (позитив, негатив, нейтрально)
1.			
2.			
3.			

До першої колонки заносяться дані щодо джерела інформації (видання, номер, дата, автор та ін.), до другої – зміст інформаційного повідомлення (конспективно), до третьої – загальна характеристика матеріалу (позитивне, негативне або нейтральне забарвлення).

II етап – контент-аналіз матеріалів ЗМІ. За матеріалами моніторингу, не частіше ніж раз на тиждень, але не рідше ніж раз на місяць, проводиться змістовний аналіз зібраних матеріалів з метою переведення якісних показників та характеристик у кількісні. Результати такого аналізу закладаються у відповідну таблицю, де слід передбачити чотири колонки (табл. 4.2.).

Табл. 4.2. Шаблона структура звіту за результатами контент-аналізу

№ з/п	ЗМІ	Дата	Назва статті, автор	Тематика	Фігурант	Коротке викладення змісту	Забарвлення
Друковані ЗМІ							
Державні							
1.							
2.							
Суспільно-політичні							
3.							
4.							
Бізнес тематика							
5.							
Профільні							
6.							
Телебачення							
7.							
8.							
Радіо							
9.							
10.							
Інтернет-видання							
11.							

Табл. 4.3. Структура аналітичного звіту

ТЕМАТИКА		РЕЗУЛЬТАТИ МОНІТОРИНГУ	ВИСНОВКИ	РЕКОМЕНДАЦІЇ
Досліджуване питання		1. Загальна кількість згадувань (позитив, нейтрально та негатив)	1. Про що свідчить: - зниження інтересу з боку громадськості - не актуальність - політичні фактори - зовнішні фактори - сезонний аспект - інші причини	
		2. Які ЗМІ. Скільки разів згадували (позитив, нейтрально та негатив)	2. Чому ЗМІ так реагують: - політика керівництва - політична приналежність - лобіювання - пошук "смажених" фактів - інші причини	
		3. Тенденції збільшення або зменшення інтересу з боку ЗМІ порівняно з попереднім періодом	3. Про що свідчить: - зниження інтересу громадськості - не актуальність - політичні фактори - зовнішні фактори - сезонний аспект - інші причини	
ЗАГАЛЬНА СИТУАЦІЯ				
1				
2				
СПЕЦІАЛІЗОВАНІ ПИТАННЯ				
3				
4				

У першій зазначається тема або питання, що досліджується. В другій подаються кількісні показники згадувань теми або питання в ЗМІ, в контексті загальної оцінки (скільки негативних, позитивних, нейтральних) джерел (в яких ЗМІ в цілому і скільки по кожному з них) та тенденцій (збільшення або зменшення інтересу ЗМІ до зазначеного питання порівняно з попереднім

звітним періодом). У третій колонці дається інтерпретація кількісних показників попередньої колонки (загальна кількість, джерела, тенденції) та складаються висновки (чому саме так). Четверта колонка відведена для формулювання рекомендацій щодо шляхів нейтралізації негативних або стимулювання позитивних тенденцій, зазначених у трьох попередніх колонках.

III етап – складання загального звіту. В разі потреби результати вивчення матеріалів ЗМІ, зроблених у форматі контент-аналізу, можна звести до вигляду текстового звіту із визначенням або встановленням акцентів на найбільш актуальних темах (табл. 4.3.). Потреба в презентації результатів первинного аналізу в такому форматі може виникнути у разі небажання або відсутності вільного часу в тих, кому він готувався для ознайомлення зі змістом.

4.3.2. Засоби експрес-опитування в соціальних мережах

За допомогою соціальних он-лайн мереж можна проводити типові соціологічні дослідження і перш за все опитування громадської думки. Порівняно з класичними соціологічними дослідженнями результати опитування в соціальних мережах мають більш значну статистичну похибку. Це відбувається через те, що поле є нестабільним (опитування іноді видаляють або не дають дозвіл на розміщення в групах, вибірка по групах не завжди репрезентативна та ін.). Втім, отримані результати доволі чітко віддзеркалюють загальні тенденції, в територіальному розрізі або в контексті конкретних цільових груп.

Для проведення дослідження думки представників цільових груп можна скористатися відповідними власними сервісами провідних соціальних мереж або міжмережевими сервісами.

У переважній більшості власних сервісів анкета опитування налаштовується в шаблонному блоці для створення посту (мал. 4.1. та 4.2.).

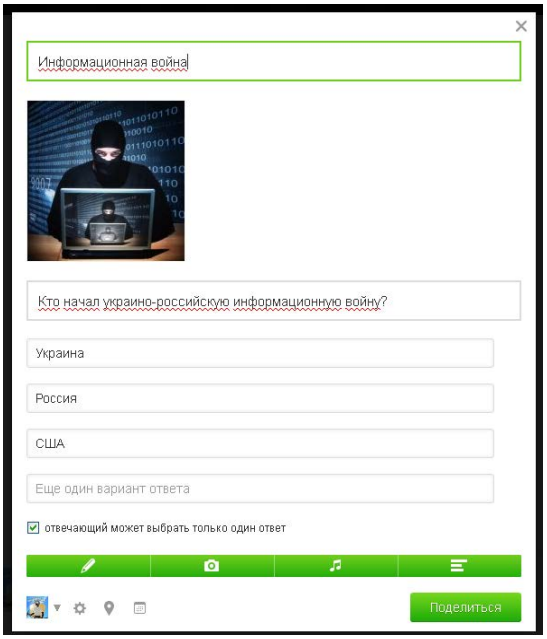
Схема створення анкети проста і формується автоматично. Від розробника вимагається лише поставити тему та головне питання із варіантами відповіді.

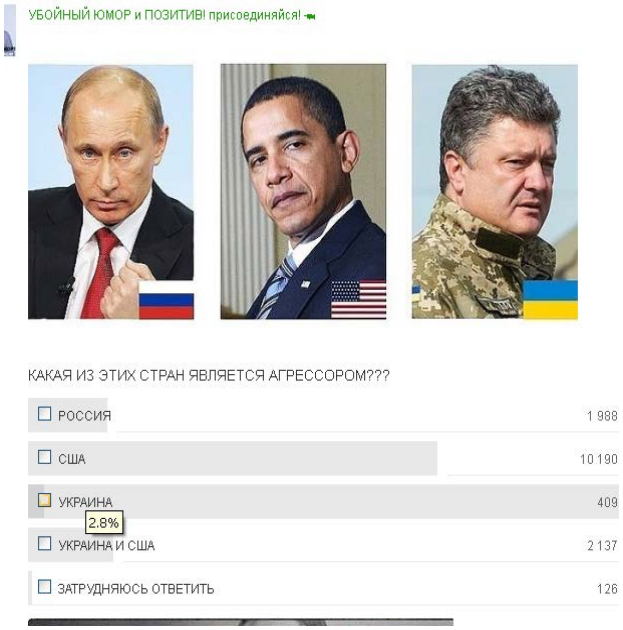
При розробці блока опитування бажано додавати певне візуальне супроводження – картинка або ролик, які допомагають швидше зрозуміти сутність опитування та привертають до нього увагу.

Для полегшення завдання підготовки та проведення опитування у соціальних мережах існують відповідні сервісні програми:

- **Facebook -** My Polls, Poll, Acepolls;
- **Twitter –** Acepolls;
- **VKontakte –** власний сервіс;
- **Odnoklassniki -** власний сервіс.

Мал. 4.1. Опитування на Odnoklassniki.ru



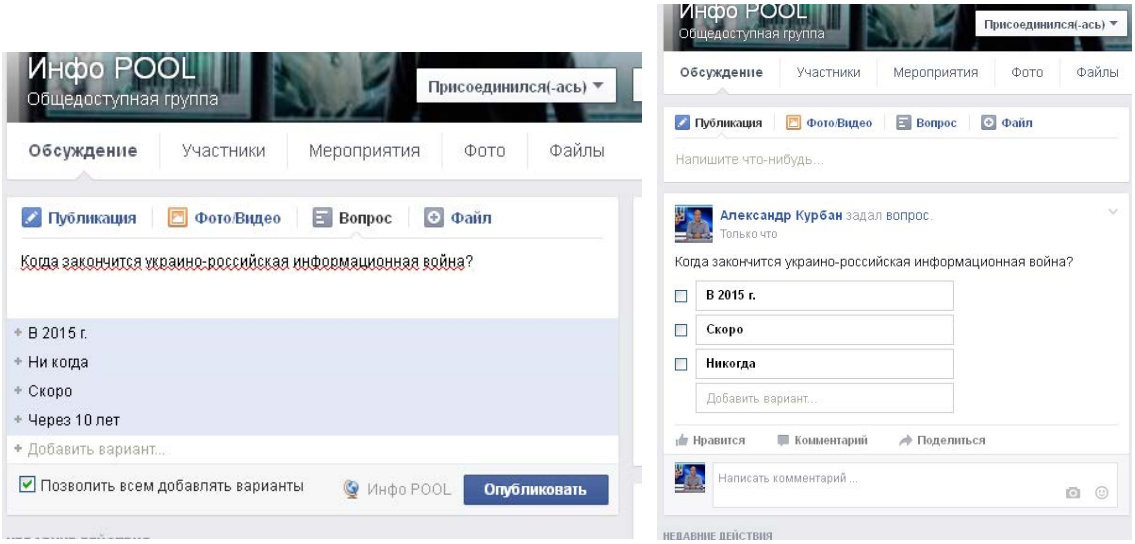


Таким чином, за рахунок переважно власних сервісів соціальних он-лайн мереж можемо проводити відповідні соціальні опитування, які зазвичай дають миттєві та достатньо об’єктивні показники по відповідних цільових групах.

Опитування у соціальних мережах, окрім функції дослідження, можуть виконувати функції промоції або здійснення агітації та пропаганди. В якості

контенту в такому разі виступає лід, який розтлумачує зміст опитування. Під камуфляжем таких пояснень можна закладати певні меседжі або психологічні установки імперативного характеру. При цьому кількісні показники голосування будуть додавати репрезентативності таким ствердженням.

Мал.4.2. Опитування на Facebook



Практичний приклад

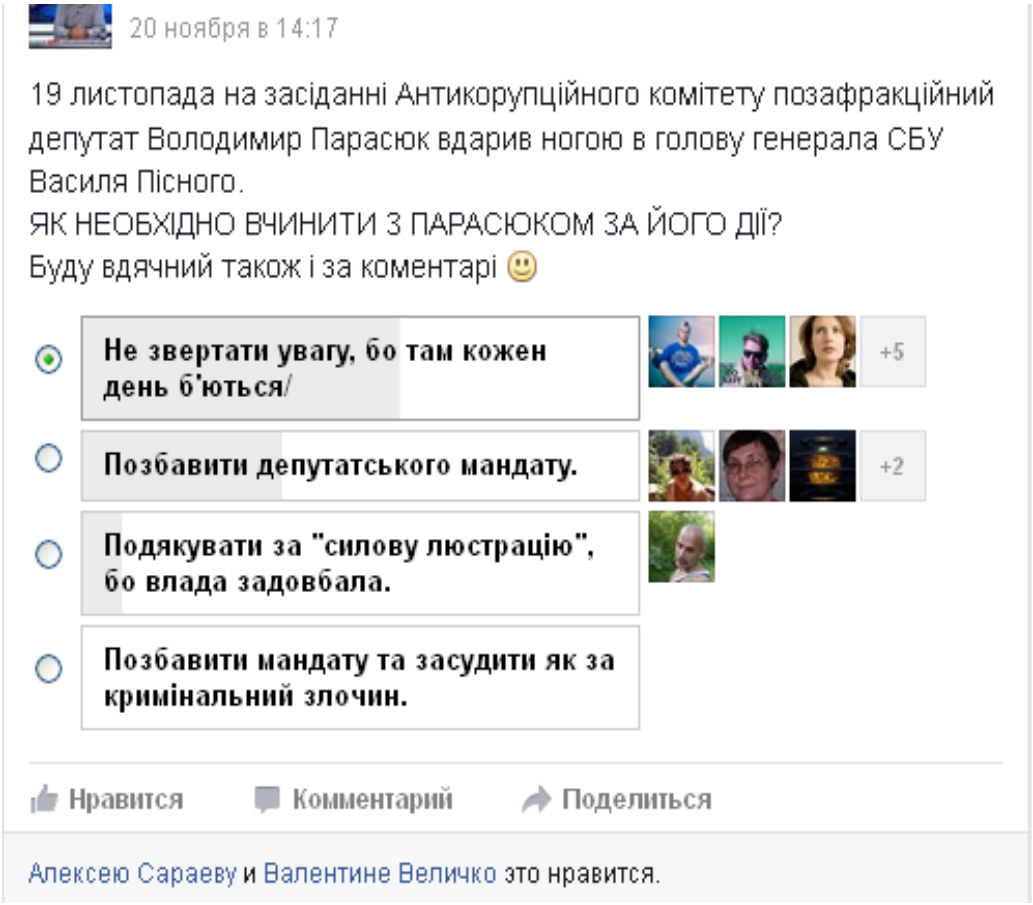
Для вивчення суспільних настроїв та відношення громадян України до інститутів влади (станом на листопад 2015 р.) як тему дослідження було обрано аналіз оцінки громадськістю бійки народного депутата В. Парасюка та генерала СБУ В. Пісного на засіданні Антикорупційного комітету Верховної Ради України [219].

Мета зазначеного дослідження - виявити суспільну оцінку цього факту та його наслідків, а також з'ясувати, яким бачить громадськість вихід із зазначеної ситуації.

Опитування щодо ситуації навколо конфлікту народного депутата В.Парасюка та генерала СБУ В. Пісного проводилося протягом 20–22 листопада 2015 року (майже одразу після події). Було складено два анкетних блоки для дослідження реакції пересічних громадян на цю подію та їхньої

думки щодо дій, які має вчинити керівництво Верховної Ради та правоохоронні органи стосовно фігурантів справи.

У рамках опитування було охоплено: груп у соціальних мережах Facebook та «Однокласники» — 56 (36 загальнонаціональних, 20 регіональних), користувачів — 827 183. Безпосередньо пости разом отримали: лайків — 81, коментарів — 56. З числа охоплених користувачів взяло участь у опитуванні 449 осіб.



На питання ***«Як оцінити поведінку Парасюка?»*** *40% респондентів підтримали твердження, що поведінка нардепа не гідна рівню відповідної політичної культури, засудивши таким чином його вчинок. Разом з тим, суто як вчинок громадянина, побиття генерала СБУ В. Пісного було сприйнято опитуваними з розумінням та прихованою підтримкою — 36%. Невпевненими в адекватності власного вибору виявилися 24%, які підтримали твердження, що так робити не можна, втім, іноді необхідно. Серйозної регіональної або*

тематичної прив'язки позицій опитуваних чітко виявити не вдалося (невелика та нерівномірна вибірка). Втім саме загальнонаціональні групи виявили базову тенденцію, яку можна охарактеризувати так: ***депутату такого робити не можна, але генерала провчити було потрібно****.*

Отримані результати щодо оцінки вчинку Парасюка свідчать про те, що в українському суспільстві існує розуміння необхідності підтримки високих стандартів політичної культури, якій мають відповідати всі без виключення представники політичної еліти. Чвари, лайка та бійки не викликають у громадськості особливого попиту, зокрема, в рамках досліджуваної цільової групи — користувачів соціальних мереж.

Той факт, що доволі високий відсоток опитуваних (політично толерантних, як свідчить попередня тенденція) із розумінням поставилися до факту насильства проти людини, яка асоціюється із старою корумпованою владою, свідчить про накопичення негативу щодо теперішньої влади в плані гальмування реформ та очищення держструктур від корупціонерів та «колишніх». І це незадоволення перебуває на критичному рівні, який певною мірою переважує політичну толерантність та терплячість представників досліджуваних цільових груп.

Блок-питання «Як оцінити поведінку Парасюка?»

Питання	Соціальна мережа		Регіони			
	Facebook	ОК	Схід	Захід	Північ	Південь
Ця поведінка не гідна нардепа		40%		18%	42%	66,3%
Так не можна, але іноді треба поступати		24%		64%	7%	22,3%
Підтримую Парасюка		36%		18%	51%	11,3%

*На питання **«Як вчинити із Парасюком?»** переважна більшість опитуваних — 72,25% підтримали тезу про необхідність висловлення публічної подяки Парасюку, що знов-таки свідчить про визначені вище тенденції — настрої протесту. Порівняно з цим показником всі інші у розглянутому блоці в розрізі 8–12,5% виглядають мізерно. Зокрема, ігнорувати такі події вважають за доцільне 8%, і це свідчення того, що політичні події мало кого залишають сьогодні байдужим. Покарати правопорушника запропонували в цілому майже 20%, серед яких трохи більше 7% вважають за доцільне позбавити Парасюка мандата, а понад 12% пропонують також і притягнути його до кримінальної відповідальності.*

Блок-питання «Як вчинити з Парасюком?»

Питання	Соціальна мережа	
	Facebook	ОК
Подякувати за його вчинок	72,25%	
Ігнорувати	8%	
Позбавити мандата	7,25%	
Позбавити мандата і притягнути до кримінальної відповідальності	12,5%	

***Загальний висновок:** широкі кола громадськості втомилися від політичних негараздів та скандалів у владних кабінетах й на різноманітних ток-шоу. Але попри спад електоральної активності, про що свідчать результати останніх виборів, політична активність населення в цілому тримається на досить високому рівні за рахунок настроїв протесту. Про що*

свідчать, зокрема, останні події на Майдані, під Адміністрацією президента та в Херсонській області.

Проаналізувавши такий стан суспільства з точки зору класичної психології, можна дійти висновку, що він відповідає другій стадії депресії, що умовно визначається як «образа». В цьому стані людина, зрозумівши, що не може ігнорувати або ліквідувати подразнюючий фактор, починає шукати винного та переносити свою образу на оточуюче середовище.

Саме в такому психологічному стані перебувала найактивніша частина українського суспільства напередодні Євромайдану. Втім, різниця між ситуацією, що мала місце у 2013 та у 2015 роках, є суттєвою. Революційна ситуація дворічної давнини мала конструктивне спрямування — люди прагнули конкретних змін, руху до Європи, припинення тиску на громадськість та бізнес. Сьогодні настрої значної частини суспільства мають переважно деструктивний характер — знищити, відсторонити, ліквідувати.

Зрозуміло, що на такому тлі, рівень довіри до офіційної влади демонструє стійку тенденцію до падіння. Серйозних перспектив на покращення суспільних настроїв, на жаль, поки що не спостерігається.

Сьогодні суспільство потребує зняття напруги. Будь-яка політична колізія може викликати миттєву, неконтрольовану негативну громадську реакцію, яка матиме деструктивний характер. Останнім може скористатися будь-який енергійний політик-популіст для реалізації власних цілей. Саме ці тенденції яскраво проявляються в результатах опитування щодо конфлікту між Парасюком та Пісним.

Виходячи із зазначеного, владі було б варто:

- *припинити будь-яку негативну, подразнюючу політичну активність у вищих ешелонах влади та серед політичних еліт у цілому хоча би на певний час;*
- *перемкнути увагу населення на позитивні речі, приміром, скориставшись святами, що наближаються;*
- *наповнити медіа простір позитивними матеріалами, пов'язаними із темами, що викликатимуть зацікавленість у плані найближчих перспектив.*

4.4. SMM-аудит

Сучасний стан розвитку соціальних мережевих технологій потребує постійного вдосконалення методів моніторингу та оцінки ефективності соціальних комунікацій. А це означає, що автор інформаційного повідомлення обов'язково має отримати інформацію не тільки про кількість «лайків» та зміст коментарів, але й зрозуміти загальні тенденції уподобань його цільових груп та передбачити характер їх подальшого розвитку. Розв'язати зазначене питання може профільна інтегрована методика – комплексне застосування якісних та кількісних характеристик шляхом використання окремих інструментів моніторингу, контент-аналізу та систематизації профільних даних. Такою є методика SMM-аудиту.

Зазначена методика базується на механізмах моніторингу контенту та його змістовного аналізу. При цьому схема реалізації завдань у контексті методики є гнучкою. Збирання матеріалів для дослідження може здійснюватися або в автоматичному режимі (відповідні інтернет-сервіси) або засобом прямого збирання та сегментації контенту в ручному режимі.

Мета дослідження в рамках SMM-аудиту - виявлення ефективності розповсюдження в певній зоні Інтернет інформації про досліджувану структуру.

Головними завданнями аудиту є:

- Розробка базового інструментарію та методології проведення комплексного поглибленого дослідження та систематичного моніторингу інформаційної активності досліджуваного об'єкта в мережі Інтернет;
- Формування цільових баз даних щодо поширення інформації про діяльність об'єкта в мережі Інтернет;
- Проведення комплексного дослідження щодо ефективності інформаційної політики об'єкта в мережі Інтернет у рамках певного хронологічного заміру (не менше ніж 6 місяців).

Методологічною основою дослідження є технологія інформаційного діагностування ефективності процесів промоції діяльності організації в мережі Інтернет.

Методика проведення роботи. Комплексне моніторингове дослідження проводилося на основі профільних баз даних, що репрезентують цільові групи досліджуваного об'єкта в мережі Інтернет. Процедура здійснюється в форматі трьох рівнів моніторингового дослідження. Загальна процедура роботи передбачала *підготовчий* та *чотири робочі* послідовні етапи.

На ***підготовчому етапі*** формуються бази даних по профільних веб-ресурсах, що відповідають цільовим групам об'єкта в мережі Internet. Серед них можуть бути:

1. *Соціальні мережі,* в яких можуть бути розміщені матеріали або згадування про діяльність об'єкта.
2. *Засоби масової інформації,* зокрема сайти газет, журналів, інтернет-видань, телеканалів, радіостанцій.

3. *Сайти профільних організацій* у досліджуваній галузі.

4. *Інформаційно-довідкові портали* за профілем діяльності об’єкта або близькою тематикою.

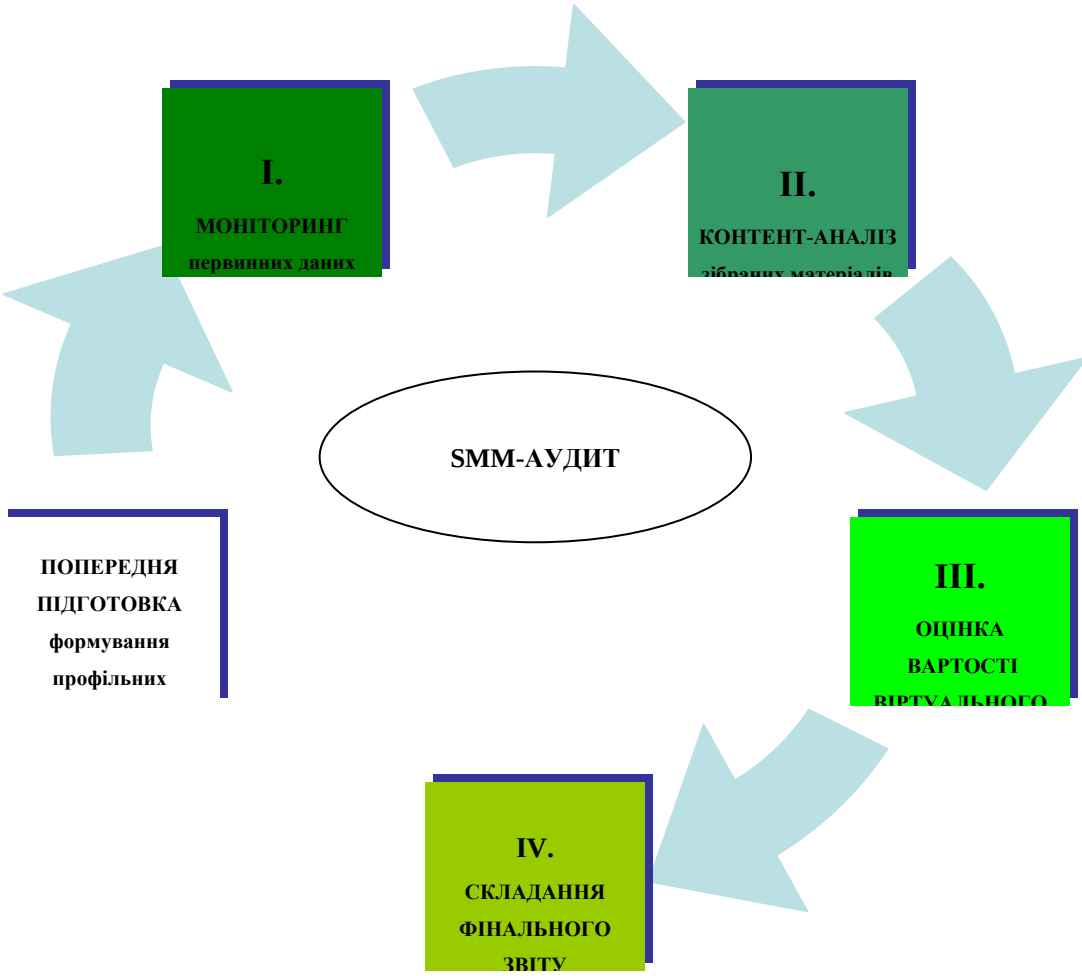
5. *Веб-портали* центральних та місцевих органів державної влади та самоврядування.

6. *Корпоративні сайти* громадських організацій, що працюють у полі діяльності об’єкта, а також профільних проектів за міжнародними програмами.

7. *Веб-сайти* політичних об’єднань та громадських рухів, що мають певний вплив на загальну громадсько-політичну ситуацію в країні.

8. *Особисті веб-сторінки* публічних осіб (політики, громадські діячі, чиновники), що мають пряме або опосередковане відношення до тематики діяльності об’єкта.

Мал.4.3. Схема SMM-аудиту



Зазначена методика передбачає процедуру проходження чотирьох етапів. *Перший етап (формування пошукових баз та критеріїв пошуку).* На цьому етапі формується перелік критеріїв пошуку (ключові слова та фрази), а також бази пошуку (соціальні мережі, тематичні портали, блоги та ін.).

Табл.4.4. Шаблона структура звіту за результатами контент-аналізу

№ з/п	Веб-ресурс	Дата	Назва статті, автор	Тематика	Фігурант	Коротке викладення змісту	Забарвлення
Інтернет-версії друкованих видань							
Телебачення							
Радіо							
Інформаційні портали							
Рекрутингові агенції							
Веб-портали органів державної влади							
Соціальні мережі							
Громадські організації							
Особисті сторінки публічних осіб							
Веб-портали політичних об’єднань							

Другий етап (збір матеріалів). Для збору базової інформації по ключових критеріях пошуку можуть бути передбачені два варіанти дій – звернутися до регіональних адміністраторів досліджуваних соціальних мереж та, за певну суму, отримати потрібну інформацію, або застосувати певну пошукову програму. За будь-яким варіантом пошуку його результати вносяться до таблиці узагальнення (табл.4.5).

Третій етап (контент-аналіз). Отримані на попередньому етапі матеріали систематизуються у відповідності до ключових показників та переводяться в якісні та кількісні оцінки.

Четвертий етап (складання звіту). Отримані результати дослідження оформлюються в текстовому варіанті із висновками та практичними рекомендаціями.

Табл. 4.5. Таблиця узагальнення первинних даних («моніторинг-конспект»)

№	**Критерії пошуку** (товар, послуга, захід, персоналії, організація)	**Кількісні показники** (де та скільки матеріалів знайдено)	**Якісні характеристики** (позитив, негатив, нейтрально)	**Рекомендації** (потрібні практичні кроки)	**Примітки**

Зазначений тип дослідження дає можливість ретельного вивчення профільного інформаційного поля із можливістю деталізації окремих питань та конкретизацією майже до кожного конкретного представника цільових груп.

4.5. Моніторинг та ідентифікація достовірності контенту в мережі Інтернет та соціальних он-лайн мережах

В умовах сучасної інформаційної війни одним з головних завдань у роботі з контентом є його ідентифікація та встановлення походження текстової інформації, відео та графіки.

Як свідчить практика, за умови необхідності підтримки інформаційного потоку високої щільності, не завжди вистачає реального матеріалу. Тому при формуванні контенту атакуюча сторона може залучати чужі відео, графічні та текстові матеріали. Особливо показовою в цьому плані була російська інформаційна агресія проти України, що відбувалася протягом 2014-2015 рр. Російські медіа неодноразово ловили на підробках, розкриваючи фейки, особливо, коли мова йшла про чисельні жертви від артобстрілів серед мирного населення або певні ситуативні події.

Технічно розкрити фальшування не складно. Для цього можна використати певні сервіси пошукових систем, зокрема у Google або Yandex або застосувавши окремні програмні продукти.

Найбільш популярним на сьогодні серед провідних пошукових систем є Google, який пропонує такі методи ідентифікації контенту.

Для перевірки автентичності тексту можна використати такі методи [368]:

1. Внести пошуковий запит (цитата, ключові слова) у лапки «...» та задати пошук – програма шукатиме сторінки зі вказаною формою слова, без зайвої інформації та реклами.

2. У разі, коли в цитаті відсутнє слово або кілька слів, необхідно взяти в лапки всю цитату, а відсутню частину замінити на зірочку **«*»** - програма шукатиме повну версію.

3. Коли необхідно шукати контент у певному місці, то можна застосувати такі символи:

- ***inurl*** - для пошуку всередині URL;
- ***intitle*** - у заголовку;
- ***intext*** - у тексті;
- ***inanchor -*** у тексті посилань.

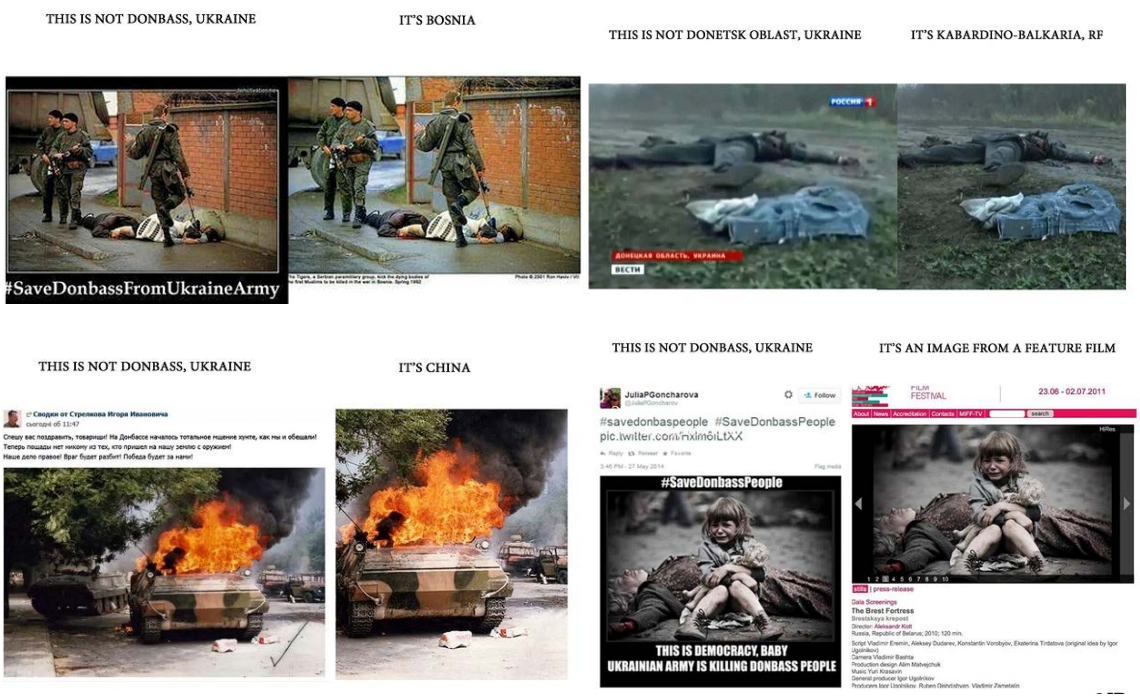
4. У разі, коли необхідно дізнатися, хто посилався на конкретний матеріал, необхідно використати оператор ***link***. Останній необхідно поставити разом із двокрапкою перед URL, який є пошуковим.

5**.** Якщо контент, який розшукується, неможливо знайти за прямою адресою, необхідно шукати в кеші. В такому разі необхідно звернутися до http://cachedview.com. Google обов'язково зберігає інформацію про сайт та його зміст на певний момент.

Пошук та ідентифікація фото передбачає дещо складнішу процедуру, втім розвінчання таких фейків дає найбільш значний ефект та максимально сприяє процесам контрпропаганди.

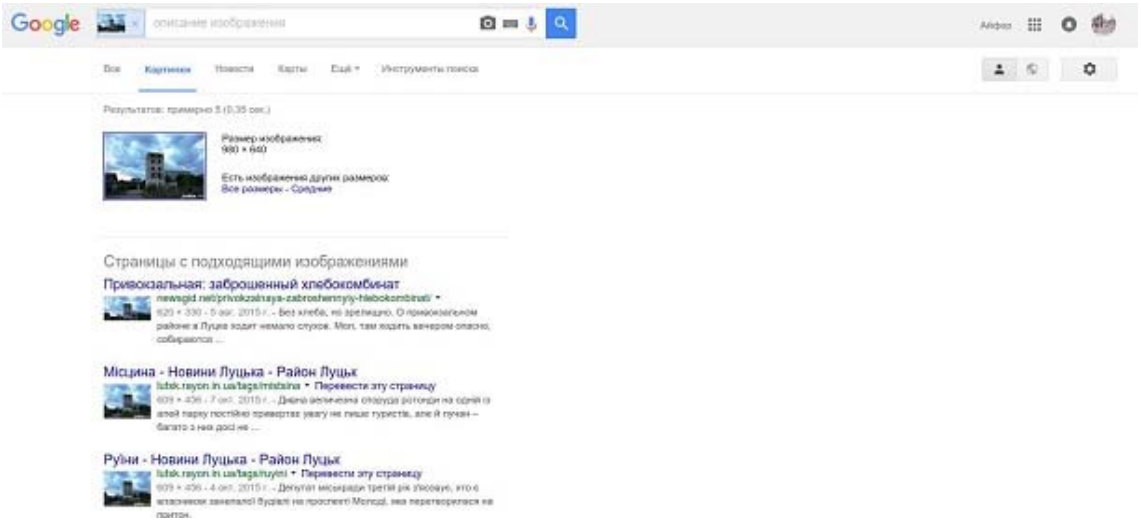
В якості такого прикладу можна навести результати роботи Джулії Девіс із американського видання Examener.com, яка розвінчувала кремлівські фейки, що базувалися на чужих фото. Типовими були ілюстрації з «подій в Донбасі», для яких використовували фото з Боснії, Китаю, Саудівської Аравії, Африки, самої Росії й навіть іноді з художніх фільмів (мал.4.4).

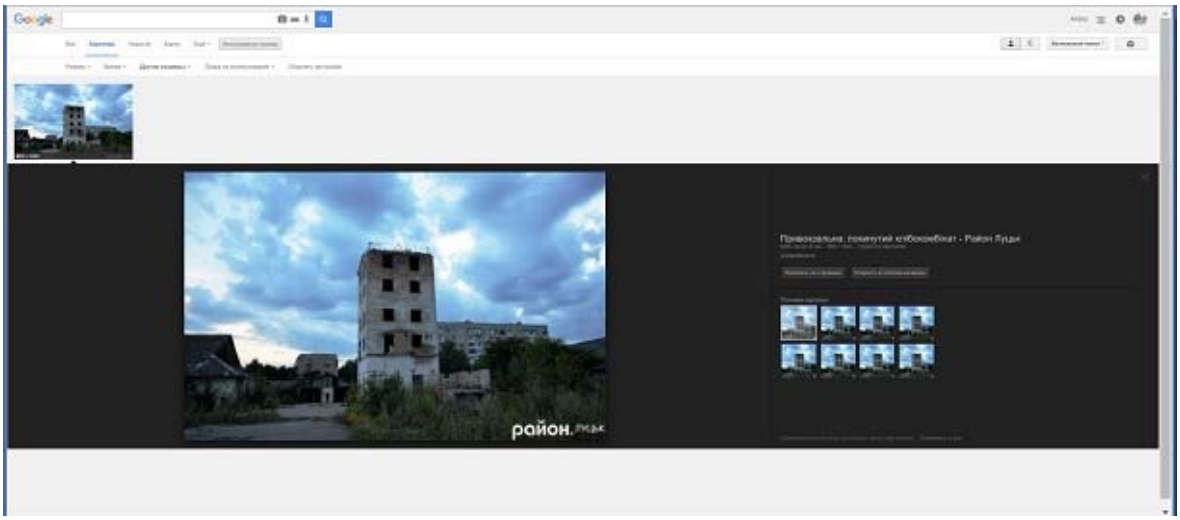
Мал.4.4. Російські фейки про війну в Донбасі



Для того, щоб оцінити фото на предмет його автентичності, можна скористатися сервісом **google image search.** Зазначений сервіс через гіпертекст допомагає знайти адреси, де первинно фігурувало фото, і який супроводжувальний текст воно мало [368]. В такому разі через діалогове вікно та функцію «Пошук цього зображення в Google» можна отримати необхідні дані (мал. 4.5.)

Мал.4.5. Алгоритм пошуку майданчика первісного розміщення фото





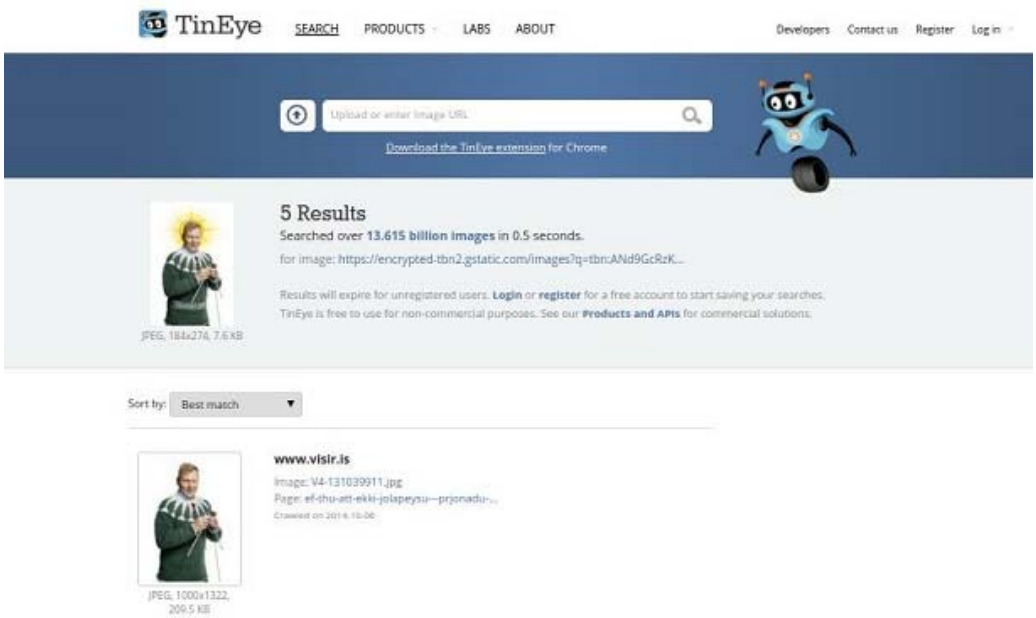
Крім програмного забезпечення від Google, існує ще низка ресурсів, які допомагають ідентифікувати матеріали. Найбільш популярними серед них є Foto Forensics та TinEye.

Foto Forensics - веб-сайт, що дозволяє виявляти фальсифікації фотоматеріалів, а також підробки із нехарактерними доданими фрагментами, які на перший погляд можуть виглядати цілком природно. Сервіс показує особливості графічного редагування, розкриває всі додані частини зображення.

Мал. 4.6. Інтерфейс Foto Forensics

TinEye - сервіс, що шукає зображення, які виявляють подібність до заданого фото. Програма може ідентифікувати обличчя на зображеннях навіть із низьким розширенням.

Мал. 4.7. Інтерфейс TinEye



Ідентифікація відеоматеріалів є більш складною, втім вирішення цього завдання є цілком можливим навіть за відсутності системних знань у галузі ІТ. Для цього необхідно виконати низку таких дій:

1. Якщо ролик на сайті або в групі має посилання на інше місце, зокрема YouTube, необхідно перейти на базовий майданчик і дослідити його походження. Доволі часто саме від того, хто його розмістив, стає зрозумілим мета цього контенту.

2. Ознайомитися із коментарями, що знаходяться під роликом, у місці його базового або подальшого розташування. Серед тих, хто висловився з цього приводу, можна знайти опосередковане підтвердження або спростування його фейковості.

3. Уважно роздивитися деталі відеоряду – написи, номери машин, назви вулиць та ін. При наявності звукового ряду необхідно уважно вислухатися у все, що промовляють учасники подій та ін. Певні деталі можуть допомогти викрити фейк.

4. Скласти опис зображення словами у пошукову систему та перевірити їх на інші варіанти розташування та використання.

5. Зробити скриншот найбільш виразного кадру ролика та на його основі зробити запит через систему пошуку зображень.

Разом з наведеними вище елементарними засобами перевірки відео, існують відповідні сервіси та сайти, втім це вже є царина профільних фахівців, які розбираються в деталях виробництва та монтажу відеоматеріалів.

На сьогодні можна знайти достатньо багато різноманітних сервісів, програмного забезпечення та окремих сайтів, які допомагають у питаннях ідентифікації текстів, зображень та відеоматеріалів (див. додаток). А обрання конкретного інструмента залежить зазвичай від специфіки та особливостей кожного з них та завдань, які ставить перед собою дослідник.

РОЗДІЛ 5. Соціальні он-лайн мережі в системі сучасних форматів ведення війни

5.1. Сучасна гібридна війна та її відображення у віртуальній реальності

5.1.1. Гібридна війна: структура та базові прийоми

Трансформація технологій, специфіка соціальних, економічних та політичних умов розвитку сучасного світового співтовариства впливають на характер та особливості ведення сучасних війн.

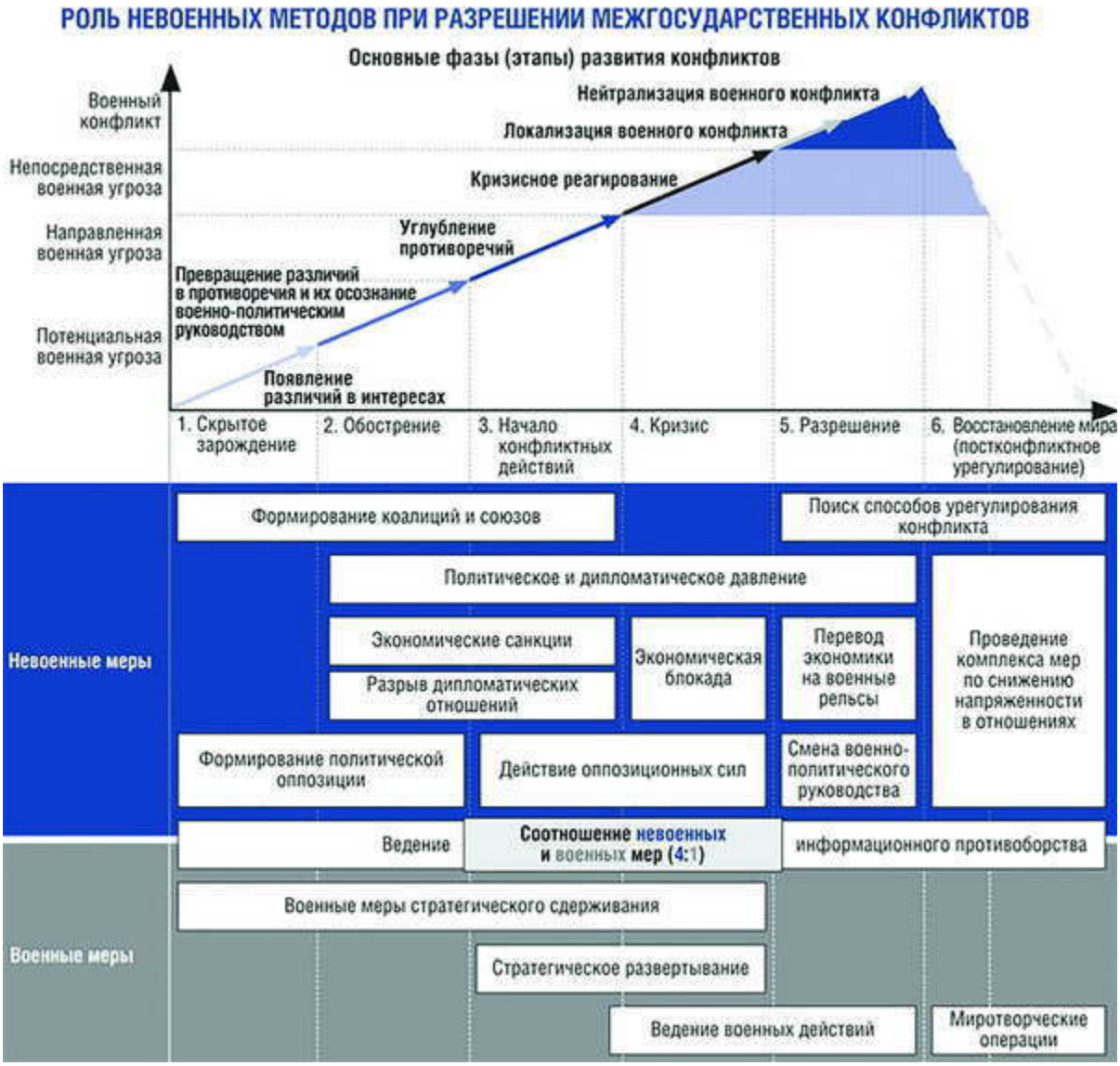
Провідні країни світу виділяють сьогодні на оборону значні бюджети, що дозволяють їм тримати міліонні армії, мати найсучаснішу зброю, в тому числі таку, що відноситься до категорії зброї масового знищення. В цих умовах конфлікт двох або кількох таких країн, пов'язаних з іншими подібними країнами різними угодами та союзами, може автоматично перетворитися на глобальну війну і, можливо, навіть до застосування ядерної зброї.

У таких умовах виникає потреба пошуку більш безпечного засобу вирішення конфліктних ситуацій, що не призведе до негативних глобальних наслідків. Таким засобом стала гібридна війна, яка являє собою комбіноване, інтегроване військово-політичне та економічне протистояння у вигляді безстатусного, часто прихованого, конфлікту.

Однією з провідних країн, яка активно використовує сьогодні інструменти гібридної війни, є Росія. Узагальнивши досвід гібридних конфліктів кінця XX – початку XXI ст., які вели США, провідні країни ЄС та азійського регіону, профільні російські фахівці розробили нову концепцію такого роду війн та застосували її на практиці проти своїх сусідів і намагаються боротися за відновлення системи двополярного світу, який існував за часів СРСР.

Базові складові частини російської стратегії і тактики сучасної гібридної війни були сформульовані в 2013 р. начальником генерального штабу ВС РФ В.Герасимовим (мал.5.1.) [342].

Мал.5.1. Схема гібридної війни (російське бачення)



Саме на основі цих принципів було сплановано та реалізовано напад на Україну, захоплення Криму та розв’язання війни в Донбасі. Серед ключових складових російської концепції зазначалися збільшення ролі невійськових методів тиску на противника, насамперед, за допомогою політичних

(дипломатичних), економічних і гуманітарних елементів. Що стосується інформаційної складової, то вона визначалася як основа діяльності на всіх етапах конфлікту: його зародження, супроводу і в постконфліктний період. Особлива увага в Концепції відводиться і «асиметричним заходам», до яких були віднесені: діяльність підрозділів спеціального призначення; підтримка внутрішньої опозиції і колабораціоністів, а також збільшення цілеспрямованого інформаційного впливу на об'єкт нападу.

Послідовними, типовими складовими етапами гібридної війни в Концепції було визначено [342]:

- ***інноваційна агресія*** (кібервійна, економічний тиск, інформаційно-психологічні атаки та ін.);
- ***застосування нерегулярних збройних формувань або приватних армій*** (повстанський, партизанський рух, тероризм);
- ***офіційні військові дії або демонстрація сили*** (ідентифікована уніформа, зброя, офіційне визнання участі в конфлікті).

Перший етап гібридної війни починається із ***інноваційних агресій,*** які зазвичай мають ***прихований характер***.

Аналізуючи перебіг багатьох гібридних конфліктів, дійсно іноді доволі складно виявити і тим більш ідентифікувати приховану економічну атаку, яка може бути замаскованою під виглядом конкуренції та боротьби за лідерство між країнами та транснаціональними корпораціями, в окремих секторах або галузях економіки. Так само не завжди в просуванні національної культури однієї країни на теренах іншої можна простежити акт агресії. Схожа ситуація має місце і в просуванні ЗМІ, які здійснюють боротьбу за цільові аудиторії та зони впливу, що можуть поширюватися на сусідні держави та навіть окремі континенти.

Навіть у разі можливості відстеження зазначених тенденцій, вкрай важко обґрунтувати і довести звинувачення та змусити опонента припинити агресивні

дії. До цього залучаються міжнародні третейські інституції, присуди яких виносяться роками та мають нечіткі рішення. Крім того, процедура прийняття рішень такими структурами є доволі тривалою, в той час, як гібридні атаки здійснюються швидко.

Етап інноваційної агресії іноді може бути розтягненим на роки і десятиліття. Класичним прикладом тому може бути така агресія Росії проти України. Типовими ознаками її були газові і торговельні війни, намагання захопити стратегічні підприємства, поширити вплив власних ЗМІ, тиск на політичному рівні в питаннях захисту прав російськомовного населення, просуванні елементів російської культури (кіно, література, твори мистецтва та ін.).

Саме на цьому етапі відбувається закладання конкретних масових психологічних установок, які згодом, у моменти переходу конфлікту до відкритої фази, використовують для послаблення сторони, проти якої здійснюється агресія.

Другий етап гібридної війни набуває характеру певної відкритості, з якого вже стає зрозумілим, хто є ініціатором агресії, втім з наведенням доказів у цьому випадку доволі складно, бо атакуюча сторона не розкриває остаточно своїх карт.

На цьому етапі головними засобами здійснення гібридної агресії є:

- створення атмосфери бездуховності, накручування конфліктних ситуацій, знищення авторитету державної влади;
- дестабілізація політичної ситуації (конфлікти, репресії, терор);
- блокування інформаційної діяльності органів центральної влади та місцевого самоврядування;
- підрив авторитету та дискредитація органів державної влади всіх рівнів;

- провокування соціальних, політичних, національних, релігійних зіткнень – аж до розв'язання громадянської війни;
- ініціювання масових акцій протесту та безладів на вулицях, погромів офіційних установ та громадських структур.

Фактично всі представлені вище засоби були випробувані російською стороною під час захоплення Криму, розпалювання війни в Донбасі та дестабілізації ситуації в середині України з кінця 2013 р. і до теперішнього часу.

Характерною ознакою другого етапу є застосування ***нерегулярних збройних формувань або приватних армій,*** які діють під виглядом партизанських груп, повстанських об'єднань або терористичних організацій.

У переважний більшості випадків, на другому етапі, держава-агресор може виказати себе через:

- офіційну політичну підтримку сепаратистських рухів на рівні публічних заяв чи через відстоювання інтересів повстанців у міжнародних установах;
- надання матеріально-технічної допомоги у вигляді техніки, зброї, продуктів харчування, коштів та інших ресурсів.

На цьому етапі держава-агресор у боротьбі із противником спирається вже не тільки на окремих інсайдерів та певні групи впливу в середині країни, проти якої здійснює агресію, але й починає застосовувати власні закамуфльовані війська або залучає приватні армії.

Так, у війні, яку розпалила Росія на Сході України, були ідентифіковані такі угруповання, як [360]:

1. Козаки (щось середнє між поліцією і солдатами).
2. Військовослужбовці регулярної армії («зелені чоловічки»).
3. Чеченські найманці (підрозділи створені А.Кадировим).
4. Інші найманці (представники арабських країни та деяких країн ЄС).

5. Колишні співробітники "Беркута" (розформований спецпідрозділ МВС України).
6. Місцеві етнічні росіяни, що живуть в Україні.
8. Російські «туристи» (колишні військовослужбовці, що діють як найманці).
9. Реальні актори (використовуються з ціллю пропаганди або навмисно шукають західні камери, щоб розіграти свою драматичну роль і висловити свою порцію пропаганди).
10. Колишні українські солдати і офіцери (дезертирували з української армії чи служать у ній і діють як зрадники / шпигуни).
11. Місцевий криміналіте, що пройшов навчання і отримав зброю.
13. Місцеві жителі, які були змушені воювати (через гроші, примус або під впливом пропаганди).
14. Російські кримінальники або ув'язнені, що потрапили під амністію в обмін стати найманцем в Україні.
16. Агенти ФСБ.
17. Російські генерали та вищий офіцерський склад, які «координують припинення вогню» на українській стороні фронту.
18. Іноземні журналісти, що збирають цінну інформацію та створюють негативні сюжети про Україну.

Що сьогодні собою являють типові приватні армії, можна зрозуміти, проаналізувавши діяльність потужних транснаціональних корпорацій, які для захисту своїх економічних інтересів залучають до співпраці певні незалежні озброєні групи або створюють власні формування.

Традиційно такі військові групи визначають, як ***приватні військові компанії*** (далі - ПВК) – комерційні підприємства, що пропонують послуги, пов’язані із охороною, захистом певних об’єктів або персон. Доволі часто вони беруть активну участь у військових конфліктах, а також здійснюють збирання

розвідувальних даних, надають послуги із стратегічного планування, логістики та консультують [175].

У квітні 2001 р. була створена міжнародна організація «Peace Operations Association», головним завданням якої є координація та представництво інтересів усіх її членів на різних рівнях. Після початку війни в Іраку було створено «Private Security Company Association of Iraq» - асоціацію приватних військових та охоронних компаній, що контролювали ситуацію в цій країні. До складу зазначеної структури увійшло понад 40 компаній [390].

Серед прикладів типових послуг, які надають приватні армії, є такі, як [90, с. 348]:

- набір особового складу для контингенту міжнародних поліцейських місій та управління ними (DynCorp);
- охорона об'єктів, у тому числі тих, що мають важливе і стратегічне значення (так, "DynCorp" забезпечувала охорону стратегічно важливого нафтового резерву США);
- охорона нафтових родовищ і трубопроводів, охорона енергетичної системи (Hart Group, Blackwater Security Consulting, Erinys Iraq Limited);
- охорона посольств та керівників держави (Triple Canopy);
- супроводження конвоїв ООН (Kroll);
- навчання особового складу урядових збройних сил, поліції та інших сил безпеки (так, у лютому 2002 року 70 співробітників ізраїльської компанії "Levdan" займалися навчанням збройних сил Конго);
- надання послуг військових перекладачів (CACI);
- охорона в'язниць (Titan Corporation);
- розмінування мінних полів і знищення боєприпасів (RONCO, MAG, BACTEC, Armor Group, Minetech, EODT);
- протипожежний захист (Group 4 Falck);

- тилове постачання військ (KBR);
- авіарозвідка (AirScans Inc., Eagle Aviation Services & Technology);
- збройний супровід і захист морських суден від піратів (Global Marine Security Systems).

Слід зазначити, що поступово роль і значення ПВК зростає. Приміром, станом на 2007 р. близько 25% усіх розвідувальних операцій для силових структур США забезпечували саме такі структури [348, с. 355].

У західних країнах діяльність таких приватних військових структур чітко регламентується законом та контролюється. Сьогодні в світі сформувався чітко структурований ринок військових послуг із загальним обсягом у понад $100 млрд. Серед найбільш відомих сьогодні визначаються такі компанії, як: «Hulliburton», «Blackwater», «DynCorp», «Logicon», «Brown&Root», «MPRI», «Control Risks», «Bechtel», «ArmorGroup», «Erinys», «Sandline International», «International Defense and Security» [348, с. 350].

На відміну від європейської та американської практики в Росії специфіка діяльності таких організацій має дещо інший характер. Перші приватні армії з'явилися в Росії в 2007 р., у складі компаній «Транснефть» та «Газпром» [93] з метою захисту від зазіхань криміналу. Втім згодом вони перетворилися на неформальні силові структури, що діють під прикриттями та за настановами ФСБ і особисто кремлівського керівництва. Формально вони регулюються профільними нормативно-правовими актами, але в реальності їх діяльність повністю контролюється офіційною владою. Саме такі російські структури починали агресію в Донбасі та виконували допоміжні функції при захопленні Криму.

На **третьому етапі гібридної війни**, боротьба фактично набуває відкритої форми і може перейти в офіційний збройний конфлікт.

Це здійснюється або у форматі відкритої інтервенції, або під виглядом введення миротворчих сил. В обох випадках головним офіційним приводом є

намагання зупинити внутрішньо національні конфлікти або припинити неправомірні дії офіційної влади, що суперечать сучасним нормам та принципам захисту прав людини, встановленим та закріпленим у міжнародних угодах та деклараціях ООН, ЮНІСЕФ, Ради Європи та ін.

Маємо зазначити, що складні для офіційного контролю форми діяльності ПВК ідеально підходять для застосування у так званих ***гуманітарних інтервенціях***, що є типовою ознакою гібридної війни [348, с. 364]. Такі інтервенції визначають, як примусові дії особливої форми, які застосовуються міжнародною спільнотою або окремими державами [348, с. 365].

Найбільш легітимним сьогодні, для здійснення миротворчих операцій або камуфлювання під них, вважається мандат Ради Безпеки ООН, який дозволяє:

- розгортання сил для запобігання конфлікту і його виходу через кордони;
- стабілізацію конфліктної ситуації після припинення вогню;
- створення умов для досягнення угоди про встановлення міцного миру між сторонами;
- забезпечення здійснення всеосяжних мирних угод;
- надання сприяння країн чи територій у подоланні перехідного періоду і створенні стабільного уряду на основі демократичних принципів, ефективного управління та економічного розвитку.

Слід зазначити, що саме наприкінці XX – на початку XXI ст. кількість таких гуманітарних інтервенцій зросла в рази, що можна пояснити такими факторами, як [348, с. 365]:

- зникнення біполярної конфронтації США та СРСР, яка ускладнювала діяльність Ради Безпеки ООН щодо питань санкціонування миротворчих операцій;

- різке зростання геополітичного впливу США та їх прагнення до встановлення власних правил гри на міжнародній арені;
- посилення тиску на слаборозвинуті країни, що володіють стратегічними ресурсами (газ, нафта та ін.) чи вигідним геополітичним положенням;
- наявність країн із антидемократичними режимами та терористичних організацій світового масштабу, з якими необхідно вести боротьбу;
- зміна норм міжнародного права щодо збільшення уваги до проблем захисту прав людини.

На відміну від загальновизнаного світовим співтовариством мандату на миротворчі операції, іноді країни агресори намагаються використовувати квазі мандати або локальні міждержавні угоди під прикриттям яких здійснюється окупація чужих територій. Саме так було, коли Росія використала своїх «миротворців» у Придністров'ї (1992 р.), Абхазії (1994 р.), Південній Осетії (2008 р.).

Специфіка та особливості сучасної гібридної війни стимулює створення нових форм військово-політичної агресії, які мають усі необхідні формальності або забезпечуються ґрунтовним юридичним прикриттям. Саме так відбулося під час захоплення Криму. Анексія частини української території була легітимізована через проведення народного референдуму, волевиявлення під час якого контролювалося та забезпечувалося силами спеціальних операцій ВС РФ [59].

При здійсненні російської агресії в Донбасі в 2014 році, кремлівське керівництво планувало застосувати технології миротворчої місії за мандатом Організації договору про колективну безпеку (ОДКБ або Ташкентська угода) [269; 288]. Втім реакція світової спільноти та економічні санкції завадили реалізації цих планів, і Росія зупинилась на варіанті відкритої, але офіційно не визнаної військової агресії.

Після невдалих спроб здійснення фронтальних атак на позиції українських силовиків у Донбасі, як це було, приміром, під час п'ятиденної війни в Грузії, Росія в Україні перейшла до іншої тактики – активності переважно в форматі діяльності диверсійно-розвідувальних груп та провокаційних артилерійських обстрілів. Також застосовується тактика партизанської боротьби.

Крім того, слід зазначити, що російські підрозділі в Донбасі сьогодні активно застосовують так звану тактику «трьох кварталів», що передбачає скомбінованість дій одного і того ж підрозділу, який в одному кварталі міста може виконувати загальновійськові функції, в другому – здійснювати поліцейські функції, в третьому – виконувати гуманітарні місії [117]. Цю тактику ми сьогодні наочно спостерігаємо в діях ополченських підрозділів так званих «ДНР» та «ЛНР».

Інформаційна складова гібридної війни, на усіх її етапах несе в собі функції забезпечувального характеру. На першому етапі вона створює умови для виникнення конфліктної ситуації, на другому – забезпечує привід для опосередкованого втручання держави агресора у внутрішні справи атакованої країни, на третьому – створює відповідний медійний фон для легітимізації дій агресора.

У цьому разі цільовими групами для інформаційних атак є [117]:

- цивільне населення, що знаходиться в зоні конфлікту;
- цивільне населення атакованої країни в цілому;
- цивільне населення країни агресора;
- представники світової спільноти.

За змістом, інформаційна складова гібридної війни має вигляд «війни сенсів» із застосуванням передових методів агітації та пропаганди. Зокрема активно використовуються так звані **симулякри** – ***образи, яких в природі не існує*** [94]. Головна мета таких дій – нав'язати атакованій стороні бачення та

психологічні установки, які допомагатимуть агресору в реалізації його планів [117].

У форматі зазначеного, особливої ваги набуває завдання встановлення контролю над інформаційним простором країни, проти якої здійснюється агресія, а також тих країн, які можуть якимось чином впливати на перебіг конфлікту.

В якості допоміжного засобу використовують діяльність різноманітних громадських структур – благодійних фондів, аналітичних центрів, культурних товариств та ін.

У контексті останнього особливого значення набувають технології web 2.0, які надають атакуючій стороні – країні агресору, необмежені можливості у здійсненні впливу на населення країни, проти якої здійснюється агресія. При цьому згадані можливості мають широкий спектр – від впливу на масову аудиторію до здійснення інформаційного контакту на індивідуальному рівні, тобто адресний.

5.1.2. Сучасні інноваційні засоби ведення гібридних війн

В рамках сучасних гібридних війн, напрямок роботи із соціальними он-лайн мережами найближче всього стоїть до питань функціонування **структур інформаційно-психологічних операцій** (далі ІПсО) та так званих **сил спеціальних операцій** (далі ССО).

Польовий устав Армії США визначає ***інформаційно-психологічні операції, як планову пропагандистську та психологічну діяльність, розраховану на іноземні, ворожі, дружні або нейтральні аудитори, що здійснюється з метою впливу на їх відношення та поведінку у потрібному напрямку для досягнення політичних, та військових национальных цілей*** [162].

Інформаційно-психологічні операції поділяються на стратегічні, оперативні та тактичні. Такі операції передбачають використання засобів масової інформації та допоміжну діяльність у мирний і воєнний час, котра має на меті послаблення престижу і впливу образу противника у ворожих, нейтральних або союзних країнах і зміцнення свого впливу та престижу.

Допоміжна діяльність передбачає [224]:

- демонстрацію сили;
- підвищення ступеня бойової готовності військ;
- перекидання військ;
- програми громадянських дій;
- громадянську непокору; мітинги;
- демонстрації;
- програми в галузі освіти, сільського господарства і медицини;
- певні способи ведення бойових дій.

Кожен з названих видів діяльності може впливати на прийняття рішень політичних діячів або населення країн, обраних в якості об'єктів атакування.

У війні з застосуванням звичайних засобів збройної боротьби інформаційно-психологічні-психологічні операції можуть підвищувати бойову ефективність військ при збереженні незмінної їх чисельності. Такі операції, коли їх здійснення було розпочато завчасно і вони проводилися з високою ефективністю, можуть дозволити відмовитися від фактичного застосування військової сили [239].

Інформаційно-психологічні операції можуть проводитися у кризовій ситуації, доки справа не дійшла до військових дій, в інтересах консолідації громадської думки на підтримку цілей атакуючої сторони, щоб не вдаватися до введення регулярних військ на іноземну територію. Зазначені операції є також невід'ємною частиною заходів з тактичної дезінформації, забезпечення

внутрішньої безпеки інших країн, підтримки миру, боротьби з тероризмом і інших спеціальних операцій [240].

Стратегічні інформаційно-психологічні операції здійснюються в інтересах досягнення довгострокових цілей, покликаних створити сприятливу психологічну атмосферу для ведення військових дій. Такі операції зазвичай носять глобальний характер [331].

Оперативні інформаційно-психологічні операції здійснюються в інтересах досягнення середньострокових цілей, на підтримку військових кампаній в рамках великих операцій. Об'єктом таких операцій зазвичай є населення певного регіону [331].

Тактичні інформаційно-психологічні операції здійснюються в інтересах досягнення короткострокових цілей, на підтримку командирів тактичної ланки. Об'єктом таких операцій зазвичай є протистоїть угруповання військ противника [331].

Відповідно специфіки та характеру завдань, на забезпечення яких орієнтуються зусилля сил ІПсО, вони можуть супроводжувати військові дії стратегічного, оперативного та тактичного рівнів.

Психологічні операції орієнтовані на підтримку військових дій стратегічного характеру використовуються для досягнення цілей національної політики або для демонстрації загрози застосування військової сили. Психологічні операції в підтримку стратегічних завдань ґрунтуються на використанні в своїх інтересах вразливих сторін іноземних урядів, збройних сил і населення для досягнення довгострокових цілей. Приміром в США, Національне військове керівництво країни, через Комітет начальників штабів видає директивні вказівки і зазвичай керує стратегічними психологічними операціями. Головнокомандувач на театрі війни (військових дій) сприяє їм шляхом спонукання політичного керівництва іноземних держав до підтримки позицій, які не суперечать національним цілям США і їх союзників [331].

Інформаційно-психологічні операції в підтримку військових дій оперативного рівня є проміжними між військовими діями стратегічного і тактичного рівнів. На цьому рівні здійснюються планування і ведення військових кампаній і великих операцій у відповідному театрі військових дій. В практиці армії США, командувачі збройними силами та їх штаби зазвичай планують і проводять військові кампанії. Групи армій і армії, як правило, розробляють великі операції сухопутних військ, які ведуться армійськими корпусами і дивізіями. Хоча поняття «командир оперативної ланки» зазвичай асоціюється з головнокомандувачем збройними силами на театрі, немає такого ланки командування, яке єдино або виключно прив'язувалася б до оперативного мистецтва. Відповідальність за дії військ на оперативному рівні може змінюватися в залежності від характеру військових завдань, розмірів і географічних особливостей театру війни, а також чисельності і концентрації військ [331].

На оперативному рівні сили психологічних операцій надають підтримку виходу в райони зосередження формувань звичайних збройних сил і їх тилового забезпечення; наземним і повітряним маневреним силам; ведення вогню з використанням звичайних і ядерних засобів ураження, а також діям сил спеціальних операцій. Основні особливості пропаганди та психологічних акцій, здійснюваних в рамках психологічних операцій, полягають в тому, що вони прямо або опосередковано сприяють поразці сил противника, викликаючи в нього невіра в можливість перемогти і примушуючи до відступу [331].

Психологічні операції в підтримку військових дій тактичного рівня відносяться до загальних завдань командира польового підрозділу, що передбачають знищення сил противника або пряме припинення його намірів. На цьому рівні армійські корпуси, дивізії або частини і підрозділи використовують специфічні способи або методи дій. Психологічні операції в підтримку військових дій тактичного рівня плануються і здійснюються в

інтересах досягнення найближчих або короткострокових цілей. Психологічні операції можуть сприяти досягненню наступних тактичних цілей:

- ізоляції живої сили, техніки і матеріальних засобів супротивника;
- безпосередньої вогневої підтримки;
- розвідці і спостереження;
- вибору позицій і передислокації систем зброї.

Психологічні операції в підтримку військових дій тактичного рівня включають використання візуальної, звукової та відео-звукової техніки для надання безпосередньої підтримки в бойових частинах і підрозділах. Психологічні операції на цьому рівні плануються з розрахунком здійснення впливу на цивільний і військовий персонал противника в зоні відповідальності командира тактичної ланки.

Конкретно взята категорія психологічних операцій (стратегічна, оперативна, тактична) може проводитися на підтримку більш ніж одного будь-якого рівня військових дій. Спільні завдання і цілі можуть служити для розмивання чітких меж між різними категоріями психологічних операцій.

Головна умова успіху в реалізації ІПсО - на будь-якому рівні психологічні операції повинні проводитися за єдиним задумом, з метою полегшення проведення військових операцій, зниження перешкод з боку цивільного населення і завоювання його підтримки. Ці операції повинні бути винахідливими, інтерактивними, проводитися в інтересах зниження ефективності і підриву лояльності військ противника, дії якого заважають досягненню поставлених цілей.

В структурі військових сил арміх США, підрозділи ІПсО мають в своєму складі команди 27 різних типів. Така організація дозволяє командиру, що координує психологічні операції, створювати спеціалізовані частини і підрозділи для вирішення конкретних завдань [331].

Всі команди умовно можна розділити на три категорії - управління, оперативні, постачання та обслуговування. Ці команди, в свою чергу,

об'єднуються в частини і підрозділи ІПсО трьох типів - група, батальйон і рота. Склад частин і підрозділів може бути різним у залежності від поставленого завдання.

З метою забезпечення максимальної гнучкості у виконанні поставлених завдань, частини і підрозділи ІПсО ВС США можуть надаватися загальновійськовим формуванням або здійснювати їх загальну або безпосередню підтримку в залежності від вимог. Вони можуть також передаватися в оперативне підпорядкування загальновійськових формувань. В усіх випадках частини і підрозділи ІПсО отримують директивні вказівки щодо ведення інформаційно-психологічних операцій і спеціальне тилове забезпечення по зовнішніх каналах психологічних операцій.

Групи ІПсО загальної підтримки зазвичай надаються або виділяються для супроводження підрозділів сухопутних військ в зоні бойових дій. При цьому батальйон ІПсО загальної підтримки, в зоні військових дій використовують з метою досягнення стратегічних та оперативних цілей, а також для здійснення пропаганди серед цивільного населення.

Спеціально навчені і підготовлені батальйони психологічних операцій можуть бути передані в оперативне підпорядкування командування військової поліції по роботі з військовополоненими для забезпечення порядку в таборах військовополонених.

В переважній більшості випадків, директивні вказівки щодо ведення психологічних операцій надходять з штабу групи психологічних операцій. Батальйони ІПсО, безпосередньої підтримки надаються для підтримки армійських корпусів; роти безпосередньої підтримки – для дивізії або окремої бригади. Накази з проведення психологічних операцій вони отримують від штабу групи ІПсО, яка надається або підтримує угруповання військ в зоні військових дій.

Частини та підрозділи ІПсО розробляють кампанії з метою підтримки звичайних збройних сил і сил спеціальних операцій, використовуючи такі інструменти, як [331]:

- аналіз завдання підтримуваного об'єднання (з'єднання, частини);
- визначення завдання психологічної операції;
- збір інформації та моніторинг ситуації;
- аналіз об'єкта на який здійснюється вплив;
- вибір тем і символів;
- вибір засобів поширення інформації;
- підготовка інформаційних матеріалів;
- попередня перевірка ефективності запланованих заходів;
- отримання остаточного дозволу на проведення кампанії;
- реалізація операції;
- оцінка ефективності пропагандистських заходів.

В армії США, відповідальність за узгодження психологічних операцій в процесі вироблення рішення покладається на начальника оперативного управління (відділу, відділення) відповідного штабу. Саме він зобов'язаний планувати проведення психологічних операцій при підготовці будь-якої військової операції і починати їх планування завчасно, одночасно з оперативним плануванням. Завчасне планування дає можливість синхронізувати зусилля особового складу частин (підрозділів) ІПсО з проведенням військової операції, щоб створити найбільш сприятливі умови для досягнення успіху.

Методологічна база підготовки та управління підрозділами ІПсО ВС США складається з таких джерел:

- Доктрина JP 3-13 «Інформаційні операції»;
- Доктрина спільних психологічних операцій JP 3-53;

- Польовий устав СВ США FM 3-05.301 «Тактика, прийоми, засоби та порядок проведення інформаційно-психологічних операцій»;
- Польовий устав СВ США FM 3-05.302 «Тактика, прийоми, засоби та порядок проведення інформаційно-психологічних операцій»;
- Кішеньковий довідник «Технічні засоби ІПсО: види, ТТХ та можливості»;
- Кішенькове «Керівництво командира із планування психологічних операцій».

Також, в якості нормативно-методичної документації використовуються програми бойової підготовки ARTEP, серед яких:

- ARTEP 33-712-MTP «Завдання бойового планування для штаба та штабної роти групи ІПсО і роти штабної та обслуговування батальону ІПсО»;
- ARTEP 33-715-MTP «Завдання бойового планування для батальона підготовки та поширення матеріалів ІПсО»;
- ARTEP 33-737-30-MTP «Завдання бойового планування для роти тактичних ІПсО»;
- ARTEP 33-727-MTP «Завдання бойового планування для регіональної роти психологічних операцій».

В роботі профільних підрозділів використовується також низка документів, що регламентують питання бойової підготовки особистого складу сил ІПсО, в тому числі: довідник офіцера ПСО STP 33-37II-OFS «Положення про основні стандарти офіцера ІПсО» та настанови з підготовки фахівців ІПсО рядового складу STP 33-37F14-SM-TG.

У контексті гібридних технологій ведення сучасних військових протистоянь особливе значення мають так звані **сили спеціальних операцій** (далі ССО) та специфіка їх комунікаційного, в тому числі за допомогою соціальних он-лайн мереж, забезпечення.

У країнах євроатлантичного блоку головним призначенням сил спеціальних операцій є протидія асиметричній агресії, боротьба з тероризмом, партизанським рухом та здійснення психологічного і територіально-адміністративного впливу на населення певних територій, на яких розгортаються важливі події.

За визначенням, сили спеціальних операцій – ***підрозділи спеціально навчених фахівців, які мають спеціальні можливості в сферах розвідки, прямих акцій і військової підтримки для виконання складних, небезпечних, інколи політично чутливих операцій, що проводить командування*** [92, с. 44].

Під **спеціальними операціями** розуміють різновид військової діяльності, яку здійснюють спеціально створені сили, організовані, треновані та оснащені для цієї мети, що використовують оперативну техніку й методи, відмінні від традиційних військових [348, с. 44].

На думку Ф.Моссера, характерними ознаками ССО є [348, с. 44]:

- прихованість дій;
- здатність виконувати операції, котрі приводять до тактичної або стратегічної переваги;
- спеціальна навченість та оснащеність;
- високий рівень спеціалізації;
- підвищений рівень адаптованості;
- мобільність й здатність проводити операції автономно;
- відносно невелика кількість особового складу;

- спроможність працювати в трьох середовищах (повітря, земля, море).

До типових завдань ССО відносяться [348, с. 45]:

- рейди та сучасні бойові дії;
- психологічні операції (Psy-Ops);
- робота «цивільної адміністрації» (залучення на свій бік населення);
- навчання іноземних армій, поліційних і безпекових сил (так зване «примноження сили»);
- пошук, евакуація й доставка полонених, заручників;
- медична допомога;
- здобуття розвідувальної інформації за лінією фронту;
- виявлення, ідентифікація та визначення цілей для власних засобів ураження;
- антитерористичні операції.

У своєму розпорядженні євроатлантичні ССО мають розгалужену інфраструктурну мережу «глобальної присутності» та «передового базування» - сухопутні оперативні бази, координаційні центри та морські склади-платформи [348, с. 50].

Безумовним лідером у питаннях створення та застосування ССО серед країн євроатлантичного блоку є США. Для координації власних підрозділів та ССО союзників при військовому відомстві США створено Командування спеціальних операцій (USSOCOM), основними завданнями якого є [348, с. 56]:

- координація діяльності ССО США;
- планування та проведення спеціальних операцій;
- організація бойової підготовки та підтримки в належному стані підрозділів ССО.

Мал. 5.2. Емблеми ССО США.

Крім провідних терористичних організацій, головним опонентом США та його союзників у питаннях застосування ССО сьогодні є Російська Федерація.

Створені в 2009 році російські ССО - це високо мобільне, спеціально навчене, технічно оснащене, добре екіпіроване армійське угрупування сил Міністерства оборони Російської Федерації, призначене для виконання спеціальних завдань (при необхідності - із застосуванням військової сили) як усередині країни, так і за кордоном з метою захисту інтересів Росії як у мирний, так і у воєнний час, що знаходиться в постійній і високої готовності до негайного застосування [380].

За структурою, функціями та практичним призначенням російські ССО мало чим відрізняються від євроатлантичних, хіба що вони не на стільки якісно забезпечені озброєнням та засобами комунікації.

Згідно з відповідними нормативно-правовими та профільними статутними положеннями, російські ССО здійснюють спеціальні операції як сукупність узгоджених за цілями, завданнями, місцем і часом спеціальних дій військ (сил), що проводяться за єдиним задумом і планом для досягнення певних цілей. Спеціальні дії таких військ - заходи, що проводяться спеціально призначеними, організованими, підготовленими і оснащеними силами, застосовувати не характерні для звичайних сил методи і способи бойових дій (розвідувально-

диверсійні, підривні, контртерористичні, контрдиверсійні, контррозвідувальні, партизанські, антипартизанські та інші дії) [380].

Мал. 5.3. Емблеми ССО Росії.

Широкому колу російські ССО знайомі під назвою «зелені чоловічки» з часів початку агресії проти України - захоплення Криму та міст на сході країни. Саме ці підрозділи стали основою для формування незаконних збройних формувань так званих «ДНР» і «ЛНР» у вигляді «ополчення» та різноманітних сепаратистських «бригад» та «батальйонів» [189].

В Україні в 2015 році було розпочато процес створення власних ССО за стандартами НАТО. Каталізатором цього рішення, зрозуміло, стала російська агресія та війна на сході країни.

Серед завдань українських ССО [224]:

- спеціальна розвідка;
- спеціальні заходи;
- контртерористичні заходи;
- прямі військові дії;
- аналіз і обробка інформації для вироблення правильної стратегії та залучення необхідних ресурсів;
- нетрадиційні методи ведення війни - психологічні та інформаційні операції.

Згідно з концепцією і законопроектом, підготовленими експертами Центру оборонної реформи, організаційно ССО будуть складатися з різних департаментів: інформаційно-психологічних операцій, інформаційно-аналітичної роботи, технічної підтримки і декількох бойових підрозділів. У складі ССО буде і управління нетрадиційних методів ведення війни, яке відповідатиме за створення руху опору, партизанських загонів, підпільних організацій. Також буде створено логістичний підрозділ і окремий навчальний центр [224].

Новостворене Командування ССО, за штатним розкладом, очолює керівник із військовим званням генерал-лейтенант. Перший заступник командувача — командувач високо мобільних десантних військ (у званні до генерал-майора), як можна побачити з назви посади керує частинами ВДВ у складі ССО ЗС України [150].

Відповідно до наявної інформації можна приблизно передбачити структуру Сил спеціальних операцій [150]:

- Командування ССО
- Командування ВДВ (у складі КССО)
- 140-й центр спеціального призначення
- 73-й морський центр спеціального призначення
- 3-й окремий полк спеціального призначення
- 8-й окремий полк спеціального призначення
- 25-а повітряно-десантна бригада
- 79-а окрема аеромобільна бригада
- 80-а окрема аеромобільна бригада
- 81-а окрема аеромобільна бригада
- 95-а окрема аеромобільна бригада

Мал. 5.4. Українські підрозділи зі складу ССО

Як варіант, 3-й та 8-й полки спеціального призначення можуть бути розгорнуті в бригади. Можливе входження до складу ССО 801-го окремого загону боротьби з підводними диверсійними силами та засобами.

Аналізуючи типові функції окремих підрозділів та командування ССО, стає зрозумілим, що в їх діяльності одним з провідних компонентів є робота із соціальними он-лайн мережами, які є фактично специфічним полем бою та джерелом для збирання розвідувальної інформації.

Відповідно до технічних та комунікаційних можливостей віртуальних соціальних мереж ССО можуть використовувати їх для:

- здійснення впливу на населення в місці проведення спецоперацій (чутки, офіційні звернення, попередження);
- дезінформації противника щодо дій власних підрозділів, їхнього складу та завдань;
- збирання розвідувальної інформації про дії супротивника, його сили та керівний склад;
- координації дій власних груп та співпрацю з місцевими групами, що надають їм допомогу;
- створення та координація дій агентурних мереж на території супротивника.

Отже, весь наявний потенціал і комунікаційні можливості соціальних он-лайн мереж можуть стати важливим інструментом у діяльності ССО. Відповідно в структурі окремих підрозділів та керівних органів ССО мають бути фахівці і навіть групи, які забезпечуватимуть відповідні функції.

Особливої ваги це набуває в контексті наукового прогресу та вдосконалення технічних засобів комунікації, які дозволятимуть мати доступ до мережі Інтернет за умови значного віддалення від стаціонарних місць доступу та зберігання такої можливості протягом тривалого часу.

5.2 Інтернет-технології та соціальні он-лайн мережі в структурі гібридної війни

Як вже зазначалося вище, головним завданням мережевих он-лайн проектів у рамках гібридної війни є створення певної віртуальної реальності (симулякри), що формує необхідне для атакуючої сторони бачення ситуації конкретними цільовими групами, які є об'єктами інформаційно-психологічної агресії. При цьому, головною метою такої діяльності є забезпечення сприятливих умов для реалізації атакуючих дій в режимі оф-лайн, на економічному, військовому, політичному полях, або одночасно в усіх площинах.

Вирішення зазначених питань можливе лише за умови інтегрованого підходу – поєднання сучасних технічних комунікацій та психотехнологій. При цьому, тривалість дії та глибина ударного ефекту залежать від часу, впродовж якого здійснюється обробка свідомості цільових груп та потужності тиску. Роль і значення в цих процесах соціальних он-лайн мереж важко переоцінити.

За аналогією, технології web 2.0, в цьому контексті можна визначити як високоточну зброю, що може поцілити не просто в певні цільові групи, але й в конкретних її представників, чітко визначених персоналій. Така адресність та,

за необхідністю, вибірковість дає можливість досягати максимального ефекту із оптимізацією витрат у плані часу, інтелектуальних та матеріально-технічних ресурсів.

Аналізуючи результати найбільш відомих міжнародних військових, політичних та економічних конфліктів кінця XX – початку XXI ст., стає зрозумілим, що інформаційно-психологічна зброя сьогодні має бути прирівняна до зброї масового знищення. Не вбиваючи фізично, психотехнології стають причиною групових, а також масових психічних розладів, що призводять до соціальних конфліктів, в яких позбавляються життя конкретні індивідууми.

У форматі використання всього спектра інформаційно-психологічних операцій соціальні он-лайн мережі мають можливість забезпечувати:

- координацію протесту та терористичних рухів;
- поширення контенту, що відноситься до категорії інформаційної зброї;
- збирання важливої інформації про персон або організації, що представляють інтерес для атакуючої сторони;
- збирання розвідувальної інформації про оф-лайн дії противника;
- відстеження суспільних настроїв;
- локалізація джерел інформації, що представляють небезпеку.

Однією з головних функцій соціальних он-лайн мереж є можливість координації інформаційних потоків, що розгортаються навколо реальних військових дій.

У сучасних умовах як гібридних, так і лінійних військових конфліктів важливе значення має система доступу до інформації, що надходить із зони бойових дій. А головним завданням будь-якої профільної військової структури є обмеження доступу до джерел інформації сторонніх осіб і поширення інформації у вигідному для себе контексті.

У контексті реалізації зазначеного вище завдання, роботу із соціальними мережами необхідно вибудовувати, базуючись на принципах встановлення контролю трьох інформаційних потоків, які мають місце навколо будь-якого об’єкта, в якості якого в даному випадку виступатиме зона бойових дій.

Для чіткого розуміння процедури здійснення контролю за рухом інформації, необхідно скласти карту інформаційного поля, на якій змоделювати спрямування та складові частини трьох базових інформаційних потоків: ***вхідного***, ***вихідного*** та ***внутрішнього*** [217, с. 42].

Кожен з визначених інформаційних потоків формують певні джерела інформації або інформаційні носії, які мають певний контент та механізм його накопичення, зберігання та поширення і в цілому формують загальні обриси та структуру профільного інформаційного процесу. Серед тих, що відносяться до он-лайн мережевих соціальних структур можна виділити такі, як:

- мережеві групи та сторінки центральних органів державної влади;
- мережеві групи та сторінки органів місцевої влади;
- мережеві групи та сторінки координаційних центрів громадських структур (волонтери, ГО, БФ та ін.);
- мережеві групи та сторінки окремих силових підрозділів;
- мережеві групи та сторінки координаційних центрів силових структур (штаби, логістичні центри, центри надання допомоги);
- мережеві групи та сторінки місцевих ЗМІ;
- мережеві групи та сторінки територіальних громад.

Для цих інформаційних потоків визначаються певні цільові групи. Зокрема для вхідного та внутрішнього інформаційних потоків такими цільовими групами будуть:

- цивільне населення в зоні конфлікту;
- керівництво місцевих органів влади;
- силовики (військові та поліцейські структури);

- волонтерські структури (благодійні або громадські організації);
- представники ЗМІ (власні та іноземні);
- офіційні спостерігачі (військові та цивільні місії).

Для контенту, що рухається за вихідним інформаційним потоком, цільовими групами будуть:

- цивільне населення, що мешкає поза зоною конфлікту;
- керівництво центральних органів влади;
- національні та іноземні медіа;
- представники національних та міжнародних громадських організацій;
- керівництво та представники іноземних державних установ.

Карта інформаційного поля в кожній конкретній ситуації формується індивідуально, на основі визначених вище елементів, із врахуванням місцевих особливостей та специфіки.

Для перетворення такої моделі в реально діючий механізм також необхідно визначити принципи та правила контролю і фільтрації інформаційних потоків. Під час роботи із соціальними мережами це завдання є доволі складним, бо потенційним джерелом інформації може виступити фактично кожна людина, яка має доступ до мережі Інтернет і володіє певним цінним контентом.

У такому разі необхідно налагодити систему регулярного моніторингу всього локального мережевого інформаційного простору в ручному (переглядання змісту профільних сторінок та груп) або за допомогою відповідних програмних сервісів.

Крайньою мірою контролю за мережевою складовою зони конфлікту може бути блокування доступу до певних інтернет-ресурсів та мереж, утім, як свідчить практика, в наші часи це майже не реально. Тому, найкращий засіб контролю за інформаційним процесом – координування інформаційних потоків

та формування правильних меседжів із відповідним контентним супроводженням.

Також ефективним засобом посилення власних можливостей щодо координації інформаційних потоків може стати залучення до активної співпраці волонтерів.

Волонтерський рух в он-лайн мережевому середовищі, в якості інструмента протидії інформаційної агресії або для здійснення аналогічних атак на інформаційне поле супротивника, став одним із засобів протидії російської агресії проти України. В принципі світова практика інформаційних війн знає багато таких прикладів.

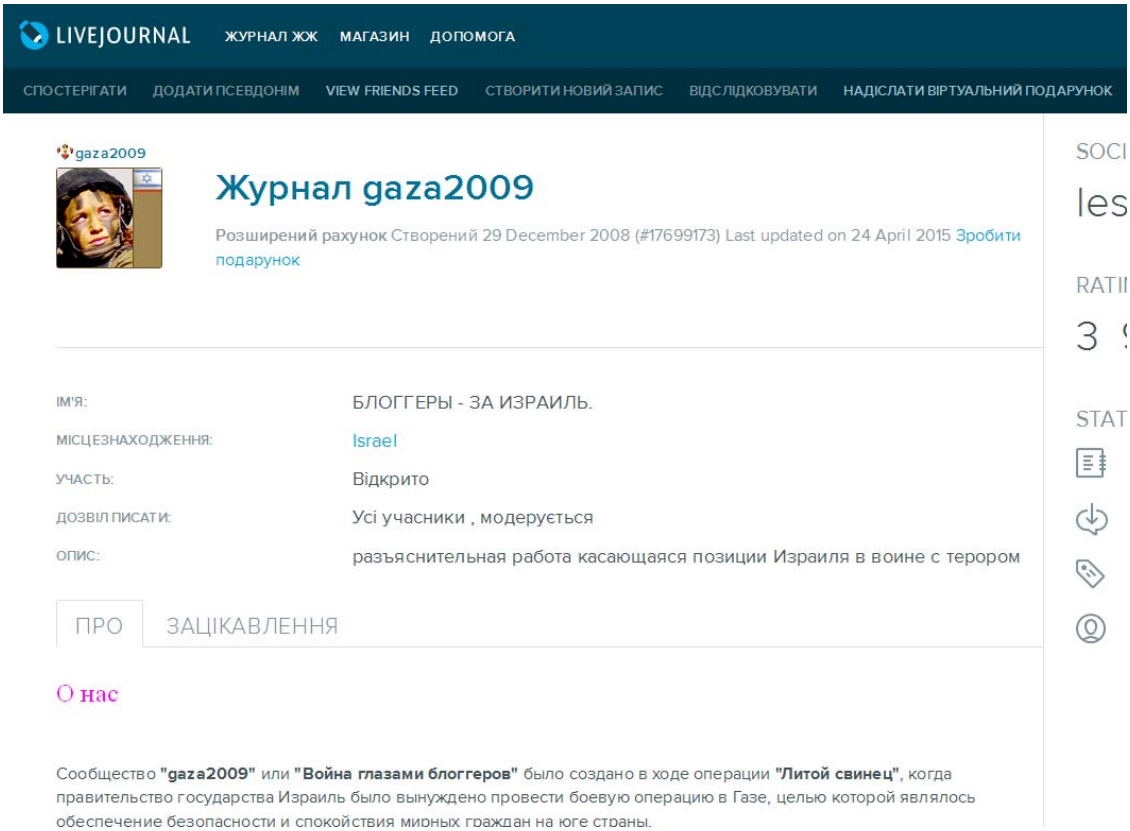
Практичний приклад

За прикладом використання соціальних мережевих он-лайн структур для забезпечення військового протистояння із залученням волонтерського компоненту, можна звернутися до досвіду інформаційного супроводження військової операції «Литий свинець», що здійснювалася Ізраїлем в секторі Газа в 2009 р.

Ця віртуальна інформаційно-психологічна операція стала однією з найперших та найуспішніших у своєму роді.

Унаслідок програного інформаційного протистояння під час Другої Ліванської війни (2006 р.) ізраїльське керівництво вирішило посилити інформаційний сегмент в структурі ЦАХАЛ та його щільну співпрацю із громадськістю. До співпраці, окрім офіційних ЗМІ, було залучено волонтерів, головним завданням яких було відстежувати інформацію, що з'являлася у соціальних мережах, та поширювати контент, який дає об'єктивну інформацію про перебіг подій і показує діяльність ізраїльських військових у вигідному для них контексті. Також волонтерські групи та окремі блогери орієнтувалися на виявлення та нейтралізацію джерел (інтернет-майданчиків) противника.

Реальні бойові дії розпочалися 27 грудня 2008 р. і вже з перших днів січня 2009 р. провідні блогери-волонтери відкрили у найбільш популярній на той час соціальній мережі LiveJornal.com групу «gaza2009». Модераторами цієї групи Стали Марк Бибичков (радник міністра оборони Ізраїля) та Давід Ейдельман (прес-секретар політичної партії «Кадима»).



Зазначена група стала майданчиком, навколо якого відбулася консолідація громадськості, а також джерелом інформації для світових медіа. Модераторам вдалося досягнути рівня відвідуваності до 30 тис. на день, що на ті часи та для цієї соціальної мережі було безумовним рекордом.

Крім того, зазначена група виконувала функції віртуального штабу. У разі виявлення джерел ворожої пропаганди модератори збирали усіх волонтерів та давали адресу місця, де відбувається ворожа інформаційна атака. Також фоловери групи виявляли та розвінчували фейки, поширюючи викривальну інформацію. Через певний час аналогічні групи було створено у мережах Facebook, Odnoklassniki, VKontakte.

Станом на січень 2010 р. ця діяльність перетворилась на глобальний рух, який допоміг ізраїльським військовим в плані комплексного інформаційного супроводу.

Серед аналогічних українських волонтерських проектів, які діють в якості допоміжних віртуальних ресурсів у інформаційно-психологічній війні з російськими агресорами та сепаратистськими рухами можна визначити такі як: «Inform Napalm» та «Информационное сопротивление», центр «Миротворець».

Практично всі згадані вище проекти діють за схемою роботи так званої **OSINT (Open source intelligence)** – ***розвідувальної практики, яка передбачає пошук, вибір та збирання інформації, отриманої із відкритих джерел.*** Важливою складовою частиною такої роботи є системний аналіз наявної інформації із відповідною оцінкою та висновками, що дозволяють зрозуміти логіку та передбачити дії противника.

Одним з базових золотих правил такої практики є те, що близько 90% необхідної для аналізу та прийняття відповідних рішень інформації знаходиться у відкритих джерелах. До таких джерел можна віднести:

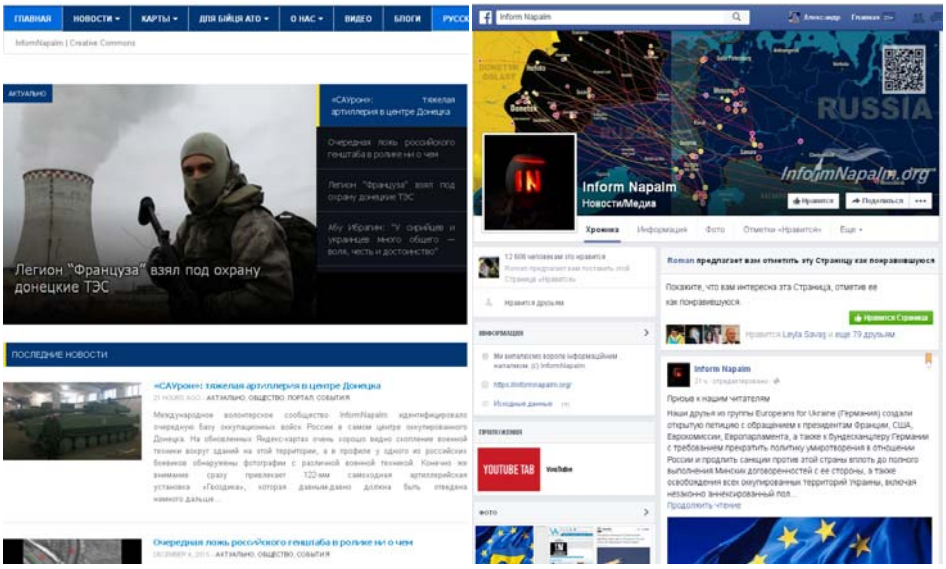
- традиційні ЗМІ (газети, журнали, радіо, телебачення);
- інтернет-видання, що відносяться до ЗМІ (сайти новин та портали, інтернет-ресурси профільних структур);
- акаунти та віртуальні майданчики в соціальних он-лайн мережах;
- офіційні звіти державних структур;
- публічні заяви політиків та державних службовців;
- спостереження — радіомоніторинг, використання загальнодоступних даних, аерофотозйомок (наприклад, Google Earth);
- професійні та академічні звіти, конференції, доповіді, статті;
- звіти та виступи в ЗМІ окремих незалежних експертів та експертних груп.

У провідних країнах світу система OSINT є важливим інструментом захисту національних інтересів та провідною складовою в діяльності профільних силових відомств. Зокрема в США та країнах НАТО існують окремі мережі центрів, що займаються збиранням та обробкою відповідної інформації із подальшим формуванням відповідних баз даних та практичним їх застосуванням для прийняття відповідних рішень.

«Inform Napalm» (https://informnapalm.org) – *громадський проект з інформаційного висвітлення подій, що стосуються неоголошеної війни Росії проти України, окупації Криму і терористичної діяльності російських спецслужб, а також фанатично налаштованих бойовиків "ДНР", "ЛНР", "Новоросії". На волонтерських засадах в команду "InformNapalm" увійшли колишні військові, журналісти, аналітики, перекладачі та активісти. У мирному житті кожен з нас представляє самі різні професії, але з приходом війни в Україну вони всі стали солдатами інформаційного фронту.*

На теперішній час серед волонтерів проекту є ті, хто знаходиться в зоні АТО в якості військовослужбовців. Також до співпраці залучаються місцеві мешканці територій, які знаходяться під окупацією.

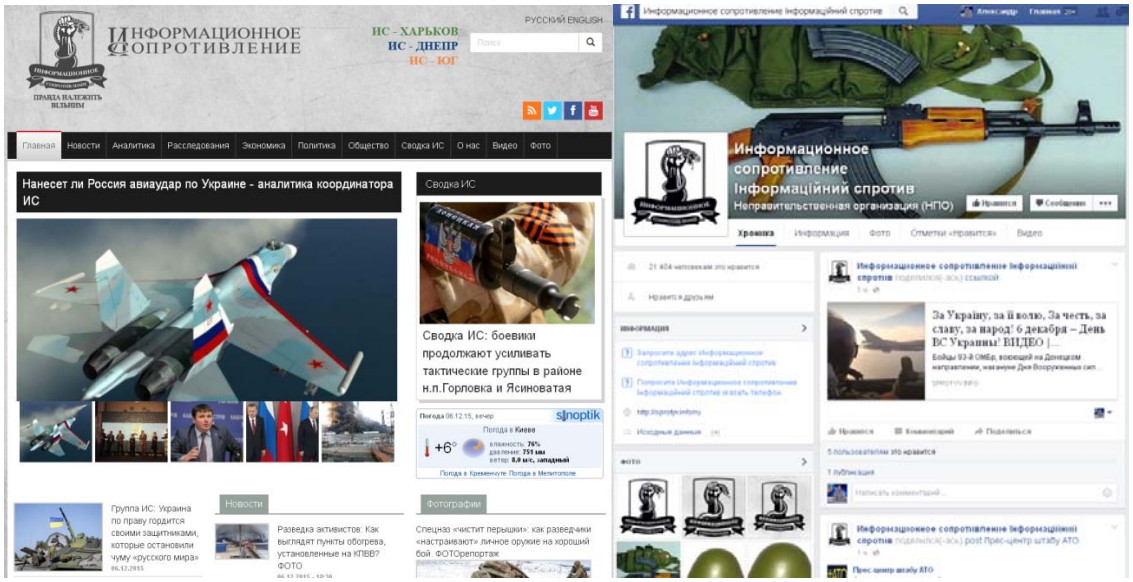
Серед матеріалів, які активісти проекту публікують, є фото та відео матеріали, офіційні документи, свідчення очевидців, що підтверджують російську агресію та розкривають військові злочини бойовиків ДНР-ЛНР.

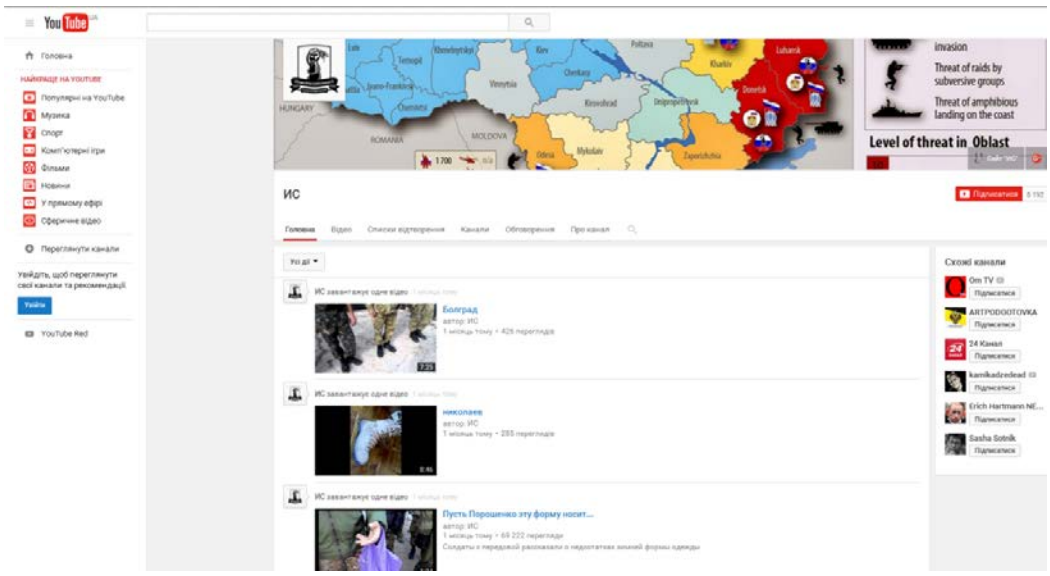


«Информационное сопротивление» *(http://sprotyv.info) - неурядовий проект, головним завданням якого є протидія в інформаційному полі зовнішнім загрозам, що виникають для України в основних сферах: військовій, економічній та енергетичній, а також у сфері інформаційної безпеки.*

Проект функціонує як ініціатива неурядової організації «Центр військово-політичних досліджень» (м.Київ). Початок роботи проекту з 2 березня 2014 (з вторгнення Росії до Криму).

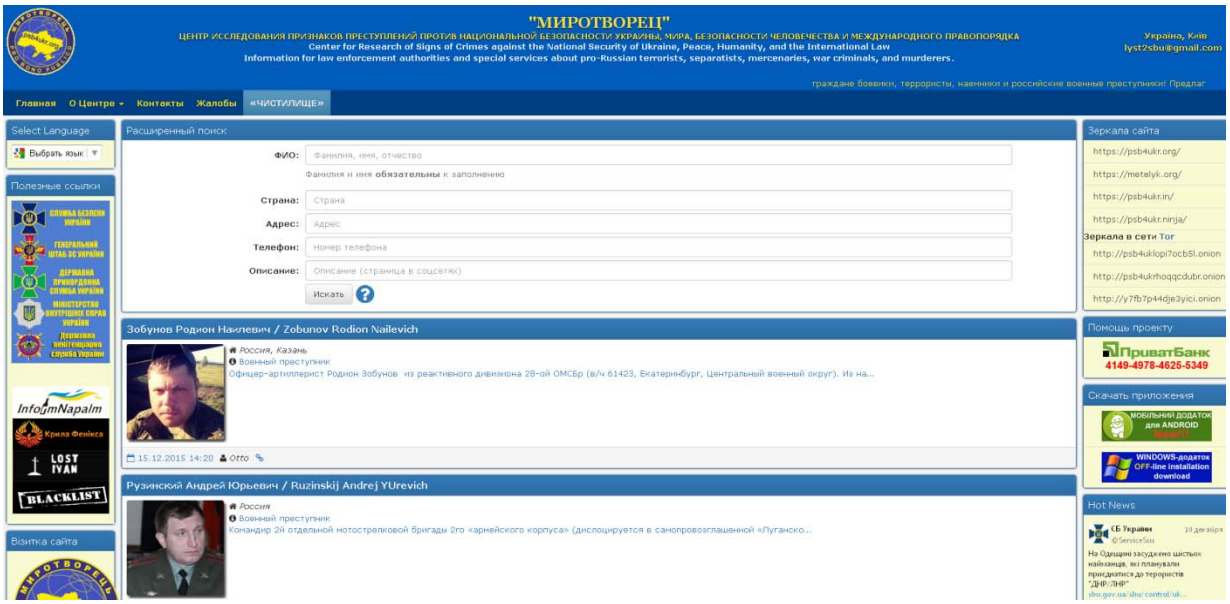
Матеріали, що публікують на сайті та мережевих сторінках проекту, це візуальні (фото та відео) матеріали, офіційні документи, свідчення та коментарі очевидців, які надають докази російської агресії та злочинів керівництва ДНР-ЛНР.





Також одним з найважливіших та найпопулярніших ресурсів є портал ***«Миротворець»*** *(https://psb4ukr.org/), створений групою вчених і фахівців з питань дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку, що займаються творчою науковою та журналістською діяльністю.*

Волонтерами центру здійснюється фіксація і зберігання інформації щодо об'єктів дослідження, в діях яких присутні ознаки злочинів проти національної безпеки України, життя і здоров'я людини, миру, безпеки людства та міжнародного правопорядку.



Основними джерелами інформації, використовуваними Центром «Миротворець» для проведених наукових досліджень, є відкриті для загального доступу матеріали, які друкуються і розміщуються: в соціальних мережах, в web-виданнях, на приватних web-сторінках, в спеціалізованих форумах і блогах, транслюються по каналах телебачення і радіомовлення.

Зазначені вище вітчизняні мережеві проекти, демонструють яскравий приклад того, як за допомогою належним чином розбудованої інформаційної мережі та системи роботи можна ефективно забезпечувати та результативно супроводжувати оф-лайн процеси.

Таким чином, стає зрозумілим весь спектр наявних на теперішній момент інструментів ведення інформаційної війни, головний принцип яких гнучкість, оперативність та масштабність процесів, системність роботи. І лише від тих, хто приймає відповідні управлінські рішення, залежить наскільки якісно ці інструменти можуть спрацьовувати.

5.3. Мережеві он-лайн проекти в гібридній війні: структура та принципи функціонування

5.3.1. Формат та специфіка он-лайн мережевих проектів

Одним з базових напрямків роботи в рамках інформаційної війни в соціальних он-лайн мережах є **тематичні проекти**. Останні мають монотематичне спрямування, гнучку схему управління та принципи і схеми розбудови комунікацій із відповідними, чітко визначеними цільовими групами.

За теоретичним визначенням «проект» - ***це сукупність дій та завдань, що внаслідок їх унікальності й неповторності*** має такі відмінні ознаки, як [184, с. 8]:

- чіткі цілі, що досягаються одночасним виконанням певних технічних, технологічних та інших вимог;
- внутрішні та зовнішні взаємозв'язки завдань, робіт, операцій і ресурсів, що потребують чіткої координації в процесі реалізації проекту;
- визначені терміни початку й завершення проекту та обмеженість ресурсів;
- визначений ступінь унікальності проекту та умов його здійснення.

За складністю визначаються [184, с. 10]:

- монопроекти – окремі конкретні проекти чітко визначеної орієнтації та масштабу; припускають певні спрощення щодо проектування та реалізації, формування команди проекту тощо;
- мультипроекти – комплексні проекти, які складаються з монопроектів;
- мегапроекти – комплексні проекти, які охоплюють окремі регіони, сектори суспільства, економіки; складаються з моно- і мультипроектів, об'єднаних однією метою.

У контексті функціонування мережевого он-лайн простору, в якості засобу ведення інформаційної війни, може використовуватися будь-який формат і тематика проектів. Головна вимога до таких проектів – наявність прямого доступу до конкретних цільових груп, а також можливість здійснення прямого або опосередкованого впливу та безперешкодного функціонування.

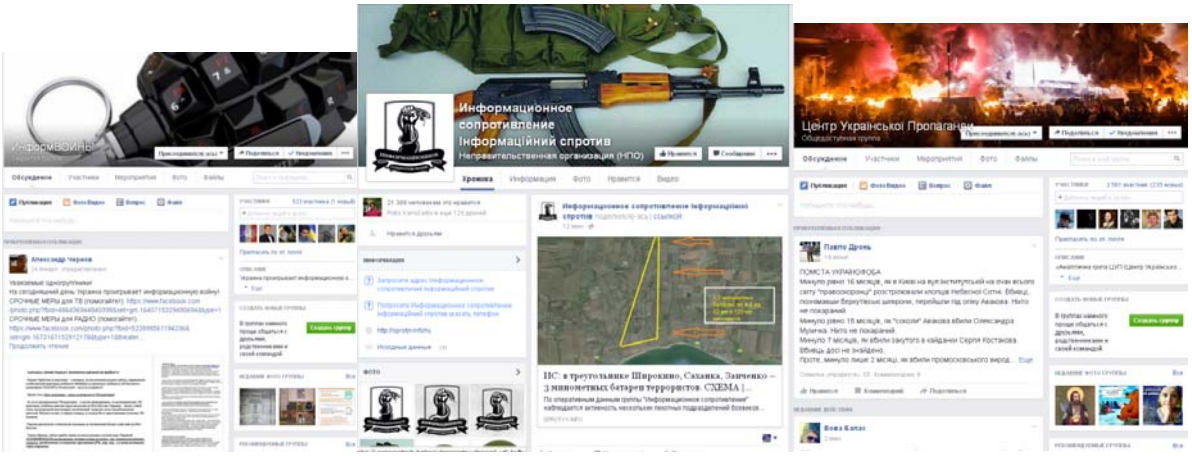
Формат мережевих проектів може бути у вигляді блогів (авторські або тематичні), груп (авторські, тематичні, регіональні, корпоративні), сторінок

(авторські, тематичні, регіональні, корпоративні), подій (разові івенти). При цьому їх спрямованість може мати прямий (відкритий) або опосередкований (прихований) характер.

Мережеві он-лайн проекти відкритого формату орієнтовані на цільові групи, що підходять під категорії своїх та нейтральних. З такими цільовими групами можна працювати, не приховуючи власних намірів. Умовно, за характером контенту, їх можна поділити на: **захисні**, **нейтральні** та **атакуючі**.

Проекти, що містять інформацію, спрямовану проти конкретного супротивника, у вигляді прямих звинувачень, викриття, попередження, пошуку винних, відносяться до категорії з умовною назвою «захищаючі». Незважаючи на їх агресивний характер, вони використовуються переважно з метою оберігання - створення тимчасового або постійного ментального бар'єру в свідомості «своїх» цільових груп (мал. 5.5.). Також за допомогою таких проектів можна частково здійснювати вплив на представників цільових груп, що не визначилися, або нейтральні по відношенню до певного системного конфлікту (міждержавний внутрішньодержавний), чи певної конфліктної ситуації.

Мал. 5.5. «Захисні» мережеві проекти



Мета захисних проектів – підготовка цільових груп до можливих негативних ситуацій, викликання певних емоційних станів (позитивні або

негативні), внесення легких психологічних установок на свідомому та підсвідомому розумовому рівні.

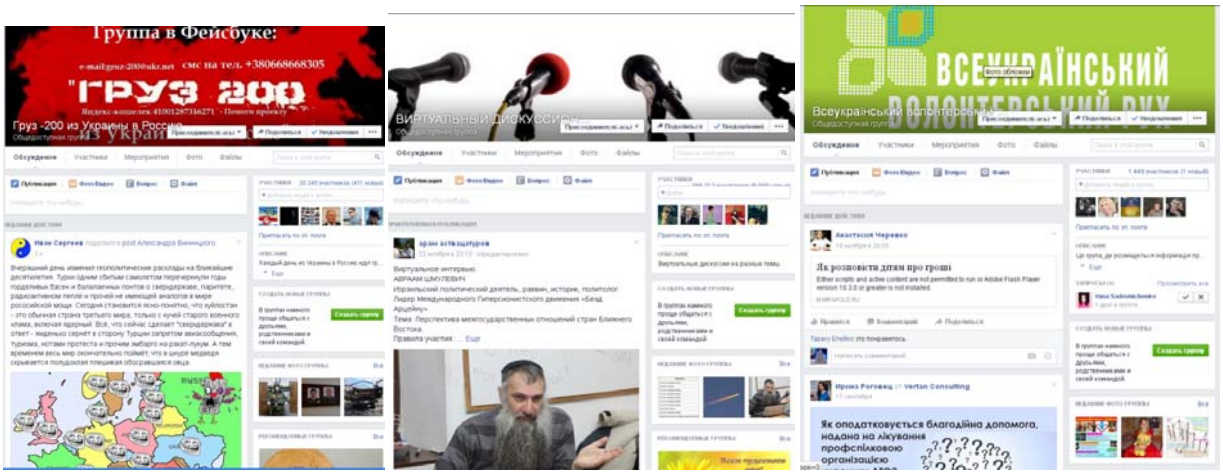
Зазначені проекти використовуються в рамках реалізації таких стратегій, як консолідація та заспокоєння. В тактичному плані це робота переважно на власних майданчиках.

Мережеві проекти, що містять інформацію про зміст та перебіг основних моментів конфліктів, без чітко визначених установок із зміщеними чи прихованими акцентами, маючи менш агресивний або взагалі нейтральний вигляд, насправді мають доволі потужний атакуючий потенціал.

Мета таких проектів – привертання уваги до конфлікту, викликання певних емоційних станів (позитивні або негативні), внесення певних легких психологічних установок на свідомому розумовому рівні.

Такі проекти використовуються в рамках реалізації різних варіантів стратегій – консолідація, заспокоєння, залякування, невдоволення, протест. У тактичному плані передбачається робота на власних майданчиках та використання чужих для промоції власних проектів (мал. 5.6).

Мал. 5.6. «Нейтральні» мережеві проекти



Мета атакуючих проектів – поширення інформації з прихованими інформаційними меседжами, викликання переважно негативних емоційних станів (агресивність або депресія), внесення ґрунтових та легких психологічних установок на підсвідомому рівні (мал. 5.7).

Такі проекти допомагають у реалізації стратегій, спрямованих на залякування, викликання невдоволення, дії протесту. В тактичному плані це може бути робота на власному майданчику, як опорному з акцентом на посіви на чужі майданчики.

Мал.5.7. «Атакуючі» мережеві проекти

5.3.2. Методи та засоби управління проектами

Слід зазначити, що специфіка та особливості інтернет-технології web 2.0 та 3.0 дають можливість певним чином корегувати систему управління проектами. Кожен такий проект створює власну, локальну мережу фоловерів, яка керується за відповідною схемою, що продиктована метою, завданнями та особливостями комунікаційної ситуації.

Найбільш зручною типологією для визначення таких систем є класифікація типів соціальних оф-лайн мереж, яка існує в системі розбудови оф-лайн соціальних мереж, а саме в Networking.

Відповідно до характеру або особливостей створення мережі в Networking визначається чотири базових типи: **променева**, **павуччя**, **3D** та **мисливська** [217, с.141-142].

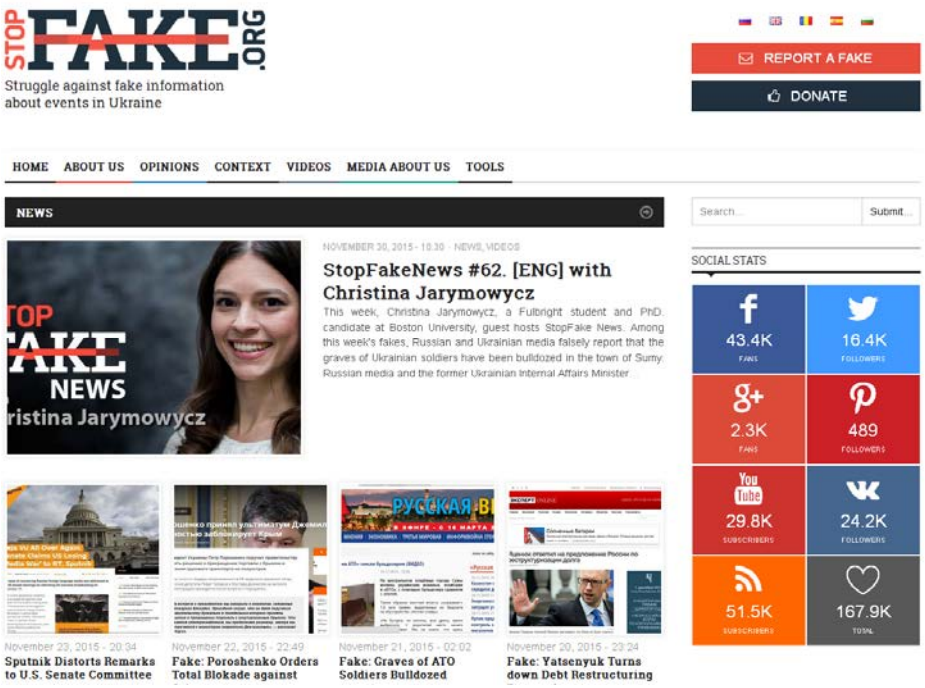
Променева мережа – структура, яка має центральну одиницю (особа або організація), об'єднує інших членів мережі, що не мають між собою контактів. Центральна одиниця є точкою, через яку здійснюються всі контакти. Така модель активно використовується в MLM і є типовою мережею із розповсюдження товарів та послуг (Oriflaime, Mary Kay, Amway та ін.).

Практичний приклад

В якості наочного прикладу проекту, створеного на базових принципах променевої мережі, для ведення інформаційної війни можна навести інтернет-проект «StopFAKE».

Цей проект створено з метою виявлення та викриття неправдивої інформації, яку поширюють російські ЗМІ та структури, що практикують мережевий тролінг. В основі системи управління проектом принцип радіального розповсюдження інформації з єдиного центру, яким є портал www.stopfake.org.

Базовий майданчик доповнюють групи в провідних соціальних мережах: Facebook (43,4 тис. фоловерів), VKontakte (24,2 тис. фоловерів), Twitter (16,4 тис. фоловерів), Google+ (2,3 тис. фоловерів), RSS. Останні використовують виключно з метою поширення інформації та посилення надійного ефекту від повідомлень.

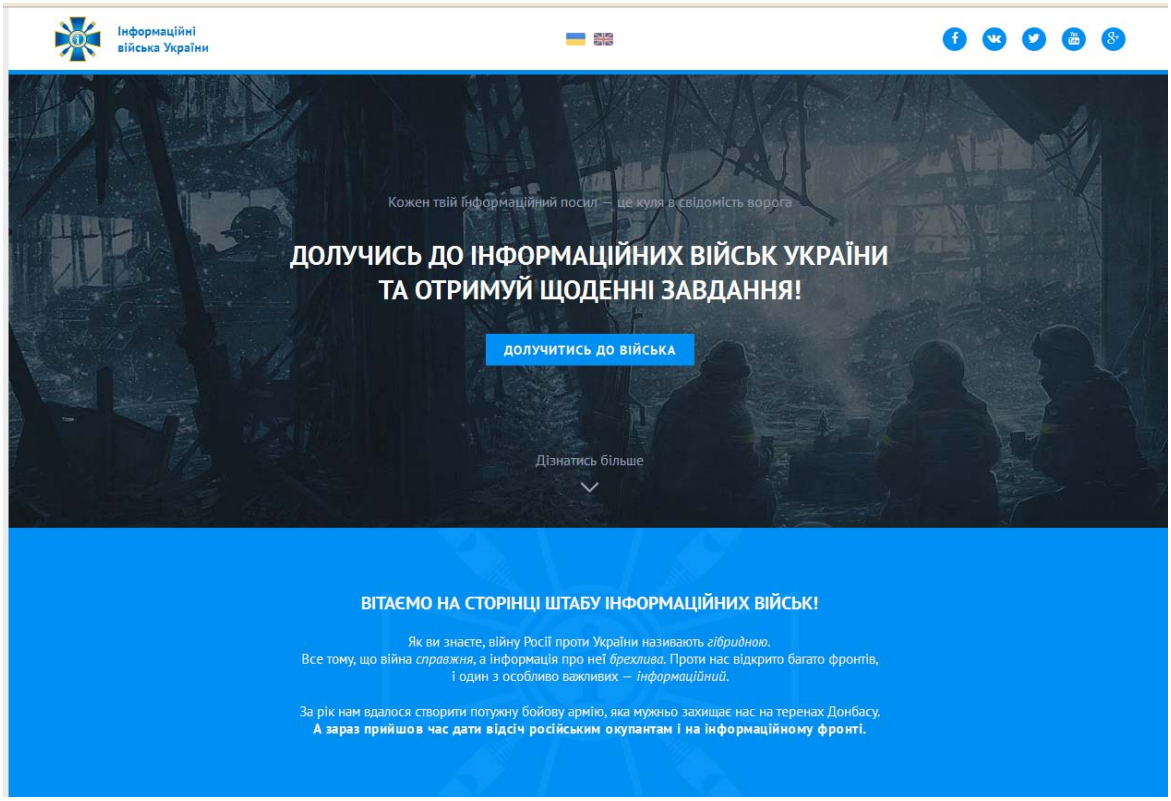


Павуччя мережа – структура спільноти, що передбачає можливість контактів між усіма членами мережі, в разі збереження координуючої функції її засновника – центральної одиниці. За такої моделі діють мережеві рекламні та консалтингові агенції, структури, що працюють за франшизою та ін. У рамках інформаційної війни така технологія управління є найбільш характерна для відкритих мережевих товариств – переважно мережевих тематичних груп, які ґрунтуються навколо одного сайту. В такому разі сайт виконує функції координуючого центру, а безпосередньо контакти та спілкування відбуваються в мережевих групах.

Практичний приклад

В якості практичного прикладу проекту, в основі якого закладено зазначений принцип, можна навести «Інформаційні війська України».

Зазначений проект, створений в лютому 2015 р. Міністерством інформаційної політики України, в якості інструмента здійснення відповіді на російську інформаційну агресію.

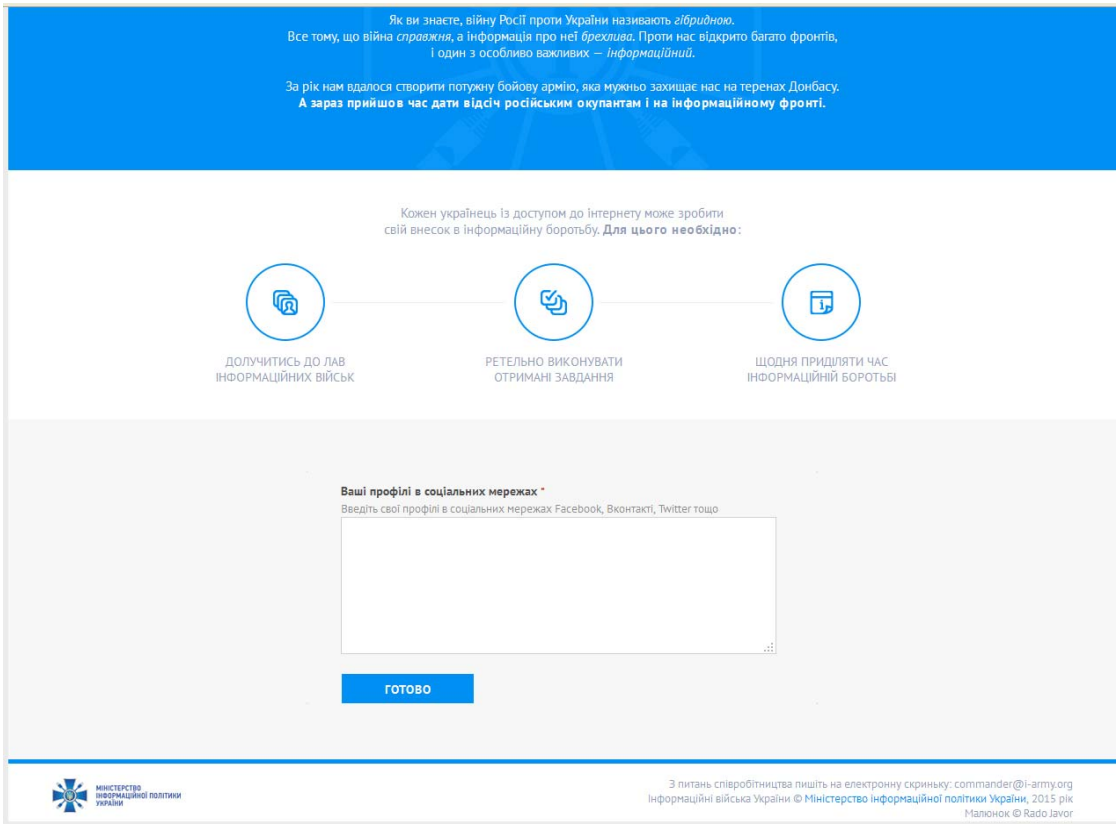


http://3.i-army.org/

Принцип та система управління проектом передбачає координацію кіберволонтерів із поширення певної інформації та збирання контенту, який може знаходитися в сфері інтересів проекту.

На перших етапах існування даного проекту він в цілому відповідав принципам променевої мережі. З часом, у процесі трансформації, він набув рис саме павучої мережі, створивши тим самим систему більш гнучкою та відкритою для ефективних комунікацій.

Для того, щоб долучитися до проекту, необхідно пройти процедуру реєстрації, яка передбачає заповнення блоку питань – адреса електронної пошти, персональні профілі. На основі цієї інформації претендента включають у поштову розсилку новин та приєднують до груп «Інформаційних військ» у тих соціальних мережах, де претендент має персональні акаунти.



http://3.i-army.org/

Серед інформації, яка поширюється в рамках проекту, є репости цікавих матеріалів та власний контент (тексти, інфографіка, відео, меми). Відповідні матеріали доповнюються коментарями від модераторів проекту, які містять певні меседжі та психологічні установки.

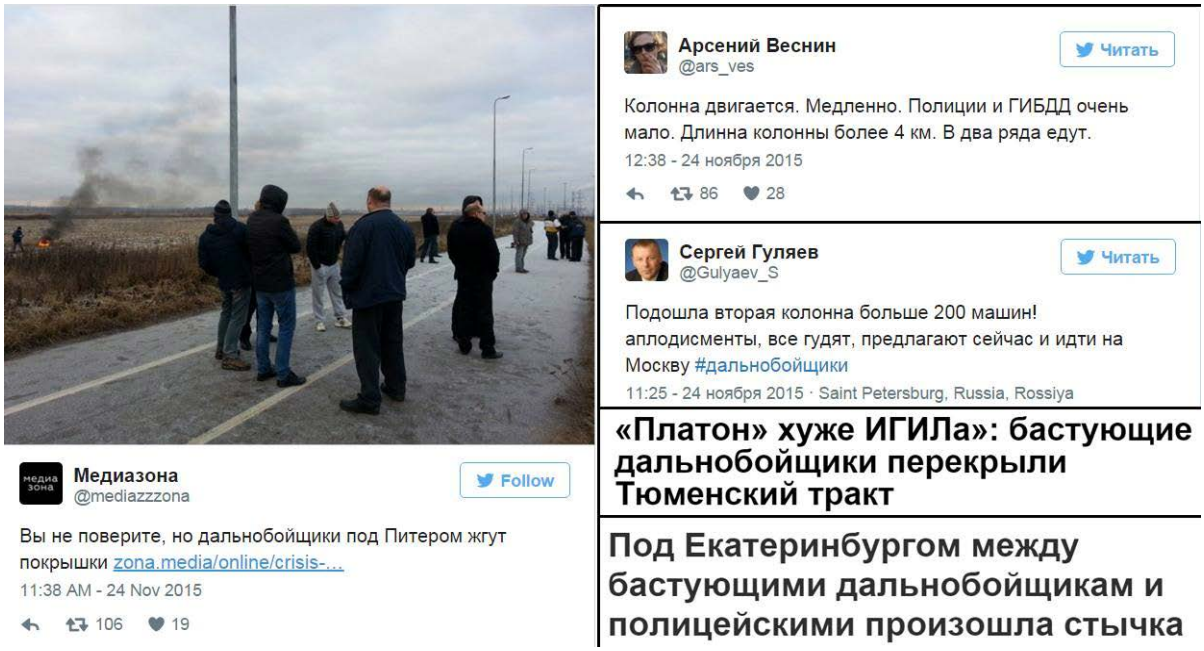
До контенту власного виробництва проекту можна віднести порівняльний моніторинг – подання різних поглядів на певні події з позиції, російських ЗМІ, європейських та українських.

Також активно поширюються матеріали із розвінчання російських фейків, на конкретних прикладах, з посиланнями й відповідною доказовою базою. В якості базового прийому, в такому разі, застосовується порівняння між автентичними матеріалами та підробленими.

Крім того, використовуються твіти або цитати лідерів громадської думки з приводу різноманітних подій для конкретизації певної позиції або тези, яку промотіюють модератори проекту.

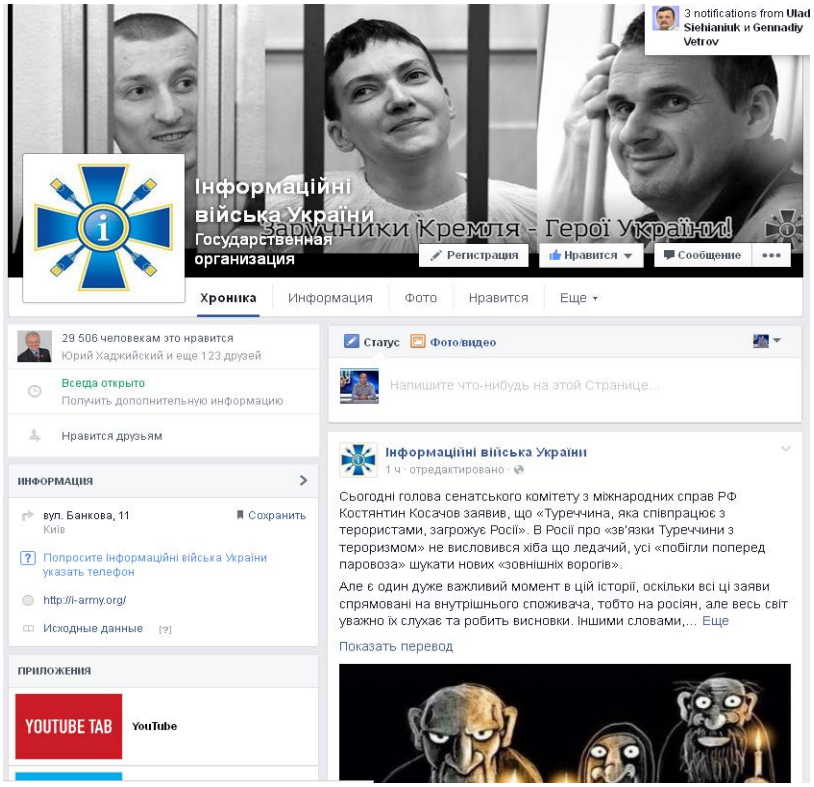
На початку існування проект мав значну підтримку серед представників патріотично налаштованого мережевого суспільства, втім останнім часом він втрачає популярність як через відсутність сенсаційних інформаційних приводів, так і через пасивність адміністраторів та модераторів проекту.

Вочевидь падіння популярності ресурсу є наслідком директивного та певною мірою примусового характеру комунікаційної схеми, яку пропонують адміністратори проекту. За умовами співпраці, кожен фоловер має поширювати контент, що продукується в рамках проекту. А також від учасників вимагається здійснювати моніторингові дії щодо інформаційного простору, до якого вони мають відношення.



У процесі роботи учасники проекту отримують інформацію на пошту та на інформаційні стрічки у соціальних мережах. Ця інформація має бути поширена в групах, в яких зареєстрований учасник та на особистому акаунті.

У рамках проекту функціонують групи та тематичні сторінки у таких соціальних мережах, як: Facebook, VKontakte, Twitter, Google+, YouTube.

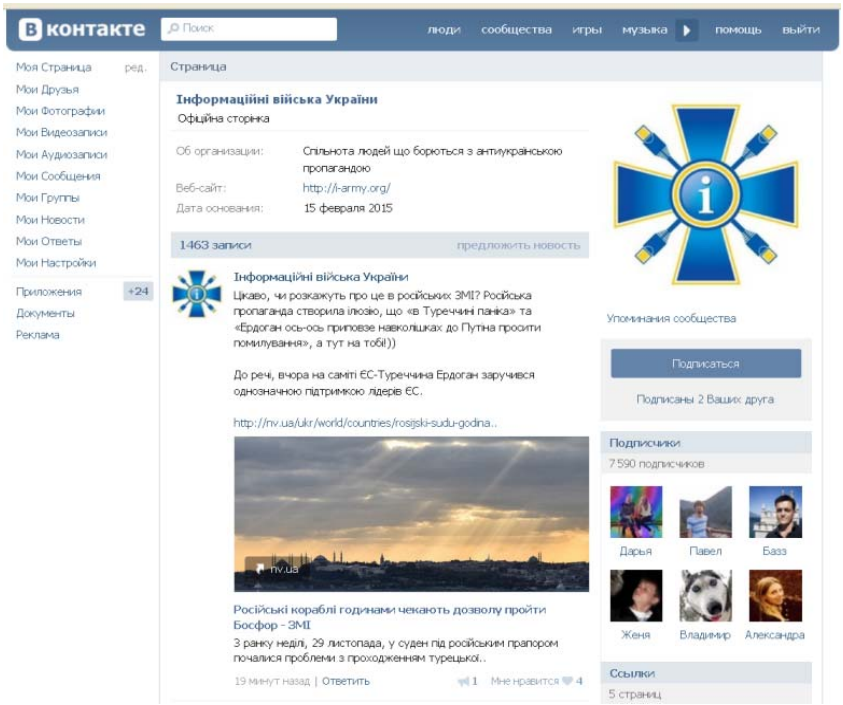


Сторінка проекту у Facebook налічує зараз майже 30 тис. фоловерів. На сторінці фоловери можуть ставити лайки, коментувати, робити репост матеріалів. Також передбачена функція залишення повідомлень для інших фоловерів та модераторів сторінки.

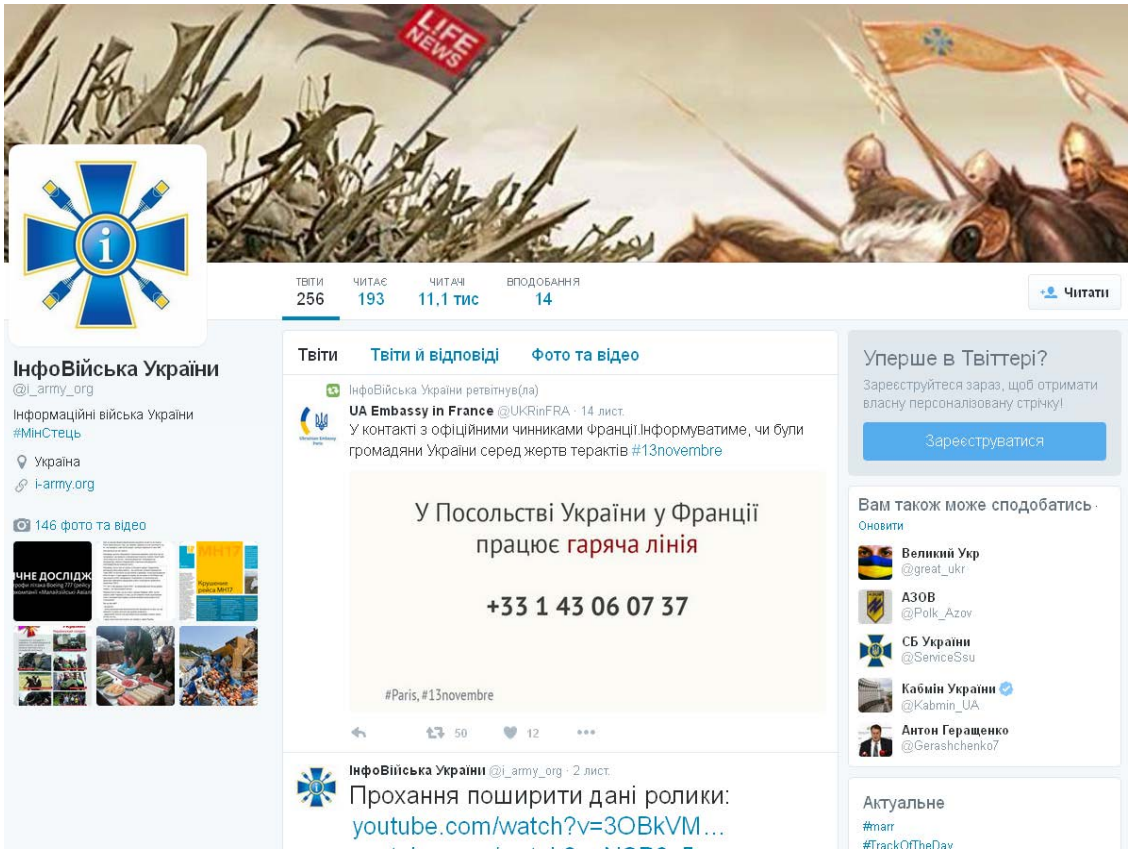
Пости на сторінці набирають у середньому від 10 до 100 лайків, найбільш популярні матеріали можуть отримувати до 500 лайків. Кількість репостів коливається в середньому 20-30, найбільш рейтингові матеріали можуть давати кілька сот репостів. Коментарів під цікавими публікаціями може нараховуватися 2-5. Популярні матеріали можуть зібрати кілька десятків коментарів. Останнім часом спостерігається падіння популярності групи проекту у Fecbook так само, як і проекту в цілому.

У соціальній мережі VKontakte нараховується близько 8 тис фоловерів, а сам майданчик має статус офіційної сторінки або закритої тематичної групи з можливістю пропонувати власні новини на розгляд модераторів.

Активність відвідувачів та фоловерів групи дає в середньому 5-15 лайків, 5-10 репостів та кілька коментарів під цікавими матеріалами. Резонансні матеріали можуть мати до 60-70 лайків, відповідно 20-30 репостів та до десятка коментарів.



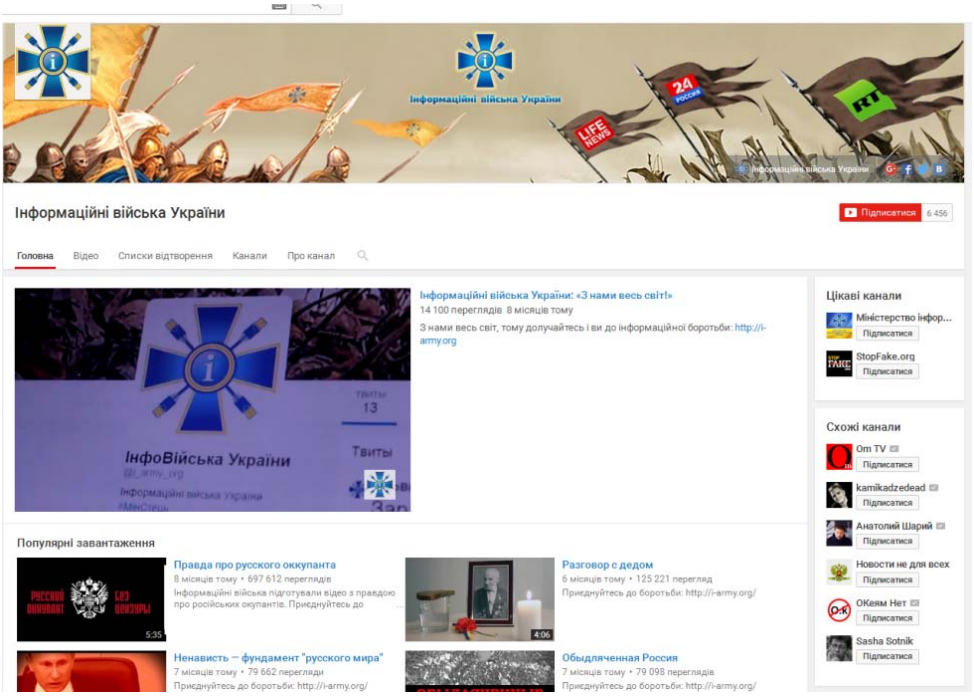
Так само, як і у випадку із попередньою соціальною мережею в сторінці проекту в VKontakte, останнім часом спостерігається значне падіння активності. На кількісні показники сторінки також впливає той факт, що зазначена мережа знаходиться під контролем відповідних російських структур.



У мережі Twitter сторінка проекту нараховує 11,1 тис фоловерів, регулярно знайомляться з твітами близько 200 фоловерів, в цілому створено близько 300 твітів. В середньому кожний більш-менш значущий твіт має 5-15 лайків та до 10 ретвітів. Важливі матеріали можуть назбирати 100-150 лайків та до сотні ревітів.

Слід зазначити, що модератори акаунту та адміністратори проекту «Інформаційні війська» не в повній мірі використовують усі можливості цієї соціальної мережі, що й позначається на результативності. Зокрема

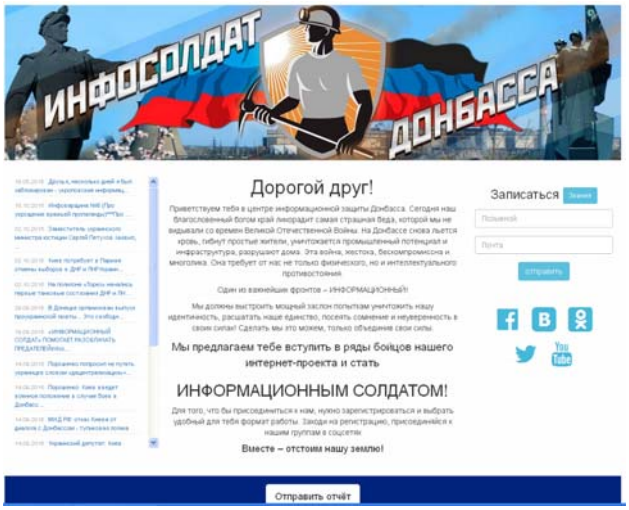
абсолютно не використовується можливість миттєвого поширення новин або анонсів, зважаючи на достатньо значний потенціал.

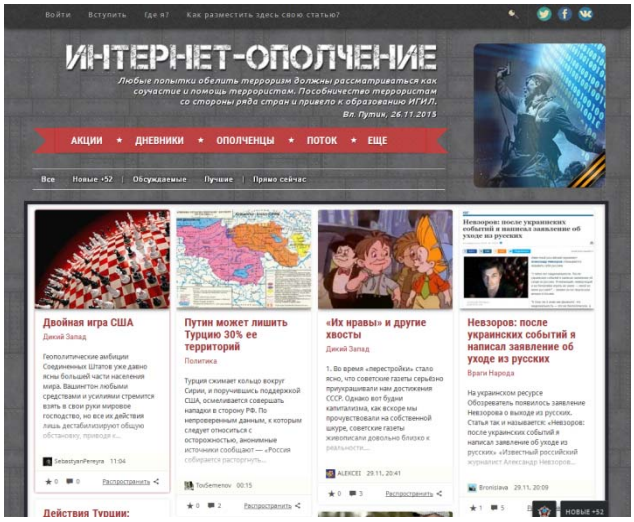


У соціальній мережі YouTube канал проекту «Інформаційні війська» нараховує майже 6,5 тис фоловерів, загальна кількість переглядів усіх матеріалів 1,14 млн на кілька десятків розміщених матеріалів.

Акаунт у соціальній мережі Google+ має 1,3 тис фоловерів та є одним з найменш розвинутих в усьому проекті. Матеріали розміщуються нерегулярно і рідко. Відповідно реакція фоловерів на такі матеріали досить слабенька.

Серед проектів, подібних до «Інформаційних військ України», що діють в рамках інформаційної війни, російська сторона використовує низку централізованих (під контролем держструктур) та громадських проектів. Останні мають різноманітне спрямування – в цілому по Україні («Интернет ополчение», «Киберберкут», «Антимайдан») або на окремі регіони («Информационный солдат Донбасса»).





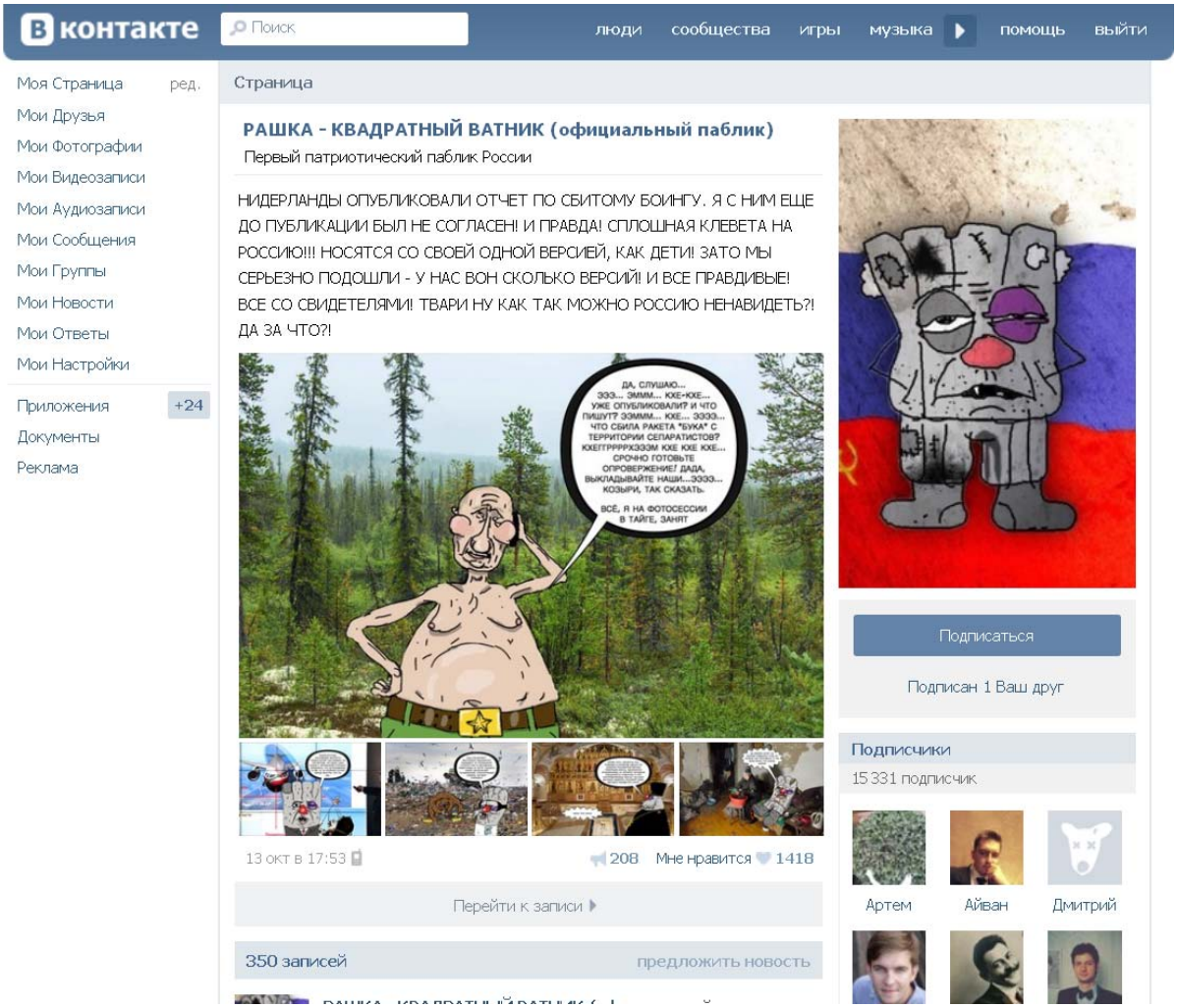
3D-мережа – об'єднання незалежних учасників, взаємодію яких регулюють принципи доцільності та корисності співпраці в межах даної мережі. Єдиного координаційного центру не існує.

Практичний приклад

Практичний приклад проекту, який функціонує за зазначеною схемою – офіційний паблік мережі VKontakte – «Ватник». Проект починався зі звичайного інтернет-мему і перетворився на знаковий в зв'язку із подіями2014-2015 рр. в Криму та на Сході України і в цілому в рамках російсько-української інформаційної війни.

На теперішній момент паблік нараховує 15,3 тис фоловерів. У середньому кожний матеріал має 100-200 лайків, 20-30 репостів, кілька десятків

коментарів. Найбільш популярні пости збирають 500-800 лайків, 100-150 репостів та до сотні коментарів.



http://vk.com/public_rushka

В якості контенту використовуються посилання на статті, відеоматеріали, меми, лоли, інфографіку. В рамках дискусій, у коментарях іноді застосовується ненормативна лексика, специфічні формати дискусії та інші форми спілкування, які забороняються та контролюються в переважній більшості подібних суспільств.

Система управління зазначеним проектом передбачає головного адміністратора (Антон Чадський) та чотирьох модераторів, які разом

здійснюють наповнення контентом паблік і відповідно корегують політику проекту.

У часи найбільшої активності даний паблік змінив систему координації з променевої на павуччю і на теперішній момент поповнюється контентом фактично за рахунок фоловерів, існуючих на доволі демократичних засадах.

Мисливська мережа – мережа, що утворюється внаслідок реструктуризації великих утворень шляхом розподілу на окремі юридично незалежні структури. Зазвичай таким шляхом йдуть потужні холдинги в тому разі, коли кон'юнктура передбачає більшу ефективність у діяльності дрібних компаній, які здатні гнучко реагувати на економічні виклики та налаштовуватися під нові ринкові умови.

Практичний приклад

В якості прикладу інтернет-проекту, в системі координації якого закладається принцип мисливської соціальної мережі, – структура, яка спеціалізується на тролінгу. Зазвичай її називають «Ольгінка» або офіційно «Агентство интернет-исследований» [111].

Зазначена структура не є публічною, втім, аналізуючи систему та принципи розбудови управлінських принципів, вдалось встановити її базову схему роботи.

Основна робоча структура складається з великої кількості автономних блогерів, які обслуговують велику кількість персональних фейкових акаунтів (до 50 на одного троля). Тактика роботи передбачає кілька режимів:

- *<u>режим вільного пошуку</u> – моніторинг визначеної дільниці віртуального простору з метою відстеження ситуації, появи нових проектів, лідерів, ідей та меседжів;*
- *<u>режим концентрованої атаки</u> – об'єднання атакуючого потенціалу в коментарях під конкретним матеріалом в інтернет-виданнях або під постами в соціальних мережах;*

- *<u>режим персонального контролю</u> – спостерігання та поміркована участь у дискусіях по конкретному об'єкту (блог або акаунт).*

Принцип управління такими проектами передбачає створення певних координаторських одиниць, навколо яких гуртуються інші тролі.

Також в якості робочих одиниць можуть виступати окремі інтернет-проекти або групи із вузько спеціалізованим профілем. Зазвичай це може бути регіональний або тематичний принцип.

5.4. Медіа-віруси та їх використання в якості інформаційної зброї

Будь-яка ефективна інформаційна атака починається з латентної фази – прихованого проникнення в інформаційне поле противника з метою дослідження середовища, апробації певних ідей та потенційного ефекту їх застосування, а також для створення і закріплення власних інформаційних майданчиків для подальшої агресії.

Найкращим інструментом для проникнення на вороже інформаційне поле є так званні **<u>медіа-віруси</u>** – ***інформаційні носії (події, скандали, чутки, діяльність організацій та окремих осіб), що несуть у прихованому вигляді завуальовані ідеї та меседжі.***

Зазвичай медіа-віруси можуть поширюватися у вигляді мемів та лолів – окремих семіотичних фрагментів [185].

Д.Рашкофф визначає декілька типів медіа-вірусів, серед яких [351, с. 124]:

1. Цілеспрямовані віруси - реклама, передвиборчі гасла, штучно детоновані «інформаційні бомби»;

2. Віруси-тягачі - спонтанно виникають та миттєво підхоплюються, а також наповнюються певним змістом, що спрямований на вирішення певних завдань;

3. Спонтанні віруси – народжуються та поширюються без конкретної цілі, в разі успішності можуть бути використані для вирішення певних завдань.

Найбільш вдалою формою камуфляжу для медіа-вірусів є події, винаходи, інноваційні технології, наукові теорії, філософськи системи та культурологічні концепції. Саме за допомогою таких форматів простіше всього здійснювати проникнення в певне інформаційне середовище, не викликаючи особливих підозр.

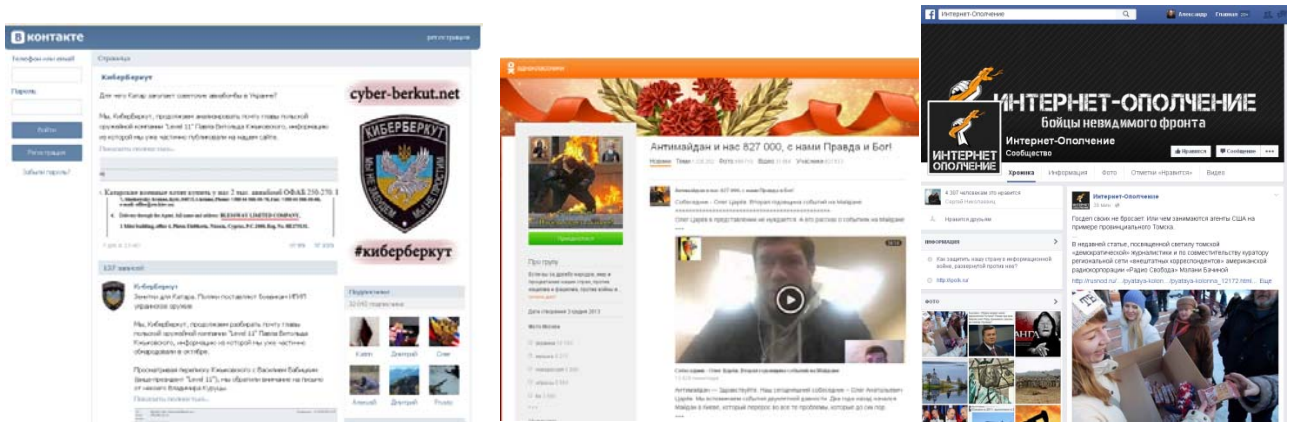
У рамках еволюції медіа-вірусів з'явилося таке явище, як **медіа-активізм** – ***тактика партизанської інформаційної війни, що реалізується окремими медіа-активістами або групами таких активістів.***

Тактика медіа-активізму передбачає створення певних розкручених персон або організацій (рухів, громадських ініціатив та ін.), які є авторами та трансляторами тематичних медіа-вірусів.

В он-лайн соціальних мережах до медіа-активістів можна віднести тематичні групи або окремих блогерів, які виконують функції своєрідних кібер-диверсантів.

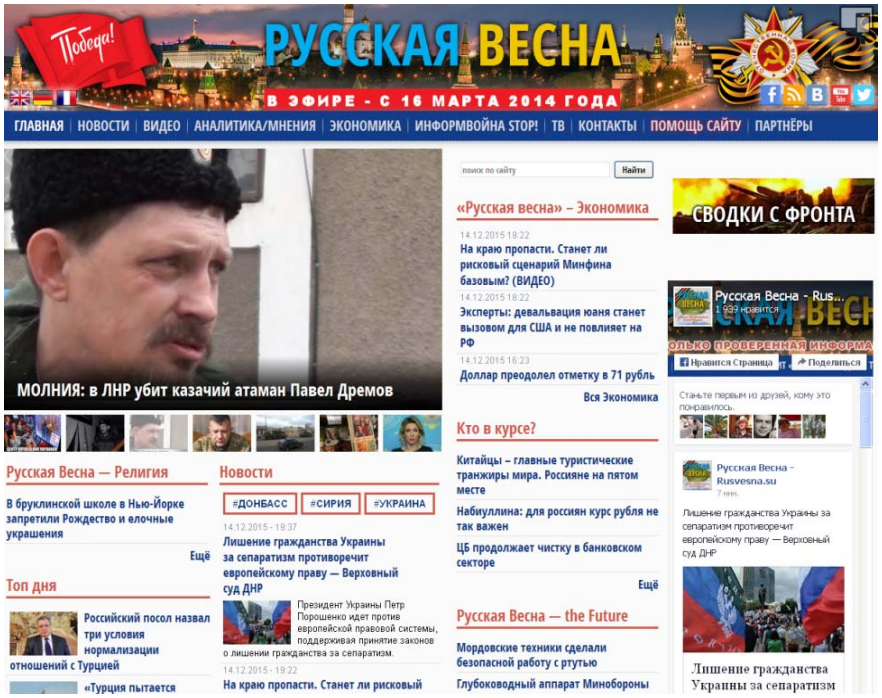
Особливо активно ця технологія застосовувалася в піковий період російської агресії в Криму та східних регіонах України. До кола таких товариств можна віднести низку груп під загальним брендом «Антимайдан», «Кибер Беркут», «Интернет-ополчение» та ін.

Мал.5.8. Медіа-активіські рухи



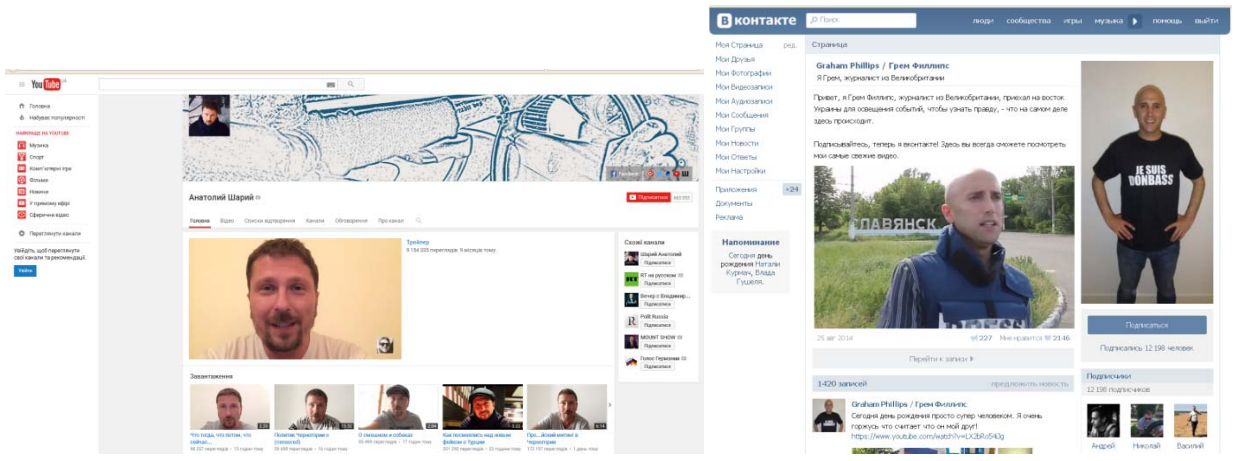
Також достатньо відомим трендовим медіа-вірусом став інтернет проект «Русская весна», який є уособленням та головною ідеологічною платформою російською агресії в Україні.

Мал. 5.9. Медіа-вірус «Русская весна»



Серед персоналій, яких можна вважати медіа-активістами, стали Анатолій Шарій, Грем Філліпс, Ігор Стрєлков та інші відомі медіа-персонажі, які уособлюються із інформаційно-психологічною війною, що супроводжувала російську агресію в Криму та на Сході України в 2014-2015 рр.

Мал. 5.10. Медіа-активісти в російсько-український війні (2004-2015 рр.)



В якості прикладу медіа-вірусів подій можна навести прес-конференції екс-президента України В.Януковича в Ростові. Мета цієї інформаційної атаки - сприяння розколу в українському суспільстві, підбурення лояльних до президента-втікача проти офіційної української влади, яка отримала мандат Майдану.

Мал. 5.11. Медіа-вірус «Прес-конференція В.Януковича в Ростові»

Серед останніх найбільш гучних медіа-вірусів скандалів можна визначити звинувачення російських медіа прем'єр-міністра України щодо його участі в чеченській війні. Абсурдність звинувачення була очевидною з самого початку і саме цей медіа-вірус носив характер фарсу.

Мал.5.12. Медіа-вірус «Яценюк в Чечні»

Також можна визначити медіа-віруси як інструменти інформаційно-психологічних атак, які за сутністю є поліваріативними та носять у собі класичні ознаки інформаційної війни другого покоління із елементами асиметрії. За своїми базовими ознаками та характеристиками вони відповідають визначенню інформаційної зброї.

Разом з наочними перевагами медіа-вірусів необхідно зазначити й певні технологічні недоліки, які виходять, перш за все, з суб'єктивного характеру цього явища. Сприйняття, підтримка або ігнорування такого інформаційного повідомлення цілком залежить від персональної реакції кожного конкретного отримувача.

Також слід зазначити, що вірусний характер контенту в соціальних он-лайн мережах може бути неконтрольований. Вдалий медіа-вірус, який отримує масову підтримку користувачів, починає існувати за законами та принципами притаманними внутрішньо груповій комунікації. Крім того, в певних ситуаціях його рух здійснюється за принципами та механізмами ройового інтелекту, який спрацьовує як засіб саморегулювання інформаційних потоків у певних соціальних суспільствах, до яких також відносяться і соціальні он-лайн мережі.

ВИСНОВКИ

У системі сучасних економічних, політичних та військових протистоянь інформаційні війни в соціальних он-лайн мережах посідають провідне місце, як один з ключових супроводжувальних процесів. Головне призначення таких процесів – шляхом концентрації зусиль на певних ключових ланках, забезпечувати суттєві переваги в рамках комплексного протиборства сторін. Інформаційна зброя такого типу здатна знищувати чи, як мінімум, блокувати системи координації, поширення інформації та інші відповідні управлінські процеси, а також перешкоджати роботі відповідних центрів керування. Спектр інструментів при цьому доволі широкий – від кібератак до організації акцій протесту, терористичних актів та організованого збройного опору.

Інформаційно-психологічні операції є сьогодні невід'ємною частиною систем управління військами, політичними та економічними процесами. У зв'язку з активною віртуалізацією людства, такі конфлікти переносяться у інтернет-простір і набувають формату мережевих он-лайн протистоянь.

Останнє викликає необхідність налагодження системної роботи за двома напрямками. Перший – розробка та впровадження стандартів і алгоритмів ведення мережевих інформаційних війн, які допомагатимуть швидко реагувати на певні виклики та компенсувати в певних обставинах відсутність досвіду та власних інструментів. Другий напрямок – налагодження системної роботи із підготовки відповідних фахівців, що спиратиметься на чітку методологічну базу та практичні методики навчання.

Важливість роботи за двома зазначеними вище напрямками полягає в тому, що інформаційні війни, на відміну від торгово-економічних, політичних та збройних протистоянь, ніколи не закінчуються. Тому питання державної інформаційної безпеки в зазначеному контексті є завжди актуальним.

Словник профільних термінів та понять

А

Аватар – графічне персоніфіковане зображення, що асоціюється з конкретним користувачем.

Анонімус – більшість відвідувачів фоловерів, які вільно висловлюють свої найсміливіші думки.

Акаунт – персональна або корпоративна сторінка у соціальній мережі.

Б

Бан (від англійського ban - забороняти) - Жаргонний вираз: 1) спосіб покарання адміністрацією сайту за некоректну поведінку користувача або використання спамерських прийомів, який полягає у видаленні облікового запису з бази. Відновлення не гарантоване, звичайно вимагає особистого листування з адміністрацією і в будь-якому випадку займає тривалий час; 2) видалення учасника з групи за некоректну поведінку через занесення його в чорний список. Учасник групи, занесений в такий, не має можливості потрапити в групу. Після виведення з чорного списку, учасник у групі автоматично не відновлюється. Бан-лист - список користувачів, які за некоректну поведінку та з інших причин, заблоковані. Користувачі, занесені в Бан-лист, не можуть відправляти повідомлення та переглядати інформацію.

Блогер – автор мережевого блогу.

Блогосфера – мережевий простір, у рамках якого функціонують блоги.

Блогінг – процес створення й просування блогів.

Бот (англійське bot скорочення від robot) - віртуал, створений спеціальною програмою для виконання певної дії в соціальній мережі, як правило, розсилки спаму. На питання і повідомлення інших користувачів бот не відповідає. Звернення до боту може спровокувати візит до користувача великої кількості його «братів».

В

Веб-браузер - програмне забезпечення для перегляду веб-сайтів. Призначений для запиту веб-сторінок, їх обробки, виведення і переходу від однієї сторінки до іншої. Популярні веб-браузери: Mozilla Firefox, Opera, Internet Explorer, Safari, Chrome.

Вебінар - різновид веб-конференції, проведення он-лайн-зустрічей або презентацій через Інтернет у режимі реального часу.

Віджет – змістовний модуль з контентом, який монтується на веб-сторінці або браузері.

Віки-проект - веб-сайт, структуру та зміст якого користувачі можуть самостійно створювати й змінювати за допомогою інструментів, що надаються адміністрацією ресурсу.

Вірусна реклама – активне розповсюдження (як правило, у геометричній прогресії) рекламного матеріалу, в якому беруть участь представники цільових груп.

Г

Гео-сервіси – географічні інформаційні системи, картографічний сервіс.

Гібридна (асиметрична) війна - засіб протистояння, який поєднує в собі комплекс різноманітних інструментів політичного, економічного, військового та ідеологічного характеру.

Д

Діалогові комунікаційні канали – канали взаємодії із цільовим групам (безкоштовні гарячі телефонні лінії, форуми та ін.)

Домен – певна зона в мережі Інтернет, виділена для забезпечення доступу до наданої на веб-сайті інформації, що належить власникові домена.

Е

Емограма – графічний символ, що використовується для вираження емоцій.

І

Інсайдер – особа, що має доступ до конфіденційної інформації в організації.

Інтегровані дослідження комунікаційних процесів – комплексні процеси дослідження та аналізу інформаційних процесів, для здійснення яких залучаються традиційні інструменти та інноваційні методики.

Інформація - відомості або дані про явища та предмети навколишнього середовища, яке оточує людину.

Інформаційна атака/зброя - здійснення тимчасового або остаточного виведення з ладу систем та підрозділів противника, що відповідають за процеси управління та інформування.

Інформаційний процес - діяльність із створення, накопичення, зберігання, пошуку та розповсюдження відомостей або даних певного тематичного характеру.

Інформаційний вибух - суттєве прискорення процесів створення, накопичення, пошуку та поширення інформації.

Інформаційна війна - циклічний або лінійний обмін інформацією, яка може/має спричинити певну шкоду отримувачу, а автору надати певну перевагу.

Інформаційне поле - соціальний або географічний простір, у межах якого відбуваються типові комунікаційні процеси, що охоплюють їх учасників (суб'єкти) на основі обміну інформацією (об'єкт).

Інформаційна революція - докорінна зміна методів створення, накопичення, зберігання, пошуку та поширення інформації.

К

Карта інформаційного поля – схематичне зображення інформаційно-комунікаційних каналів компанії, за допомогою яких остання взаємодіє із зовнішніми та внутрішніми цільовими групами.

Кібервійна – протистояння сторін на рівні програмного забезпечення шляхом видобування закритої інформації та виведення з ладу програмно-апаратних

засобів противника з метою отримання суттєвих переваг в економічних, політичних та військових протистояннях.

Комунікація - процес передання або обміну інформацією.

Контент – (англ. content – вміст) будь-яке інформаційно значиме наповнення інформаційного ресурсу (наприклад, веб-сайту) – тексти, графіка, мультимедіа; вся інформація, яку користувач може завантажити на диск комп'ютера з дотриманням відповідних норм.

Кроспостінг – цілеспрямоване автоматичне, напівавтоматичне або ручне розміщення однієї статті, посилання або теми, у форуми, блоги, будь-які інші форми веб-ресурсів або публічне листування, в тому числі й у режимі он-лайн спілкування.

Л

Лайк – позначка на уподобаному контенті.

Лінійна модель комунікації - цілеспрямований процес передання інформації від автора повідомлення до отримувача.

Лінкбайтінг – засіб отримання зворотних посилань на свій сайт природнім шляхом за власною ініціативою відвідувачів.

Лічка – персональне листування власника акаунту.

М

Маніпуляція - засіб психологічного впливу, що застосовується задля прихованого проникнення в психіку жертви з метою занесення цілей, бажань, намірів, відносин або установок маніпулятора.

Мас-медіа - технології та засоби трансляції інформації від конкретного джерела на широку аудиторію, що обмежується рамками певного інформаційного поля, в якому ці мас-медіа діють.

Медіа - канали та засоби зберігання, передачі й подання інформації або даних.

Медіавірус (англ. media virus) – медіаподія, що прямо чи опосередковано викликає зміни в житті суспільства.

Медіатероризм (media terrorism) - цілеспрямоване, планомірне, систематичне використання можливостей засобів масової інформації (мас-медіа) для створення і тиражування почуттів страху (жаху, неспокою, тривоги) і розповсюдження їх в інформаційному просторі з метою маніпулювання суспільною свідомістю.

Інтернет-мем (англ. Internet meme) – назва явища спонтанного поширення якоїсь інформації чи фрази, часто безглуздої, що випадково набула популярності в інтернет-середовищі завдяки поширенню усіма можливими способами (електронною поштою, на форумах, у блогах тощо).

Мережева інформаційна війна - інформаційно-комунікаційне протистояння у форматі оф-лайн та он-лайн мережевих структур.

Мобільний маркетинг — комплекс маркетингових заходів, спрямованих на промоцію товарів або послуг із використанням засобів стільникового зв'язку.

Н

Нік (від англ. nick, nickname – прізвисько) – переважно вигадане ім'я, яким називає себе користувач соцмереж або на різноманітних чатах, форумах, месенджерах тощо.

О

Об'єкти інформаційних процесів - інформація або ті, хто отримує цю інформацію, в процесі спрямованої комунікації.

П

Психографіка – характерні психологічні особливості представників певних цільових аудиторій.

Р

Рерайтинг – написання унікального тексту на основі вже існуючої новини, статті. Для рерайтинга типово використання синонімічних слів, переклад прямої мови в непряму, переміщення абзаців.

С

Соціальна мережа – це соціальна структура, створена об'єднаними за однією або декількома ознаками взаємозалежності вузлами, які здебільшого представлені індивідуальними членами або організаціями. Соціальні мережі можуть бути створеними на тлі спільності цінностей, дружби, родинності, неприязні, конфлікту, торгівлі, зв'язків у мережі Інтернет, сексуальних зв'язків, релігійних поглядів тощо.

Співтовариство віртуальне - група людей із схожими інтересами, які спілкуються один з одним в основному через Інтернет.

Споук-персона **–** офіційна особа, що презентує позицію компанії, є транслятором інформаційних меседжів.

Стіна **-** спосіб публікації відкритих записів особистого і загального характеру тимчасової значущості, відсортованих у зворотному хронологічному порядку, тобто останній запис знаходиться зверху.

Суб'єкти інформаційних процесів – учасник комунікацій, індивідуум, соціальні групи, організації (ЗМІ, громадські, державні, комерційні структури).

Т

Таргетування **–** вибір цільової групи або цільового сегменту інтернет-простору.

тИЦ (тематичний індекс цитування**) -** технологія оцінки авторитетності інтернет-ресурсів з врахуванням якісної характеристики – посилань на інших сайтах. Даний показник розраховується як сумарна вага посилань через систему апдейтів (рахівників показників) з оновленням два рази на місяць.

Тред – група повідомлень, об'єднаних єдиною тематикою.

Тренд – популярна тема обговорення в соцмережах.

Тролінг *(*від англ. trolling) – розміщення в Інтернеті (на форумах, в групах новин Usenet, у вікі-проектах та ін.) провокаційних повідомлень з метою викликати конфлікти між учасниками, образи, війну правок, марнослів'я тощо.

Тролінг є грубим порушенням мережевого етикету (нетикету). Особу, яка займається тролінгом, називають тролем.

Ф

Флог / Фейк – фальшивий блог або акаунт, на якому міститься неправдива інформація.

Фолловер – підпис на новини й оновлення.

Флуд – повідомлення у форумах і чатах, що займають великі об'єми і не несуть корисної інформації.

Х

Хай-х'юм технології (англ. high-hum — високі гуманітарні технології) - сукупність знань, духовних та культурних цінностей, а також методів транслювання інформації, що стимулює людей до певної колективної діяльності.

Ц

Цільова аудиторія – аудиторія, на яку спрямовані зусилля інформаційного процесу комунікацій. Визначається за певними соціально-демографічними характеристиками (стать, вік, освіта, прибуток, споживацькі уподобання, стиль життя та ін.)

Циклічна модель комунікації - взаємний обмін інформацією, в процесі якого учасники комунікації поступово змінюють ролі автора та отримувача повідомлення.

D

dDoS-атака (Distributed Denial Of Service Attack) - атака з використанням безлічі адрес нічого не підозрюючих користувачів для заблокування каналу, через відкриття максимально можливої кількості з'єднань із соціальною мережею. Послання великої кількості паразитного трафіку для перевантаження і виведення з ладу операційної системи, яка не встигає обробити всі з'єднання, в результаті чого, користувачі соціальної мережі не мають можливості з'єднання з сервером, на якому розміщений сайт.

P

PageRanke **-** алгоритм виміру популярності інтернет-ресурсу за 10-ти бальною шкалою. Оцінює «важливість» та «авторитетність» за кількістю посилань. Використовується системою Google для ранжування сайтів при видачі результатів пошуку за запитами користувачів.

S

SMM-аудит – методика оцінки впізнаваності та характеру іміджу досліджуваного об'єкта в соціальних мережах та в мережі Інтернет у цілому.

SEO (Search Engine Optimization) – комплекс заходів із пошукової оптимізації, орієнтований на підвищення позиції веб-сайту в пошукових системах.

SMO (Social Media Optimization) – комплекс заходів із просування веб-ресурсів у мережі Інтернет.

SMM (Social Media Marketing) – комплекс заходів із просування персонального акаунту або окремого контенту в соціальних мережах.

Додаток. Сервіси для соціальних мереж

Створення сторінки

Wix – допомогає створити сайт або сторінку та легко інтегрувати її з Facebook.

Coolmojito - дозволить створити сторінку в Facebook з унікальним дизайном і легко оформити її, використовуючи стандартні шаблони і налаштовуючи елементи інтерфейсу.

Tabsite - безкоштовна версія інструмента пропонує сторінку з двома вкладками, набір віджетів для роботи з контентом. Можна додати зображення, RSS, email-форму.

Facebook

Agora Pulse - цей інструмент відстежує активність у Facebook, допомагає планувати публікацію постів і запускати рекламні кампанії.

EdgeRank Checker - пропонує огляд та аналіз сторінки в безкоштовному варіанті та рекомендації, відстеження активності в реальному часі і багато іншого для PRO-акаунтів.

ShortStack - допоможе створити рекламну кампанію будь-якого типу. Має набір шаблонів і візуальний редактор.

Facebook Page Barometer – показує статистику за охопленням, залученням та іншими параметрами. Ви можете порівняти показники сторінки з середніми показниками +8193 сторінок в Barometer.

AgoraPulse Contest - це програма допомагає визначити переможця в конкурсах декількох типів.

Likealyzer - аналізує сторінку і дає загальну оцінку та рекомендації щодо поліпшення, потрібно тільки вказати посилання на сторінку.

FanPage Karma – дає структурований огляд та рекомендації щодо поліпшення сторінки.

Wolfram Alpha Personal Analytics - аналізує персональні профілі Facebook і розповідає все про його власника.

Pagemodo – допомагає провести конкурси, створити обкладинку профілю, налаштувати розклад публікацій і знайти потрібний контент.

Twitter

TwitterCounter - дозволяє наочно побачити зростання фоловерів у Twitter за останні 3 місяці, місяць або тиждень.

WhoTweeted Me – показує, хто поширює по Twitter контент з базового акаунта.

TweetStats - дозволяє аналізувати твіти з будь-якого Twitter-аккаунта.

Google+

Steady Demand Pro – допомагає дізнатися, скільки людей відвідує сторінку, як часто вони заходять, а також аналізує інші важливі параметри.

CircleCount - аналізує передплатників і їх діяльність, а також країни їхнього проживання.

SumAll - надає порівняльну інформацію про діяльність у соціальних медіа, використовуваних для просування.

Вконтакте

Postee - аналізує статистику своїх і чужих груп у «ВКонтакте».

Popsters – допомагає провести аналіз ефективності спільнот з можливістю сортування постів по лайкам і репоста.

Allsocial - рейтинг популярних акаунтів (від 50000 учасників) Паблік у «ВКонтакте» - з вбудованою аналітикою і власним ранжируванням.

Random – допомагає в проведенні конкурсів. Додаток вибирає випадкового фоловера групи, який попередньо лайкнув обраний пост і поділився ним з друзями.

Розширення для браузера

Buffer - дозволяє розповсюджувати контент будь-якого сайту, блогу чи сторінки.

Giphy - дозволяє шукати потрібну гифку через величезні архіви Giphy.com і вставляти скорочені URL для картинок.

Instagram для Chrome – дозволяє переглядати власну стрічку і профілі друзів,

лайки і коментарі до фотографій, отримувати повідомлення і навіть заглиблюватися в деталі, наприклад, у фільтри, не відходячи від монітора.

Bitly - містить всі стандартні функції скорочування посилань: звичайне скорочення, аналітика і кнопки скопіювати та розповсюдити. Також програма може повідомити, коли посилання досягне необхідної кількості переглядів.

Window Resizer - перевірка твітів, постів і оновлення, на екрані будь-якого розміру.

Social Analytics - дозволяє швидко подивитися статистику поширення контенту на будь-якій сторінці.

Feedly Mini – дозволяє зберегти RSS-стрічку сайту, на якому перебуває користувач.

Візуалізація даних

Easel.ly – дозволяє створювати інфографіки.

Recitethis – дозволяє створювати зображення і оформляти його цитатами.

OmniGraffle - програма призначена для створення схем і діаграм, створення прототипів мобільних і веб-інтерфейсів.

PicMonkey – дозволяє редагувати зображення, міняти фон, додавати на картинку потрібні елементи, зробити колаж, обкладинку на Facebook та багато іншого.

Phonto – дозволяє створити зображення з текстом.

GoogleCharts – сервіс, призначений для побудови графіків і діаграм.

AdobeInDesign - програма для роботи з цифровим контентом, створюються електронні книги для планшетів, макети веб-сторінок. Формати файлів FLV, F4V, MP3, JPEG, PDF, SWF, EPUB, XFL.

Infogr.am - безкоштовний он-лайн-сервіс для створення схем, графіків і карт з можливістю завантаження відео та фото.

ShareAsImage - сервіс, за допомогою якого можна накласти текст на зображення, включаючи особисту фотографію, а також змінити зображення за допомогою ефектів заливки, градієнта, зміни фону.

Список літератури

Нормативно-правова база

1. Конституція України [Текст]: прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. // Відом. Верхов. Ради України. – 1996. - №30
2. Закон України «Про інформацію» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка. – т. 1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 9-28
3. Закон України «Про друковані засоби масової інформації (пресу) в Україні» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 29-43
4. Закон України «Про телебачення та радіомовлення» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1. - Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С.44-69
5. Закон України «Про інформаційні агентства» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1. Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 73-82
6. Закон України «Про рекламу» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 106-123
7. Закон України «Про телекомунікації» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 124-165
8. Закон України «Про порядок висвітлення діяльності органів державної влади та місцевого самоврядування в Україні засобами масової інформації» [Текст] // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 166-176
9. Закон України «Про захист персональних даних» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2297-17
10. Закон України «Про видавничу справу» // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 234-247

11. Закон України «Про державну таємницю» // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С.252-276

12. Закон України «Про захист інформації в авторизованих системах» // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1. - Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 277-282

13. Закон України «Про доступ до публічної інформації» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу http://zakon0.rada.gov.ua/laws/show/2939-17

14. Закон України «Про державну службу спеціального зв'язку та захисту Інформації України» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/3475-15

15. Закон України «Про наукову та науково-технічну експертизу» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80

16. Закон України «Про електронні документи та електронний документообіг» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/851-15

17. Закон України «Про засади державної мовної політики» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/5029-17

18. Закон України «Про Національну систему конфіденційного зв'язку» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2919-14

19. Закон України «Про основи національної безпеки» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15

20. Закон України «Про підтвердження відповідності» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2406-14

21. Закон України «Про радіочастотний ресурс» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1770-14

22. Закон України «Про систему Суспільного телебачення та радіомовлення України» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/485/97-%D0%B2%D1%80

23. Закон України «Про науково-технічну інформацію» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon5.rada.gov.ua/laws/anot/3322-12

24. Закон України «Про Національну програму інформатизації» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80

25. Окінавська Хартія Глобального інформаційного суспільства [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/998_163

26. Декларация принципов «Построение информационного общества – глабальная задача в новом тысячелетии (12 декабря 2003 г.)» // Інформаційне законодавство: Збірник законодавчих актів: у 6 т. / за заг. ред. Ю.С.Шемшученка, І.С.Чижа. – Т.5. Міжнародно-правові акти в інформаційній сфері. – К.: ТОВ «Видавництво «Юридична думка», 2005. – С.307-320

27. Політичне послання комітету міністрів Усесвітньої зустрічі на найвищому рівні з питань інформаційного суспільства // Інформаційне законодавство: Збірник законодавчих актів: у 6 т. / за заг. ред. Ю.С.Шемшученка, І.С.Чижа. – Т.5. Міжнародно-правові акти в інформаційній сфері. – К.: ТОВ «Видавництво «Юридична думка», 2005. – С.296-301

28. Берлінська декларація про відкритий доступ до наукового та гуманітарного знання // Інформаційне законодавство: Збірник законодавчих актів: у 6 т. / за заг. ред. Ю.С.Шемшученка, І.С.Чижа. – Т.5. Міжнародно-правові акти в інформаційній сфері. – К.: ТОВ «Видавництво «Юридична думка», 2005. – С.286-290

29. Концепція національної безпеки України [Електронний ресурс] // Міністерство інформаційної політики України: [сайт]. - Режим доступу: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20%28%D0%A2%D0%B5%D0%BA%D1%81%D1%82%29%20-%2030.09.15.pdf

30. Указ Президента України «Про доктрину інформаційної безпеки України» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009

Наукові та науково-прикладні статті і видання

31. Албитов А. Facebook: как найти 100 000 друзей для вашего бизнеса [Текст] / А.Албитов. – Москва: Манн, Иванов и Фербер, 2013. – 140 с.

32. Амзин А. Новостная интернет-журналистика [Текст] / А.Амзин. – Москва: Аспект Пресс, 2011. – 144 с.

33. Ананьїн В. Інформаційна безпека у контексті сучасних подій в Україні [Текст] / В. Ананьїн, О. Пучков // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – № 14-15. С. 28–29.

34. Андреєва О.М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією [Текст] / О.М. Андреєва. – Київ: Парламентське видавництво, 2009. – 360 с.

35. Аниловская И. Война: переписка одноклассников [Текст] / И.Аниловская. – Київ: Альфа Реклама, 2014. – 122 с.

36. Аніщенко В.О. Сутність операцій з підтримки миру (миротворчі операції) [Текст] / В.О.Анищенко // Труди академії оборони України. – К.: НОАУ, 2001. – Вип. 34. – С. 67-72

37. Анцупов А.Я. Конфликтология [Текст]: учебник / А.Я.Анцупов, А.И. Шипилов. – Санкт-Петербург: Питер, 2007. – 496 с.

38. Аронсон Э. Эпоха пропаганды: механизмы убеждения, повседневное использование и злоупотребление [Текст] / Э.Аронсон, Э.Пратканис. – Санкт-Петербург.: Прайм-Еврознак, 2003. – 384 с.

39. Артьомов О.Ю. Сучасна українська культура, її вплив на соціальне і політичне життя [Текст] / О.Ю. Артьомов // Актуальні проблеми державного управління. – 1999. – № 2 (4). – С. 8–13.

40. Аслунд А. Програли Путін і Газпром, виграли Меркель і Тимошенко [Електронний ресурс] // УНІАН: [сайт]. – Режим доступу: http://www.unian.ua/news/298827-prograli-putin-i-gazprom-vigrali-merkel-i-timoshenko.html.

41. Ачкасова В.А. Связи с общественностью как социальная инженерия [Текст] / В.А. Ачкасова, Л.В. Володина. – Санкт-Петербург: Речь, 2005. – 336 с.

42. Бабаев А. Контекстная реклама [Текст] / А.Бабаев, Н.Евдокимов, А.Иванов. – Санкт-Петербург: Питер, 2012. – 304 с.

43. Бабіч О. Особливості маніпуляції масовою свідомістю в друкованих ЗМІ під час висвітлення воєнних подій [Текст] / О. Бабіч // Вісник Київського національного університету імені Тараса Шевченка: військово-спеціальні науки. – 2007. – Вип. 14 – 15. – С. 89–92.

44. Бажан О. Г. Українська Гельсінська група: легальна форма протистояння тоталітарному режимові в УРСР [Текст] / О. Г. Бажан // Національний ун-т «Києво-Могилянська академія». Наукові записки. – Київ, 1999. – Т.14: Історія. – С.73–79.

45. Бала В. Чому потрібно формувати позитивний імідж України та її влади [Електронний ресурс] / В. Бала // Ліга. Блоги: [сайт]. - Режим доступу: http://blog.liga.net/user/bala/article/1164.aspx.

46. Барыкин В.М. Силы специальных операцій и способы борьбы с ними [Текст] / В.М.Барыкин, С.Л. Велесов // Военная мисль. – 2001. - №2. – С. 12-15

47. Батичко Г. І. Архітектоніка європейського культурного простору/ [Електронний ресурс] / Г. І. Батичко //НБУ [сайт] – Режим доступу: http://www.nbuv.gov.ua/portal/Soc_Gum/Gileya/2010_42/Gileya42/F21_doc.pdf.

48. Бебік В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рілейшнз [Текст]: монографія / В.М. Бебік. – Київ: МАУП, 2005. – 440 с.

49. Бебик В. Політологія для політика і громадянина [Текст]: монографія / В.Бебик. – Київ: МАУП, 2003. – 146 с.

50. Бек Д. Спиральная динамика. Управляя ценностями, лидерством и изменениями в XXI веке [Текст] / Д.Бек, К.Кован. – Москва: Открытый мир, 2010. – 424 с.

51. Белоногов Г. Г. Еще раз о гносеологическом статусе понятия «информация» [Текст] / Г. Г. Белоногов, Р. С. Гиляревский // Научно-техническая информация. Серия 2. Информационные процессы и системы. – 2010. – № 2. – С. 1–6.

52. Белогуров С. Психологические операции США в Боснии и Герцоговине [Текст] / С.Белогуров // Солдат удачи. – 1999. - №11. – 11-17

53. Бендлер Р. Рефрейминг [Текст] / Р.Бендлер, Дж. Гриндер. – Воронеж: Флинта, 2003. – 232 с.

54. Березкин Г.А. Уроки и выводы из войны в Ираке [Текст] / Г.А.Березкин // Военная мысль. – 2003. - №7. – С.58-65

55. Берестова Т. Ф. Функции разных видов информации как основа формирования многоуровневой структуры информационного пространства [Текст] / Т. Ф. Берестова // Научно-техническая информация. Серия 1. Организация и методика информационной работы. – 2009. – № 8. – С. 3–12.

56. Бжезинский З. Великая шахматная доска. Господство Америки и его геостратегические императивы [Текст] / З.Бжезинский. – Москва: Междунар. отношения, 1994. – 256 с.

57. Бжезинский Зб. Выбор. Глобальное господство или глобальное лидерство [Текст] / Зб. Бжезинский. – Москва: Международные отношения, 2004. – 288 с.

58. Белоножкин В. И., Остапенко Г. А. Информационные аспекты противодействия терроризму [Текст] / В.И. Белоножкин, Г.А.Остапенко. — Москва: Горячая линия - Телеком, 2009. — 112 с.

59. Березовец Т. Анексія: Острів Крим. Хроніки «гібридної війни» [Текст] / Т.Березовець. – Київ: Брайт Стар Паблішінг, 2015. - 392 с.

60. Бінько І. Інформаційний простір України: стан та тенденції розвитку [Текст] / І. Бінько// Бібліотечний вісник. – К., 2001. – № 2. – С. 15–18.

61. Биструхін Г.С. Війна в кам’яних джунглях. Міська партизанська війна як феномен збройної боротьби та спеціальної діяльності. 1945-2005 рр. [Текст]: монографія / Г.С.Биструхін, Д.В.Вєдєнєєв. – Київ: Генеза, 2006. – 512 с.

62. Блэк С. Паблик рилейшнз. Что это такое? [Текст] / С. Блэк. – Москва, 1990, – 240 с.

63. Богуш Д. Две новости для инвестиционного имиджа Украины [Электронный ресурс] / Д. Богуш // Publicity [сайт]. – Режим доступа: http://www.publicity.kiev.ua/srv5/one/Dve_novost.html?rnd=489598.

64. Бодріяр Ж. Симулякри і симуляція [Текст] / Ж.Бодріяр. – Київ: «Основи», 2004. – 230 с.

65. Бондар Ю. Поле битви – інформаційний простір (закінчення) [Електронний ресурс] / Ю. Бондар // Персонал: [сайт]. – 2006. – № 3. – Режим доступу: // http://www.personal.in.ua/article.php?ida=247.

66. Бондаренко Г. Трансформація звичаєво-обрядової культури та морально-ціннісних орієнтацій сільського населення України в умовах глобалізації [Текст] / Г. Бондаренко // Українська культура в контексті світових глобалізаційних процесів. – 2005. – С. 26–35.

67. Бортніков В.І. Політична участь і демократія [Текст]: українські реалії: монографія / В.І. Бортніков. – Луцьк: РВВ «Вежа» Волинь. держу н-ту ім. Л.Українки, 2007. – 524 с.

68. Боярский А., Оставненко Е. Пиар всемирного масштаба [Электронный ресурс] / А. Боярский, Е. Оставненко // Деньги: [сайт]. – Режим доступа: http://www.kommersant.ru/doc-rss.aspx?DocsID=1123618.

69. Бугоркова О. Армия тролей на службе Кремля [Электронный ресурс] /О.Бугоркова // BBC (русская служба): [сайт]. – Режим доступа: http://www.bbc.com/russian/russia/2015/03/150320_kremlin_internet_trolls_bugorkova

70. Брайант Дж. Основы воздействия СМИ [Текст] / Дж. Брайант, С.Томпсон. – Москва: София, 2004. – 432 с.

71. Браун М.П. Посібник з аналізу державної політики / М.П.Браун. – Київ: Основи, 2000. – 243 с.

72. Бржестовский Д.С. Особенности современной информационной войны между Израилем и Палестиной [Текст] / Д.С. Бржестовский // Вопросы германской истории: сборник научных трудов. – 2002. – С. 211 – 217.

73. Бредемайер К. Искусство словесной атаки [Текст] / К.Бредемайер. – Москва: Альпина Бизнес Букс, 2007. - 178

74. Брекенридж Д. PR 2.0: новые медиа, новые аудитории, новые инструменты [Текст] / Д.Брекенридж. – Москва: Эксмо, 2009. – 245 с.

75. Броган К., Смит Дж. Формула эффекта. Как получить реальный результат в социальных сетях [Текст] / К.Броган, Дж. Смит [пер. англ. У.Сапцина]. – Москва: Манн, Иванов и Фарбер, 2013. – 245 с.

76. Брусницын Н.А. Информационная война и безопасность [Текст] / Н.А.Брусницын. – Москва: Вита-Пресс, 2001. - 279

77. Буланов А. Г. Национальные подходы к определению информационной войны [Текст] / А. Г. Буланов // Гуманітарний вісник Запорізької державної інженерної академії. – 2002. – № 11. – С. 164–170.

78. Булгак П. «Ми з майбутнього – 2». Нові технології кремлівського агітпропу[Електронний ресурс] / Павло Булгак // Телекритика: [сайт]. – Режим доступу: http://www.telekritika.ua/column/2010-02-27/51364.

79. Бунакова І. Трансформація цінностей української сім'ї [Текст] / І. Бунакова // Філософія, культура, життя. Міжвузівський збірник наукових праць. – 2003. – Вип. 21. – С. 42–47.

80. Бурков В.Н. Модели и механизмы управления безопасностью [Текст] / В.Н. Бурков, Е.В.Грацианский, С.И.Дзюбко, А.В.Щепкин. – Москва: СИНЕГ, 2001. – 160 с.

81. В Росії вийде комп'ютерна гра про війну з Україною, Грузією і Польщею [Електронний ресурс] // Гуртом – українське гніздечко [сайт]. – Режим доступу: http://www.hurtom.com/computers/games/2637-v-ros-vijjde-kompjuterna-gra-pro-vjjnu.html.

82. В России издаются антиукраинские книги [Электронный ресурс] // SITEUA.ORG: [сайт]. – Режим доступу: http://news.siteua.org/system_category/45718.

83. Валецкий О. Югославская война 1991-1995 гг. [Текст] / О. Валецкий. – Москва: Крафт, 2006. – 528 с.

84. Вайнерчук Г. Лайкни меня. Экономика благодарности [Текст] / Г.Вайнерчук. – Москва: Альпина Паблишер, 2012. – 296 с.

85. Вайнштейн Г. Интернет как фактор общественных трансформаций [Текст] / Г.Вайнштейн // Мировая экономика и международные отношения. – 2002. - №7. – С.17

86. Васильова Н. Державний брендінг: зарубіжний досвід та перспективи для України. Державний брендінг: що це таке? [Электронный ресурс] / Н. Васильова // Українська PR-ліга: [сайт]. Режим доступу: http://www.pr-liga.org.ua/2/33/412.

87. Васютинський В.О. Психологічні виміри спільноти [Текст]: монографія / В.О. Васютинський. – Київ: Золоті ворота, 2010. – 119 с.

88. Васько А.А., Ткаченко В.И. Силы специальных операций иностранных государств и их боевое применение в современных условиях: учебное пособие / А.А.Васько, В.И.Ткаченко. – К.: ИПИК СБ Украины, 1994. - 356 с.

89. Вебер М. Избранные произведения [Текст] / М. Вебер [пер. с нем. Ю. Н. Давыдова]. – Москва: Прогресс, 1990. – 808 с.

90. Вєдєнєєв Д.В. Гострі когті орла. Сили спеціальних операцій США: історія та сучасність [Текст]: монографія / Д.В. Вєдєнєєв, Г.С. Биструхін, А.І.Семука. – Київ: К.І.С., 2010. – 400 с.

91. Вєдєнєєв Д.В. «Міжнародний тероризм» : цілісне явище модерної військової історії чи пропагандиський штамп [Текст] / Д.В.Вєдєнєєв // Труди Національного університету оборони України. – 2009. - №2. – С.186-192

92. Вепринцев В. Б. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник [Текст] / В.Б. Вепринцев, А.В.Манойло, А.И.Петренко, Д.Б.Фролов. — 2-е изд., стереотип. — Москва: Горячая линия - Телеком, 2011. — 495 с.

93. Веремеев Ю. Частные армии в России / Ю.Веремеев [Електронний ресурс] / Анатомия армии: [сайт] – Режим доступу: http://army.armor.kiev.ua/hist/privat-army-2.shtml

94. Вершинин М.С. Политическая коммуникация в информационном обществе [Текст] / М.С.Вершинин. – Санкт-Петербург: Изд-во В.А.Михайлова, 2001. – 253 с.

95. Вирин Ф. Интернет-маркетинг. Полный сборник практических инструментов [Текст] / Ф.Вирин. – Москва: Эксмо, 2012. – 288 с.

96. Витале Д. Гипнотические рекламне тексты: как искушать и убеждать клиентов одними словами [Текст] / Д.Витале [пер. англ. В.Гарбарук]. – Москва: Манн, Иванов и Фербер, 2011. – 240 с.

97. Витковски А. Пятилетка без плана. Украина, 1991-1996: формирование национального государства, экономика, элиты [Текст] / А. Витковски. – Киев: Сфера, 1998. - 240

98. Вишняков О. Інформаційна війна з Росією: уроки виживання [Електронний ресурс] / Олег Вишняков // ICTV: [сайт] — Режим доступу: fakty.ictv.ua/index/read-blog/id/1713.

99. Владиславова Н. Базовые техники НЛП и хорошо сформированный результат [Текст] / Н.Владиславова. - Москва: София, 2011. – 288 с.

100. Власенко И.С. Информационная война: искажение реальности [Текст] / И.С.Власенко, М.В.Кирьянов. – Москва: Канцлер, 2011. – 196 с.

101. Вовкун В. Державна стратегія культурного поступу [Текст] / В. Вовкун // Культура і життя. – №7-8. – 2010. – С. 11–22.

102. Войтасик Л. Психология политической пропаганды [Текст] /Л. Войтасик. – Москва: Прогресс, 1981. – 277 с.

103. Войцехович В.Э. Эволюция культурных ценностей в эпоху глобализации (синергетический подход) [Текст] / В.Э. Войцехович // Межкультурный и межрелигиозный диалог в целях устойчивого развития : материалы международной конференции, (Москва, 13-16 сентября 2007 г.) / под общ. ред. В.К. Егорова. – Москва: РАГС, 2008. – 848 с.

104. Волович О. Інформаційно-психологічні операції США в Іраку [Текст] / О.Волович, Г. Шелест // Ірак на шляху випробувань і відродження. – Одеса: Фенікс, 2010. – С. 114–126.

105. Воронцова Л. В. История и современность информационного противоборства [Текст] /Л.В.Воронцова, Д.В. Фролов. — Москва: Горячая линия - Телеком, 2006. — 192 с.

106. Волковский Н. Л. История информационных войн: т. 1 (с древнейших времён по XIX век), т. 2 (XX век) [Текст] / под ред. И. Петрова. — Санкт-Петербург.: Полигон, 2003. — т.2 736 с.

107. Выдрин Д.И. Политика: история, технология, экзистенция [Текст] / Д.И.Выдрин. – Киев: Лыбидь, 2001. – 432 с.

108. Гаєвський Б.А. Політичне управління [Текст]: навч. посібник / Б.А.Гаєвський, В.А.Ребкало, М.В. Туленков. – Київ: УАДУ, 2001. – 160 с.

109. Галака О. Основні тенденції розвитку та ймовірні форми воєн та збройних конфліктів майбутнього [Текст] / О.Галака, О.Ільяшов, Ю.Павлюк // Наука і оборона. – 2007. -№4. – С.10-15

110. Галфорд Р., Грин Ч., Майстер Д. Советник которому доверяют [Текст] / Р.Галфорд, Ч.Грин, Д.Майстер [пер. с англ. В.Фербер]. – Москва: Манн, Иванов и Фербер, 2009. – 272 с.

111. Гармажапова А. Где живут тролли. Как работают интернет-провокаторы в Санкт-Петербурге и кто ими заправляет [Електронний ресурс] / Новая газета: [сайт]. – Режим доступу: http://www.novayagazeta.ru/society/59903.html

112. Геродот История в девяти томах [Текст] / Геродот. – Москва: АСТ, 1999. – 752.

113. Гетьманець М.Ф., Михайлин І.Л. Сучасний словник літератури і журналістики [Текст] / М.Ф. Гетьманець, І.Л. Михайлин. - Харків: Прапор, 2009. – 384 с.

114. Глотов А. Воспитание «советского человека» как функция культовой литературы соцреализма [Текст] / Александр Глотов // Тернопільський держ. пед. ін-т. Лабораторія славістичних студій. Сер. філософії та методології. – Тернопіль, 1996. – Вип. 2: Суб'єкт пізнання: онтологічні та методологічні аспекти проблеми. – С.135–138.

115. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення [Текст] / Ю.О. Горбань // Вісник НАДУ. – 2015, №1. – С. 136-141

116. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання [Текст]: монографія / В. П. Горбулін, О.Г. Додонов, Д.В. Ланде. – Київ: Інтертехнологія, 2009. – 164 с.

117. Горбулин В. «Гибридная война» как ключевой инструмент российской геостратегии реванша [Електронний ресурс] / Зеркало недели: [сайт], 23.11.2015. Режим доступу: http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html

118. Грачев Г.В. Манипулирование личностью: организация, способі и технологи информационно-психологического воздействия [Текст] / Г.В.Грачев, И.К.Мельник. – Москва: Алгоритм, 2002. – 288 с.

119. Гриняев С. Н. Поле битвы – киберпространство : Теория, приемы, средства, методы и системы ведения информационной войны [Текст] / С. Н. Гриняев. – Минск : Харвест, 2004. – 448 с.

120. Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива [Текст] / С.Н. Гриняев // Агентура.ру.: [сайт] Архивировано из первоисточника 4 июня 2012. - http://www.agentura.ru/

121. Гриняев С.Н. Интеллектуальное противодействие информационному оружию [Текст] / С.Н.Гриняев. – Москва: Изд-во «СИНТЕГ», 1999. – 232 с.

122. Гриценко О. Культурна політика України: короткий історичний огляд [Текст] / О. Гриценко, М. Стріха // Культурна політика: методологічні, правові, економічні проблеми. – Київ: Основи, 1995. – С. 5–26.

123. Гудби Д. Неразделенная Европа. Новая логика мира в американо-российских отношениях [Текст] / Д.Гудби. – Москва: Международные отношения, 2000. – 336 с.

124. Гуляєв О. В. Спін-операції як специфічна форма інформаційного впливу в сучасному політичному процесі [Текст] / О. В. Гуляєв // Гілея:

науковий вісник. Збірник наукових праць. – Київ: ВІР УАН, 2011. – Випуск 44. – С. 548–553.

125. Гуцало Є.П. Ментальність орди [Текст]/ Є.П.Гуцало. – Київ: Києво-Могилянська академія, 2007. – 206 с.

126. Дайзард У. Наступление информационного века. Новая технократическая волна на Западе[Текст] / У.Дайзард. – Москва: Наука, 1988. – 218 с.

127. Далворт М. Социальные сети: руководство по эксплуатации [Текст]/ Майк Далворт [пер. с англ. О.Петрова]— Москва: Добрая книга, 2010. — 248 с

128. Данилова А.А. Манипулирование словом в средствах массовой информации [Текст] / А.А.Данилова. – Москва: Добросвет; Киев: КДУ, 2009. – 234 с.

129. Девриз К. Великие сражения Средних веков 1000 – 1500 [Текст]/ К. Девриз, М. Догерти, Й. Дикки, Ф. Джестайс, К. Йоргенсен [пер. с англ. С.Иванов]. – Москва: Эксмо, 2007. – 224 с.

130. Домарев В. В. Інформаційна зброя: принципи дії та основні види [Електронний ресурс] / В. В. Домарев // Секьюрити: [сайт]. - Режим доступу: http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=729.

131. Дергачов О.П. Партнерський потенціал України: становлення і реалізація [Текст] / О.П.Дергачов. – Київ: Парламентське видавництво, 2009. – 496 с.

132. Діденко Н.Г. Управління, влада, держава: філософські аспекти взаємодії: монографія [Текст] / Н.Г.Діденко. – Донецьк: ДонДУУ, 2005. – 128 с.

133. Дилтс Р. Изменение убеждений с помощью НЛП [Текст] / Р.Дилтс. – Москва: Класс, 1997. – 192 с.

134. Донченко О. Архетипи соціального життя і політика: монографія [Текст] / О.Донченко, Ю.Романенко. – Київ: Либідь, 2001. – 334 с.

135. Дорошко М. Сталінська «селекція» партійно-державної номенклатури УРСР в 1930-ті роки: причини та наслідки [Текст] / М. Дорошко // Україна ХХ ст.: культура, ідеологія, політика. – Київ, 2005. – Вип.8. – С.147–155.

136. Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита [Текст] / Е.Л. Доценко. – Москва: Речь, 2003. – 304 с.

137. Дубас О.П. Інформаційно-комунікаційний простір: культурно-політичні детермінанти: монографія [Текст] /О.П.Дубас. – Київ: Генеза, 2011. – 256 с.

138. Ерасов Б. С. Социальная культурология: учебник для студентов высших учебных заведений [Текст] / Б. С. Ерасов. – Москва: Аспект Пресс, 2000. – 591 с.

139. Егорова-Гартман Е.В. В тумане войны. Наступательные военные коммуникативные технологии [Текст] / Е.В. Егорова-Гартман. – Москва: Николло М, 2010. – 432 с.

140. Ермолова Н. Продвижение бизнеса в социальных сетях Facebook, Twitter, Google+ [Текст] / Н.Ермолова. – Москва: Альпина Паблишер, 2014. – 358 с.

141. Жарков Я. Інформаційно-психологічне протиборство в сучасному світі: проблемно-історичний аналіз [Текст] / Я. Жарков, М. Онищук // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – 14-15. – С. 101–104.

142. Жарков Я. Цілі, напрями проведення інформаційно-психологічних операцій [Текст] / Я. М. Жарков, Л. М. Бєсєдіна // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – Вип. 16. С. 124–130.

143. Жданов І. Україні у XXI столітті: виклики для політичної еліти [Текст] / І.Жданов, Ю.Якіменко // Національна безпека і оборона. – 2004. - №9. – С.2-30

144. Жуков К. Азбука избирательной кампании [Текст] / К.Жуков, А.Карнышев. - Москва: ИМА-пресс, 2001. – 328 с.

145. Журавльов А. В. Інтернет-спільноти у новій хвилі інформаційних війн [Електронний ресурс] / А. Журавльов // Відкриті очі [сайт]. – Режим доступу: http://www.vidkryti-ochi.org.ua/2009/01/blog-post.html.

146. Забурдаева Е.В. Политическое консультирование в США и России: учебное пособие [Текст] / Е.В.Забурдаева. – Москва: Проспект, 2010. – 248 с.

147. Загадарчук Г. М. Культурний простір регіону як чинник формування особистості [Текст] / Г. М. Загадарчук // Культура і сучасність. – Київ, 2000. – № 1. – С.36–41.

148. Запорожець О.Ю. Технології «кольорових революцій» [Текст] / О.Ю. Запорожець // Актуальні проблеми міжнародних відносин. Збірник наукових праць. – 2006. – Випуск 59 (Частина ІІ). – С. 60–67.

149. Захарченко О. О. Нацистська пропаганда про злочини сталінщини напередодні і на початку Другої світової війни / О. О. Захарченко // Науковий вісник Миколаївського державного університету імені В. О. Сухомлинського: збірник наукових праць. – Випуск 21. – С. 121–142.

150. Збройні сили України: реформа 2015 [Електронний ресурс] // Ukraine Military Pages [сайт]. – Режим доступу: http://www.ukrmilitary.com/2015/02/2015_13.html

151. Зеркалов Д. В. Информационные войны [Электронный ресурс] : Хрестоматия / Д. В. Зеркалов [сайт]. – Киев: Рукопись, 2009. – 1 электрон. опт. диск (CD-ROM); 12 см. – Систем. требования : Pentium; 512 Mb RAM; Windows 98/2000/XP; Acrobat Reader 7.0. – Название с тит. экрана.

152. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни [Текст] / В.В. Зеленін. – Вінниця: Віндрук, 2014. – 384 с.

153. Зеленін В.В. Сучасні агітаційно-пропагандиські технології в регіональних виборчих кампаніях: дайджест навчально-методичних рекомендацій [Текст] / В.В.Зеленін. – Киев: ЦСВТ, 2013. – 116 с.

154. Зеленін В. Політична пропаганда як засіб партійного будівництва [Текст] / В. Зеленін, П. Бублик, Б.Мотузенко, Д.Рождественська. – Донецьк: Інноваційний центр соціально-політичних і гуманітарних наук ДонНТУ, ФППР, 2003. – 180 с.

155. Зимичев А.М. Психология политической борьбы [Текст] / А.М.Зимичев. – Санкт-Петербург: Санта, 1993. – 160 с.

156. Зиновьев А.А. Русская трагедия [Текст] / А.А.Зиновьев. – Москва: Алгоритм, 2007. – 608 с.

157. Зирка В.В. Манипулятивные игры в рекламе: лингвистический аспект: монографія [Текст] / В.В.Зирка. – Днепропетровск: Днепропетровский нац. ун-т, ИМА-пресс, 2004. – 290 с.

158. Илларионов С.И. Террор и антитеррор в современном мироустройстве [Текст] / С.И.Илларионов. – Москва: РИЦ ПрофЭко, 2003. – 592 с.

159. Иванов В.Ф. Аспекты массовой коммуникации: монография [Текст] / В.Ф. Иванов. – Киев: ЦВП, 2009. – 190 с.

160. История письменности [Электроний ресурс]// ИнтересNik [сайт]. – режим доступу: http://interesnik.com/istoriya-pismennosti/

161. Информационно-психологическая безопасность в эпоху глобализации: учеб. пособ. [Текст] / под. ред.В. М. Петрик, В. В. Остроухов, А. А.Штоквиш. – Киев: Белоцерковская книжная фабрика, 2008. – 544 с.

162. Исторические аспекты гибридной войны (в американском измерении) [Електронний ресурс] // Борисфен Интел [сайт]. - Режим доступа: http://bintel.com.ua/ru/article/10-AmericanHybridWar/

163. Інтернет становить загрозу для інформаційної безпеки України [Електронний ресурс] // Телекритика (Звіт за підсумками круглого столу «Інформаційна безпека України. Медійний аспект», 30 вересня 2008 р.) [сайт]. Режим доступу: http://www.telekritika.ua/bezpeka/2008-10-24/41481.

164. Інформаційна війна коштує Росії 4$ мільярди [Електронний ресурс] // Укрінформ [сайт]. — Режим доступу: www.ukrinform.ua/ukr.news/2030605

165. Информационная война. Информационное противоборство: теория и практика: монография [Текст]/ под. ред. В. М. Щекотихин, А. В. Королёв, В. В. Королёва. – Москва: Академия ФСО России, ЦАТУ, 2010. – 999 с.

166. Казакова О.М. Політика нацистської Німеччини щодо населення окупованих польських територій 1939 – 1941 рр. [Текст] / О.М. Казакова // Культурологічний вісник: науково-теоретичний щорічник Нижньої Наддніпрянщини. – 2007. – Випуск 18. – С. 41–44.

167. Каплунов Д. Копирайтинг массового поражения [Текст]/ Д.Каплунов. – Санкт-Петербург: Питер, 2012. – 230 с.

168. Как работает фабрика «кремлевских тролей?» [Електронний ресурс] / Gordon.com [сайт]. – Режим доступу: http://gordonua.com/news/worldnews/Kak-rabotaet-fabrika-kremlevskih-trolley-71305.html

169. Кара-Мурза С. Г. Манипуляция сознанием [Текст] / Сергей Кара-Мурза. – Москва: Эксмо, 2008. – 864 с.

170. Кара-Мурза С. Г. Революции на експорт [Текст] / Сергей Кара-Мурза. – Москва: Алгоритм, 2006. – 528 с.

171. Кара-Мурза С.Г. Власть манипуляции [Текст] / С.Г.Кара-Мурза. – Москва: Академ. проект, 2007. – 380 с.

172. Карнеги Д. Как приобретать друзей и оказывать влияние на людей [Текст] / Д.Карнеги. – Москва: Дом славянской книги, 2004. – 590 с.

173. Карнышев А.Д. Психология и технология политического соперничества [Текст] / А.Д.Карнышев, К.С.Жуков, В.Ф.Шестак. – Москва: ИМА-пресс, 2001. – 208 с.

174. Катвалюк А.Л. Социальные технологии [Текст] / А.Л.Катвалюк. – Тернополь: Экономична думка, 2001. – 284 с.

175. Кашников Б.Н. Частные военные компании и принципы «jus in bello» [Текст] /Б.Н.Кашников // Военно-юридический журнал. - № 12. – 2010. - С.27-32

176. Квіт С. Масові комунікації [Текст]: підручник / С.Квіт. - Київ: видавничий дім «Коєво-Могилянська академія», 2008. – 206 с.

177. Квітка О. Комп'ютерні ігри... Це добре чи погано? [Електронний ресурс] / О. Квітка // Нова ера [сайт]. – Режим доступу: http://novaera.te.ua/article_view.php?article=613.

178. Кемаль А. Кибер война. как Россия манипулирует миром [Текст] / А.Кемаль. - Москва: Алгоритм, 2015. – 208 с.

179. Киссейн Э. основы контентной стратегии / перв. англ. П.Миронов. – Москва: Манн, Иванов и Фарбер, 2012. – 125 с.

180. Клаузевиц К. О войне / Карл фон Клаузевиц. – Москва: Эксмо, 2007. – 864 с. [Електронний ресурс]. – Режим доступу: http://menegerbook.net/menegment/1276-karl_fon_klauzevic_o_voiyne_kniga.html.

181. Клименко В. Морально-психологічні аспекти інформаційних війн сучасності [Текст] / В. Клименко // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – 14-15. – С. 104–106.

182. Климовский С. Гибридная война в Украине, как пролог глобальной войны [Електронний ресурс] / С.Климовский // Обозреватель [сайт]. Режим доступа: http://obozrevatel.com/blogs/04827-gibridnaya-vojna-v-ukraine-kak-prolog-globalnoj-vojnyi.htm

183. Князев А. А. Информационная война [Текст] /А.А.Князев // Энциклопедический словарь СМИ. — Бишкек: КРСУ, 2002. – 234 с.

184. Кобиляцький Л.С. Управління проектами[Текст]: навч. посібник / Л.С.Кобиляцький. – Киев: МАУП, 2002. – 200 с.

185. Кожаринова А.Р. Медиа-вирусы как носители идеологических кодов / А.Р.Кожаринова [Електронний ресурс] / Информационный, гуманитарный портал [сайт]. - Режим доступа: http://www.zpu-journal.ru/e-zpu/2013/5/Kozharinova_Media-Viruses/

186. Козер Л.А. Функции социального конфликта [Текст] / Л.А. Козер. – Москва: Идея-пресс, 2000. – 295 с.

187. Козлітін В.Д. Основні напрями світових глобалізаційних процесів кінця XX – початку XXI ст., дискусії між глобалістами та антиглобалістами про їх наслідки /В.Д.Козлітін // Збірник наукових праць. Серія «Історія та географія». – 2004. – Вип.17. – С. 26–30.

188. Колесов Э. Е. Информационная война в военных конфликтах второй половины 21 столетия: исторический аспект [Текст] / Э.Е. Колесов. — Киев: Национальная академия обороны Украины, 2007. – 256 с.

189. Комахидзе И. Российские Силы специальных операций – всё новое это хорошо забытое старое / И.Комахидзе [Електронний ресурс] // Inform Napalm [сайт]. – Режим доступу: https://informnapalm.org/61-rossyjskye-syly-spetsyalnyh-operatsy/

190. Кононов Н. Код Дурова. Реальная история «ВКонтакте» и ее создателя [Текст] / Н.Кононов. – Москва: Манн, Иванов и Фарбер,2012. – 208 с.

191. Коник Д. Расставьте сети. Как использовать Интернет в інтересах вашого бизнеса [Текст] / Д.Коник. С.Рендел. – Киев: ЛИК, 2011. – 120 с.

192. Коньков Н. Война пятого поколения [Електронний ресурс]/ Н.Коньков // Завтра [сайт]. – Режим доступу: http://www.zavtra.ru/content/view/2011-03-1543/

193. Кормич Б. А. Інформаційна безпека: організаційно-правові основи [Текст] / Б. А. Кормич. – Київ: Кондор, 2004. – 384 с.

194. Коровай І. Служба web 2.0 [Електронний ресурс] / І.Коровай // Соціальні мережі [сайт]. – Режим доступу: http://www.socialnetwork.com.ua/2012/02/sluzhba-veb-2-0/

195. Коровин В. Третья мировая сетевая война [Текст] / В.Коровин. – Санкт-Петербург: Питер. 2014. – 352 с.

196. Королько В. Г. Основы паблик рилейшнз[Текст] /В.Г.Королько. – Москва: Рефл-бук; Киев: Ваклер. – 2001. – 528 с.

197. Королько В.Г. Основы паблик рилейшнз [Текст] / В.Г. Королько. – М.: Рефл-бук; Киев: Ваклер. – 2000. – 528 с.

198. Костенко А.А. Современное общество и культурные традиции прошлого (на примере развития китайской цивилизации) [Текст] / А. А. Костенко, А. С. Миносян // Прогресивні ресурсозберігаючі технології та їх економічне обґрунтування у підприємствах харчування. Економічні проблеми торгівлі: збірник наукових праць. – 2003. – С. 681–688.

199. Кочубей Л. О. Виборчі технології [Текст]: навч. посіб. / Л. О. Кочубей. – Київ, 2008. – 331 с.

200. Кочубей Л.О. PR у політичній сфері [Текст]: підручник / Л.О.Кочубей. – Київ: ІПіЕНД ім.. І.Ф.Кураса НАН України, 2013. – 472 с.

201. Кошик А. Веб-аналитика 2.0 на практике. Тонкости и лучшие методики [Текст] / А.Кошик. – Москва: Вильямс, 2011. – 528 с.

202. Кравченко В. В. Національна стратегічна культура у політиці безпеки й оборони Франції [Текст] / В. В. Кравченко // Гілея: науковий вісник. Збірник наукових праць. – 2010. – Випуск 34. – С. 174–178.

203. Кракович Д. Проигрывает ли Украина в информационной войне на своей территории? [Електронний ресурс] / Д. Кракович // Диалог.UA [сайт]. - Режим доступу: http://dialogs.org.ua/ru/project/page9802.html.

204. Крисенко Д. С. США на Близькому Сході межі XX- XXI століть: іракський рахунок [Текст]: монографія / Д. С. Крисенко. – Київ: НАУ, 2011. – 208 с.

205. Кролл А., Пауэр Ш. Комплексный веб-мониторинг [Текст] / [пер. англ. О.Огнева – Москва: Эксмо, 2010. – 768 с.

206. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) [Текст] / В.Г.Крысько. – Минск: Харвест, 1999. – 448 с.

207. Куликов Е.М., Кубиякин Е.О. Слухи как коммуникационный и социокультурный феномен современного общества [Текст] / Е.М. Куликов, Е.О.Кубиякин. – Краснодар: Кубанский гос. ун-т, 2009. – 234 с.

208. Курбан О.В. PR-процес у системі сучасних соціальних комунікацій [Текст] / О.В.Курбан // Інформаційне суспільство. – 2009. – Вип.9. – С. 51-53

209. Курбан О.В. Класифікація соціальних мережевих технологій як PR-інструментів [Текст] / О.В.Курбан // Інформаційне суспільство. – 2013. – Випуск №17. – С.41-43

210. Курбан О.В. Соціальні мережеві комунікаційні технології в структурі сучасниxx інформаційних потоків [Текст] / О.В.Курбан // Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців. Матеріали II Всеукраїнської наукової конференції (Львів, 25-26 жовтня 2013 р.). – Львів: Лігі-Прес, 2013. – С.137-143

211. Курбан О.В. PR-аспекти інформаційної безпеки організаційних структур [Текст] / О.В.Курбан // Вісник книжкової палати. – 2014. – №5. – С.48-51

212. Курбан О.В. Соціальні мережі в роботі сучасного PR-фахівця [Текст] / О.В.Курбан // Вісник Харківської державної академії культури. – 2014. – Вип.44. – С.154-161

213. Курбан О.В. Соціальні мережеві технології: типологія та класифікація [Текст] / О.В.Курбан // Вісник КНУКіМ. Серія “Соціальні комунікації”. –2014. – Випуск 2. – с.48-53

214. Курбан О.В. Стратегія та тактика сучасної інформаційної активності у соціальних мережах [Текст] / О.В.Курбан // Вісник книжкової палати. – 2014. – №9. – С.42-45

215. Курбан О.В. Соціальні мережі як інструмент у галузі PR [Текст] / О.В.Курбан // Вісник книжкової палати. – 2014. – №10. – С.45-47

216. Курбан О.В. Технології та методи оцінки ефективності роботи в соціальних мережах (за матеріалами комплексного SMM-аудиту Київського міського центра зайнятості) [Текст] / О.В. Курбан // Інформаційне суспільство. – 2014. – Вип.20. – С.52-56

217. Курбан О.В. PR у маркетингових комунікаціях [Текст]: навчальний посібник / О.В. Курбан. - Київ: Кондор-Видавництво, 2014. – 246 с.

218. Курбан О.В. Діагностика та моделювання PR-процесів [Текст]: навчальний посібник / О.В.Курбан. - Київ: Українська конфедерація журналістів, 2012. – 160 с.

219. Курбан О. Не треба нам видовищ, дайте хліба [Електронний ресурс] / О.Курбан // Ракурс [сайт]. – Режим доступу: http://ua.racurs.ua/1025-ne-treba-vydovysch-dayte-nam-prosto-hliba#comments

220. Курбан О. Що думають громадяни про реформу децентралізації [Електронний ресурс] / О.Курбан // Ракурс [сайт]. – Режим доступу: http://ua.racurs.ua/1026-scho-dumaie-narod-pro-reformu-decentralizaciyi

221. Куцька О. М. Інформаційно-психологічне протиборство в період конфлікту НАТО-Югославія 1999 року [Текст]: дис... канд. іст. наук: 20.02.22 / Куцька Олеся Миколаївна. – Львів: Львівська політехніка, 2004. – 215 с.

222. Куцька О. М. Інформаційна війна в Югославії під час проведення військової кампанії НАТО [Текст] / О. М. Куцька // Військово-науковий вісник. – 2002. – Випуск 4. – С. 108–122.

223. Лаврик А. Балакучий «спецназ» [Електронний ресурс] / А. Лаврик, Б. Буткевич // Тиждень [сайт]. – Режим доступу: http://tyzhden.ua/Publication/2562.

224. Лавриненко И. Силы специальных операций – основа будущей армии Украины [Електронний ресурс] / И.Лавриненко // Ракурс [сайт]. – Режин доступу: http://racurs.ua/817-sily-specialnyh-operaciy-osnova-buduschey-armii-ukrainy

225. Ластовченко І. О. Зміни соціокультурного середовища в Україні як фактор формування системи цінностей молоді [Текст] / І. О. Ластовченко // Наукові праці МАУП. – 2002. – Вип. 4. – С. 34–36.

226. Лауэр Е. Проигравшие навсегда! [Текст]/ Е. Лауэр // Телекритика. – Київ, 2008. – №10. – С. 12–16.

227. Лебедев-Любимов А.Н. Психология рекламы [Текст] / А.Н. Лебедев-Любимов. – Санкт-Петербург: Питер, 2002. – 368 с.

228. Леонтьєва Л. Інформаційна війна: Україна-Росія – може, вистачить поразок? [Електронний ресурс] / Л. Леонтьєва // Ї – наша позиція [сайт]. Режим доступу: http://www.ji-magazine.lviv.ua/position/2000/leontjeva-iv.htm.

229. Леонтьєва Л. Зброєю масованого ураження почуттів і розуму[Текст] / Л.Леонтьева // Віче. – 2004. – № 1.

230. Леонтьєва Л. Інформаційно-психологічний вплив: теоретико-методологічні засади аналізу [Текст] / Л.Леонтьева // Людина і політика. – 2004. – № 5.

231. Лесів Ксеня Російський режисер приїхав до Києва розповісти українцям, що їх не існує [Електронний ресурс] / Ксеня Лесів // УНІАН [сайт]. – Режим доступу: http://www.unian.ua/news/309370-rosiyskiy-rejiser-prijihav-do-kieva-rozpovisti-ukrajintsyam-scho-jih-ne-isnue.html.

232. Лешкевич Т.Г. Проблемы социокультурной самоидентификации в контексте коммуникации и глобализационных процессов [Текст] / Т.Г. Лешкевич, Л.В. Евсеева // Межкультурный и межрелигиозный диалог в целях устойчивого развития: материалы международной конференции, (Москва, 13-16 сентября 2007 г.) / под общ. ред. В.К. Егорова. – М. : РАГС, 2008. – 848 с.

233. Лігачова Н. Телебачення спецопераций [Текст] /Н.Лігачова, С.Черненко, В.Іванов. – Київ: ТелеКритика, 2003. – 266 с.

234. Ливинская Н. Частные военные компании: вчера, сегодня, завтра [Текст] / Н.Ливинская // Атташе. – 2007. - №2. – С.96-103

235. Лисенко В. Чутки – активний засіб модифікації суспільної свідомості [Текст] / В.Лисенко // Політичний менеджмент. – 2004. - № 6. – С. 96-102

236. Лисичкин В. А. Третья мировая информационно-психологическая война [Текст] / В.А.Лисичкин, Л.А.Шелепин. — Москва: Академия социальных наук, 1999. – 207 с.

237. Литвиненко О. Інформаційний простір та його захист: теорія і практика [Текст] / О. Литвиненко // Віче. – Київ, 2000. – № 10. – С. 119–127.

238. Литвиненко О.В. Інформаційний вплив та операції: теоретико-аналітичні нариси: монографія [Текст] / О.В. Литвиненко. – Київ: НІСД, 2003. – 240 с.

239. Литвиненко О. Проблеми захисту від масованих інформаційних операцій [Електронний ресурс] / О. Литвиненко // Національний інститут стратегічних досліджень [сайт]. – Режим доступу: http://www.niss.gov.ua/book/Litv/009_1.htm#a1.

240. Литвиненко О. Система захисту інформаційного простору від спеціальних інформаційних операцій [Електронний ресурс] / О. Литвиненко // Національний інститут стратегічних досліджень [сайт]. – Режим доступу: http://www.niss.gov.ua/book/Litv/010_1.htm#a1.

241. Литвак Б.Г. Разработка управленческого решения [Текст]: учебник / Ю.Литвак. – Москва: Дело, 2002. - 392

242. Логунов А. Зарубежные негосударственные субъекты военно-политических отношений в XXI веке [Текст] /А.Логунов // Зарубежное военное обозрение. - № 3 (708), март 2006. - стр.2-11

243. Луковенко І. Г. Ідеологічні засади державної політики СРСР

(УРСР) щодо Руської православної церкви (40-і – 60-і рр. XX ст.) [Текст] / І. Г. Луковенко // Роль науки, релігії та суспільства у формуванні моральної особистості. – Донецьк, 2005. – С. 46–49.

244. Лунеев В.В. Терроризм и организованная преступность в условиях глобализации мира [Текст] / В.В.Лунеев, В.Н.Кудрявцев, В.Е.Петрищев // Борьба с тероризмом. – Москва: Наука, 2004. – С. 134-145

245. Магда Є. Гібрида війна. Вижити і перемогти [Текст] / Є.Магда. – Київ: Віват, 2015. – 304 с.

246. Майерс Д. Социальная психология [Текст] / Д.Майерс. – Санкт-Петербург: Питер, 1997. – 688 с.

247. Макклелланд Д. Мотивация человека [Текст] / Д. Макклелланд. - Санкт-Петербург: Питер, 2007. – 672 с.

248. Макконнелл Б. Эпидемия контента: маркетинг в социальных сетях и блогосфере [Текст] / Б. Макконнелл, Д.Хуба. – Москва: Вершина, 2008. – 234 с.

249. Мак-Люен М. Галактика Гутенберга: становлення людини друкованої книги [Текст] / М.Мак-Люен. – Київ: Ніка-Центр, 2001. – 464 с.

250. Маклюэн Г.М. Понимание Медиа: внешнее расширение человека [Текст] / Г.М.Маклюэн. – Москва: Канон-пресс-Ц, 2003. - 464 с.

251. Манжола В.А. Нейтралітет та позаблоковість у європейський системі міжнародних відносин: монографія [Текст] / В.А. Манжола, В.М.Вдовенко. – Київ: Вид-во Київського ун-ту, 2007. – 167 с.

252. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны [Текст] / А.В.Манойло, А.И.Петренко, Д.Б.Фролов. — Москва: Горячая линия - Телеком, 2012. — 542 с.

253. Малик Я. Інформаційна війна і Україна [Електронний ресурс] /Я.Малик // Демократичне врядування: науковий вісник. – 2015. – вип.15. - Режим доступу: http://webcache.googleusercontent.com/search?q=cache:2JYjGcIKKMUJ:irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAGE_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF/DeVr_2015_15_3.pdf+&cd=1&hl=uk&ct=clnk&gl=ua

254. Манн *С.* Реакция на хаос [Электронный ресурс] /С.Манн // Интелросс [сайт]. – Режим доступу: www.intelros.ru/index.php?newsid=175

255. Маначинский А. Я. Югославия: приговор вынесен [Текст] / А. Я. Маначинский. – Киев: Румб, 2005. – 288 с.

256. Маначинский А. Я. Ирак: тайные пружины войны [Текст]/ А. Я. Манчинский. – Киев: РУМБ, 2005. – 416 с.

257. Мандаты и правовые основы [Електронний ресурс] // Операции ООН по поддержанию мира [сайт]. – Режим доступу: http://www.un.org/ru/peacekeeping/operations/pkmandates.shtml

258. Мартьянов О. Частные военные компании США: предназначение и роль в военных конфликтах[Текст] / О.Мартьянов // Зарубежное военное обозрение. - № 5 (770). - 2011. - С.8-13

259. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України [Текст] / Олександр Маруненко // Освіта регіону. Політологія, психологія, комунікації. Український науковий журнал. — 2011. — № 4. — С. 92.

260. Марущенко В. Информационная безопасность войск и защита личного состава от негативного информационного воздействия [Текст] / В. Марущенко // Ориентир. – 2001. – № 2. С. 50–53.

261. Матвєєв Ю. М. Розпад Югославії як етап створення нового світопорядку [Текст] / Ю. М. Матвєєв //Науковий вісник Миколаївського державного університету. – Миколаїв: МДУ, 2005. – Вип. 11. – С. 209–214.

262. Мелин А. Развитие форм и способов ведения военных действий в начале XXI века [Текст] / А.Мелин // Зарубежное военное обозрение. – 2003. - №4. – С.25-28

263. Мединский В.Р. Особенности национального пиара. PRавдивая история Руси от Рюрика до Петра [Текст]/ В.Р.Мединский. – Москва: ОЛМА Медиа Групп, 2010. – 624 с.

264. Мезенцев Я. Ирак. Война в эфире [Текст] / Я.Мезенцев // Неизвестная разведка. – 2005. - №3-4. – С.26-32

265. Миллер П. Роевой интеллект: Муравьи, пчелы и птицы способны многому нас научить [Текст] / П. Миллер // National Geographic Россия. — 2007. — № 8. — С. 88—107.

266. Миллер М. YouTube для бизнеса. Эффективный маркетинг с помощью видео[Текст] / [пер. с англ. М.Фербер]. – Москва: Манн, Иванов и Фербер, 2012. – 330 с.

267. Михайлюк О. В. Про деякі особливості соціальної психології часів революції та громадянської війни (1917–1920 рр.) [Текст] / О. В. Михайлюк // Дніпропетровський держ. ун-т. Збірник наукових праць молодих вчених. – Дніпропетровськ, 1999. – Вип.1: Історія. – С. 85–93.

268. Миронова Т. Л. Как из нас делают быдло (о технологии информационного террора) [Текст] / Т.Л.Миронова. — Москва: Люберецкая газета, 2000. — 48 с.

269. Миротворцы ОДКБ готовы к возможности участия в миссии на Украине [Электронный ресурс] // РИА Новости [сайт]. – Режим доступа: http://ria.ru/world/20140829/1021900972.html

270. Мисюров Д.А. Политика и символы [Текст] / Д.А.Мисюров. – Москва: РИП-холдинг, 1999. – 124 с.

271. Мичковская Н. Принудительные ценности [Электронный ресурс]/ Н. Мичковская // СЕЙЧАС [сайт]. Режим доступа: http://times.liga.net/articles/gs012913.html.

272. Міжнародна інформаційна безпека: сучасні виклики та загрози [Текст] / за аг. редакцією С.М.Іванов. – Київ: Центр вільної преси, 2006. – 916 с.

273. Мілютіна К.Л. Траєкторії життєвого шляху особистості в динамічному середовищі [Текст]: монографія / К.Л.Мілютіна. – Ніжин: Аспект-Поліграф, 2012. – 298 с.

274. Міщенко М. Перші підсумки газової війни: перемоги і втрати [Електронний ресурс] / М. Міщенко // УНІАН [сайт]. – Режим доступу: http://www.unian.ua/news/294730-pershi-pidsumki-gazovoji-viyni-peremogi-i-vtrati.html.

275. Мошес А. Россия-Украина: проблемы взаимоотношений [Текст] / А.Мошес // Современная Европа. – 2000. - №3. – С.63-73

276. Мухин А. А. Информационная война в России [Текст]/ А.А. Мухин. — Москва: ГНОМ и Д, 2000. — 256 с.

277. Назаренко Т.В. Українська національна культура: проблеми та перспективи розвитку в сучасному суспільстві [Текст] / Т.В. Назаренко // Проблеми самоідентифікації сучасного українського суспільства: політичні, економічні, соціальні та культурні аспекти. – 2009. – С. 93–98.

278. Назаретян А.П. Агрессивная толпа, массовая паника, слухи. Лекции по социальной и политической психологии [Текст] / А.П.Назаретян. – Москва: Питер, 2004. – 190 с.

279. Назаретян А.П. Психология стихийного массового поведения: Лекции [Текст] / А.П.Назаретян. – Москва: ПЭР СЭ, 2001. – 112 с.

280. Найбільше книг видається в Києві та Харкові [Електронний ресурс] // Урядовий портал [сайт]. – Режим доступу:http://www.kmu.gov.ua/control/uk/publish/article?art_id=245563969.

281. Наумова Л. Фактор екранного видовища. Культурні трансформації [Текст] / Л. Наумова // Мистецтвознавство України : збірник наукових праць. – 2005. – Вип. 5. – С. 181–189.

282. Националисты подадут в суд на создателей фильма "Война 08.08.08" [Электронный ресурс] // РИА НОВОСТИ [сайт]. Режим доступу: http://www.rian.ru/society/20081120/155539614.html.

283. Некоторые аспекты российско-украинских отношений. События на Севере Кавказе: мнение жителей Украины и России [Електронний ресурс] // Research & Branding Group [сайт]. – Режим доступу:
http://www.rb.com.ua/rus/politics/group-3353/.

284. Нечаєва-Юрійчук Н. До питання про причини та ймовірні наслідки грузино-російського конфлікту у серпні 2008 року[Текст] / Н.Нечаєва-Юрійчук // Історична панорама: Збірник наукових статей ЧНУ. – Чернівці: Рута, 2008. – С. 157–165.

285. Нікішенко Ю.І. Поняття «етнічна культура» і традиційна культура в етнокультурології [Текст] / Ю.І. Нікішенко // Наукові записки. – 2004. – т.24. – С. 5–12.

286. Новиков В. К. Информационное оружие - оружие современных и будущих войн [Текст] / В.К. Новиков. — Москва: Горячая линия-Телеком, 2013. — 264 с.

287. Оганов А. А. Исторические судьбы национальных культур в эпоху глобализации [Текст] / А. А. Оганов, И. Г. Хангельдиева // Межкультурный и межрелигиозный диалог в целях устойчивого развития : материалы международной конференции, (Москва, 13-16 сентября 2007 г.) / под общ. ред. В.К. Егорова. – Москва: РАГС, 2008. – 848 с.

288. ОДКБ хочет отправить своїх миротворцев в Донбасс [Електронний ресурс] // Цензор.нет [сайт]. – Режим доступу: http://censor.net.ua/news/329200/odkb_hochet_otpravit_svoih_mirotvortsev_na_donbass

289. Одноколенко О. Гибридная война: проблемы и перспективы постконфликтного урегулирования [Електронний ресурс] // Независимое военное обозрение [сайт]. Режим доступа: http://nvo.ng.ru/concepts/2015-03-13/1_gybrid.html

290. Окара А. Спасибо Василю Волге и Александру Голубу за... Голодомор А. Окара [Електронний ресурс] // Українська правда. Блоги. Блог Андрія Окари [сайт]. Режим доступу:
http://blogs.pravda.com.ua/authors/okara/491ac48079e1f/.

291. Олійник О. Державна інформаційна політика та інформаційна безпека України: політико-правові аспекти [Текст] / О.Олійник // Право України. – 2005. – № 5. – С. 108–111.

292. Ольшанский Д.В. Политический консалтинг[Текст] / Д.В.Ольшанский. – Санкт-Петербург: Питер, 2005. – 448 с.

293. Онищук М. І. Вибір об’єктів і врахування їх психологічних особливостей в період підготовки і проведення інформаційно-психологічних операцій [Текст] / М.І. Онищук // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – Вип. 11. С. 106–109.

294. Онищук М. І. Особливості психологічного впливу в ході проведення психологічних операцій [Текст] / М. І. Онищук, Я. М. Жарков // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – Вип. 16. С. 136–139.

295. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник [Текст] / В. Б. Вепринцев, А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – Москва: Горячая линия – Телеком, 2005. – 495 с.

296. «Операція «Галичина» – українофобська гра [Електронний ресурс] // офіційний сайт ВО «Свобода» [сайт]. – Режим доступу: http://www.svoboda.org.ua/dokumenty/zayavy/002224/.

297. «Операція Галичина»: Російська комп’ютерна гра пропонує придушити повстання українців [Електронний ресурс] // Портал Українця

[сайт]. – Режим доступу: http://www.vox.com.ua/data/2005/07/11/operatsiya-galychyna-rosiiska-komp-yuterna-gra-proponuye-prydushyty-povstannya-ukraintsiv.html

298. ОПЕРАЦІЯ Ы: Проти нас ведеться щоденна інформаційна війна [Електронний ресурс] // Майдан-ІНФОРМ [сайт]. – Режим доступу: http://maidan.org.ua/static/news/2007/1216638627.html.

299. Описание книги Глеба Боброва «Эпоха мертворожденных [Электронный ресурс] // OZON.ru [Текст]. – Режим доступа: http://www.ozon.ru/context/detail/id/4016584/.

300. Орбан-Лембрик Л. Е. Соціальна психологія[Текст] / Л.Е. Орбан-Лембрик. – Київ: Академвидав, 2003. – 446 с.

301. Остапенко Г.А. Информационные операции и атаки в социотехнических системах[Текст] / Г.А.Остапенко. — Москва: Горячая линия - Телеком, 2007. — 134 с.

302. Основи інформаційного права України [Текст] / В. С. Цимбалюк, В. Д. Гавловський, В. В. Гриценко та ін. – Київ: Знання, 2004. – 274 с.

303. Павловська С. Інформаційно-психологічний вплив як фактор досягнення мети в ході воєнних дій [Текст]/ С.Павловська // Воєнна історія. – 2008. - №5. – С. 126-136

304. Пазенок В. Цінності китайської філософської культури: сучасність і традиція [Текст] / В. Пазенок // Збірник наукових праць. – 2006. – Вип. 48. – С. 88–95.

305. Панарин И. Н. Информационная война и дипломатия [Текст] / И.Н.Панарин. — Москва: Городец, 2004. — 528 с.

306. Панарин И.Н. Информационная война и геополитика[Текст] / И.Н.Панарин. – Москва: Поколение, 2006. – 506 с.

307. Панарин И.Н. Информационная война, PR и мировая политика [Текст] / И.Н.Панарин. – Москва: Горячая линия - Телеком, 2006. – 264 с.

308. Панарин И. Н. Информационная война и мир [Текст] / И.Н.Панарин. Л.И Панарина. — Москва Олма-Пресс, 2003. — 384 с.

309. Панарин И. Н. Технология информационной войны [Текст]/ И.Н.Панарин. — Москва: КСП+, 2003. — 320 с.

310. Панарин И.Н. СМИ, пропаганда и информационные войны [Текст]/ И.Н.Панарин. – Москва: Поколение, 2012. – 411 с.

311. Панкратов В.Н. Уловки в спорах и их нейтрализация [Текст]: методическое пособие / В.Н.Панкратов. – Москва: Дельта, 1996. – 52 с.

312. Панов М. Военные конфликты на рубеже 2030 года [Текст] / М.Панов, В.Маневич // Зарубежное военное обозрение. – 2008. – №1. – С. 3-15

313. Пашков М. Відносини Україна – НАТО у фокусі громадської думки [Текст] / М.Пашков, В.Чалий // Національна безпека і оборона. – 2002. - №8. – С.50-60

314. Перепелиця І.М. Конфлікти в посткомуністичній Європі [Текст] / Г.М. Перепелиця. – Київ: Національний ін-т стратегічних досліджень, 2003. – 432 с.

315. Пелагеша Н. Україна у смислових війнах постмодерну: трансформація української національної ідентичності в умовах глобалізації [Текст] / Н. Пелагеша. – Київ: НІСД, 2008. – 288 с.

316. Петрик В. М. Сучасні технології та засоби маніпулювання інформаційних війн і спеціальних інформаційних операцій [Текст]: навчальний посібник / В.М. Петрик, О.І. Штоквиш, В.В. Кальниш, В.І. Полевий, В.В. Остроухов. – Київ: Росава, 2006. – 207 с.

317. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / Валентин Петрик [сайт]. — Режим доступу : www.justinian.com.ua/article.php.

318. Переслегин С. О влиянии литературы на общество и об ответственности писателя [Электронный ресурс] / С. Переслегин // Интерпресскон [сайт]. – Режим доступа:http://www.rusf.ru/interpresscon/1998/doclad/do98prsl.htm.

319. Подкур Р. Ю. Деякі стереотипи світогляду чекістів під час «великого терору» (1937 – 1938 рр.) [Текст] / Р. Ю. Подкур // Наукові праці історичного факультету. – Запоріжжя, 2008. – Вип. 23: Політична еліта в історії України. – С. 255–263.

320. (48) Прокофьев В. Ф. Тайное оружие информационной войны: атака на подсознание [Текст] / В.Ф.Прокофьев. - Москва: СИНТЕГ, 2003, 408 с.

321. Полянський П. Освіта як об’єкт інформаційної війни Росії проти України і як ресурс протидії такій війні [Електронний ресурс] / П. Полянський [сайт]. — Режим доступу : maidanua.org/2015/03.

322. Потеряхин А.Л. Информационно-психологическое воздействие: к определению понятия [Текст] / А.Л. Потеряхин // Інформаційна безпека людини, суспільства, держави. – 2009. – №2 (2). – С. 28–32.

323. Почепцов Г.Г. Информационно-политические технологи [Текст] / Г.Г. Почепцов. – Москва: Центр, 2003. – 384 с.

324. Почепцов Г. Г. Информационно-психологическая война [Текст] / Г. Г. Почепцов. – Москва: СИНЕГ, 2000. – 180 с.

325. Почепцов Г.Г. Теория и практика информационных войн [Текст] / Г. Г. Почепцов. – Ровно: Волинські обереги, 1999. – 124 с.

326. Почепцов Г.Г. Теория и практика коммуникации (от речей президентов до переговоров с террористами) [Текст] / Г.Г. Почепцов. - Москва: Центр, 1998. – 352 с.

327. Почепцов Г.Г. Психологические войны [Текст] / Г.Г. Почепцов. - Москва: Рефл-бук; Київ: Ваклер, 2000. – 576 с.

328. Почепцов Г.Г. Коммуникативные технологи двадцятого века [Текст] / Г.Г.Почепцов. – Москва: Рефл-бук; Киев: Ваклер, 1999. – 352 с.

329. Почепцов Г. Г. Информационные войны. Основы военно-коммуникативных исследований [Текст] / Г.Г.Почепцов. — Москва: Рефл-бук, Киев: Ваклер, 2000. — 576 с.

330. Почепцов Г. Від Facebook'у і гламуру до Wikileaks: медіа комунікації [Текст] / Г.Г.Почепцов. – Київ: Спадщина, 2012. – 464 с.

331. Почепцов Г. Анатомия гибридной войны [Электронный ресурс] / Украина криминальная [сайт]. Режим доступа: http://cripo.com.ua/?sect_id=8&aid=199931

332. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/

333. Почепцов Г.Г. Пропаганда и контрпропаганда [Текст] / Г.Г.Почепцов. – Москва: Центр, 2004. – 252 с.

334. Почепцов Г.Г. Символы в политической рекламе [Текст] / Г.Г.Почепцов. – Київ: Принт Сервис, 1997. – 323 с.

335. Прибутько П.С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах [Текст] / П.С. Прибутько, І.Б. Лук'янець. – Київ: Вид. А. В. Паливода, 2007. – 252 с.

336. Приходько А.Я. Информационная безопасность в событиях и фактах [Текст] / А.Я.Приходько. – Москва: СИНЕГ, 2001. – 260 с.

337. Приходько А.Я. Словарь-справочник по информационной безопасности [Текст] / А.Я.Приходько. – Москва: СИНЕГ, 2001. – 124 с.

338. Присяжнюк М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування [Текст] / М. Присяжнюк, Я. Жарков // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – № 14-15. С. 42–44.

339. Прокофьев В.Ф. Тайное оружие информационной войны [Текст] / В.Ф. Прокофьев. – Москва: СИНТЕГ, 1999. – 152 с.

340. Прокофьев В.Ф. Тайное оружие информационной войны: атака на подсознание [Текст] / В.Ф. Прокофьев.– Москва: СИНТЕГ, 2003. – 408 с.

341. Проти України ведеться інформаційна війна з дискредитації підготовки до Євро-2012 [Електронний ресурс] // ZAXID.NET [сайт]. – Режим доступу: http://zaxid.net/home/showSingleNews.do?proti_ukrayini_vedetsya_informatsiyna_viyna_z_diskreditatsiyi_pidgotovki_do_yevro2012__surkis&objectId=1061926.

342. Радковець Ю. Гібридна політика сучасної Росії [Електронний ресурс] /Ю. Радковець // Урядовий кур'єр [сайт]. – 2015. – 20 жовтня. – Режим доступу: http://ukurier.gov.ua/uk/articles/gibridna-politika-suchasnoyi-rosiyi/

343. Радковець Ю. «Гибридная политика» современной России как стратегия реализации ее национальной геополітики [Електронний ресурс] / Ю.Радковец / Борисфен Интел [сайт]. – Режим доступу: http://bintel.com.ua/ru/article/gibrid-politics/

344. Райт Дж. Блог-маркетинг: Новый рэволюционный путь увеличения продаж, усиления потенциала бренда и достижения выдающихся результатов в би знесе[Текст] / Дж.Райт. – Москва: Эксмо, 2008. – 243 с.

345. Рассел Дж. Веб-аналитика[Текст] / [пер. с англ.] – Москва: Книга по Требованию, 2013. – 106 с.

346. Расторгуев С. П. Введение в формальную теорию информационной войны [Текст] / С.П.Расторгуев. – Москва: Вузовская книга, 2002. – 120 с.

347. Расторгуев С. П. Информационная война [Текст] / С.П.Расторгуев. — Москва: Радио и связь, 1999. — 416 с.

348. Райхель Ю. Призначення ворогом. Антиукраїнська істерія викликана внутрішніми проблемами Росії [Електронний ресурс] // День [сайт]. – Режим доступу: http://www.day.kiev.ua/201758

349. Райан М. Энциклопедия сил специального назначения [Текст] / М. Райан, К.Мэнн, А.Стилуэлл. –Москва: Эксмо, 2004. – 256 с.

350. Рашкофф Д. Медиавирус. Как поп-культура тайно воздействует на ваше сознание [Текст] / Д. Рашкофф; [пер. с англ. Д. Борисова]. – Москва: Ультра.Культура, 2003. – 368 с.

351. Рашкофф, Д. Вступление. Характер заражения [Электронный ресурс] // Дуглас Рашкофф. Медиавирус [сайт]. – Режим доступа: http://mediavirus.narod.ru/02.html

352. Рижков М.М. Інформаційний потенціал України в міжнародних відносинах [Текст]: монографія / М.М.Рижков, Кучмій О.П., Бєлоусова Н.Б., Є.А. Макаренко, О.М. Фролова, І.А.Кост, Г.А.Піскорська, Н.О. Піпченко. – Київ: Центр вільної преси, 2014. – 284 с.

353. Рогоза С. Засекреченные войны [Текст] / С.Рогоза. – Москва: Полигон, 2004. – 558 с.

354. Романишин Ю. Форми друкованої пропаганди УПА: способи виготовлення та розповсюдження [Текст] / Ю. Романишин // Збірник праць Науково-дослідного центру періодики. – Львів, 2003. – Вип.11. – С.105–119.

355. Романюк О. Посткомуністичні революції [Текст] /О.Романюк // Політичний менеджмент. – 2005. - №4. – С.16-28

356. Росія не припиняє інформаційної війни проти Києва [Електронний ресурс] // OtherSide [сайт]. – Режим доступу: http://otherside.com.ua/news/print.php?id=58978&lang=1.

357. Росія проти майдану: історія інформаційної війни [Електронний ресурс] // І.Преса [сайт]. — Режим доступу: http://www.ipress.ua/mainmedia/rosiya_proty_maydanu_istoriya_informatsiynoi_viyny_58729.html

358. Росія розгорнула інформаційну війну проти України з брехнею і маніпуляціями [Електронний ресурс] // ТСН [сайт]. — Режим доступу: http://www.tsn.ua/politika/rosiya-rozgornula-informaciynu-viynu-proti-ukrayuni-z-brehneyu-i-manipulyaciami-338574.html

359. Россия открыто набирает антиукраинских «троллей» [Електронний ресурс] // Цензор.net [сайт]. – Реждим доступу: http://censor.net.ua/news/319106/rossiya_otkryto_nabiraet_antiukrainskih_trolleyi

360. Россия ведет гибридную войну гибридной армией [Електронний ресурс] // InformNapalm [сайт]. Режим доступу: https://informnapalm.org/6631-gibridnaja-vojna-armija

361. Ротовский А.А. Системний PR [Текст]/ А.Ротовский. – Дніпропетровськ: Баланс Бізнес Букс, 2006. – 256 с.

362. Роуз Р. Управление контент-маркетингом. практическое руководство по созданию лояльных аудиторий для вашего бизнеса [Текст] / [пер. англ. В.Манн] . – Москва: Манн, Иванов и Фербер, 2014. – 240 с.

363. Румунія проти України [Електронний ресурс] // Главред [сайт]. – Режим доступу: http://ua.glavred.info/archive/2008/10/22/184222-2.html.

364. Рудич Ф.М. Много ли власти нужно власти? Украина в контексте трансформации политических систем в странах СНГ и Балтии, Центральной и Восточной Европы [Текст] / Ф.М.Рудич. – Киев: Наукова Думка, 2009. – 300 с.

365. Русак І.С. Розвиток форм і засобів ведення інформаційної боротьби на сучасному етапі [Текст]/ І.С.Русак, В.М.Телелим // Наука і оборона. – 2000. – №2. – С.18-23

366. Рыбаков Б.А. Язычество древних славян [Текст] / Б.А. Рыбаков. – Москва: Академический проект, 2013. – 627 с.

367. Саєнко О.Г. Інформаційна війна як прояв інформаційного протиборства [Текст] / О.Г. Саєнко, С.Л. Степаниця // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – Вип. 12. – С. 142–147.

368. Савош Я. Як ефективно гугнити та перевіряти інформацію [Электронный ресурс] // Media Sapiens [сайт]. - Режим доступу: http://osvita.mediasapiens.ua/mediaprosvita/how_to/yak_efektivno_gugliti_y_perevir yati_informatsiyu/

369. Сас П. М. Політична міфологема козацтва в українській книжності початку 20-х рр. XVII ст. [Текст] / П. М. Сас // Запорозьке козацтво в українській історії, культурі та національній самосвідомості. – Київ; Запоріжжя, 1997. – С. 237–248.

370. Сватко Я. Національна безпека України в умовах ведення інформаційних війн [Електронний ресурс] / Я. Сватко // Західна аналітична группа [сайт]. - Режим доступу: http://zgroup.com.ua/print.php?articleid=1606.

371. Светлов В.А. Конфликт: модели, решения, менеджмент [Текст]/ В.А.Свтлов. – Санкт-Пттербург: Питер, 2005. – 540 с.

372. Семенюк Г. С. Медіавіруси на тлі еволюційних процесів медіапростору: суть і проблематика [Текст] / Г. С. Семенюк // Інформаційне суспільство. –2012. – Вип. 15. – С. 46–51.

373. Сенаторов А. Битва за подписчика "ВКонтакте". SMM-руководство [Текст] / А.Сенаторов. – Москва: Альпина Паблишер, 2016. – 168 с.

374. Сенченко М. Стратегія «Керованого хаосу» - головний складник інформаційно-економічної війни в Україні [Електронний ресурс] / М.Сенченко // Персонал плюс [сайт]. - № 22 (173). – 2006. – Режим доступу: http://www.personal-plus.net/173/746.html

375. Сенявская Е.С. «Образ врага» в сознании участников Первой мировой войны [Текст] / Е.С. Сенявская // Россия и Европа в XIX-XX веках: проблемы взаимовосприятия народов, социумов, культур. Сборник научных трудов. – 1996. – С. 75 – 85.

376. Сергацкова Е. Война на три буквы. Между внутренним конфликтом и внешним вмешательством: хроника противостояния в репортажах и свидетельствах [Текст] / Е.Сергацкова, А.Чапай, В.Максаков. – Харьков: Фолио, 2015. – 381 с.

377. Серебрянников В.В. Социология войны [Текст]/ В.В.Серебрянников. – Москва: Научный мир, 1997. – 398 с.

378. Серновиц Э. Сарафанный маркетинг. Как умные компании заставляют о себе говорить [Текст] / Э.Серновиц. – Москва: Манн, Иванов и Фербер, 2012. – 210 с.

379. Сідак В. С. Спецслужба держави без території: люди, події, факти [Текст] / В. С. Сідак, Т. В. Вронська. – Київ: Темпора, 2003, 2003. – 240 с.

380. Силы специальных операций (ССО) [Електронний ресурс] // Министерство обороны Российской Федерации [сайт]. – Режим доступа: http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14234@morfDictionary

381. Ситуационный аналіз в свіязях с общественностью [Текст]: ученик / Л.В. Азарова, В.А. Ачкасова, К.А. Иванова. - Санкт-Петербург: Питер, 2009. – 256 с.

382. Слипченко В.И. Войны шостого поколения: оружие и военное искусство будущого [Текст] / В.И.Слипченко. – Москва: Вече, 2002. – 384 с.

383. Слюсаревський М. М. Інформаційний простір: критика існуючих визначень і спроба побудови теорії [Текст] / М. М. Слюсаревський // Харківський держ. ун-т. Вісник. – Харків, 1999. – № 439, ч.4, 5: Сер. Психологія, політологія: Особистість і трансформаційні процеси у суспільстві. – С. 337–342.

384. Слюсаренко А. В. Особливості проведення психологічних операцій в зоні перської затоки (1990-1991) та в Іраку (2003) [Текст] / А. В. Слюсаренко, В. І. Дивень // Збірник наукових праць. – Київ: Національна академія оборони України, 2004. – С. 60–68.

385. Снігур С. Особливості формування моралі та моральності в культурі Київської Русі-України [Текст] / Світлана Снігур // Тернопільський держ. пед. ун-т ім. В. Гнатюка. Наукові записки. Сер.: Філософія. – Тернопіль, 2000. – Вип.5. – С. 71–77.

386. Собор: підписання «мовного закону» означає дискримінацію українців [Електронний ресурс] // УНІАН [сайт]. – Режим доступу:

http://www.unian.ua/news/519530-sobor-pidpisannya-movnogo-zakonu-oznachae-diskriminatsiyu-ukrajintsiv.html.

387. Соловьев В. Первая «мятежвойна» практически завершена [Текст] / В. Соловьев // Независимое военное обозрение. – 2001. - №47. – С.1-2

388. Соловьев В.Р. Манипуляции: атакуй и защищайся! [Текст]/ В.Р.Соловьев. – Москва: Эксмо. – 352 с.

389. Сороченко В. Кино как средство информационно-психологической войны [Электронный ресурс] / В. Сороченко // Энциклопедия методов пропаганды [сайт]. - Режим доступа: http://psyfactor.org/kinoprop/kino.htm.

390. Сотников Г. Деятельность американских охранных фирм в Ираке [Текст] /Г.Сотников // Зарубежное военное обозрение. - № 12 (729). - 2007. – С. 76

391. Сохань Л.В. Маргіналізація особистості в контексті глобалізації [Текст] / Л.В. Сохань // Українське суспільство: десять років незалежності. – 2001. – С. 307–315.

392. Социальные коммуникации (теория, методология, деятельность [Текст]: словар-справочник / [под. редакцией В.А. Ильганаевой]. – Харьков: Городская типография, 209. - 392 с.

393. Степанов Ю.Г. Сражения, изменившие ход истории: 1945 – 2004 [Текст] / А. В. Баранов, А. А. Герман, Д. М. Креленко, Е. Ю. Лыкова, Ю. Г. Степанов. – Саратов: Лицей, 2005. – 560 с.

394. Стелзнер М. Контент-маркетинг. Новые методы привлечения клиентов в эпоху Интернета [Текст] / [пер. англ. В.Манн]. – Москва: Манн, Иванов и Фербер, 2012. – 288 с.

395. Стратегия и тактика в контексте военной агрессии России [Електронний ресурс] // Борисфен Интел [сайт]. - Режим доступа: http://bintel.com.ua/ru/article/gibrid-war/

396. Субботін С. О. Неітеративні, еволюційні та мультиагентні методи синтезу нечіткологічних і нейромережних моделей [Текст]: монографія / Під заг. ред. С. О. Субботіна. — Запоріжжя: ЗНТУ, 2009. — 375 с.

397. Сурмин Ю.П. Теория социальных технологий [Текст]: учебное пособие / Ю.П. Сурмин, Н.В. Туленков. – Киев: МАУП, 2004. – 608 с.

398. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій [Текст]: навч. посіб. / под. ред. В. М. Петрик, О. А. Штоквиш, В. І. Полевий – Киев: Росава, 2006. – 208 с.

399. Тапскотт Д. Викиномика. как массовое сотрудничество изменяет все [Текст] / пер. с англ. П.Мироно, Г.Василенко. – Москва: BestBusinessBooks, 2009. – 392 с.

400. Тарашвили Е. Связи с общественностью в государственных структурах [Электронный ресурс] Е. Тарашвили // Библиотека «Полка букиниста» [сайт]. - Режим доступа: http://society.polbu.ru/tarashvili_gospr/ch02_i.html.

401. Титиш Г. Російське чтиво. Запастись валер'янкою [Електронний ресурс] / Г. Титиш // Українська правда. Життя [сайт]. – Режим доступу: http://life.pravda.com.ua/society/2009/03/11/15344/.

402. Тихомирова Є.Б. PR – формування відкритого суспільства [Текст] / Є.Б. Тихомирова. – Київ: Наша культура і наука, 2003. – 196 с.

403. Тодорова О.В. PR в цифровую эру. Искусство коммуникаций [Текст] / О.В.Тодорова. – Киев: Huss, 2012. – 240 с.

404. Тоффлер Е. Третя Хвиля [Текст] / Елвін Тоффлер. – Київ: Всесвіт, 2000. – 480 с.

405. Требін М. Інформаційне суспільство. Війни нової епохи [Текст] / М. Требін // ВІЧЕ. – 2002. – № 4 (121). – С. 64–68.

406. Україна і Росія в історичній ретроперспективі [Текст] / під ред. В. Ф. Верстюк. – К.: Наукова думка, 2004. – 504 с.

407. Требин М. Войны XXI века [Текст] / М. Требин. – Москва: АСТ; Минск: Харвест, 2005. – 568 с.

408. Тюрин Д. Психологические операции ВС США в Афганистане [Текст] / Д.Тюрин, В.Сафонов // Зарубежное военное обозрение. – 2002. - №3. – С.11

409. Україна в сучасному геополітичному просторі: теоретичний і прикладний аспект [Текст]: монографія / За ред. Ф.М.Рудича. – Київ: МАУП, 2002. – 488 с.

410. Українська мова домінує у кінопрокаті, російська – у ЗМІ [Електронний ресурс] // Телекритика [сайт]. – Режим доступу: http://www.telekritika.ua/news/2011-11-09/67101.

411. Ульяновский А.В. Мифодизайн: коммерчиские и социальные мифы [Текст] / А.В.Ульяновский. – Санкт-Петербург: Питер, 2005. – 544 с.

412. Уотсон Т. Методы оценки деятельности PR-подразделения компании / Т.Уотсон, П.Нобл. – Днепропетровск: Баланс Бизнес Букс, 2006. – 257 с.

413. Усенко В. Многоуровневый характер гибридной войны [Електронний ресурс] / В.Усенко // Информационное сопротивление [сайт]. – Режим доступу: http://sprotyv.info/ru/news/13956-mnogourovnevyy-harakter-gibridnoy-voyny

414. Устинов Г.Н. Основы обеспечения информационной безопасности систем и сетей передачи данных [Текст] / Г.Н.Устинов. – Москва: СИНЕГ, 2000. – 248 с.

415. Уэбстер Ф. Теории информационного общества [Текст] / Ф.Уэбстер. – Москва: Аспект-Пресс, 2004. – 126 с.

416. Фартушний А. Українська культура [Текст] / А. Фартушний.– Львів: Львівська політехніка, 2000. – 112 с.

417. Федотова Л.Н. Социология массовой коммуникации [Текст] / Л.Н.Федотова. – Санкт-Петербург: Питер, 2003. – 345 с.

418. Фёдоров А. В. Трансформации образа России на западном экране: от эпохи идеологической конфронтации (1946–1991) до современного этапа (1992–2010) [Текст] / А.В. Федоров. — Москва: Информация для всех, 2010. — 202 с.

419. Фролов Д.В. Информационная война: эволюция форм, средств и методов [Текст] / Д.В. Фролов // Социология власти. – 2005. - №5. – С. 121-146

420. Философский энциклопедический словарь [Текст] / редкол.: С. С. Аверинцев, Э. А. Араб-Оглы, Л.Ф. Ильичев и др. – 2-е изд. – М.: Сов. энциклопедия, 1989 – 815 с.

421. Фильм «Брат-2» способствует росту ксенофобии [Электронный ресурс] // Новый Регион 2 [сайт]. – Режим доступа: http://www.nr2.ru/kiev/140229.html.

422. Филатова О. Г. Социология массовой коммуникации [Текст]: учебное пособие / О.Г.Филатова. — Москва: Гардарики, 2006. – 303 с.

423. Фісун А. О. Теоретично-категоріальне осмислення поняття «інформаційна війна» в структурі інформаційно-політичного простору [Текст] / А. О. Фісун // Інформаційне суспільство. – 2011. – Вип. 13. – С. 43–48.

424. Фоллс Дж. Маркетинг в социальных медиа. Просто о главном [Текст]/ [пер. с англ. В.Иващенко] - Москва: Манн, Иванов и Фербер, 2012. – 336 с.

425. Фролов Д. Б. Информационная война: эволюция форм, средств и методов [Текст] / Д.В.Фролов // Социология власти. — Москва: РАНХиГС при Президенте РФ, 2005. — № 5. — С. 121-146.

426. Фурашев В.М. Системна інформатизація виборчих і референдум них процесів в Україні [Текст] : монографія / В.М.Фурашев, М.І. Коваль, С.А. Маглюй. – Київ: Парламентське видавництво, 2004. – 608 с.

427. Хайятт М. Платформа: как стать заметным в интернете [Текст]/ [пер. англ. О.Медведь]. – Москва: Манн, Иванов и Фарбер, 2013. – 345 с.

428. Халидов Д. Ш. Информационная война в России: горькие плоды западничества [Текст] / Д.Ш.Халидов// Научно-аналитический журнал Обозреватель — Observer. — Москва: Институт диаспоры и интеграции (Институт стран СНГ), 2011. — Т. 259, № 8. — С. 14-25

429. Халилов Д. Маркетинг в социальных сетях [Текст] / Д.Халилов. – Москва: Ман, Иванов и Фербер, 2013. – 240 с.

430. Хасслер М. Веб-аналитика [Текст] / [пер. англ.] – Москва: Эксмо, 2010. – 432 с.

431. Цвєтков О. Інформаційна війна в Інтернеті [Електронний ресурс] // Перехід IV [сайт]. – Режим доступу: http://www.perehid.kiev.ua/16.html.

432. Цуладзе А.М. Политические манипуляции или покорение толпы [Текст] / А.М.Цуладзе. – Москва: Университет, 1999. – 144 с.

433. Цыганков В.Д. Психотронное оружие и безопасность России [Текст]/ В.Д.Цыганков, В.Н.Лопатин. – Москва: СИНЕГ, 1999. – 152 с.

434. Цыганов В. Медиа-терроризм: терорризм и средства массовой информации [Текст] / В. Цыганов. – Киев: Ника-Центр, 2004. – 120 с.

435. Чалдини Р. Психология влияния [Текст] / Роберт Чалдини. – Санкт-Петербург: Питер, 2001. – 288 с.

436. Червак Б. Як виграти інформаційну війну [Електронний ресурс] / Б. Червак // Українська правда [сайт]. - Режим доступу: http://www.pravda.com.ua/news/2006/5/29/42237.htm.

437. Чиж І.С. Правове забезпечення інформаційної діяльності в Україні [Текст] / І.С.Чиж, Ю.С. Шемшученко. – Київ: Юридична думка, 2006. – 384 с.

438. Чумиков А. PR в Интернете: Web 1.0, Web 2.0, Web 3.0 [Текст] / А.Чумиков, М.Бочаров, М.Тишкова. – Москва: Альпина Паблишер, 2010. – 134 с.

439. Чумиков А.Н. Связи с общественностью [Текст] / А.Н.Чумиков, М.П.Бочаров. – Москва: Дело, 2006. – 551 с.

440. Шапталов Б.Н. Феномен государственного лидерства: экспансия в мировой истории [Текст] / Б.Н.Шапталов. – Москва: Крафт +, 2008. – 636 с.

441. Шарков Ф.И. Коммуникология: энциклопедический словарь-справочник [Текст] / Ф.И. Шарков. – Москва: Дашков и К, 2009. – 766 с.

442. Шатило Я. С. Информационная война и трансгенные продукты [Текст] / Я. С. Шатило // Информационная безопасность регионов. — Саратов: СГСЭУ, 2008. — № 2. — С. 22-28

443. Шатило Я.С. Информационная война третьего поколения [Текст] / Я.С.Шатило // Информационная безопасность регионов. - Саратов. – 2009. - №1. – С.42-45

444. Шафаренко Ю.М. Аналітика у паблік рилшейшнз [Текст]: монографія / Ю.М.Шафаренко. – Київ: ПАЛИВОДА А.В. – 2014. -144 с.

445. Шевченко О. Інформаційно-психологічні операції: концептуальні підходи НАТО і провідних країн світу [Текст] / О. Шевченко // Соціальна психологія. – 2004. – № 2 (4). С. 111–121.

446. Шевченко Д.А. Реклама. Маркетинг. PR. Учебно-справочное пособие [Текст] / Д.А. Шевченко. – Москва: МГОУ, 2009. – 476 с.

447. Шейнов В.П. Искусство убеждать: технология скрытого управления людьми [Текст] / В.П.Шейнов. - Москва: Харвест, 2007. – 464 с.

448. Шерихов А. Война с Украиной: книжная формула «российской дружбы» [Электронный ресурс] / А. Шерихов // ФЛОТ2017 [сайт]. - Режим доступа: http://flot2017.com/item/analitics/4246

449. Шефер М. Маркетинг в Твиттере / пер. англ. О.Медведь. – Москва: Манн, Иванов и Фарбер, 2013. – 345 с.

450. Шиллер Г. Манипуляторы сознанием [Текст] / Г.Шиллер. – Москва: Мысль, 1980. – 326 с.

451. Шинкарук К. Україна як об’єкт м’якої сили: чинник національного самосприйняття [Текст] / К. Шинкарук // Актуальні проблеми міжнародних відносин. Збірник наукових праць. – 2007. – Вип. 69. – Ч. 2. – С. 232–237.

452. Шишкин Д.Н. PR-кампании: методология и технология: учеб. пособие [Текст] / Д.П.Шишкин, Д.П.Гавра, С.Л. Бровко. – Санкт-Петербург: Роза мира, 2004. – 187 с.

453. Ших К. Эра Facebook, как использовать возможности социальных сетей для развития бизнеса [Текст] / К.Ших. – Москва: Манн, Иванов и Флобер, 2012. – 304 с.

454. Шолохов С. Информационное оружие [Электронный ресурс] / С. Шолохов // Alltoday.RU [сайт]. - Режим доступа:http://www.alltoday.ru/seo_articles/articles5779.html.

455. Шоріна А. Український інформаційний простір: потрібна агресія [Електронний ресурс] / А. Шоріна // Диалог.UA [сайт]. - Режим доступу: http://dialogs.org.ua/ru/project/page9787.html.

456. Штогрін І. Називай агресію “захистом”: принципи інформаційної війни проти Росії [Електронний ресурс] / Ірина Штогрін [Текст]. — Режим доступу : www.radiosvoboda.org/cntent/article/25293307.html

457. Шумка А. В. Інформаційне протистояння в ході російсько-грузинського конфлікту (8-12 серпня 2008 року) [Текст] / А. В. Шумка // Військово-науковий вісник Львівського ордена Червоної Зірки інституту Сухопутних військ імені гетьмана Петра Сагайдачного Національного університету «Львівська політехніка». – Львів, 2009. – Випуск 11. – С. 254–260.

458. Щербаков С. Партизанский маркетинг в социальных сетях. Инструкция по эксплуатации SMM-менеджера [Текст] / С.Щербаков. – Санкт-Питербург: Питер, 2014. – 170 с.

459. Щербатых Ю. Искусство обмана: популярная энциклопедия [Текст] / Ю.Щербатых. – Москва: ЭКСМО-Пресс, 2000. – 345 с.

460. Ющук Е. Блог. Создать и раскрутить / [Текст] Е.Ющук. – Москва: Вершина, 2007. – 168 с.

461. Яковенко, М. Інформаційний простір: філософські аспекти формування поняття [Текст] / М.Яковенко // Вісник. – Львів, 2011. – N 692: Філософські науки. – С. 22–27

462. Яцко Н.Б. PR та маніпуляції: практичний словник [Текст] / Н.Б.Яцко. – Київ: Карпенко В.М., 2013. – 472 с.

КУРБАН

Олександр Васильович

Спеціалізація: фахівець у галузі соціальних комунікацій (PR, реклама, маркетингові комунікацій, журналістика). Незалежний практик-консультант, проект-менеджер, фахівець із інформаційних війн, член Української PR-ліги. Розробник та викладач тематичних політичних та бізнес-тренінгів. Журналіст-фрілансер, член Асоціації парламентських журналістів України.

Вчене звання та ступень: кандидат наук із соціальних комунікацій, доцент.

Викладацька діяльність: Доцент кафедри реклами та зв'язків з громадськістю Київського університету імені Бориса Грінченка та кафедри журналістики Військового інституту Київського національного університету імені Тараса Шевченка. Викладав у Інституті журналістики Київського національного університету імені Тараса Шевченка та Інституті журналістики та міжнародних відносин Київського національного університету культури та мистецтв. Проводить тренінги в Інституті права і систем управління Песоцьких.

Авторські роботи: монографія «Діагностика та моделювання PR-процесів» (2012 р.), навчальний посібник «PR у маркетингових комунікаціях» (2014 р.) та понад 50 тематичних наукових та прикладних публікацій з теоретичних та практичних аспектів розвитку сфери зв'язків з громадськістю, реклами, маркетингу, політичного менеджменту, різноманітних аспектів соціальної політики та інші.

Для нотаток

Для нотаток

Навчальне видання

Курбан О.В.

СУЧАСНІ ІНФОРМАЦІЙНІ ВІЙНИ У МЕРЕЖЕВОМУ ОН-ЛАЙН ПРОСТОРІ

Навчальний посібник

Підписано до друку 03.06.2016р. Формат 60х84 $^{1}/_{16}$.

Гарнітура Times. Папір офсетний. Наклад 300 прим.

Ум. друк. арк. 18,25. Зам. № 46-16.

Надруковано в навчальному картографічному комплексі ВІКНУ

03689, Київ, вул. Ломоносова, 81

т. 521-32-89