УДК 32.019.5

І. В. Ващенко, Е. М. Полтавський

ТЕОРІЯ І ПРАКТИКА ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Проаналізовано роль і місце інформаційних війн у сучасному світовому політичному процесі. Досліджено особливості розгортання російсько-української інформаційної війни. Розглянуто алгоритм дій під час проведення спеціальних інформаційних операцій, де пропагандистська та психологічна робота проводиться з метою безпосереднього впливу на свідомість і поведінку будь-якої аудиторії задля досягнення політичних чи військових цілей.

Ключові слова: *дезінформація, засоби масової інформації, інформаційна війна, інформаційно-психологічна операція, інформаційний вплив, комунікаційні технології, маніпуляція, система національної безпеки, світове співтовариство, психологічна операція, пропаганда, фейк.*

Постановка проблеми. Розвиток глобального інформаційного простору і технологій, специфіка соціальних, економічних, політичних умов розвитку сучасного світового співтовариства активно впливають на особливості ведення збройних конфліктів. Сьогодні переважна більшість держав-лідерів розглядають вплив інформацією на свого противника як один з ефективних інструментів реалізації власної зовнішньої політики, що дає змогу чинити інтенсивний тиск на всіх рівнях державного й суспільного устрою в будь-якому регіоні світу. Такі виклики потребують створення відповідної специфічної системи національної безпеки держави.

Науковці переконують, що в майбутньому світі лідерство визначатиметься здатністю держав контролювати інформаційний простір. Наразі ключову роль відіграють ЗМІ, Інтернет-канали, системи контролю за інформаційними потоками. Тому невипадково, що під час формування нового світового порядку держави-лідери роблять рішучі дії для прориву саме в інформаційній сфері.

Актуальним питанням залишається невідповідність між об'єктивною потребою у створенні ефективної системи протидії операціям інформаційного впливу і низьким рівнем готовності громадянського суспільства чинити опір спробам маніпулювання свідомістю його членів. У масовій свідомості громадян остаточно не сформувалося розуміння загрози, яку становлять сучасні комунікаційні технології, особливо якщо їх приховану агресію використовують із політичною метою [1].

Сьогодні інформаційна агресія російської федерації проти України охоплює групу засобів, які застосовують деструктивні інформаційні методи впливу і спрямовані на систему державного управління, внутрішній розкол українського суспільства шляхом інтенсивного використання дезорієнтуючих, дезорганізуючих, дезінформуючих, дестабілізуючих чинників.

Аналіз останніх досліджень і публікацій. Проблема сучасних інформаційних війн досліджувалась як зарубіжними, так і вітчизняними науковцями.

Особливості ведення сучасної інформаційної війни в онлайн-просторі охарактеризував дослідник О. Курбан [2]. У колективній монографії (за редакцією В. Горбуліна) ґрунтовно досліджувалася сутність гібридної війни як новітнього виду глобального протистояння. Науковці детально розглянули особливості ведення гібридної війни в різних вимірах: воєнному, політичному, економічному, соціальному, гуманітарному, інформаційному [3]. Детально проаналізував феномен інформаційної війни та охарактеризував засоби її ведення Ю. Горбань [4]. Питання необхідності забезпечення інформаційної безпеки держави як результат поширення інформаційних загроз порушила Я. Чмир [5]. Колективом авторів під керівництвом В. Ф. Смолянюка розкрито технологічні способи впливу на політичні процеси з метою отримання бажаних результатів, а також вивчено залежність демократичної політики від технологічного насичення, що має як позитивні, так і негативні наслідки для політичної системи й суспільства [6].

Однак зазначена тема досліджена недостатньо щодо впровадження нових методів розгортання інформаційної агресії проти України. Російсько-українська війна породжує нові форми інформаційного впливу, що постійно привертає увагу дослідників і спонукає до подальшого її вивчення.

Мета статті – проаналізувати термін «інформаційна війна», дослідити методи й особливості російсько-української інформаційної війни, розкрити роль новітніх інформаційно-комунікаційних технологій як зброї сучасних збройних конфліктів, що використовують технологічно розвинуті держави у боротьбі за світове лідерство.

Виклад основного матеріалу. Людська цивілізація завжди зазнавала інформаційного впливу на

всіх рівнях, а будь-яка військова перемога над противником вже вказувала на факт поразки в інформаційній війні. За допомогою інформації можна було спостерігати за ходом ведення бойових дій, аналізувати події, доводити потрібну інформацію до підлеглих. Поява інформаційних систем стала невід'ємною частиною суспільно-політичного життя і початком кардинальних змін у методах ведення бойових дій, які вже забезпечувалися великим масивом інформації. З розвитком інформаційних технологій удосконалюються й методи успішного ведення бойових операцій, що уможливлює маніпулювання інформацією супротивників.

Можна дати таке визначення: інформаційна війна – це комунікативна технологія впливу на інформаційні системи противника з метою досягнення інформаційної переваги в інтересах національної стратегії за одночасного захисту власної інформації. Отже, інформаційна війна є ключовим засобом, який використовують для проведення стратегічної атаки на противника.

Історія запровадження цього терміну починається із 70-х років XX ст., коли вийшла друком книга А. Далласа «Таємна капітуляція» (1967 р.). Зазначене словосполучення вживалось як назва особливого виду спецоперацій розвідки. Термін «інформаційна війна» у 1976 р. застосував Т. Рона у звіті «Системи зброї та інформаційна війна», в якому наголосив, що інформаційна інфраструктура стає ключовим компонентом американської економіки, уразливою мішенню навіть за мирних часів.

Термін «інформаційна війна» входить в активний вжиток наприкінці XX ст. після закінчення «холодної» війни. У подальшому військовими теоретиками в основу збройних конфліктів покладався поділ всього театру бойових дій на два складники: традиційний простір і кіберпростір, де останній має важливіше значення щодо нейтралізації збройних сил противника [7].

Таким чином, до традиційних сфер ведення бойових дій, окрім землі, моря, повітря та космосу, додається інформаційна сфера, де головними об'єктами ураження стають інформаційна структура держави та психіка противника. Поступово боротьба за лідерство у світовому політичному процесі переміщується в інформаційне середовище.

Інформаційне середовище являє собою сукупність окремих осіб, організацій і систем, які збирають, обробляють, поширюють інформацію. Воно включає три виміри.

Фізичний вимір – це система управління, що дає змогу проводити інформаційні операції у повітрі, на землі, морі й космосі. До нього належать комунікаційні мережі та інфраструктура життєдіяльності держави.

Інформаційний вимір – середовище, де інформація збирається, обробляється, зберігається, поширюється. До нього відносять усі потоки інформації.

Когнітивний вимір – це свідомість і середовище осіб, які безпосередньо приймають рішення (їхні емоції, обізнаність, розуміння).

Інформаційна війна реалізується на двох рівнях.

1. Державний. Мета інформаційної боротьби полягає в послабленні позицій конкуруючих держав, порушенні системи державного управління шляхом інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери, а також шляхом проведення психологічних операцій, підривних пропагандистських акцій.

2. Військовий. Мета інформаційної боротьби – досягнення інформаційної переваги шляхом впливу на інформацію та інформаційні системи противника з одночасним захистом власної інформації та інформаційних систем.

У подальшому військовими теоретиками поняття «інформаційна війна» визначалося таким чином. *Інформаційна війна* – це сукупність інформаційних операцій, спрямованих на систему державного і військового управління противника, що в мирний час призводить до прийняття сприятливих для ініціатора інформаційного впливу рішень, а в ході збройного конфлікту повністю нейтралізує роботу інфраструктури управління противника [8].

Як показала військова практика, інформаційна війна не буває випадковою, вона має узгоджену діяльність щодо використання інформації як на реальному полі бою, так і в економічній, політичній, соціальній сферах.

Поступово військово-політичне керівництво держав-лідерів в офіційних документах почали віддавати перевагу терміну «інформаційна операція».

Інформаційна операція – це комплексне використання можливостей електронної боротьби, комп'ютерних мережевих операцій, психологічних операцій, операцій з військової дезінформації та операцій безпеки з метою здійснення інформаційного впливу на процес прийняття рішень противником за одночасного захисту власної інформації та інформаційних систем.

Інформаційні операції насамперед передбачають здійснення впливу на рішення і процес прийняття рішень. Стратегічною метою інформаційних операцій є стримування потенційного противника від дій, які загрожують національним інтересам держави.

Основні напрямки діяльності інформаційної операції надзвичайно різноманітні й охоплює такі сфери.

1. Інфраструктура життєдіяльності держави. Розрізняють інфраструктуру виробничу (дороги, канали, порти, склади, система зв'язку) і соціальну (школи, лікарні, бібліотеки, театри). Іноді цим терміном позначають комплекс інфраструктурних галузей господарства (телекомунікації, транспортні мережі, електростанції, банківські системи, зв'язок, освіта, охорона здоров'я).

2. Промислове шпигунство. Воно спрямоване на розкрадання патентованої інформації, здобуття конкурентної переваги шляхом витіснення суперника, знищення важливих даних.

3. Зламування особистих паролів VIP-персон, ідентифікаційних номерів, банківських рахунків.

4. Електронне втручання у процеси управління військовими об'єктами, виведення з ладу систем військових комунікацій.

5. Усесвітня комп'ютерна мережа Інтернет.

Отже, можна наголосити, що інформаційна війна – це нова форма конфлікту, де відбуваються прямі атаки на інформаційні системи для впливу на противника з метою подальшого його знищення [9].

До складників інформаційної операції відносять такі.

1. Психологічна операція передбачає заходи щодо поширення спеціально підготовленої інформації з метою впливу на емоційний стан, мотивацію та аргументацію дій, прийняття рішень і поведінку окремих керівників, організацій, соціальних або національних груп у сприятливому для країни-агресора напрямку.

2. Дезінформація – спосіб психологічного впливу, який полягає в наданні об'єктові неправдивої або перекрученої інформації, яка вводить його в оману стосовно справжнього стану справ і створює викривлену реальність. Як правило, об'єктами психологічної операції є групи людей, а дезінформації – окремі особистості.

3. Електронна війна перешкоджає противникові отримати точну інформацію, зокрема радіоелектронне придушення та радіоелектронний захист. Радіоелектронна боротьба стала одним із найважливіших напрямків російсько-української війни, де сторони змушені постійно вдосконалювати свої технології та прийоми, які впливають на інтенсивність ведення бойових дій.

4. Мережева безпека охоплює комп'ютерні мережеві атаки, захист і використання комп'ютерних мереж противника з власною метою.

5. Інформаційна безпека передбачає заходи щодо захисту інформації та інформаційних систем шляхом забезпечення їх цілісності, конфіденційності та непідробленості.

6. Фізична безпека спрямована на захист персоналу, який володіє інформацією інформаційних систем, запобігає неавторизованому доступу до обладнання, захищає документи від шпигунства, пошкоджень, крадіжки.

7. Інформаційна атака – цілеспрямовані дії з використанням технічних і програмних засобів із метою порушення інформаційної безпеки системи, що дає змогу впливати на її зміст.

8. Фізична атака спрямована на систему управління противника для того, аби вплинути на його здатність здійснювати управління цільовою аудиторією.

9. Контррозвідка передбачає збирання інформації або діяльність, спрямовану на захист від шпіонажу, вбивств, замовлених від імені іноземних урядів, організацій чи терористичних угруповань.

Слід зауважити, що допоміжні компоненти інформаційної операції не завжди мають військові мету, але діють вони в інформаційному середовищі, аби впливати на інформаційні можливості противника [10].

Вітчизняні науковці наголошують, що головне завдання інформаційних операцій полягає в маніпулюванні масовою свідомістю, спрямованому на таке:

– внесення в суспільну свідомість і свідомість окремих громадян ворожих ідей і поглядів;

– дезорієнтація суспільства та його дезінформація;

– ослаблення державницьких переконань і залякування населення;

– контроль інформаційного простору противника і захист від ворожих дій інформаційних функцій власних збройних сил.

Огляд пропонованого матеріалу переконливо доводить, що інформаційна агресія російської федерації проти України невипадкова і була не лише порушенням існуючого міжнародного права, а й узгодженою діяльністю щодо використання інформаційної зброї для ведення реальних бойових дій. Інформаційний вплив ведеться на різних напрямках, як правило, це сфери життєдіяльності держави [11].

Кореспонденти АрміяInform зауважують, що людина краще засвоює ту інформацію, котра вже існує в її уявленні, тому будь-яка пропагандистська кампанія спрямована на «ефект резонансу», де інформацію використовують для того, аби змінити поведінку аудиторії. Зазвичай така інформація замаскована під ті знання і стереотипи, що вже існують в уявленні конкретної соціальної групи. За таких обставин ефективність інформаційного впливу досягається шляхом надання факту чи проблемі штучно перебільшеного значення, яке поступово починає руйнувати існуючу в суспільстві систему

цінностей і моральні норми поведінки, котрі регулюють суспільні відносини [12].

Військові експерти зазначають, що вплив на інформаційні системи за допомогою спеціально підготовлених операцій створює таку інформаційну перевагу, яка дає змогу не лише збирати, обробляти, розподіляти весь потік інформаційних подій, але й діяти на випередження противника в його відповідних діях.

До класичних визначень інформаційно-психологічної операції (ІПсО) відносять сплановані дії з передавання конкретної інформації іноземним аудиторіям, аби вплинути на їхні почуття, мотиви, критичне мислення, на діяльність іноземних урядів, організацій, груп чи індивідів.

Визначення ІПсО офіційно закріплено в Польовому статуті Збройних Сил США, де психологічні операції становлять компонент національної могутності, яка безпосередньо впливає на національну волю дружніх, нейтральних і ворожих сил та суспільств. Вона досягається за допомогою впливу на настрої і дії груп, які є об'єктами психологічних операцій, аби схиляти їх до підтримки національної політики та національних цілей.

Російський агресор активно застосовує ІПсО проти України з метою створення сприятливих умов для контролю території і зробити все, щоб українці не чинили опір російським військам. До поширених елементів ІПсО належать пропаганда, маніпуляція інформацією та кібератаки, де елементами можуть бути реальні події.

Отже, визначення «інформаційно-психологічні операції» є лише термінологічно замаскованою пропагандою таємної операції, яка проводиться за допомогою спеціально підготовлених служб [13].

У висновках Інституту національно-стратегічних досліджень США наголошено, що ключову роль у здійсненні інформаційної операції відіграє психологічна операція, де планова пропагандистська і психологічна робота розрахована на будь-яку аудиторію з метою впливу на її поведінку для досягнення політичних і військових цілей. У широких колах військових теоретиків таємна операція деструктивного характеру, проведена спецслужбами задля послаблення державного й суспільного устрою, отримала назву спеціальної інформаційної операції.

Спеціальні інформаційні операції – це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення поставленої мети. Таку операцію проводять на макро- і мікрорівні.

Макрорівень визначає, що агітаційно-пропагандистська робота орієнтована на конкретні соціальні групи людей і здійснюється переважно через ЗМІ та канали комунікацій.

Мікрорівень передбачає агітаційно-пропагандистську роботу ідеологічного характеру, вона персоналізована і здійснюється через міжособистісне спілкування. Для цього використовують діяльність, яка спрямована на поширення чуток, підбурювання населення держави до негативної поведінки [14].

Задля створення сприятливої політичної, ідеологічної, соціальної, економічної обстановки під час проведення спеціальної інформаційної операції спецслужби для здійснення прихованого інформаційного впливу використовують загальновідомі методи *дезінформування,* які передбачають уведення об'єкта в оману щодо справжності намірів і спонукають до запрограмованих агресором дій. Основні інструменти дезінформації такі.

1. *Підробка документів* – важливий інструмент поширення неправдивої інформації. Деструктивні впливи, негативні наративи, викривлення офіційних повідомлень Міністерства оборони України, особистих листів українських посадовців поширені у практиці проросійських інформаційних ресурсів, які мають на меті дезінформувати суспільство. Наприклад, фейкове донесення СБУ про факти систематичного порушення українськими військовослужбовцями міжнародного законодавства та їх відповідальності за вчинені злочини.

2. *Замовні матеріали статей у місцевій та іноземній пресі* мають чітко визначених адресатів, для поширення таких статей у медіапросторі іноземних країн використовуються агенти впливу в колах журналістів, публічних діячів і рекламних ресурсів.

3. *Використання медіа третіх країн* для потрапляння дезінформації в інформаційний простір, де активно використовують Інтернет видання, які мають формальний зв'язок із державою. До чинників, що сприяють поширенню фейків, можна віднести: низький рівень обізнаності населення щодо обговорюваних актуальних питань; відсутність подібних матеріалів у пошукових системах щодо їх достовірності; здатність цивільного населення сприймати шокові новини, вища за здатність сприймати звичайні новини; суспільна недовіра до експертизи; надлишок інформації в Інтернеті; розвиток журналістики, заснованої на витоках [15].

Серед маркерів маніпуляцій у пресі й онлайн-медіа такі:

– використання інформаційних джерел, які неможливо перевірити;
–штучне поєднання в одному матеріалі не пов'язаних між собою подій;
– емоційне забарвлення слів, якими описують людей та явища;
– категоричні судження, які закликають до агресивних дій.

Маркерами фейків у соціальних мережах є:
– новостворені акаунти, з яких поширюється інформація;
– неймовірна, шокуюча інформація;
– хвилеподібне поширення повідомлення;
– відсутність посилань на першоджерело.

Як приклад наведемо трансляцію улюбленої теми для російського телеканалу –сюжетів про злочинні дії військовослужбовців Збройних Сил України. Цілковита брехня миттєво поширюється російськими ЗМІ та соціальними мережами, унаслідок чого російська аудиторія отримує порцію нагнітання страху й ненависті до української армії.

Маніпуляція вирішує такі завдання:
– внесення в суспільну та індивідуальну свідомість ворожих ідей і поглядів;
– дезорієнтація та дезінформація населення;
– послаблення переконань щодо існуючих моральних норм поведінки;
– залякування свого населення образом ворога;
– залякування противника власною могутністю та майбутнім терором за непокору.

Одним із поширених методів інформаційного впливу є *пропаганда.* Вона передбачає поширення політичних, філософських, наукових, художніх, мистецьких ідей із метою управління громадською думкою у ставленні до певної ситуації, яке вигідне організаторам.

Яскравим прикладом ведення пропагандистських кампаній була діяльність ідеолога нацизму Й. Геббельса, який проголосив ключові принципи пропаганди:
– пропаганда має бути масштабною і безперервною, вестися з кількох різних джерел одночасно, адже люди засвоюють лише повторене тисячі разів;
– спрощені форми будь-яких повідомлень сприймаються навіть примітивними індивідуумами;
– максимальна одноманітність зрозумілих, коротких повідомлень, які повинні повторюватися в кожному інформаційному повідомленні;
– пропаганда не передбачає жодних диференційованих підходів, не допускає коливань, різних варіантів і можливостей;
– звернення до емоцій натовпу з мінімальним використанням раціональності: можна плести мотузки з натовпу, що перебуває під емоціями;
– шок і брехня становлять основу ефективної пропаганди, шокуючі повідомлення повинні поширюватися миттєво через привабливе середовище та викликати інтерес в аудиторії.

Центр протидії дезінформації при РНБО України дослідив аналогії пропагандистських підходів нацистів у Другій світовій війні та сучасних рашистів у війні проти України. З'ясовано, що кремлівське керівництво активно наслідує методи та прийоми ідеологів нацистської Німеччини. Сьогодні для маніпулювання громадською думкою в російській федерації змінюють свідомість своїх громадян простою, але масштабною брехнею шляхом установлення жорсткого державного контролю над ЗМІ та культурою. Так, анексію Криму в 2014 р. російській аудиторії було подано як «торжество історичної справедливості» та «захист на півострові російськомовних громадян». Прикладом може бути документальний фільм продюсера Ф. Бондарчука «Севастополь. Русская Троя» [16].

Найпопулярнішим джерелом інформації в Україні з моменту широкомасштабного російського вторгнення став Інтернет, де користувачі соціальних мереж можуть отримати відповідь на будь-яке запитання. Через брак редакційного контролю дезінформація може дуже швидко поширюватися. Поступово набувають великої популярності соціальні мережі, де кожен має можливість створювати власний контент.

Тому переповнений інформацією Інтернет потребує вміння громадян виявляти джерела, які вводять в оману. Це варто здійснювати таким чином.

1. Перевірка джерела інформації. Слід шукати авторитетні інформаційні агентства, яким можна довіряти, або офіційні ресурси, що надають точну інформацію.

2. Перевірка послідовності інформації. Як правило, дезінформація містить невідповідності, розбіжності, суперечливі деталі.

3. Перевірка оцінки доказів. Дезінформація не має доказової бази, вона спирається на епізодичні розповіді та вибірково подає інформацію.

Отже, виникає нагальна потреба протидіяти дезінформації на платформі, з якої вона поширюється. Facebook, Google і Twitter мають власні системи, що дають змогу читачам повідомляти про неправдиву інформацію. Правдива історія містить багато фактів, переданих цитатами експертів, офіційною статистикою або свідченням очевидців.

Важливо чітко і впевнено розуміти, що дезінформація залишається одним із головних викликів українській державі через свій негативний вплив на свідомість людини, на суспільну думку, національну безпеку. Варто наголосити, що в інформаційну еру дезінформація стала одним із головних викликів як для окремих держав, так і для всього міжнародного співтовариства [17].

Загрозою національній безпеці України слід вважати механізми *диверсифікації суспільної свідомості.* Вона передбачає розпорошення уваги правлячої еліти держави на різні штучно створені проблеми та їх відволікання від вирішення першочергових завдань суспільно-політичного та економічного розвитку. Кремлівські теоретики використовують проти України такі форми диверсифікації суспільної свідомості:

– дестабілізація суспільно-політичної ситуації в державі та окремих її регіонах;

– активізація принизливої кампанії проти політичного курсу держави та окремих її лідерів у різних міжнародних організаціях;

– ініціювання скандальних судових процесів, застосування міжнародних санкцій.

Таку форму інформаційної атаки використовують для того, аби чинити тиск на політичне керівництво держави з метою змусити його приймати кремлівський сценарій щодо врегулювання збройного конфлікту. В інформаційній агресії російська федерація зосереджує увагу на таких напрямках:

– нав'язування думки про неспроможність української влади управляти державою та ухвалювати раціональні рішення;

– створення уявлень про те, що для української еліти головним є власні інтереси, ніж події на фронтах;

– формування негативної оцінки діяльності воєнно-політичного керівництва держави з приводу того, що хаотичні бойові дії призводять до невиправданих втрат серед сил оборони України;

– поширення фейків про те, що Збройні Сили України деморалізовані й неспроможні вести організовані бойові дії.

Британський інститут вивчення війни пояснює, що цільовою аудиторією для кремлівських теоретиків є населення самої російської федерації, російськомовна діаспора, громадяни країн західної Європи. Тому сьогодні переважну частину контрінформаційних заходів повинні взяти на себе державна влада та дипломатичні представництва за широкої підтримки ЗМІ.

Поширеним впливом із боку російської федерації на українську аудиторію є *психологічний тиск*, який передбачає вплив на психіку людини шляхом погроз, залякування, з метою спонукання до запланованої моделі поведінки. Проти українського населення застосовуються такі форми психологічного тиску:

– доведення до громадян інформації про неіснуючі загрози;

– прогнози щодо майбутніх репресій і переслідувань;

– вчинення терористичних актів, захоплення заручників.

В інформаційній агресії проти України російськими телеканалами були активно застосовані технології 25-го кадру з використанням маніпулятивних технологій для інформаційно-психологічного впливу на глядачів.

До активних засобів модифікації суспільної свідомості належить *поширення неправдивих чуток* – діяльність щодо поширення неправдивої інформації серед широких верств населення через неофіційні канали з метою дезорганізації суспільства та держави або її окремих установ. За допомогою неформальної комунікації люди, які перебувають у критичній ситуації, стихійно об'єднуються в групи однодумців для роз'яснення проблемної ситуації, де спільно використовують свої інтелектуальні можливості.

В інформаційній війні проти України країна-агресор застосовує практично весь арсенал впливу на свідомість громадян. І, як результат, українці для пересічного росіянина постають «бандерівцями», «американськими маріонетками», ворожим народом. Відповідно змінилося ставлення й українців до росіян, адже такої масованої інформаційної атаки до цього часу не бувало [18].

Під час російсько-української інформаційної війни поширеною схемою в соціальних мережах стало створення фейкових сторінок українських волонтерів, військових і журналістів, де росіяни ставлять перед собою мету заволодіти певною інформацією, дискредитувати сили оборони України, дезорієнтувати суспільство, вкинути фейк.

Під виглядом журналістів, організаторів продюсерських проєктів зловмисники проросійських каналів знайомляться з військовими, аби довідатись їхні персональні дані. Сьогодні значна кількість TikTok-акаунтів маскується під особисту сторінку військовослужбовців сил оборони, які публікують справжні відео українських воїнів, але зовсім з іншим наративом. Така сторінка-клон може мати велику кількість підписників, набирати мільйони переглядів. Злочинці використовують фотографії і відео справжніх акаунтів, для того щоб замаскуватись і втертися в довіру користувачів. Отже, необхідно бути максимально уважним, не ділитись особистою інформацією, поки не буде переконання, що переписка відбувається зі справжньою людиною. Коли виявили, що перед вами – фейк, слід поскаржитися на нього, аби адміністрація соціальної мережі могла заблокувати шкідливу сторінку [19].

На початку 2024 р. у звіті TikTok повідомлялося про виявлення великої кількості фейкових акаунтів, які поширюють дезінформацію про російсько-українську війну. За даними організаторів платформи, пости на сайті для обміну відео були спрямовані на українських, російських та європейських користувачів. Російські фейки призначалися для штучного посилення проросійських наративів про війну, поширеним явищем стали неправдиві заяви про те, що після початку широкомасштабної війни проти України високопоставлені українські чиновники та їхні родичі купують розкішні автомобілі та вілли за кордоном. Такий відеоматеріал має очевидну мету – зупинити підтримку Заходу.

За повідомленням Укрінформ Єврокомісія оприлюднила звіт дотримання Кодексу поведінки щодо дезінформації, до якого добровільно долучилися ключові міжнародні інтернет-платформи, зокрема Google, Meta, Microsoft, TikTok [20].

Зауважимо, що Україна, її державні органи, суспільство, ЗМІ повною мірою не були готові до такої масованої інформаційної агресії, яка в широкому сенсі отримала назву «гібридна війна». Тому першочерговим завданням усіх державних, громадських, наукових інститутів є розроблення ефективних заходів щодо нейтралізації інформаційно-психологічної діяльності російської федерації. Виклики, які постали перед Україною, потребують оперативних заходів із модернізації системи інформаційної безпеки держави. Обставини, що склались у сфері інформаційної безпеки українського суспільства після широкомасштабної агресії російської федерації, стали реальною загрозою для існування української державності.

Необхідно додати, що під час аналізу стану інформаційної безпеки слід ураховувати політичні, соціальні, технічні чинники, які безпосередньо впливають на національну безпеку держави. Наслідком впливу інформаційних загроз на соціальні групи є загострення суперечностей між різними соціальними верствами, посилення політичної боротьби, розпалювання релігійних та етнічних суперечок, зниження культури населення, зростання злочинності та поширення антигуманних ідей.

Вплив інформаційних загроз на органи державної влади, які відповідальні за підготовку та прийняття рішень, порушує контроль та управління, призводить до витоку інформації, котра містить державну таємницю. Доцільно зауважити, що інформаційна безпека в системі державного управління є складником національної безпеки України, який має забезпечувати захист системи державного управління від агресивних інформаційно-комунікаційних загроз і захист громадян від інформаційної агресії.

Наразі реальними загрозами національній безпеці України в інформаційній сфері вбачаються такі:

– спрямованість російського ІПсО на деморалізацію особового складу Збройних Сил України, створення панічних настроїв, загострення суспільно-економічної ситуації, розпалювання національних конфліктів, домінування в українському інформаційному просторі;

– недостатній розвиток інформаційної інфраструктури, що заважає протидіяти інформаційній агресії та реалізовувати власні національні інтереси через медіапростір;

– неефективність державної інформаційної політики, недосконаліть законодавства та низький рівень медіакультури;

– відсутній механізм захисту інформації та забезпечення підготовки кадрів для державного управління у сфері інформаційної безпеки.

Фронт інформаційної агресії російської федерації надзвичайно широкий: від органів державного управління й сектору національної безпеки до простих громадян. Ворог використовує будь-яку можливість, аби нашкодити українській державності. Найпоширеніший сьогодні тип кібератак – електронні листи зі шкідливим програмним забезпеченням, які через механізм заволодіння обліковими даними спрямовані на знищення інформаційних систем [21].

Під час російсько-української інформаційної війни одним із пріоритетів кремлівського керівництва є приховані інформаційні загрози, саме вони дають змогу штучно створювати внутрішні суперечності й цілеспрямовано управляти політичною системою ззовні. За таких обставин утворюється керована політична система, поведінку якої можна легко спрогнозувати в режимі реального часу і через відповідний алгоритм інформаційного впливу змусити до бажаного рішення.

Висновки

Отже, інформаційна війна являє собою форму протистояння між державами в сучасному світовому політичному процесі, яка передбачає завдання максимальної шкоди противникові в інформаційному середовищі. Варто наголосити, що інформаційний вплив чиниться за допомогою спеціально підготовлених інформаційних операцій шляхом безпосереднього негативного впливу на систему державного управління для послаблення її реальних і потенційних можливостей, створення проблем внутрішнього розвитку, проведення зовнішньополітичної діяльності, підтримання міжнародних зв'язків, завдання шкоди політичному іміджу держави.

Поширений різновид інформаційних операцій сьогідні становлять ІПсО, що передбачає використання узгоджених, скоординованих форм і методів психологічного впливу. Вони складаються з політичних, військових, економічних, дипломатичних, інформаційно-психологічних заходів, спрямованих на конкретну людину або групу людей з метою впровадження в їхнє середовище ворожих ідеологічних або соціальних установок із подальшим формуванням помилкових стереотипів поведінки та спрямування громадської думки в необхідному напрямку.

У російсько-українській інформаційній війні проти України використовуються всі елементи ІПсО: дезінформація, пропаганда, диверсифікації суспільної свідомості, психологічний тиск, поширення чуток, кібератаки. Їх ґрунтовне вивчення дасть змогу не лише планувати заходи з виявлення, запобігання, припинення негативного інформаційного впливу, а і здійснювати підготовку у проведенні контрінформаційних заходів.

Російські ІПсО – складна система впливу на психологічний стан української аудиторії, вони використовуються для зниження морально-психологічного стану через соцмережі та месенджери. Проблема захисту інформаційних систем від негативної інформації як ніколи актуальна, адже цілеспрямований інформаційний вплив призводить до самознищення політичної системи, деградації громадської думки. Створення універсального захисного алгоритму, що сприятиме виявленню факту початку інформаційної агресії, залишається складним завданням. Боротьба з російським ІПсО потребує уваги та цілеспрямованих заходів із боку кожного громадянина, тому важливо розвивати критичне мислення та аналітичні прогнози, аби відрізняти об'єктивну інформацію від маніпуляцій та дезінформації. Слід пам'ятати, що головне завдання ІПсО – порушити думки та переконання.

Інформаційна зброя може досягати максимального ефекту, коли застосовується проти вразливих частин політичної системи, до яких належить система прийняття рішення і сфера системи державного управління. Тому в подальших дослідженнях планується систематизувати прояви інформаційної агресії російської федерації під час психологічного тиску та диверсифікації громадської думки в Україні.

Перелік джерел посилання

1. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навч. посіб. / за заг. ред. В. О. Жадька; ред.-упор.: О. І. Харитоненко, Ю. С. Полтавець. Київ : НПУ ім. М. П. Драгоманова, 2018. 356 с.
2. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі : навч. посіб. Київ : ВІКНУ, 2016. 286 с.
3. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : Національний інститут стратегічних досліджень, 2017. 496 с.
4. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. № 1. С. 136–141.
5. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного управління*. 2018. Т. 6. № 9. С. 16–22. URL: http://nbuv.gov.ua/UJRN/aplup_2018_6_9_4 (дата звернення: 15.04.2024).
6. Політичні технології в сучасних владних процесах: навч. посіб. / В. Ф. Смолянюк, С. С. Бульбенюк, Ю. М. Манелюк та ін. Київ : КНЕУ, 2021. 328 с.
7. Баглікова М. Інформаційна війна і Україна. *Науковий вісник Ужгородського університету. Політологія. Соціологія. Філософія.* 2010. Вип. 14. С.158–161.
8. Шугаєв А. В. Феномен інформаційної війни. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Філологія. Соціальні комунікації.* 2019. Т. 30 (69). № 4. Ч. 2. С.151–156.
9. Панченко В. М. Інформаційні операції в системі стратегічних комунікацій. *Стратегічні пріоритети. Політика.* 2016. № 4. С. 72–79. URL: http://nbuv.gov.ua/UJRN/sppol_2016_4_11 (дата звернення: 18.04.2024).

10. Запорожець О. Ю. Інформаційне протиборство у зовнішній політиці США. *Актуальні проблеми міжнародних відносин*. 2012. Вип. 107. С.157–164.

11. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.

12. Савченко-Галушко Т. Інформаційні та психологічні операції держави-агресора: як це працює. URL: https://armyinform.com.ua/2021/11/04/informaczijni-ta-psyhologichni-operacziyi-derzhavy-agresora-yak-cze-praczyuye/ (дата звернення: 18.04.2024).

13. Гордієнко С. Інформаційна війна, інформаційно-психологічні операції, пропаганда чи дезінформування на війні? URL: https://lexinform.com.ua/dumka-eksperta/informatsijna-vijna-informatsijno-psyhologichni-operatsiyi-propaganda-chy-dezinformuvannya-na-vijni/ (дата звернення: 23.04.2024).

14. Троян С. С. Спеціальні інформаційні операції. *Велика українська енциклопедія.* URL: https://vue.gov.ua/ (дата звернення: 18.04.2024).

15. Дубов Д. В., Баровська А. В., Каздобіна Ю. К. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії : метод. матеріал. Київ : Українська фундація безпекових студій, 2020. 60 с.

16. Фашизм і рашизм – аналогії інформаційних війн. *Центр протидії дезінформації при РНБО України*. URL: https://cpd.gov.ua/main/fashyzm-i-rashyzm-analogiyi-informaczijn/ (дата звернення: 05.05.2024).

17. Миронюк О. Дезінформація: як розпізнати та боротися. URL: https://law.chnu.edu.ua/dezinformatsiia-yak-rozpiznaty-ta-borotysia/ (дата звернення: 18.04.2024).

18. Новицька Н. Б., Петрик В. М., Кудико В. М. Пропаганда, диверсифікація громадської думки, психологічний тиск та поширення чуток як методи ведення спеціальних інформаційних операцій РФ проти України. *Ірпінський юридичний часопис. Право.* Ірпінь : Державний податковий університет, 2022. Вип. 2 (9). С. 105–113.

19. Tiktok виявив понад 12 тисяч акаунтів, які поширювали російські фейки. URL: https://www.ukrinform.ua/rubric-technology/3800648-tiktok-viaviv-ponad-12-tisac-akauntiv-aki-posiruvali-rosijski-fejki.html (дата звернення: 12.03.2024).

20. Роспропаганда взялася імітувати українських військових – створює фейкові акаунти і сторінки-клони в соцмережах – ЗМІ. URL: https://www.5.ua/svit/rospropahanda-vzialasia-imituvaty-ukrainskykh-viiskovykh-stvoriuie-feikovi-akaunty-i-storinky-klony-v-sotsmerezhakh-zmi-301381.html (дата звернення: 16.03.2024).

21. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління.* 2022. Вип. 2 (62). С. 149–154. URL: https://journals.maup.com.ua/index.php/political/article/view/2153/2650 (дата звернення: 06.05.2024).

Стаття надійшла до редакції 26.05.2024 р.

Ващенко Ігор Владиславович – кандидат історичних наук, доцент, доцент кафедри військової підготовки Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1444-7538

Полтавський Едуард Михайлович – кандидат юридичних наук, доцент кафедри правового забезпечення Національної академії Національної гвардії України
https://orcid.org/0000-0002-7434-7061