DOI: 10.18372/2410-7840.24.16930
УДК 004.946.5

ІНФОРМАЦІЙНА ЗБРОЯ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ

Володимир Хорошко, Юлія Хохлачова, Тіна Пірцхалава, Ігор Іванченко

Інформаційна зброя – це новий еволюційний крок на шляху розвитку новітніх зразків зброї. Така зброя має специфічні та характерні тільки їй ознаки. В сучасних умовах військової агресії Росії збройна боротьба набула ознак не тільки інформаційної війни. Її акценти змістилися у бік реалізації інформаційних технологій. При цьому дедалі більше значення у досягненні політичних та воєнних цілей набувають інформаційно-психологічні операції, акції, дії та інформаційна зброя, недооцінка можливостей якої у сучасній інформаційній війні може стати фатальною під час подальшого загострення воєнно-політичної обстановки. Це підтверджується тими бойовими діями, які зараз ведуться в Україні. В сучасній війні неможливо досягти поставлених цілей без постійного здійснення заходів інформаційної війни. Тому фахівці виділяють інформаційну зброю як самостійний вид зброї, яка розглядається як засіб ведення інформаційної боротьби. Інформаційна війна та впливи можуть проводитися у політичній, економічній, оборонній, науково-технічній та інших сферах шляхом: впливу на елементи інформаційно-телекомунікаційних систем з метою знищення елементів інфраструктури державного та військового управління, перехоплення та обробка відкритої інформації, що циркулює в інформаційних системах і друкується в засобах масової інформації; несанкціонованого доступу до інформаційних ресурсів та з їх наступним перегрупуванням, знищення або розкраденням; перехоплення та дешифрування інформаційних потоків, переданих каналами зв'язку, побічними випромінюваннями або отриманих за рахунок використання спеціальних технічних засобів перехоплення інформації; формування та поширення інформаційними каналами супротивника або глобальних мережах дезінформації з метою впливу на оцінки, наміри та орієнтацію людини, групи людей, суспільства в цілому та військово-політичне керівництво держави. Інформаційна війна – це поширення певних ідей, поглядів чи ідеології, є засобом певної політики. Глобальним інструментом її реалізації є засоби масової інформації та різні комунікації. У статті також розглянуто теорію інформаційної війни у політичній сфері, слід враховувати, що вона відбувається на стратегічному, оперативному та тактичному рівнях.

В основному на стратегічному рівні діє вища політична еліта держави, а інформаційні підрозділи політичного шляху – на оперативному та тактичному рівнях.

Ключові слова: *інформаційна війна, інформаційна зброя, інформаційне протиборство, інформаційно-психологічні впливи, інформаційна боротьба.*

ВСТУП

Досвід збройних конфліктів, які були і ведуться у теперішній час, показують, що одним з найважливіших механізмів війни стають не тільки зміни у військовій справі, але й інформаційна революція. Значні досягнення якої в області комп'ютерних, інформаційних і телекомунікаційних технологій зробили світ уразливим перед новою зброєю, можливо, більш небезпечною, ніж ядерна. Мова йде про війну нового покоління – інформаційну, спрямовану не стільки на безпосереднє знищення супротивника, скільки на досягнення політичних цілей без ведення бойових дій, значимість якої останнім часом на теренах України стала доволі високою. Теоретично та практично кожен конфлікт відрізняється один від одного масштабом, інтенсивністю загострення відносин, часом протікання тощо, але всім їм притаманні характерні особливості та тенденції розвитку.

Перший досвід ведення інформаційної війни в оперативному масштабі, як однієї із складових військових протиборств, був започаткований у операції «Буря в пустелі» у 1991 році. Успіх застосування інформаційної зброї показав, яку ефективність має застосування її, а також її роль у інформаційній

війні. Ці дії надали приклад іншим державам як і де її застосовувати. Прикладом масштабного застосування інформаційної зброї (ІЗ) є інформаційна війна, яку веде Росія проти України. Нині під інформаційною війною розуміють закономірний об'єктивний процес у стосунках між протиборчими сторонами, спрямований на досягнені останніми цілей власної державної політики в мирний та воєнний час шляхом комплексного впливу на систему державного та військового управління протиборчої сторони та її військово-політичне керівництво, а також захист своїх інформаційних об'єктів і ресурсів від подібного впливу. Інформаційна війна та впливи можуть проводитися у політичній, економічній, оборонній, науково-технічній та інших сферах шляхом: впливу на елементи інформаційно-телекомунікаційних систем з метою знищення елементів інфраструктури державного та військового управління, перехоплення та обробка відкритої інформації, що циркулює в інформаційних системах і друкується в засобах масової інформації (ЗМІ); несанкціонованого доступу до інформаційних ресурсів та з їх наступним перегрупуванням, знищення або розкраденням; перехоплення та дешифрування інформаційних потоків, переданих каналами зв'язку, побічними випромінюваннями або отриманих за рахунок використання спеціальних технічних засобів перехоплення інформації; формування та поширення інформаційними каналами супротивника або глобальних мережах дезінформації з метою впливу на оцінки, наміри та орієнтацію людини, групи людей, суспільства в цілому та військово-політичне керівництво держави.

Розглянемо теорію інформаційної війни у політичній сфері, слід враховувати, що вона відбувається на стратегічному, оперативному та тактичному рівнях.

В основному на стратегічному рівні діє вища політична еліта держави, а інформаційні підрозділи політичного шляху – на оперативному та тактичному рівнях.

Інформаційна війна – це поширення певних ідей, поглядів чи ідеології, є засобом певної політики. Глобальним інструментом її реалізації є ЗМІ та різні комунікації. У [1] визначається, що ІВ або пропаганда, це цілеспрямовані, системні спроби формувати сприйняття, маніпулювання свідомістю та спрямувати поведінку суспільства у напрямку, який необхідний. Хоча ІВ замовчувала свою історію з початком історії суспільства, першою науковою школою, що спеціально та цілеспрямовано досліджувала проблему ІВ, стала американська школа вивчення ЗМІ. Ця школа вивчила її передусім на матеріалі Першої Світової війни. Вона, зокрема визначила три основні типи впливів у ІВ:

1. «Білий» вилив. Його основною характеристикою є те, що журналіст відкрито називає себе і дозволяє нав'язати тексти зі справжнім джерелом.

2. «Сірий» вилив. Журналіст використовує для поширення матеріалів спеціально створені джерела чи забезпечує просування матеріалів у певних незалежних ЗМІ.

3. «Чорний» вплив. Журналіст поширює матеріали від імені третьої особи [2].

За твердженням французького дослідника другої половини XX ст. Ж. Доменика, під час здійснення інформаційних операцій або компаній звичайно застосовуються п'ять основних правил [2]:

1. Правило спрощення. Виходячи з орієнтації матеріалу на найменш досвідченого члена суспільства та її апелювання до емоцій, важливою вимогою є максимальне спрощення об'єкта впливу. Багатозначність, наявність напівтонів принципово не придатні для інформаційного впливу.

2. Правило перебільшення та перекручення. Створення позитивних (негативних), іміджів викликає необхідність гіперболізації певних рис об'єкта, акцентування на подіях, не обов'язково значних, але таких, що працюють на ідею, а за умов недостатньої чіткості матеріалу його перекручування.

3. Правило оркестрування або замовчування. Як визначав Й. Геббельс, «важливо не те, про що пишуть в газетах, важливо те, про що в них не пишуть». За матеріалами Р. Герценштейна, одним із основних прийомів такої пропаганди було саме замовчування. Подібні підходи широко використовують і сьогодні, особливо це стосується російських ЗМІ.

4. Правило переливання. Одне з важливих, проте дуже дискутивних, правил Ж. Доменика полягає у відповідності інформаційного впливу настановам і стереотипам суспільства [2].

5. Правило спільності та зараження. Це правило є повним аналогом деривації В. Парето (звернення до загальновживаного) [1].

Так в сучасній війні неможливо досягти поставлених цілей без постійного здійснення заходів інформаційної війни не тільки в ході, але ж ще задовго до її початку та після завершення. Тому фахівці виділяють як самостійний вид зброї – інформаційну зброю, яка розглядається як засіб ведення інформаційної боротьби. Це має підтвердження, якщо подивитись на події війни Росії проти України.

ОСНОВНА ЧАСТИНА

На відміну від традиційної зброї, зброя інформаційна є суто наступальною, оскільки заходи щодо нейтралізації її впливу становитимуть заходи захисту, спрямовані на забезпечення власної інформаційної безпеки, а будь-які дії у відповідь з використанням ІЗ, слід розглядати як наступальні.

На сьогоднішній день ІЗ є єдиною ефективною зброєю, яка в умовах науково - технічного прогресу здатна призвести одну з протидіючих сторін до перемоги, як застосування арсеналу сучасної традиційної зброї в глобальному або локальному конфлікті здатна призвести до знищення всіх учасників протистояння або, принаймні, до непоправних витрат в структурі національної безпеки, економіки та інших важливих сферах життєдіяльності конфліктуючих сторін, такою мірою, що жодна з них не зможе скористатися результатами перемоги.

Застосування ІЗ зводиться до таких способів, як [3]:

- вплив на окремі одиниці інформаційної системи супротивника з метою нанесення збитків;
- знищення або пошкодження цінних ресурсів супротивника, подолання систем захисту та кіберзахисту, впровадження вірусів, програмних закладок і логічних бомб;
- вплив на інформаційні ресурси, інформаційних систем і систем управління з метою створення або модифікації даних;
- перехват каналів розповсюдження інформації супротивника з метою поширення дезінформації, чуток;
- вплив на персонал інформаційних і телекомунікаційних систем з використанням програмних засобів для введення інформації в підсвідомості або погіршення здоров'я людини;
- проведення терористичних дій.

Крім того ІЗ має наступні ознаки [3]:

- скритність – можливість досягнення мети без видимої підготовки та оголошення війни;
- масштабність – можливість наносити непоправної шкоди, не визнаючи державних кордонів і суверенітету, без обмежень простору у всіх сферах життєдіяльності людини та суспільства;
- універсальність – можливість багатоваріантного використання як військових, так і цивільних структур країни нападу проти військових і цивільних об'єктів цієї країни.

Критерієм віднесення до розряду ІЗ може розглядатися ефективністю того чи іншого озброєння при вирішенні завдань інформаційної війни. Доведено, що найбільших втрат збройні сили несуть від впливу вражаючих елементів ІЗ, що діють на системи управління та психіку людини. ІЗ розглядається як засіб ведення інформаційної війни, що є лише ключовим елементом повномасштабної війни. В даний час використовується класифікація ІЗ, яка включає дві підгрупи, до першої підгрупи відносяться [4]:

- засоби масової інформації;
- психотропні генератори;
- психотропні препарати.

Інформаційна зброя даної підгрупи призначена для негативного впливу на людину. Зокрема, це вплив може здійснюватися через різні ЗМІ. При цьому все більшого значення набуває інформаційно – психологічне забезпечення дій війн з боку політичного керівництва держави. Це пояснюється зростанням впливу громадської думки на прийняття рішень урядом країни. Психотропні генератори – це пристрої, які впливають на людину шляхом передачі інформації через неусвідомлюване сприйняття. А психотропні препарати – це лікарські засоби, які визивають стан залежності, здійснюють стимулюючі або депресивний вплив на центральну нервову систему людини, під впливом яких здійснюється порушення мислення, змінюється настрій та поведінка.

У другу підгрупу входять [4, 5]:

- засоби радіоелектронної боротьби;
- засоби спеціального програмно – технічного впливу.

Засоби радіоелектронної боротьби – це системи для виявлення та радіоелектронного придушення систем управління військами та радіоелектронної зброї супротивника, його систем розвідки та навігації, а також системи для забезпечення стійкої роботи своїх систем.

Засоби спеціального програмно-технічного впливу – програмні, апаратні або програмно – апаратні засоби з використанням яких може бути здійснено несанкційне копіювання спотворення, знищення інформації, її передача за межі контрольованої зони або блокування доступу до неї.

Крім того, існує і інша класифікація ІЗ [6, 7, 8], яка проводиться за наступними напрямами: з метою застосування; за об'єктами впливу; за механізмами реалізації впливу; за характером впливу на інформацію та інформаційні процеси; за масштабами вирішуваних завдань; за терміном дій тощо.

Завданням ІЗ є, за яскравим висловом М.А. Булгакова, «розруха в головах», яка небезпечніша за розруху у економіці, тому що втрата національних і духовних цінностей веде до виродження народу й краху суспільства, а в наслідок цього загибель держави. [3].

Основними об'єктами ІЗ є:

- інформаційно-технічні та інформаційно-аналітичні системи, кожна з яких вміщує особистість; інформаційні ресурси;
- системи формування суспільної свідомості та думки, що базуються на засобах масової інформації та нарешті одним з основних об'єктів ІЗ є психіка та свідомість молоді, майбутнього нації.

Отже, за об'єктами впливу ІЗ можна поділити на два основні класи [7]:

- інформаційно – технічна зброя, яка впливає на інформаційні ресурси, інформаційну інфраструктуру: збройних сил, на населення та суспільство в цілому;
- інформаційно-психологічна зброя, яка впливає на морально-психологічний стан людини, соціальних та інших груп населення та на суспільство в цілому.

Сьогодні інформаційно-психічна зброя визначається як засоби знищення, викривлення або викрадання інформаційних масивів, видобування з них необхідної інформації після подолання систем захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виводу з ладу телекомунікаційних мереж, комп'ютерних систем, усіх засобів високо – технологічного забезпечення життя суспільства та функціонування держави. Інформаційно-технологічна зброя – тобто, сукупність спеціальних засобів і технологій, що використовуються для насильницького викривлення інформаційно – психологічного простору супротивника спеціально для ураження індивідуальної та масової свідомості. Знаючи головні характеристики відповідної спільноти – від демографічних до соціально – економічних та визначивши пануючі психотропи, розуміючи менталітет, на базі певних технологій можна активно впливати на цільову групу, модифікувати суспільну свідомість і формувати громадську думку, і, відповідно до конкретних цілей, провокувати, спонукати, збурювати до певних дій або дезорієнтувати та дезінтегрувати як окремі спеціальні групи, так і цілі народи [4, 7].

Процес реалізації цих дій міститься у зомбованому ефекті на окреме суспільство виглядає наступним чином [4, 9]:

1) розслабити суспільство – розповсюджувати через засоби масової інформації (ЗМІ), що ворогів немає, обговорювати окремі історичні періоди та інтереси окремих народностей (мета – суспільство як ціле має зникнути в якості об'єкта свідомості суспільства);

2) змусити суспільство слухати тільки супротивника, не звертаючи уваги на якість іншої думки або відчуття, наприклад, акцентувати ЗМІ на якійсь одній парадигмі суспільного розвитку (наприклад, російській) виключивши будь-який інший досвід: Китай, Японія, Сінгапур (мета – процес занурення суспільної свідомості та дії формуючих сил послаблюються);

3) змусити суспільство не розмірковувати над тим, що говорить супротивник, і для цього виключити із ЗМІ результати досліджень серйозних аналітичних проблем (мета – сприяти гальмуванню безперервного потоку думок);

4) зосередити увагу суспільства на якомусь предметі окрім вхідного інформаційного потоку, наприклад, внутрішні катаклізми, війна, терористичні акти (мета – підсистема захисту, яка відповідає за обробку вхідної інформації, виявляється нездатною виконувати свою функцію та як би розбалансується);

5) постійне навіювання, що саме суспільство стає краще та краще, що всі навколишні ставляться до нього краще й краще (мета – подібне навіювання послаблює історичну пам'ять і почуття, якими характеризується нормальний стан суспільства);

6) ЗМІ – одночасно повинні переконувати членів суспільства про те, що викликало такий стан –

це не зовсім те, що повинно бути (мета – створення пасивного стану свідомості, в якому зберігається можливість залежності від інформаційних впливів супротивника).

Наведений алгоритм у загальних рисах використовувався ЗМІ Росії за часів 1990 – 1998 років. Крім того, слід відзначити, що цей алгоритм використовується проти України Російською Федерацією з 2012 року по теперішній час.

Слід відзначити, що пропагандистське бачення світу перетворює ЗМІ в ІЗ та потребує розуміти механізми впливу на особистість, групи людей та цілі народи. Відповідно до теореми Томаса [8] «щоб створювати необхідну поведінку або настрій людей, необхідно створити реальність, яка буде уявлятись людям істиною.» Масштабну реальність для нас людей створюють мас-медіа. Сфабриковану реальність люди повинні прийняти добровільно та бути впевненим, що це і є їх погляди на світоустрій.

Власники ЗМІ створюють, обробляють, оперують і контролюють поширення інформації, яка визначає уявлення людей, їх установки, а в кінцевому рахунку і поведінку. Навмисно фабрикуючи повідомлення, які створюють реальну соціальну дійсність вони перетворюються в маніпуляторів свідомістю.

Для забезпечення медіа маніпулювання основними методами поширення інформації є фрагментація та негайність [8].

При цьому, слід враховувати роль телебачення у медіа маніпулюванні виходить з того, що слова в багато разів переконливі, якщо вони підкріплені картинкою або синхронізовані з відео картинкою. Сфабриковані телесюжети, суміш правди, напівправди та інсценування, все це для глядачів є «достовірною» реальністю [8]. Для подачі «запрограмованих» та «реальних» матеріалів створюються передачі, які зрозумілі за змістом та не потребують інтелектуальної напруги, у той же час будоражать емоції. Переживання емоцій над розумом – це особистість поведінки людини.

Крім того, при медіа маніпулюванні використовуються наступні основні фактори [8]:

- коротка пам'ять людини;
- для людей немає об'єктивності, якщо вони втягнуті у конфлікт, який загрожує їх інтересам і цінностям;
- людині для осмислення явища необхідно мати назву цього явища, а назва у прихованому вигляді пояснює та програмує реакцію на нього. Через слова та поняття створюється картина світу.

Слід зауважити, що з появою Internet медіа маніпулювання отримало новий інструмент соціальної інженерії з невідомими раніше моделями прийняття рішень, який змінює пізнавальний базис сучасної людини. Internet визначає зміст інформації, яка доходить до людей по всьому світу [9].

Технології підриву легітимності влади в Internet просторі постійно вдосконалюються, що створює проблеми для системної інформаційної боротьби подібній підтримці діяльності. Ці технології деформують масову свідомість населення країни-жертви та викликають недовіру, презирства та ненависть до діючої влади. Не дивлячись на те, що в Internet є системні центри генерації контексту, користувачі Internet і соціальних мереж вважають, що контент створюється такими ж разовими користувачами, як і вони, тому довіряють цьому контексту та не схильні до перевірки достовірності новин і фактів, наведених у мережах.

Аналіз розвитку ситуації навколо України дає всі підстави стверджувати, що сьогодні наша держава зіткнулась саме із інформаційною війною та застосуванням ІЗ. Це підтверджується особливостями розвитку як і інформаційного протиборства, так і воєнного конфлікту, відмінною ознакою яких є широко масштабні бойові дії регулярних військ та існування змови Росії з недержавними формуваннями, що діють на території України [10, 11].

На підставі оцінювання рівня воєнної небезпеки для України з боку Російської Федерації в часі, можна стверджувати, що рівень воєнної небезпеки з боку Росії, починаючи з моменту відмови України від ядерної зброї та виводу її з території країни, різко зростає, тому що Російська Федерація намагається, по-перше, домінувати у Центрально-Східному регіоні Європи та реалізувати свої екстремістські цілі щодо перегляду існуючих кордонів; по-друге залишити Україну в сфері впливу та встановити контроль за важливими об'єктами та комунікаціями на території України та забезпечити вільний доступ до її стратегічних сировинних ресурсів; по-третє, гарантовано утримувати базу Чорноморського флоту в Криму.

Тому збройний конфлікт з використанням технологій інформаційної війни (які застосовує Росія проти України), як правило, стають конфліктами на

виснаження. У таких конфліктах сторона, що захищається та веде боротьбу з різного роду екстремістськими і терористичними формуваннями на своїй території, які формуються, готуються, забезпечують всім необхідним та керуються з території іншої держави. Водночас у сторони, що обороняється, з різного роду причин, насамперед, зовнішньополітичного технологічного характеру, фактично виявляються «зв'язані руки» в плані реалізації особливих форм протидії агресорові. Як наслідок, їй нав'язують конфлікт на виснаження, в якому відбувається поступове руйнування економічної та соціальної структури суспільства, матеріально-технічної та цивільної інфраструктури держави, що зазнає агресії. Ці дії проводить Росія проти України [11]. Крім того, слід враховувати, що Росія ще веде широкомасштабні бойові дії на українській території. Особливістю введення інформаційної війни Росії на Донбасі є постійний пошук і використання актуальних інформаційних приводів, здатних сформувати необхідну громадську думку. Останнім часом спостерігається тенденція розширення впливу на сфери, раніше непритаманні для інформаційного протиборства, а саме на перегляд історії державності України та Росії та міжконфесійні відносини.

Для досягнення політичних цілей Російська Федерація з метою дестабілізації обстановки у світі, значне поширення отримали інформаційно-психологічні операції з застосуванням ІЗ.

Окупувавши український інформаційний простір Росія робить все, щоб спотворити інформацію про Євросоюз, євроінтеграцію та НАТО, щоб зомбувати самих українців неправдивою історією. Фактично Росія використовує наш інформаційний простір для розколу суспільства та реалізації планів Кремля стосовно України – політичної та культурної експансії. Для цього (із 2012 року) у світогляд мешканців Донбасу та Юга України вкладається стан жаху та страху за своє життя. Стан людей доводиться до масового психозу.

Коли крапля кипіння була досягнута у 2014 році, застосували інший меседж : треба захищатися. Його мусолили біля трьох – чотирьох тижнів. Після чого був укинутий меседж необхідність утворення певного державного об'єднання. Так виникали ідеї створення ДНР і ЛНР, ополчення Донбасу тощо.

Наступний етап – об'єднання. Кремлем була висунута ідея створення Новоросії. Під неї підігнали історичне обґрунтування – нібито при Катерині Росія вклала в цей регіон дуже багато, а хитрі «укри» прийшли на усе готовеньке. Під цю фантазію практично відбулося військове вторгнення Росії, що спочатку виглядало не настільки явним, як зараз [12].

Для вирішення цих завдань Кремль активно використовував і використовує ІЗ та можливості [12, 13]:

1) групи спеціальних журналістів (з 3-4 чоловік, які мають чіткі завдання та інструкції про те, як висвітлювати події на Сході України та безпосередньо працювати на російські інформаційні канали;

2) оперативних груп психологічних операцій, які чисельністю 2-4 чоловіки виконували та виконують на території окупованого Донбасу завдання по [12, 14]:

- усній пропаганді, у тому числі й роботі з місцевим населенням;
- поширення пропагандистської літератури та іншої необхідної інформації;
- створення з місцевих активістів – сепаратистів пропагандистських груп у анексованих населених пунктах, організацій та координації їхніх дій;
- сприянню роботи російських ЗМІ, збоку інформації та визначенню найбільш гострих проблем у населення для використання цього, як ІЗ;
- моніторингу поточного морально-психологічного стану місцевого населення;

3) загону психологічних операцій, який дислокований недалеко від Ростову-на-Дону разом з пунктом управлінням розвідцентру Головного розвідувального управління Генерального Штабу Збройних Сил Росії.

В його завдання входять:

- збір, обробка та аналіз інформації про поточний морально-психологічний стан населення України та її військовослужбовців, а також підрозділів російських військовослужбовців та терористів;
- керівництво підрозділами психологічних операцій, що виконують спеціальні завдання з інформаційного впливу;
- розробка та здійснення інформаційно-психологічних операцій на території України;

4) агентів диверсійної психологічної роботи в інших областях України, які виконують завдання по:

- створенню диверсійно-пропагандистських груп в областях підконтрольних Україні;

- навчанню місцевих груп сепаратистів проведенню підривних пропагандистських акцій;
- забезпеченню цих груп необхідним матеріально-технічним майном та пропагандистською літературою;
- безпосередньому проведенню мітингів, акцій протесту та поширенню пропагандистських матеріалів.

Тим не менш, з початком нового витка військової агресії Кремля, інформаційна війна Росії застосували нові форми та методи. Можна стверджувати, що саме зараз без особливого розгойдування та попередньої підготовки почалася чергова військово-психологічна спецоперація Кремля щодо нагнітання панічних настроїв у суспільстві, яка мала привести спочатку до поразки українських військ на Сході України, а потім до повної дестабілізації ситуації в Україні взагалі. З цього приводу можна зробити висновок, що Росія роблячи ставку саме на страх намагається залякати українців і вбити їхню волю до перемоги, зосередившись при цьому на інформаційній підтримці російської військової агресії, формуванні думок про «мирні можливості співіснування» з Росією. Цільовою аудиторію інформаційної війни Росії в контексті останніх подій стали росіяни та російська діаспора, населення України (у тому числі населення усіх окупованих регіонів), аудиторія західних країн та аудиторія країн близьких до Росії по політичним поглядам [12, 13].

При цьому, дуже уважно слід враховувати те, що населення, яке мешкає в окупованій зоні, зазнає подвійного впливу – як з боку терористів і Росії, так і з боку України. Тому під час застосування ІЗ використовується весь спектр видів, методів, способів і прийомів інформаційної війни.

Слід зауважити, що основними напрямами інформаційної війни Росії проти України є [11, 12, 13, 14, 15]:

- широке застосування підконтрольних ЗМІ (у теле-, радіо-, та Internet – просторі), введення за їх допомогою пропаганди та створення спрямованого інформаційно-психологічного впливу, на українців з метою здійснення дезінформації, нагнітання обстановки, виправдання агресії, деморалізації патріотичного налаштованих кіл українського суспільства;
- контр інформаційна боротьба, виключення з радіопростору на окупованих Росією територіях загальнодержавних українських теле- та радіоканалів, взяття під контроль регіональних та місцевих ЗМІ;
- застосування пропагандистських підрозділів в інформаційних та соціальних мережах;
- широке застосування акцентів впливу серед місцевого населення та всяких «козаків», «ополчення» тощо.

Слід зазначити, що під час інформаційної війни Росією на південному сході України була здійсненна низка інформаційно-психологічних акцій та застосування ІЗ, пов'язаних з паплюженням образу та авторитету воєнно-політичного керівництва країни та військових формувань України. Ці дії проводились у вигляді як самостійних акцій, так і на підтримку бойових дій. Ознаками проведення інформаційної війни Кремлем, виявленими та зафіксованими, є [11, 15]:

- зміст інформації;
- спрямованість інформації (цільова аудиторія та її характеристика);
- наявність джерел інформації (джерел їх фінансування);
- наявність посилань на джерела інформації в інформаційних матеріалах;
- динаміка представлення інформаційних матеріалів(інтенсивність);
- факти комплексування інформації по різних інформаційних каналах – через радіомовлення, телебачення, пресу, Internet, чутки та ін.;
- поява в інформаційних матеріалах деталей, відсутніх в еталонному джерелі;
- використання спеціальних приймачів та підходів (психотехніки).

ВИСНОВКИ

Слід зазначити, що в сучасних умовах військової агресії Росії суттєво змінився характер збройної боротьби – вона набула ознак не тільки інформаційної війни. Акценти збройної боротьби зміщувався у бік реалізації інформаційних технологій. При цьому дедалі більше значення у досягненні політичних та воєнних цілей набувають інформаційно-психологічні операції, акції, дії та інформаційна зброя.

Інформаційна зброя – це новий еволюційний крок на шляху розвитку новітніх зразків зброї. Така зброя має специфічні та характерні тільки їй ознаки. Недооцінка можливостей інформаційної зброї у

сучасній інформаційній війні може стати фатальною під час подальшого загострення воєнно-політичної обстановки. Це підтверджується тими бойовими діями, які зараз ведуться в Україні.

ЛІТЕРАТУРА

[1] Бойко В.В. Устная пропаганда: критерии, показатели, условия эффективности / В.В. Бойко – Л. Лениздат, 1983 – 98 с.

[2] Нилус С.А. Протоколы Сионских Мудрецов: Всемирный тайный заговор / изд. Берлин, 1922. – 125с.

[3] Хорошко В. Особливості застосування сучасної інформаційної зброї /В.Хорошко, Т.Козел, О.Ярошенко // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, Вип 1(29), 2015. – С. 9-14.

[4] Пирцхалава Л.Г. Информационное противоборство в современных условиях / Л.Г. Пирцхалава, В.А. Хорошко, Ю.Е. Хохлачова, М.Е. Шелест – К: ЦП «Компринт», 2019. – 226 с.

[5] Баланюк Ю.В. Інформаційно – психологічні впливи у кіберпросторі / Ю.В. Баланюк, В.В. Козловський, В.О. Хорошко, Ю.Є. Хохлачова – К : ЦП «Компринт», 2020. – 109 с.

[6] Грищук Р.В. Кібернетична зброя : класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї / Р.В. Грищук, В.О. Хорошко // Сучасна спеціальна техніка №3(46), 2016. – С .94 – 101.

[7] Хозиков В. Информационное оружие /В. Хозиков – М : ОАМА – Пресс, 2003 . – 28 с.

[8] Білобородов О.О. Технології інформаційно-психологічних війн та інформаційно-психологічна зброя /О.О. Білобородов, А.С. Довгонолий // Озброєння та військова техніка, №4(24), 2019. – С. 43-97.

[9] Хорошко В. Концепція застосування інформаційних впливів та протидій інформаційній зброї / В. Хорошко, Ю. Хохлачова, М. Прокофьєв // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні; Вип. 1 (31), 2016. – С. 9-22.

[10] Чепков І.В. Операція протидії «гібридній війні» в сучасних умовах: технічний аспект. / І.В. Чепков, С.В. Леницький, А.А. Гультяєв, А.Ю. Гупало, М.М. Чепурія // Озброєння та військова техніка, №1(13), 2017. – С. 3-8.

[11] Певцов Г.В. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії / Г.В. Певцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський // Наука і оборона, №2, 2015. – С. 28 -32.

[12] Бурячок В.Л. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко – К: ТОВ «СК ГРУП УКРАЇНА», 2015. – 449 с.

[13] Світова гібридна війна : український фронт / За заг.рез. В.П. Горбуліна – К : НІСД, 2017. – 496 с.

[14] Курбан О.В. Теорія інформаційної війни і базові основи, методологія та понятійний апарат / О.В. Курбан // Scientific Journal «Science Rise», №11/1 (16), 2015. – С. 95-101.

[15] Беликова Т.В. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: коллективная монография под ред. В.В. Баранника и В.М. Безрука / Т.В. Беликова – Харків : ТОВ «Видавництво Лідер», 2017. – 600 с.

INFORMATION WEAPONS AS A TOOL OF INFORMATION WARFARE

Information weapons are a new evolutionary step on the way to the development of the latest types of weapons. Such a weapon has specific and characteristic features only for it. In the modern conditions of Russia's military aggression, the armed struggle has acquired the characteristics of not only an information war. Its emphasis shifted towards the implementation of information technologies. At the same time, information and psychological operations, actions, actions and information weapons are gaining more and more importance in the achievement of political and military goals, the underestimation of the capabilities of which in the modern information war can become fatal during the further aggravation of the military and political situation. This is confirmed by the hostilities currently taking place in Ukraine.

In a modern war, it is impossible to achieve the set goals without the constant implementation of measures of information warfare. Therefore, experts single out information weapons as an independent type of weapon, which is considered as a means of information warfare.

Information warfare and influence can be carried out in the political, economic, defense, scientific and technical and other spheres by: influencing elements of information and telecommunication systems with the aim of destroying elements of the infrastructure of state and military administration, interception and processing of open information circulating in information systems and published in mass media; unauthorized access to information resources and their subsequent rearrangement, destruction or embezzlement; interception and decryption of information flows transmitted by communication channels, side emissions or received through the use of special technical means of information interception; formation and dissemination of information channels of the enemy or global networks of disinformation with the aim of influencing the evaluations, intentions and orientation

of people, groups of people, society as a whole and the military and political leadership of the state.
Information warfare is the spread of certain ideas, views or ideology, and is a means of certain politics. The global tool for its implementation is mass media and various communications.
The article also discusses the theory of information warfare in the political sphere, it should be considered that it takes place at the strategic, operational and tactical levels.
Mainly, the highest political elite of the state operates at the strategic level, and the information units of the political path operate at the operational and tactical levels.
Key words: information war, information weapon, information struggle, information and psychological influences, information struggle.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khoroshko Volodymyr, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net..
Orcid ID: 0000-0001-6213-7086.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khokhlachova Yuliia, candidate of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Пірцхалава Тіна Павлівна, студентка Навчально наукового інституту Міжнародних відносин Київського національного університету ім. Тараса Шевченка.

Pirtskhalava Tina, student of the Educational Scientific Institute of International Relations of Kyiv National University named after Taras Shevchenko.
E-mail: kesane1827@gmail.com.
Orcid ID: 0000-0002-4320-3073.

Іванченко Ігор Сергійович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Ivanchenko Ihor, candidate of technical sciences, associate professor, associate professor of the Department of Information Technology Security of the National Aviation University.
E-mail: igor-p-l@ukr.net.
Orcid ID: 0000-0003-3415-9039.

DOI: 10.18372/2410-7840.24.16931
УДК 654.071

РОЗРОБКА БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ НА ОСНОВІ БЛОКЧЕЙНУ

Святослав Василишин, Іван Опірський

В реаліях захисту інформації у кіберпросторі існує багато засобів та підходів до безпеки урядового, бізнес та приватних секторів, одним з яких цілком ймовірно можуть стати системи побудовані на основі блокчейну. З кожним роком кількість інформації яка проходить через всесвітню павутину та кількість користувачів зростає у геометричній прогресії, разом з цими факторами росте й кількість технологій, які забезпечують безпеку та конфіденційність даних користувачів в мережі. З теперішніми темпами технології здатні старіти швидше ніж встигають зайняти свою нішу на ринку, а відтак їхня підтримка перестає бути актуально, що дозволяє зловмисникам прориватися крізь захист або знаходити нові вразливості у вже існуючих системах. Блокчейн одна з технологій яка поки не так часто використовується саме в урядових та бізнес системах, як технологія навколо якої можна побудувати захист своєї мережі. Дужче часто це зумовлено тим, що такі інституції потребують індивідуальних підходів для рішення своїх проблем та потреб, а розробка свого підходу на основі блокчейну потребує дуже багато грошових інвестицій та спеціалістів, яких на ринку в даний момент ще не так багато. Однак в майбутньому, коли блокчейн стане доступнішим не тільки для оперування крипто валютами й для використання їх у внутрішніх системах він буде