мативно-правовой и теоретико-методологической базы применения полиграфа. Слепое копирование чужого опыта неизбежно сопровождается и копированием чужих ошибок, вредной зависимостью темпов, качества и вектора развития полиграфологии конкретного государства от влияния со стороны.

Ключевые слова: субъектность, полиграфология, методики полиграфных исследований, тесты.

polygraphology of a particular state on outside influence.

Key words: subjectivity, polygraph science, methods of polygraph researches, tests.

УДК 354.42.44

ОСТРОУХОВ Володимир Васильович
ПРИСЯЖНЮК Микола Миколайович

СОЦІАЛЬНО ОРІЄНТОВАНІ ТА ЗАГАЛЬНОДОСТУПНІ РЕСУРСИ МЕРЕЖІ «ІНТЕРНЕТ» В ІНФОРМАЦІЙНІЙ ВІЙНІ ПРОТИ УКРАЇНИ

Постановка проблеми. У XXI столітті інформація стала регулятором усіх суспільних, політичних, економічних та соціальних комунікацій. Створення єдиного інформаційного простору є позитивним для людства, адже швидкий обмін економічною, політичною, технічною та іншою інформацією дає можливість людству швидко розвиватися. Однак створення інформаційного суспільства може призвести до виникнення багатьох інформаційних катастроф і руйнування духовності суспільства.

Такі негативні прояви інформаційного суспільства породжують поняття «інформаційна війна», що стала концентрованою реалізацією всього комплексу інформаційних загроз національній безпеці та реальною загрозою безпеці всього людства. Аналізуючи хід і наслідки війн та збройних конфліктів XX та XXI століть, варто зазначити, що роль інформаційного забезпечення різко зростає і свідчить про новий рівень ведення інформаційного протиборства. Інформаційна війна включає в себе багато аспектів, основними з яких є вплив на свідомість людини та суспільства.

В умовах розвитку засобів масової інформації (ЗМІ), інформаційних технологій і техніки інформаційне протиборство у світі стає масштабнішим і результативнішим. Поява технічних засобів нового покоління, що здатні ефективно впливати не тільки на психіку та свідомість людей, але й на

інформаційно-технічну інфраструктуру країн і їхніх збройних сил, дає змогу розглядати інформаційну зброю як засіб масового ураження [1].

Інформаційна війна є узгодженою діяльністю з використання інформації як зброї для ведення не лише бойових дій, а й у періоди, коли немає відкритого військового протистояння. Основною метою інформаційної війни є послаблення моральних і матеріальних сил супротивника та посилення власних, порушення обміну інформації конкурента. Головне завдання інформаційних війн полягає в маніпулюванні масовою свідомістю [2].

Стрімкий розвиток ЗМІ не міг не спричинити хвилю інтересів до можливостей масштабного психологічного впливу на політичних та бізнесових опонентів. Розвиток новітніх технологій зумовив перехід від так званої класичної війни до війни нового типу – інформаційно-психологічної.

Одним із головних методів ведення інформаційно-психологічної війни є пропаганда, тобто поширення різних політичних, філософських, наукових, художніх, інших мистецьких ідей із метою впровадження їх у громадську думку, справляння вигідного впливу на неї, провокування запрограмованих емоцій та зміни ставлення до певної ситуації або поводження певної групи людей, безпосередньо чи опосередковано вигідного організаторам.

Поява інтернету надала нові переваги при його використанні для інформаційно-психологічного впливу, що зумовлено такими чинниками:

– становлення та перехід до нового типу інтернет-ЗМІ, сайти новин яких охопили близько 90 % інтернету;

– створення сервісів соціальних мереж;

– інтеграція інтернет-ЗМІ в соціальні мережі та трансформація їх у соціальні медіа.

Виникає феномен соціальної журналістики. Формується нова медіасистема, в якій професійна та соціальна журналістика вступають у взаємодію, а нові інтерактивні канали поширення новин – соціальні мережі – дають можливість подолати односторонній, розірваний характер комунікації традиційних медіа, роблять можливим відповідь аудиторії.

Зростає рівень довіри до соціальних медіа з боку аудиторії. Соціальні мережі почали використовуватися в політичній діяльності. Основними майданчиками для об'єднання протестувальників стали не юридично зареєстровані організації, а їхні сайти в інтернеті. Соціальні мережі використовуються в організаційних цілях для розповсюдження інформації як засоби масових комунікацій. Виникає поняття «Твіттерної революції».

Аналіз останніх конфліктів свідчить про збільшення використання інтернету в інформаційних війнах. Інтернет-простір став новим майданчиком інформаційно-психологічного впливу, що має низку суттєвих переваг над класичними методами впливу.

На думку авторів, дослідження технологій використання соціально орієнтованих та загальнодоступних

ресурсів мережі «Інтернет» в інформаційній війні проти України дасть змогу здійснювати ефективні заходи протидії інформаційно-психологічному впливові в соціальних мережах.

Аналіз останніх досліджень і публікацій. Наукові дослідження у сфері ведення інформаційної війни звертають увагу на цілу низку аспектів цього явища. Серед них політичні, економічні, соціальні, психологічні тощо. Досліджували цю проблематику закордонні та вітчизняні науковці, а саме: Ю. Бабенко, Д. Догерті, В. Желіховський, М. Лібікі, В. Ліпкан, Ю. Максименко, Г. Почепцов, В. Сливка й інші.

Водночас через складність, комплексність та багатоаспектність ця проблематика досі не вичерпана. Це також пов'язано зі стрімким розвитком інформаційних технологій і, відповідно, розвитком та використанням соціальних мереж для здійснення інформаційно-психологічного впливу.

Метою статті є аналіз технологій використання соціальних мереж інтернету в інформаційній війні проти України. Завданням роботи є дослідження проблем використання соціально орієнтованих і загальнодоступних ресурсів мережі «Інтернет» на шкоду інформаційній безпеці України та шляхів протидії цим загрозам.

Виклад основного матеріалу. Наймасованішим застосуванням соціально орієнтованих і загальнодоступних ресурсів мережі «Інтернет» для здійснення інформаційно-психологічного впливу характеризується інформаційна війна Російської Федерації проти України, що розгорнулася на початку 2014 року одночасно із захопленням Криму. Тому не дивно, що саме вона стала предметом ретельних спостережень і досліджень для фахівців різних країн світу із ведення інформаційної війни та забезпечення інформаційної безпеки.

Проведення такого аналізу для самої України ще актуальніше, тож у подальшому при розгляді інформаційно-психологічних операцій як складових інформаційної війни у соціальних мережах аналізуватимуться насамперед приклади таких дій із боку пропагандистів Російської Федерації. Варто зазначити, що методи та технології не мають національної належності, а є універсальними з погляду можливості їх застосування.

Соціально орієнтовані та загальнодоступні ресурси мережі «Інтернет» у зоні операції Об'єднаних сил (ООС) характеризуються домінуванням на звільнених і тимчасово окупованих територіях України проросійської пропаганди, активним використанням соціальних мереж інтернету на шкоду інформаційній безпеці України.

Мешканці звільнених і тимчасово окупованих територій для отримання або обміну інформацією найбільше використовують соціальні мережі «Вконтакте» та «Одноклассники», програмні месенджери «Viber» і «Skype» у зв'язку з активною популяризацією проросійських електронних ЗМІ.

На території Донецької області діють понад 250 інформаційних ресурсів у соціальних мережах «Вконтакте» та «Одноклассники» з кількістю учасників від 100 осіб до 500 тисяч, основною аудиторією яких є

жителі РФ, Донецької, а також суміжних із нею областей. Їхніми основними завданнями є розповсюдження деструктивної інформації, спрямованої на дестабілізацію ситуації на сході України, доведення до жителів тимчасово окупованих українських територій неправдивої та відверто провокаційної інформації стосовно ситуації в державі та світі з метою підтримки інспірованих керівництвом РФ ідей так званих «Новороссии» та «русского мира».

Проти України ведеться інформаційна війна з боку Росії, що негативно відбивається на формуванні образу України на міжнародній арені [3].

Варто зазначити, що в умовах ведення суміжною стороною «гібридної» війни проти України однією з найактивніших зон «бойових дій» є зазначені вище інформаційні ресурси й соціально орієнтовані мережі, які використовують Російська Федерація та підконтрольні їй самопроголошені анклави «ЛНР/ДНР» для здійснення масштабних кампаній інформаційно-психологічного впливу як на мешканців тимчасово-окупованих територій сходу України, так і жителів інших регіонів держави.

До внутрішніх загроз інформаційній безпеці України належать:

– використання загальнодоступних і соціально орієнтованих ресурсів мережі «Інтернет» для здійснення протиправної діяльності, прихованої під виглядом сепаратизму, екстремізму, фінансування тероризму, не пов'язаної з діяльністю країни-агресора;

– залучення мешканців тимчасово окупованих територій до лав незаконних збройних формувань самопроголошених «ДНР/ЛНР» задля власного збагачення у зв'язку з низьким рівнем матеріально-технічного, грошового й фінансового забезпечення та їхня співпраця з представниками спецслужб РФ із поширення деструктивного контенту в мережі «Інтернет», спрямованого на дестабілізацію ситуації в країні та за її межами;

– посягання на інформаційну безпеку країни та за її межами у зв'язку із зосередженням сил і засобів електронного інформаційного простору на території країни-агресора.

Основними зовнішніми загрозами є:

– використання спецслужбами РФ найпопулярніших соціальних мереж «Вконтакте» та «Одноклассники» серед користувачів мережі «Інтернет» на звільнених і тимчасово окупованих територіях України для проведення деструктивної діяльності на шкоду інформаційній безпеці держави, залучення громадян України до незаконних збройних формувань так званих «ДНР/ЛНР», пропагування ідей «русского мира», історичного повернення РФ до моделі СРСР;

– використання спецслужбами РФ соціальних ресурсів мережі «Інтернет» із метою поширення закликів до повалення конституційного ладу силовим шляхом, зміни меж території України, фінансової та матеріальної допомоги самопроголошеним республікам, здійснення антиконституційних дій, спрямованих на дестабілізацію ситуації в Україні;

– проведення спецслужбами РФ масштабних зовнішніх інформаційних

впливів на шкоду національним інтересам України шляхом розповсюдження дезінформації стосовно діяльності військовослужбовців ЗС України в зоні ООС у проросійських ЗМІ та підконтрольних ресурсах;

– використання спецслужбами РФ соціальних мереж із метою збирання та аналізу інформації стосовно громадян України у зв'язку з відсутністю вітчизняних аналогів соціальних мереж.

Очевидно, що чітке розуміння технологій ведення воєнних дій в інтернеті, і насамперед у соціальних мережах, є необхідною складовою військової майстерності будь-якої держави, яка прагне перемоги в майбутніх протистояннях, котрі мають дедалі більше виражену інформаційно-психологічну домінанту. Саме тому аналіз дій російських пропагандистів у соціальних мережах та розробка ефективних контрзаходів на майбутнє є життєво важливими для захисту безпеки української державності.

Фактори, що негативно впливають на сучасному етапі на конструктивне вирішення проблем в Україні в період активізації «інформаційної» війни:

1. Відсутність чітко сформованих політико-правових механізмів державного управління інформаційно-психологічною безпекою України.

2. Несформульованість концепції ролі України у світовій інформаційній війні та нерозробленість нормативно-правових документів, що визначають засади участі України в інформаційній війні. І це в період, коли світова спільнота консолідується у протистоянні російській агресії.

3. Відсутність комплексної програми захисту населення країни від деструктивних впливів інформаційної війни, масової просвіти населення, включно з дітьми шкільного віку, студентською молоддю, пенсіонерами.

Варто навести порівняння, що наочно демонструють відставання України у протидії інформаційному тиску з боку Росії:

1. У РФ функціонує кілька науково-дослідних центрів, завдання яких – інформаційна діяльність на територіях колишніх республік СРСР, зокрема України.

В Україні теж є аналогічні аналітичні центри, однак у питаннях інформаційної війни вони переважно впроваджують інформаційні технології для забезпечення внутрішньополітичних інтересів. Створене у 2014 році Міністерство інформаційної політики України не виконало покладене на нього одне з ключових завдань, затверджене у Програмі дій уряду, – протидія інформаційній агресії з боку Росії та підвищення обізнаності громадян у сфері медіа. Поки що ці завдання залишаються лише на папері.

2. Російська Федерація посідає одне з перших місць у світі за державними витратами на пропаганду. Сумарна державна підтримка проурядових ЗМІ в Росії сягнула 48,65 млрд рублів на рік (1,6 млрд дол.).

Цифра підтримки українських ЗМІ в контрпропаганді конкретно не визначена.

3. У ВНЗ Росії для студентів запроваджені курси з інформаційної,

психологічної безпеки, кібербезпеки тощо.

В Україні лише в Національному університеті імені Тараса Шевченка на факультеті журналістики ведеться курс «Інформаційні війни».

4. У багатьох школах Росії читають спецкурс для учнів 11 класу «"Інформаційна війна" з кіберзлочинами, кіберекстремізмом і кібертероризмом».

У школах України немає навіть натяку на таку роботу.

5. У Росії працюють численні «фабрики тролів», що забезпечують підривну діяльність у соцмережах, розхитуючи наше суспільство зсередини.

Головними напрямами дій російських пропагандистів в інформаційній війні у соціальних мережах є такі:

– сіяння страху та паніки серед широких верств населення;

– формування громадської думки щодо конкретних тактичних дій РФ і її стратегії в цілому;

– спонукання населення та політичних лідерів України до саморуйнівних дій;

– поширення дезінформації;

– заклики до саботування розпоряджень української влади;

– підрив бойового духу українських бійців і населення;

– дискредитація політичного та військового керівництва України;

– провокування конфліктів в Україні та у середовищі її політичних сил;

– провокування користувачів соціальних мереж із метою збирання інформації;

– апелювання до світової спільноти для виправдання російської агресії проти України й дискредитації України;

– вербування «живої сили» для участі в конфлікті на Донбасі на боці сепаратистів;

– використання постів у соціальних мережах як джерела для подальшої легалізації дезінформації у ЗМІ [4].

У сьогоднішньому світі просто донести до людини певну інформацію для отримання бажаного ефекту в інформаційних війнах – зміни її світогляду та спонукання до певної поведінки. Успішність впливу насамперед залежить від того, у яку форму «запаковано» повідомлення, що його отримує реципієнт. Форма прямої, лобової агітації та пропаганди, яка домінувала ще кілька десятиліть тому, сьогодні не працює. На зміну їй прийшли маніпулятивні технології прихованого впливу, які можна віднести до категорії «soft power» – «м'якої сили» [5].

Висновки. Першочерговим завданням усіх державних, громадських, наукових, експертних, журналістських інституцій є розроблення термінових ефективних заходів щодо нейтралізації інформаційної агресивної діяльності Російської Федерації проти України та протидії її подальшому розгортанню. Виклики, що постали перед Україною, потребують вжиття негайних організаційно-правових заходів із метою модернізації всієї системи інформаційної та кібернетичної безпеки держави.

Російська інформаційна агресія в соціальних мережах проти України

є наймасштабнішим прикладом війни такого типу та набирає обертів. Технології війн четвертого покоління, до яких належать війни в соціальних мережах, постійно відшліфовуються та вдосконалюються.

Варто зауважити, що цей процес ще не сягнув свого піку – фактично він тільки розпочався. До нього активно приєднуватимуться нові країни, які вже зараз створюють і тренують підрозділи для ведення війни в соціальних мережах, і це стимулюватиме появу нових технологій і контртехнологій. Битви у віртуальному просторі та інформаційна зброя ставатимуть дедалі витонченішими. І зрозуміло, що ті, хто почне опановувати новий театр воєнних дій першими, матимуть значну перевагу в новій парадигмі війн. Відповідно, й Україні слід приділити якнайбільше уваги підготовці до бойових дій в інтернеті взагалі та війнах у соціальних мережах зокрема. «Хто хоче миру, хай готується до війни» – ця перевірена роками істина певною мірою стосується і війни інформаційної.

Ефективна реалізація стратегічних пріоритетів та основних принципів і завдань державної політики у сфері інформаційної безпеки потребує вдосконалення організаційно-правових механізмів управління інформаційною безпекою, відповідного інтелектуально-кадрового й ресурсного забезпечення. Правові аспекти організації інформаційної безпеки стали обов'язковим компонентом законів, концепцій, доктрин, стратегій і програм, зокрема законів України: «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», Стратегії національної безпеки України, Стратегії кібербезпеки України, Доктрини інформаційної безпеки України тощо. Із цією метою потребують внесення змін деякі закони України («Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про Службу безпеки України» тощо).

Отже, у процесі дотримання курсу стратегії національної безпеки України з урахуванням основних тенденцій розвитку інформаційного суспільства набуває особливого значення розроблення актуальних проблем організації забезпечення інформаційної безпеки держави, прискорення розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами.

Список використаних джерел

1. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. та ін. Інформаційна безпека : підручник / під ред. В. В. Остроухова. Київ : Видавництво «Ліра-К», 2021. 412 с.

2. Лібікі М. Що таке інформаційна війна? URL: http://viysko.com.ua/texnologiji-voyen/martin-libiki-shho-take-informacijna-vijna (дата звернення: 15.02.2020).

3. Сливка В. Інформаційна війна проти України: міф чи реальність? URL: http://intkonf.org/slivka-w–nformatsiyna-viyna-proti-ukrayini-mif-chi-realnist (дата звернення: 15.02.2020).

4. Нестеренко С. Соціальні мережі як інструмент сучасної інформаційно-психологічної війни. URL: https://www.armyua.com.ua/socialni-merezhi-yak-instrument-suchasno%D1%97-informacijno-psixologichno%D1%97-vijni (дата звернення: 15.02.2020).

5. Джил Догерті. Усі брешуть, або як трансформувалися російські ЗМІ. URL: http://osvita.mediasapiens.ua/material/33880 (дата звернення: 15.02.2020).

Аннотация. В статье рассматриваются технологии использования социально ориентированных и общедоступных ресурсов сети «Интернет» в информационной войне против Украины. Раскрываются понятия информационной войны, проблемы использования социальных сетей интернета в ущерб информационной безопасности Украины и пути противодействия этим угрозам.

В XXI столетии позитивным для человечества стало создание единого информационного пространства, что позволяет ему скорее развиваться. Но создание информационного общества приводит также к возникновению отрицательных проявлений, порождающих такое понятие как «информационная война».

Основной целью информационной войны является ослабление моральных и материальных сил противника и усиление собственных, нарушение обмена информации конкурента. Главная задача информационных войн состоит в манипулировании массами.

Стремительный рост информационных технологий позволяет эффективнее осуществлять информационно-психологическое влияние на массовое сознание. Интернет-пространство с его социальными сетями стало новой площадкой ведения информационных войн.

Социально ориентированные и общедоступные ресурсы сети «Интернет» в зоне операции Объединённых сил характеризуются доминированием на освобожденных и временно оккупированных тер-

Abstract. The article deals with technologies of using socially oriented and publicly available Internet resources in information war against Ukraine. The concept of information war, problems of using social networks to the detriment of information security of Ukraine and ways to counteract these threats are presented.

In the 21st century, the creation of a single information space that enables humankind to develop faster has become positive for humanity. However, the creation of the information society also leads to negative side effects that give rise to such a concept as information warfare.

The main purpose of information warfare is to weaken the moral and physical forces of the enemy while strengthening their own, to disrupt the exchange of information for the competitor. The main task of information wars is to manipulate the masses.

The rapid development of information technologies makes it possible to carry out information and psychological influence on the mass consciousness more effectively. The Internet space with its social networks has become a new platform for information wars.

Socially oriented and publicly available Internet resources in the Joint Forces Operation zone are characterized by the dominance of pro-Russian propaganda in the liberated and temporarily occupied territories of Ukraine, as well as by the active use of social networks to the detriment of Ukraine's information security. Their main tasks are to disseminate destructive information aimed at

риториях Украины пророссийской пропаганды, активным использованием социальных сетей интернета для нанесения вреда информационной безопасности Украины. Их основной задачей является распространение деструктивной информации, направленной на дестабилизацию ситуации на востоке Украины. Против Украины ведется информационная война со стороны России, что негативно отражается на формировании образа Украины на международной арене.

Реализация стратегических приоритетов и основных принципов и задач государственной информационной политики Украины нуждается в усовершенствовании организационно-правовых механизмов управления информационной безопасностью, интеллектуально-кадрового и ресурсного обеспечения.

Ключевые слова: информационная война, социальные сети интернета, информационно-психологическое влияние, информационная безопасность.

destabilizing the situation in Eastern Ukraine. Russia is waging an information war against Ukraine, which has a negative impact on the formation of Ukraine's image in the international arena.

The implementation of strategic priorities and basic principles and tasks of the national information policy of Ukraine requires the improvement of organizational and legal mechanisms of information security management, proper staffing and resourcing.

Key words: information war, social networks, information and psychological influence, information security.