

**INTERNATIONAL SCIENCE GROUP
ISG-KONF.COM**

**MODERN INFORMATION
TECHNOLOGIES AND THEIR
IMPLEMENTATION IN THE
PROCESSES OF SOCIAL AND
TECHNICAL PROJECT
MANAGEMENT**

**ABSTRACTS OF IV INTERNATIONAL
SCIENTIFIC AND PRACTICAL CONFERENCE
BOSTON, USA
17-18 FEBRUARY 2020**



ISBN 978-617-7886-00-5

MODERN INFORMATION TECHNOLOGIES AND THEIR
IMPLEMENTATION IN THE PROCESSES OF SOCIAL AND
TECHNICAL PROJECT MANAGEMENT
Abstracts of IV International Scientific and Practical Conference
Boston, USA
17-18 February 2020

-

UDC 01.1

BBK 91

The 4 th International scientific and practical conference“MODERN INFORMATION TECHNOLOGIES AND THEIR IMPLEMENTATION IN THE PROCESSES OF SOCIAL AND TECHNICAL PROJECT MANAGEMENT” (February 17-18, 2020)

Boston, USA 2020. 154 p.

ISBN 978-617-7886-00-5

The recommended citation for this publication is:

Kilmukhametova Yu.H., Condition of periodontal tissues in patients with urolithiasis // Modern information technologies and their implementation in the processes of social and technical project management. Abstracts of IV International Scientific and Practical Conference. Boston, USA. 2020. Pp. 165-167. URL: <http://isg-conf.com>.

The content and reliability of the articles are the responsibility of the authors. When using and borrowing materials reference to the publication is required.

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine, Russia and from neighbouring countries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

e-mail: info@isg-konf.com

homepage: isg-konf.com ©

2020 Internation Science Group “isg-konf.com” ® ©

2020 Authors of the articles

TABLE OF CONTENTS

1.	Доля К.В., Доля О. Є. РИЗИКИ ФУНКЦІОНУВАННЯ МІСЬКИХ ПАСАЖИРСЬКИХ ТРАНСПОРТНИХ СИСТЕМ	8
2.	Petrov K. E., Petrova K. K. ENSEMBLE APPROACH TO BUILDING THE MODEL OF MULTIFACTOR ESTIMATION OF ALTERNATIVES	13
3.	Babko N., Kuskova S., Orel V. THE ROLE OF STUDENTS 'INDEPENDENT WORK IN THE PROCESS OF FORMING THE BACHELOR'S PROFESSIONAL COMPETENCIES IN MARKETING	17
4.	Grechanyk V. G., Chornovol V.O., Lavryk R. V., STUDY OF IMPACT OF CO2 AND SO2 IMPOSSIBLE IMPROVEMENTS ON CORROSION OF COMPOSITION MATERIALS ON BASE OF COPPER	22
5.	Medvid I.,Kyrychenko S., MANAGEMENT OF ENTERPRISES STAFF POLICY TO IMPROVE STABILITY	25
6.	Stepanov A. DISTANCE COURSES AS A TOOL OF FOREIGN LANGUAGE TEACHING AND LEARNING: A LVIV UNIVERSITY OF TRADE AND ECONOMICS EXPERIENCE	28
7.	Sydorchuk A. S.,Sydorchuk L. I., Gaudia Deepak INFLUENZA H1N1 AND CORONAVIRUS 2019-nCoV: EPIDEMIOLOGICAL DIFFERENCES AND CLINICAL ASPECTS	31
8.	Hraniak V. F. METHOD OF WEIGHT COEFFICIENTS CALCULATION OF ARTIFICIAL NEURAL- LIKE NETWORK IN DIAGNOSTIC SYSTEMS OF HYDRAULIC UNITS	33

9.	Zaichenko S. V., Shevchuk S. P., Halem A. CREATING A PISTON COOLING SYSTEM FOR INTERNAL COMBUSTION ENGINES	38
10.	Андрияка А. А., Выдыборец С. В. АНЕМИЯ ЗЛОКАЧЕСТВЕННОГО ОБРАЗОВАНИЯ: ПРОБЛЕМА СОВРЕМЕННОЙ МЕДИЦИНСКОЙ КЛИНИКИ	40
11.	Борисенко Д. О., Видиборець С. В. ВМІСТ МОЛОЧНОЇ КИСЛОТИ В ЕРИТРОЦИТАХ ПЕРВИННИХ І РЕГУЛЯРНИХ ДОНОРІВ КРОВІ КИЇВСЬКОГО РЕГІОНУ	45
12.	Бортняк В. А. ПРАВОВИЙ ЗМІСТ ПОНЯТТЯ КООРДИНАЦІЇ ФІНАНСОВОГО КОНТРОЛЮ	48
13.	Бортняк К. В. ЮРИДИЧНИЙ АСПЕКТ ВЕРХОВЕНСТВА ПРАВА У ДІЯЛЬНОСТІ ДЕРЖАВНОГО БЮРО РОЗСЛІДУВАННЯ	52
14.	Бублій Ю. С. ГІПЕРСЕРОТОНІНЕМІЯ В ПЛАЗМІ КРОВІ І НЕВРОЛОГІЧНІ РОЗЛАДИ У ХВОРИХ НА ЗАЛІЗОДЕФІЦИТНУ АНЕМІЮ: МОЖЛИВИЙ ВЗАЄМОЗВ'ЯЗОК	55
15.	Bulgak E. D. MEDICAL AND PSYCHOLOGICAL ASPECTS OF SEXUAL EDUCATION OF YOUNG PEOPLE IN MODERN UKRAINE	60
16.	Вайда Т. С. ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА АГРЕСІЯ РОСІЇ ЯК СКЛАДОВА ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ	63
17.	Видиборець С. В. ЛЕКЦІЙНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОГО ПРОЦЕСУ НА КУРСАХ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ЛІКАРІВ	71

18.	Выдыборец Н. В. ГЕМАТОЛОГИЧЕСКИЕ НАРУШЕНИЯ У БОЛЬНЫХ ЭНДОКРИННЫМИ ЗАБОЛЕВАНИЯМИ	76
19.	Гречко А.В., Терещенко К.М. МАРКЕТИНГ І ЙОГО РОЛЬ НА ПІДПРИЄМСТВІ	81
20.	Гришко С. В., Безгинська А. О. ГЕОЕКОЛОГІЧНЕ ЗНАЧЕННЯ ЛІСОСМУГ ДЛЯ СТЕПІВ ПІВНІЧНО- ЗАХІДНОГО ПРИАЗОВ'Я	84
21.	Гришко С. В., Шелудько О. М. СУЧАСНА ГЕОЕКОЛОГІЧНА ОЦІНКА БОТІЄВСЬКОЇ ЗСУВНОЇ ДІЛЯНКИ	87
22.	Докаш В. І., Пержун В. В. НАУКОВО-ПРАКТИЧНІ ДОРОБКИ М. ВЕБЕРА ПРО ПОЛІТИКУ: ІСТОРІЯ ТА СУЧАСНІ ПРАКТИКИ ДЛЯ УКРАЇНИ	90
23.	Заря Л. О., Овчарова І. А. ОСОБЛИВОСТІ МУЗИЧНОГО СПРИЙМАННЯ ФОРТЕПІАННИХ ТВОРІВ ДЛЯ ДІТЕЙ ВІКТОРА КОСЕНКА УЧНЯМИ МОЛОДШИХ КЛАСІВ	96
24.	Казачінер О. С. САМОСТІЙНА РОБОТА У СИСТЕМІ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ДО ФОРМУВАННЯ КОМУНІКАТИВНИХ НАВИЧОК У ДІТЕЙ З ОСОБЛИВИМИ ОСВІТНИМИ ПОТРЕБАМИ	99
25.	Каспрук Н. М. ПРАКТИЧНА СКЛАДОВА У ВИКЛАДАННІ З КЛІНІЧНОЇ ІМУНОЛОГІЇ	101
26.	Кравченко А. С. ФУНКЦІОНУВАННЯ ТА РОЗВИТОК ФІНАНСОВОГО РИНКУ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА	104

27.	Логвіна-Бик Т. А., Бик Н. В. СУЧАСНІ ІНФОРМАЦІЙНІ МОДЕЛІ ОСВІТИ ТІ ЇХ РЕАЛІЗАЦІЯ В ПРОЦЕСАХ УПРАВЛІННЯ НАВЧАЛЬНОЮ ДІЯЛЬНІСТЮ ШКІЛ РІЗНИХ КРАЇН СВІТУ	107
28.	Матушак М. Р., Горошко О. М., Костишин Л. В. ЕКОНОМІЧНИЙ АНАЛІЗ СТАНУ ФАРМАЦЕВТИЧНОГО ЗАБЕЗПЕЧЕННЯ ХВОРИХ НА ГАСТРОЕЗОФАГЕАЛЬНУ РЕФЛЮКСНУ ХВОРОБУ	112
29.	Медвідь І. Ю. УПРАВЛІННЯ КАДРОВОЮ ПОЛІТИКОЮ ПІДПРИЄМСТВА З МЕТОЮ ПОКРАЩЕННЯ СТАБІЛЬНОСТІ ДІЯЛЬНОСТІ	114
30.	Мельник К. М., Пташник С. А. НАПРЯМИ ВДОСКОНАЛЕННЯ БЕЗПЕКИ КРЕДИТНОЇ ДІЯЛЬНОСТІ УКРАЇНСЬКИХ БАНКІВ В КОНТЕКСТІ ЗАРУБІЖНОГО ДОСВІДУ	117
31.	Мулярчук О. В., Выдыборец С. В. РЕЗУЛЬТАТЫ ИЗУЧЕНИЯ СОДЕРЖАНИЯ СВОБОДНЫХ ФРАКЦИЙ БИОГЕННЫХ АМИНОВ В ПЛАЗМЕ КРОВИ ДОНОРОВ	121
32.	Наумейко І. В., Сова Г. В. ДОСЛІДЖЕННЯ МОДЕЛЕЙ ЗАХИСНИХ СИСТЕМ З РІЗНОШВИДКІСНИМИ ЗМІННИМИ	127
33.	Одаренко О. В. МИЛЛЕНИАЛЫ КАК ГЕНЕРАТОР РЕПУТАЦИОННЫХ РИСКОВ ДЛЯ КОМПАНИЙ РЫНКА ТЕЛЕКОМУНИКАЦИЙ	129

34.	Перижняк А. І., Юрків О. І. ДО ДІАГНОСТИКИ ПОСТГІПОКСИЧНИХ ПОШКОДЖЕНЬ СЕРЦЕВО-СУДИННОЇ СИСТЕМИ НОВОНАРОДЖЕНИХ З ПЕРИНАТАЛЬНОЮ ПАТОЛОГІЄЮ.	131
35.	Pishchevskaia E. MENTALITY OF HISTORICAL EPOCHS (HISTORIOGRAPHY OF PROBLEM)	133
36.	Сич Л. М. ВЛИЯНИЕ ХУДОЖЕСТВЕННОГО СМЫСЛА НА МУЗЫКАЛЬНУЮ ФАКТУРУ В КЛАВИРНОМ ТВОРЧЕСТВЕ И. С. БАХА	136
37.	Тишевич Б. Л. ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ КОРОТКОСТРОКОВОГО ПРОГНОЗУВАННЯ ЕЛЕКТРИЧНОГО НАВАНТАЖЕННЯ В ЕНЕРГОСИСТЕМАХ	137
38.	Тишевич Б. Л. ЗАСТОСУВАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ІДЕНТИФІКАЦІЇ ЕНЕРГЕТИЧНИХ ПРОЦЕСІВ	142
39.	Тишевич Б. Л. ПІДВИЩЕННЯ ТОЧНОСТІ МОДЕЛЮВАННЯ ЕЛЕКТРОМЕХАНІЧНИХ СИСТЕМ ВИСОКОГО ПОРЯДКУ У ПРОСТОРІ СТАНІВ	145
40.	Ткачук Т. Ю., Чистоклетов Л., Хитра О. Л. ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ ЯК БАЗОВА АКсіОЛОГІчна КОНСТАНТА	149

Вайда Тарас Степанович, кандидат педагогічних наук,
доцент, завідувач кафедри спеціальної фізичної та вогневої
підготовки Херсонського факультету, Одеський державний
університет внутрішніх справ, Херсон, Україна,

ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА АГРЕСІЯ РОСІЇ ЯК СКЛАДОВА ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ

Актуальність дослідження. Республіку Україну її Конституція (стаття 5 Основного Закону) визначає як суверенну і незалежну, демократичну, соціальну та правову державу [1], яка в своєму становленні пройшла складні випробування і в сучасних умовах протистоїть серйозним внутрішнім та зовнішнім викликам на Півдні й Сході своїх границь щодо захисту державного суверенітету, територіальної цілісності та недоторканності державних кордонів, вирішує складні соціально-політичні проблеми подальшого розвитку державності й громадянського суспільства. При цьому людина, її безпека завжди визнаються в Україні найвищою соціальною цінністю, а захист та гарантування національної безпеки для всього населення країни визначають зміст і спрямованість діяльності правоохоронних органів держави, складають її головний обов'язок та визначають високий рівень відповідальності перед громадянином.

Виходячи з положень Доктрини інформаційної безпеки України, ми погоджуємося із точкою зору її авторів, що застосування Російською Федерацією (далі – РФ) технологій гібридної війни проти української держави перетворило інформаційну сферу на ключову арену протиборства. Саме проти України використовується найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [2].

Значна частина інформації із характеристикою соціально-політичних процесів, які відбуваються в Україні, зокрема, стосовно висвітлення резонансних подій (наприклад, бойових дій при проведенні АТО (антитерористичної операції) та ООС (операції об'єднаних сил) на Сході української держави, під час анексії Криму тощо) не завжди відповідають дійсності. За результатами [моніторингу](#) громадської організації «Інститут

масової інформації» (далі – ІМІ) у січні 2017 року, 10% новин на інформаційних сайтах терористичних організацій окремих районів Донецької і Луганської областей (далі – ОРДЛО) є відвертою брехнею. При цьому 82 % матеріалів про окупаційну владу в інтернет-засобів масової інформації (далі – ЗМІ) на непідконтрольних українській владі територіях Донбасу є компліментарними, 18% – нейтральні, проте критичних матеріалів немає взагалі [3].

Згідно з результатами досліджень організації ІМІ, загалом близько 20 % новин на місцевих сайтах присвячені окупаційній владі, тоді як про українську владу матеріалів більше – 32 % повідомлень. І переважна кількість цих матеріалів (87%) негативно забарвлені, 13 % – нейтральні, а позитивних матеріалів не було виявлено взагалі. У той же час, за даними аналітиків, діяльності російської влади присвячено в середньому 8 % новин, причому у переважній кількості вона теж висвітлюється позитивно (91 % новин), негативні або критичні матеріали – відсутні [3].

Головною причиною цього негативного соціального явища є застосування окремими ЗМІ матеріалу з метою ведення пропагандистської діяльності проти державності України: в такому випадку повідомлення новин використовуються не для інформування громадян, а для нав'язування їм точки зору, котра є вигідною проросійським силам.

У контексті піднятої нами проблеми та у відповідності до вимог статті 31 Закону України «Про національну безпеку України» Стратегією кібербезпеки України визначаються як першочергові компоненти захисту національних інтересів України у сфері кібербезпеки наступні підходи: 1) виявлення наявних та потенційно можливих кіберзагроз життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі; 2) визначення пріоритетних напрямів, концептуальних засад формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави; 3) підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі; 4) уточнення потреб бюджетного фінансування, достатніх для досягнення визначених цілей і виконання передбачених завдань; 5) обґрунтування основних напрямів використання фінансових ресурсів [4].

На практиці в сучасних умовах простежуються спроби окремих ЗМІ (в першу чергу іноземних, зокрема, РФ, на окупованих ОРДЛО, в АР Крим) викривляти державну політику щодо територіальної цілісності та незалежності України, пропагувати ідеї сепаратизму; збільшується кількість фейкових новин.

Хоча російська кібердіяльність стала широко помітною лише під час виборчої кампанії в США у 2016 році, насправді Росія постійно нарощувала та вдосконалювала свій потенціал у цій сфері протягом останніх десяти років.

Кібернетична агресія, котра все активніше проявляється в ЗМІ і ведеться в соціальних мережах, вимагає вивчення природи інформаційної війни, яку Росія фактично здійснює проти України, а також прогнозування наслідків цієї війни для України та пошуку шляхів щодо мінімізації негативного впливу держави-агресора [5].

Проведений аналіз ряду наукових робіт вітчизняних вчених дає підстави констатувати, що потенційні можливості ЗМІ в частині їх впливу на формування суспільства чи певних її суб'єктів були предметом вивчення та монографічних досліджень багатьох науковців. За результатами їх узагальнення можна виділити наступні напрямки діяльності сучасних медіаресурсів та їх роль і значення у соціальному житті країни: 1) засоби масової комунікації як інструмент моделювання політичної свідомості у виборчому процесі розглядали О.О. Заславська, О.А. [Семченко](#) та ін.; 2) дослідження моделі медіаполітичної системи у сучасній Україні, інформаційного розвитку та глобалізації комунікаційного простору здійснювали С.В. [Демченко](#), Т.Я. [Лильо](#) та ін.; 3) можливості впливу мас-медіа на створення та функціонування стереотипів масової свідомості аналізували М.В. [Бутиріна](#), І.А. [Чудовська-Кандиба](#) та ін.; 4) освітньо-виховну роль ЗМІ як чинника формування людини обґрунтовували А.М. [Бахметьєва](#), І.І. [Курлішук](#), С.І. [Семчук та ін.](#); 5) проблемою свободи преси та її впливу на формування соціуму переймалися В.М. [Гвоздєв](#), О.В. [Кабачна](#), Б.І. [Мотузенко](#), Н. Хомский та ін.; 6) методи діяльності та форми взаємодії ЗМІ з суб'єктами державного управління вивчали Н.В. [Коритнікова](#), Я.О. [Легеза](#), О.І. [Трухачов](#) та ін.; 7) місце засобів масової комунікації у системі соціалізації окремих верств населення (вихованні суспільно

орієнтованого способу життя) аналізували А.А. [Согорін](#), Н.С. [Удріс](#) та ін.

У свою чергу окремі суб'єкти вітчизняного медіапростору недостатньо уваги, на нашу думку, приділяють спростуванню неправдивої інформації про Україну, не протистоять їй висвітленням проявів масових прикладів патріотизму та героїзму українського народу при проведенні військових та службово-бойових дій під час АТО й ООС на сході держави. ЗМІ також слабо використовується дієвий стратегічний наратив з метою об'єднання українського народу навколо вирішення існуючої проблеми протидії зовнішній агресії (наратив – спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію – уточнено нами) [2].

Результати дослідження. Огляд основних методів інформаційної війни та аналіз хронології розвитку російської кіберагресії в Україні, а також використання результатів сучасних досліджень вчених М. Безнер та П. Робіна ([Центр з досліджень безпеки](#) при Федеральній вищій технічній школі м. Цюриха, 2017) дає нам підстави, зокрема, виокремити чотири основні внутрішні та зовнішні наслідки російсько-українського конфлікту [6].

1. Соціальні наслідки. Внаслідок кібернетичної та інформаційної війни, яку веде Росія проти України, жителі окупованої частини східної України та анексованого Росією українського Криму стали «повністю ізольованими від інформації, що надходить із зовнішнього світу», адже у них є доступ лише до російського радіо та телебачення.

Підтримання ізоляції є важливою частиною російської інформаційної війни, метою котрої перш за визначено встановлення контролю за думками громадськості та здійснення впливу на прийняття необхідних рішень на користь РФ. Російська пропаганда є ефективною, діє через багато різних каналів – від традиційного телебачення до соціальних мереж і чатів, що дозволяє донести потрібну проросійські владі пропаганду до великої кількості людей. На відміну від ЗМІ у соціальних мережах не витрачається час на перевірку правдивості інформації, через що дезінформація швидко поширюється в інтернеті. Для підвищення правдивості російської пропаганди ЗМІ запрошують також відомих людей (наприклад, американського журналіста Ларі Кінга).

Вчені (М. Безнер, П. Робін, 2017) [7] за наслідками проведеного дослідження пояснюють, що інформаційні атаки можуть призвести до відчуття вразливості і в українському суспільстві, котре стане вважатиме себе беззахисним з боку держави перед зовнішніми інформаційними загрозами.

Врешті-решт, це підтвердили події не тільки в Україні, а й в багатьох країнах Європи та Азії внаслідок зараження комп'ютерів і серверів державних установ і організацій вірусом Retja, що призвело до значних збитків.

2. Економічні наслідки. Російська кіберагресія у формі зламу веб-сторінок державних та бізнес-підприємств зазвичай має негативні наслідки для їхніх доходів або рівня продуктивності, адже «середні економічні збитки складають 22000 доларів США за кожну хвилину простою комп'ютера як засобу-регулятора багатьох процесів щодо управління ними (наприклад, внаслідок недоступності веб-сторінки), у той час як подібна атака у середньому триває приблизно 54 хвилини» [7]. Також фахівцям потрібно значний час для ремонту та налаштування комп'ютерів, відновлення втрачених даних тощо.

Непрямі наслідки кібератак на підприємства включають й негативний вплив на репутацію компаній (наприклад, блокування електронних платежів Ощадбанку як державної установи Національного банку України).

Також у дослідженні М. Безнер та П. Робін звертають увагу на те, що в Україні жертвами російських кібератак зазвичай є веб-сайти ЗМІ, банків та урядових організацій (атака на сайти МВС України, Президента України, СБУ тощо). Вчені пояснюють, що саме злам урядових веб-сторінок може призвести у суспільстві до сумнівів щодо можливостей українського уряду захистити своїх громадян [6; 7].

3. Технологічні наслідки. У контексті конфлікту довкола України Росія поєднує фізичні атаки на важливі телекомунікаційні та інфраструктурні об'єкти (наприклад, на склади боєприпасів) з кібератаками, а також широко використовує шкідливе програмне забезпечення (програмні продукти Me.doc, 1С-Бухгалтерія тощо). Позитивним, у свою чергу, на думку вчених, є те, що винаходи методів відповідного захисту дають змогу удосконалити відповідне програмне забезпечення й розробити стратегічний план з протидії російській комп'ютеризованій війні.

4. Міжнародні наслідки. Під час анексії Криму та розгортання бойових дій на сході України Росія вжила всіх необхідних заходів, щоб ізолювати ці території та не допустити іноземні ЗМІ для отримання об'єктивної інформації про події. Той факт, що західні ЗМІ не могли підтвердити присутність російських військових в Україні протягом майже усього 2014 року, у свою чергу, вказує на значний прогрес у розробці та реалізації російської інформаційної тактики. Як зазначають М. Безнер та П. Робін у своєму дослідженні, РФ використовує тактику «забруднення інформаційних каналів», щоб ввести зовнішній світ в оману [7].

Незважаючи на те, що санкції щодо Росії суттєво послабили її економіку, загальна допомога Заходу Україні у протидії російській військовій та інформаційній агресії є досить обмеженими.

Розглянемо найбільш поширені заходи, що застосовуються для обмеження впливу російської кіберагресії. Враховуючи обґрунтовані підходи, запропоновані вченими М. Бензер та П. Робін, можемо зазначити, що компетентним державним органам України необхідно зробити в першу чергу все можливе для більшої обізнаності населення держави про те, чим є насправді інформаційна війна та якими методами вона ведеться. Вкрай негативним, на нашу думку, є те, що значна частка українського населення використовує електронну пошту російських провайдерів, послуговується російськими соціальними мережами або ж іншими її інтернет-ресурсами, що дає змогу спецслужбам російської влади «перехоплювати та читати – або ж слухати – усі діалоги, які ведуться на цих платформах» [7]. Тому, на наш погляд, рішення Президента України щодо припинення дії на території України російських соціальних мереж у цій ситуації є вірним кроком [8]. Зокрема, в Указі Президента України від 15 травня 2017 року № 133/2017, яким введено у дію рішення РНБО про продовження на рік санкцій проти Росії, визначено різні форми обмежень та заборон щодо діяльності на території України 1 тис. 228 фізичних та 468 юридичних осіб, в тому числі доступ електронним засобам буде заблокований на три роки. Зокрема, провайдери повинні будуть заблокувати доступ до сервісів Mail.ru та «Мейл.РУ ГРУП».

Варто зазначити, що також заблоковано і доступ до сайту «Кинопоиск», сайтів антивірусних компаній «Лабораторія Касперського» і DrWeb. Економічні санкції (блокування активів,

заборону на транзакції і мовлення) також введене проти найбільших російських телекомпаній – «ТВ Центр», ВГТРК, «НТВ-Плюс», «Зірка», ТНТ, РЕН-ТВ [8].

Згідно з даними «Інтернет Асоціації України» домени Vkontakte, Yandex, Odnoklassniki і Mail.ru є одними з найвідвідуваніших в Україні. Так, середнє значення денної частки аудиторії у березні 2017 року в Vkontakte становило 52%, Yandex – 41%, Odnoklassniki – 33% і Mail.ru – 31%. Частка людей серед цільової аудиторії, які відвідували ресурс принаймні один раз на місяць, у Vkontakte становила 71%, Yandex – 64%, Odnoklassniki – 51%, Mail.ru – 64%.

Певні кроки щодо протидії інформаційній агресії здійснюються багатьма правоохоронними органами та відповідними державними установами на різних рівнях (кіберполіція Національної поліції України, Служба безпеки України, Рада національної безпеки та оборони України тощо).

Не менш важливим, на нашу думку, є також міжнародне відстежування кіберактивності Росії в Україні, щоб об'єктивно оцінити пов'язані з цим ризики та розробити план з протидії інформаційній агресії РФ.

Висновки. Провівши аналіз наслідків агресивного інформаційного та кібернетичного впливу медіа-засобів Росії через соціальні мережі та інші ЗМІ, можемо констатувати, що з метою виправлення вищезазначеної ситуації потрібно концентрувати увагу правоохоронних органів та суспільства в таких напрямках:

1) формувати у користувачів соціальних мереж, а також у працівників кіберполіції критичне ставлення до розміщеної в інтернет-ресурсах інформації, котра сприймається широким загалом на віру;

2) вчити визначати правдивість матеріалу про суперечливі події шляхом зіставлення інформації з різних джерел (друкованих ЗМІ, теленовін, медійних ресурсів, показів очевидців тощо);

3) вжиття правоохоронними підрозділами Національної поліції, Служби безпеки України спільно з відповідними телеканалами (інших медіаресурсів тощо) радикальних методів щодо блокування антиукраїнських ЗМІ, котрі здійснюють негативний вплив на свідомість громадян України.

У протистоянні між ворогуючими країнами не варто недооцінювати роль та значення сучасних методів ведення інформаційної війни, в котрі держава-агресор втягує й окремі

ЗМІ. Вміння громадян України та працівників кіберполіції своєчасно виявляти провокаційні (фейкові) повідомлення дають змогу правильно сприймати реальні події, проявляти адекватне (критичне) ставлення до них, формувати на цій основі відповідну суспільну думку українського народу та відображувати її в державницькій й громадсько-патріотичній позиції.

Список літератури

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України від 28 червня 1996 року (редакція від 01.01.2020). URL: <http://zakon0.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 12.02.2020).

2. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017. URL: <http://www.president.gov.ua/documents/472017-21374> (дата звернення: 12.02.2020).

3. ІМІ: Кожна 10-та новина на сайтах ОРДЛО – фейк. URL: <http://www.pravda.com.ua/news/2017/02/24/7136338> (дата звернення: 12.02.2020).

4. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: <http://zakon5.rada.gov.ua/laws/show/2469-19/page1-2> (дата звернення: 12.02.2020).

5. Про Звернення Верховної Ради України до Організації Об'єднаних Націй, Європейського Парламенту, Парламентської Асамблеї Ради Європи, Парламентської Асамблеї НАТО, Парламентської Асамблеї ОБСЄ, Парламентської Асамблеї ГУАМ, національних парламентів держав світу про визнання Російської Федерації державою-агресором: Постанова Верховної Ради України від 27 січня 2015 року № 129-VIII. URL: <https://zakon.rada.gov.ua/laws/show/129-19#n9> (дата звернення: 11.02.2020).

6. Безнер М., Робін П. Дослідження «[Кібернетична та інформаційна війна в українському конфлікті](#)» / Марі Безнер, Патріс Робін. // [Центр з досліджень безпеки](#) при Федеральній вищій технічній школі Цюриха. URL: <http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf> (дата звернення: 11.12.2020).

7. Інформаційна війна Росії в Україні та кібербезпека (огляд дослідження) / Тетяна Савчук. URL:

<https://www.radiosvoboda.org/a/28580039.html> (дата звернення: 11.12.2020).

8. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 15 травня 2017 року № 133/2017. URL: <http://www.president.gov.ua/documents/1332017-21850> (дата звернення: 12.02.2020).