настроений в Украине и проведение пропагандистских мероприятий по формированию культурной идентичности населения оккупированной территории АР Крым с населением России. Раскрыты намерения РФ относительно деструктивного информационно-психологического воздействия как извне, так и внутри Украины, направленные на то, чтобы, искусственно создавая и обостряя существующие политические, социально-экономические, этнические и другие противоречия, любым путем ослабить и расколоть страну изнутри.

Ключевые слова: государственная безопасность, информационные угрозы, гибридная война, информационная война, информационно-психологическое воздействие.

oneness of the population on the occupied territory of Crimea and the population of Russia. There revealed Russia's intentions regarding destructive methods of information and psychological influence both from outside and inside Ukraine, aimed at weakening and splitting the country from within through engineering and exacerbating existing political, socio-economic, ethnic and other contradictions.

Key words: state security, information threats, hybrid war, information war, information-psychological influence.

УДК 32.019.51

ХОДАНОВИЧ Віталій Олександрович

ПРОТИДІЯ ІНФОРМАЦІЙНИМ ВПЛИВАМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ: НАЦІОНАЛЬНИЙ ДОСВІД

Постановка проблеми. Інформаційна кампанія, яку розгорнула Російська Федерація (далі – РФ) останніми роками, має всі ознаки чітко спланованої багаторівневої агресії проти основ міжнародного порядку. Через своє геополітичне положення Україна опинилася в епіцентрі зони ворожого впливу й стала для країни-агресора «полігоном» для відпрацьовування нових технологій інформаційного впливу, переважно деструктивного, на українських громадян, суспільство, органи влади й управління. Від початку гібридної агресії у 2014 році вітчизняний інформаційний простір щоденно зазнавав втручань різного характеру з російського боку: від тенденційного висвітлення російськими ЗМІ подій в Україні й до відвертої неправди, яка виходила з вуст представників влади РФ, на-

приклад, про начебто розіп'ятого українськими військовими хлопчика в м. Слов'янську [1].

Водночас така увага до нашої держави з боку Росії зумовила формування певного рівня стійкості українського суспільства до ворожих інформаційних впливів і набуття вітчизняними державними та громадськими інституціями, а також науковими колами унікального досвіду з протидії РФ на цьому напрямі. Цей досвід має бути належно осмисленим задля вдосконалення підвалин забезпечення інформаційної безпеки як України, так і світової демократичної спільноти.

Аналіз останніх досліджень і публікацій. Питанням протидії ворожим інформаційним впливам присвячено чимало робіт вітчизняних і зарубіжних науковців, зокрема: У. Бернхардта, І. Боднара, Н. Вареньї, О. Литвиненка, А. Марущака, В. Петрика, В. Пилипчука, Р. Роджерса, Дж. Трауба, О. Юдіна й інших. Проте говорити про досягнення належного рівня інформаційної безпеки в Україні ще зарано, адже ворог щоденно змінює тактику й інтенсивність своїх дій і вдосконалює форми, методи та засоби впливу. Відпрацьовані на сьогодні способи протидії є досить різноманітними за своєю природою, тому потребують критичного оцінювання з використанням рефлексивного підходу.

Мета цієї статті полягає в тому, щоб на основі ретроспективного аналізу процесу протидії російським інформаційним впливам на українське суспільство та державу оцінити стан забезпечення інформаційної безпеки держави й визначити подальші напрями його вдосконалення.

Виклад основного матеріалу. Неочікувана агресія з боку Російської Федерації щодо України у 2014 році застала зненацька не тільки українців, а й світове співтовариство загалом. Додатковою несподіванкою для всіх стало активне супроводження Москвою своїх агресивних дій потужною інформаційною кампанією, часто дезінформаційного характеру, яка на певний час дезорієнтувала весь цивілізований світ щодо реального перебігу подій та дала змогу агресору ефективніше реалізовувати свої наміри. Її масштаб та спрямування досить наочно висвітлені в огляді основних інформаційних операцій Кремля з 2014 року, що проведений Українським кризовим медіацентром. Автори цього аналітичного звіту визначили такі ключові етапи російської інформаційної агресії: 2014–2015 роки (поляризація суспільства через інструменталізацію міфу про загрозу російськомовному населенню; дискредитація військово-політичного керівництва України; рух за «третій Майдан» з метою спровокувати контрольований Кремлем хаос; популяризація ідей «русского мира»); 2016–2018 роки (продовження руху за «третій Майдан»; політизація будь-яких тем – від питань мови та релігії до проблем освіти; операції на підрив двосторонніх відносин між Україною та партнерами, зокрема з Польщею); 2018–2020 роки (маргіналізація українського уряду та фокус на Україні як «недодержаві» для посилення суспільного невдоволення; операції, спрямовані на поширення та закріплення

антизахідної риторики; дискредитація громадянського суспільства; операції на підрив двосторонніх відносин між Україною та партнерами, зокрема Угорщиною; інформаційні операції, пов'язані з пандемією COVID-19) [2]. Зауважимо, що тенденції, окреслені в останньому етапі, залишаються актуальними й сьогодні.

Аналіз наведених даних, а також їх співставлення з результатами власних досліджень російських інформаційних операцій проти України в часово-просторовому вимірі дають можливість констатувати системність агресивної діяльності щодо України, високу адаптивність форм і методів дій супротивника за цією операційною лінією, а також наявність сталої тенденції до подальшого використання вітчизняного інформаційного простору для реалізації Росією своїх геополітичних стратегій.

Наведений огляд Українського кризового медіацентру буде корисним і для створення власної періодизації протидії інформаційним впливам Російської Федерації. За аналогією із попереднім у ній також буде виокремлено три етапи:

– перший – 2014–2015 роки;

– другий – 2016–2018 роки;

– третій – 2018 й до сьогодні.

Як уже зазначалося, агресія Росії щодо України, зокрема й інформаційна, була несподіваною для всіх, а тому перший етап протидії можна визначити як період розгубленості. Ані суспільство, ані держава не були готовими до такого виклику. Вітчизняний інформаційний простір був наповнений російськими та проросійськими джерелами інформації, які мали високий рівень довіри українського суспільства, часто навіть більший, ніж українські офіційні джерела та ЗМІ. Використання Росією дезінформації та відвертої пропаганди на всіх рівнях (від внутрішньоросійського до міжнародного) за відсутності хоча б формально створеної системи протидії не давало можливості здійснювати системний спротив цьому явищу. Про успішне проведення контрзаходів можна стверджувати лише у сфері дипломатичних зносин і поодиноких випадках протидії інформаційним операціям, але ефект від останніх зумовлений більше діями приватного сектору, аніж державною політикою, оскільки, як і в інших сферах, громадянське суспільство мобілізувалося значно швидше, ніж державний апарат. Прикладом цього може слугувати створення вже згадуваного Українського кризового медіацентру й інших інформаційних ресурсів для поширення об'єктивної інформації про події, що розгорталися в цей час, протидії дезінформації тощо. Разом із тим, маємо констатувати, що заходи, котрі застосовувала Росія в інформаційній площині, були безпрецедентними й унеможливили застосування іноземного досвіду інституціональної протидії згаданому явищу з причин відсутності його як такого.

Позитивним моментом, що дав змогу переломити ситуацію та не допустити тяжчих наслідків і водночас не залежав від України, є дисонанс між російськими наративами та фактичними діями в економічній, політичній і військовій площинах, що призвів до часткової втрати довіри до

наймасовіших інформаційних джерел агресора.

Другий етап є періодом реакції вітчизняного суспільства, а особливо держави, на зовнішню загрозу. Саме в цей період можна констатувати посилення ролі державного апарату в боротьбі з інформаційною агресією. Найефективнішим заходом була заборона діяльності у вітчизняному інформаційному просторі російських інтернет-сервісів, відома також як блокування російських соцмереж. Мова йде про Указ Президента України від 15.05.2017 № 133/2017 «Про введення в дію рішення Ради національної безпеки і оборони України "Про застосування персональних спеціальних економічних та інших обмежувальних заходів"» [3], яким, з-поміж інших, заблоковано або обмежено діяльність низки вебресурсів, таких як: «Вконтакте», «Одноклассники», «Mail.ru», «Яндекс», а також відверто пропагандистських телевізійних каналів «Russia 24» та «RT» тощо. Зазначений захід, незважаючи на потужну критику з боку ліберальної частини як українського, так і європейського суспільства, схвально оцінило керівництво країн – партнерів України, зокрема Польщі та країн Балтії, і поступово запозичується останніми.

Також слід згадати активну розробку в цей період проєкту Закону України «Про забезпечення функціонування української мови як державної» [4], який мав потужний відгук в українському суспільстві, чим частково нейтралізувалися наслідки впливу російської пропаганди. Однак необхідно вказати й негативні наслідки, як-то певна мовна поляризація вітчизняного суспільства й претензії з боку деяких суміжних країн. Разом із тим, сьогодні можемо констатувати позитивний ефект від цього кроку.

Ще одним важливим кроком української влади у протидії ворожим інформаційним впливам стала активна державна підтримка створення в Україні помісної православної церкви, що завершилася отриманням у 2019 році Томосу – правової підстави для створення автокефальної Православної церкви України. Наслідком цього стало зменшення інтенсивності негативного інформаційного впливу, що здійснювався Кремлем на українське населення через найбільшу на той час православну інституцію – Українську православну церкву (Московського патріархату). Зауважимо, що питання мови та релігії, а відповідно й суспільні відносини, що врегульовані вказаним законом України та Томосом, не були предметом нашого дослідження, а тому розглядаються виключно крізь призму впливу на стан забезпечення інформаційної безпеки України.

Водночас найголовнішим здобутком стала зміна підходів до формування засад та реалізації державної політики в інформаційній сфері. Так, Указом Президента України від 25.02.2017 № 47/2017 було введено в дію рішення Ради національної безпеки і оборони України від 29.12.2016 «Про Доктрину інформаційної безпеки України» (далі – Доктрина) [5]. Цим документом було визначено національні інтереси України в інформаційній сфері, загрози їх реалізації, а також напрями та пріоритети

державної інформаційної політики. Зміст Доктрини є цікавим для дослідження з багатьох причин.

По-перше, вона наочно демонструє основну тенденцію цього періоду – реакцію України на дії країни-агресора. Так, із визначених цим документом актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері (всього сім) чотири безпосередньо стосувалися дій РФ, дві – констатували недостатню розвиненість вітчизняної інформаційної інфраструктури або неефективність державної політики у відповідній сфері, і лише одна (поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні) визначала внутрішні загрози. При цьому поза увагою авторів Доктрини залишилися глобальніші загрози, зумовлені, наприклад, віртуалізацією людини та суспільства або неконтрольованістю інформаційних потоків у межах глобального інформаційного простору тощо. Не був урахований у документі й такий важливий момент, як здатність проникнення інформаційної сфери в усі інші сфери функціонування держави та суспільства, її самостійна здатність впливати на свідомість людини й бути інструментом посилення впливів у військовій, політичній або економічній сферах.

По-друге, метою Доктрини визначено «уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни». Інакше кажучи, її автори не передбачили створення нових правових механізмів регулювання процесів і правовідносин, що відбуваються в інформаційній сфері, або запровадження бодай якихось кардинальних змін і підходів у державній політиці. Лише вдосконалення вже існуючих (хоча й недостатніх) засад формування державної інформаційної політики та її реалізації. Проте кардинальні зміни видаються вкрай необхідними й об'єктивно зумовлені розвитком суспільства, адже в чинному на той час законодавстві у сфері національної безпеки [6] та «Стратегії національної безпеки України» [7] питанням забезпечення саме інформаційної безпеки не приділено достатньої уваги.

Третім цікавим нюансом, який пов'язаний із попереднім, є часова обмеженість дії цього документа та свідоме звуження сфери протидії впливам. Зокрема, дія Доктрини в часі обмежена формулюванням «в умовах розв'язаної Російською Федерацією гібридної війни», тобто після завершення такої «війни» її норми майже повністю втрачають свою актуальність. А серед зовнішніх чинників, які загрожують інформаційній безпеці, визначено лише дії РФ. Аналогічні дії з боку, наприклад, Угорщини або Китаю не є предметом регулювання цього нормативного акта.

Також слід зазначити, що Доктрина містить низку дуже слушних та актуальних до сьогодні положень. Зокрема, вона визначає чіткі механізми реалізації сформульованих у її тексті завдань, досить широке коло суб'єктів її реалізації та передбачає належну координацію здійснюваних заходів.

З урахуванням її положень були розроблені деякі норми Закону України «Про національну безпеку України» [8] та прийнята на його основі чинна «Стратегія національної безпеки України» [9] й інші документи. Отже, можемо стверджувати про вплив цього документа на стан забезпечення інформаційної безпеки на доктринальному рівні, що й було метою його прийняття.

На третьому (сучасному) етапі протидії інформаційним впливам нарешті відбулися зміна підходів до врегулювання інформаційних правовідносин у суспільстві та розширення вектору протидії впливам. Окрім указаних вище нормативно-правових актів було підготовлено (Міністерством культури та інформаційної політики України), схвалено (Кабінетом Міністрів України) та затверджено (Радою національної безпеки і оборони України) Стратегію інформаційної безпеки України (далі – Стратегія) [10]. У цьому документі в цілому враховано недоліки Доктрини й зміщено акценти з протидії інформаційній агресії РФ на забезпечення інформаційної безпеки України як одну з найважливіших функцій держави та справу всього Українського народу. По суті, у Стратегії визначено загальні засади інформаційної безпеки безвідносно до джерел загроз. Як і дія Доктрини, дія Стратегії також є обмеженою в часі (2026 роком), водночас, відповідно до чинного законодавства цей документ приймається на виконання Стратегії національної безпеки України. Отже, його положення мають відповідати нормам, що містяться в новій редакції останньої.

Можна стверджувати, що зазначена Стратегія охоплює майже всі сфери інформаційної діяльності та містить адекватний перелік реальних та потенційних викликів і загроз, на протидію яким мають бути спрямовані зусилля суспільства та держави, визначає їх поділ на глобальні і національні, основні напрями забезпечення інформаційної безпеки, стратегічні цілі та завдання.

До позитивних моментів належать: об'єктивна оцінка можливостей України реагувати на дезінформаційні кампанії; визнання існуючих проблем як у правовій площині, так і організаційній. Така позиція сприятиме роботі з усунення прогалин у законодавстві та ефективнішому використанню наявних на сьогодні сил і засобів протидії впливам.

Разом із тим, поточна редакція документа не позбавлена й певних вад. Так, незважаючи на більш комплексний і всеосяжний характер Стратегії порівняно з Доктриною, механізм реалізації її мети та завдань потребує доопрацювання вже зараз, тобто до введення в дію. Зокрема, деякі із завдань, визначених у стратегічних цілях документа, передусім третій (підвищення рівня медіакультури та медіаграмотності суспільства), четвертій (забезпечення дотримання конституційних прав особи на свободу вираження та захист приватного життя, захист прав журналістів і протидія поширенню незаконного контенту), сьомій (забезпечення дотримання конституційних прав особи на свободу вираження та захист приватного життя, захист прав журналістів і протидія поширенню незаконного контенту)

та восьмій (розвиток інформаційного суспільства та підвищення рівня культури діалогу), перебувають поза сферою компетенції Ради національної безпеки і оборони України (далі – РНБО) як координаційного органу з питань безпеки та оборони при Президентові України. Наприклад, забезпечення наявності програм вітчизняних телекомпаній у багатоканальних мережах інших держав шляхом сприяння створенню загальнонаціональними телеканалами супутникових іноземних версій (з урахуванням мови країн розповсюдження) для поширення програм за межами України та багато інших.

Другим недоліком є те, що цей орган може здійснювати координацію діяльності лише органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. А органи місцевого самоврядування та інститути громадянського суспільства, які забезпечуватимуть реалізацію Стратегії, матимуть змогу узгоджено діяти лише згідно з планом заходів, який повинен бути затвердженим Кабінетом Міністрів України додатково. Зазначене не сприяє налагодженню ефективної взаємодії та створює досить інертну конструкцію, не придатну до залучення, наприклад, інститутів громадянського суспільства до вжиття невідкладних заходів.

Не визначено, хто із суб'єктів забезпечення інформаційної безпеки здійснюватиме визначення пріоритетності реалізації сформульованих у документі стратегічних цілей залежно від ступеня ймовірності реалізації загроз, особливо в умовах кризової ситуації та обмежених ресурсів. Отже, у правовій площині залишається ще багато роботи, яка має бути виконана якщо не невідкладно, то протягом найближчого часу.

Набагато краще складається ситуація на інституціональному рівні протидії інформаційним впливам із боку Російської Федерації. Тільки у 2021 році було створено два центри, які реалізовуватимуть державну політику в цьому напрямі, а саме: Центр протидії дезінформації (далі – ЦПД), підпорядкований РНБО, і Центр стратегічних комунікацій та інформаційної безпеки (далі – ЦСКІБ) при Міністерстві культури та інформаційної політики. До завдань першого відповідно до Положення про ЦПД [11] належать: проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі; виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, чинників, які впливають на їх формування, прогнозування та оцінювання наслідків для безпеки національних інтересів України тощо. ЦСКІБ зосереджуватиме свою роботу на стратегічних комунікаціях, що включатимуть розробку контрнаративів РФ, проведення інформаційних кампаній, включення українських наративів у щоденну комунікацію Уряду; створення он-лайн ресурсу, який активно реагуватиме на інформаційні атаки; регулярне сповіщення про гібридну агресію з боку Росії на міжнародному рівні, спільне напрацювання механізмів протидії дезінформації з міжнародними партнерами [12].

Не залишається осторонь від процесів протидії інформаційним впливам і громадянське суспільство. Протягом останніх років було створено чимало громадських об'єднань, які опікуються питаннями виявлення фейків, генерованих за вказівкою Кремля, та протидії російській пропаганді.

Висновки. Як убачається з наведеного вище, від початку російської агресії у 2014 році Україна пройшла чималий шлях у формуванні власної державної системи протидії інформаційним впливам. Проведений аналіз і співставлення основних інформаційних операцій РФ щодо України, наведених у статті етапів російської агресії та вжитих українською державою та суспільством заходів протидії дають змогу стверджувати про проходження кризового періоду в інформаційному протиборстві та становлення вітчизняного суверенного інформаційного простору як явища. Так, якщо на перших етапах інформаційної агресії Кремль робив ставку на привабливість своїх цивілізаційних концепцій, як-то «Русский мир» або «Москва – Третій Рим», які мали б призвести до перемоги РФ «м'якою силою», то сьогодні ми бачимо зміну курсу в бік точкових впливів тенденційного характеру (проблеми в українському енергетичному секторі, «антивакцинаторські» кампанії тощо), спрямованих на дестабілізацію внутрішньополітичної ситуації в країні та внесення розбрату у відносини з іноземними партнерами. Наразі інформаційні кампанії Росії із самостійного явища (операційної лінії гібридної війни) трансформувалися в другорядні (обслуговуючі) інструменти інших напрямів агресії: військового, економічного тощо.

За складних умов багатоаспектного протистояння агресору Україна спромоглася створити основу для розвитку власного інформаційного простору та його захисту від недружніх впливів не тільки РФ, а й інших потенційно зацікавлених у цьому геополітичних гравців. Водночас, як державі, так і суспільству потрібно зосередитися на подальшому розвитку власної системи протидії, – удосконалювати чинне законодавство, розбудовувати відповідні інституції, формувати наукове та методологічне підґрунтя для застосування адекватних, а можливо й асиметричних засобів протидії Росії.

Список використаних джерел

1. «Ложь: распятие в эфире Первого канала», StopFake, 15 липня 2014 року. URL: https://www.stopfake.org/ru/lozh-raspyatie-v-efire-pervogo-kanala (дата звернення: 24.11.2021).

2. Огляд основних операцій російського інформаційного впливу в Україні за І півріччя 2021 року. URL: https://uacrisis.org/uk/operatsiyi-ros-inform/amp (дата звернення: 24.11.2021).

3. Про введення в дію рішення Ради національної безпеки і оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів» : Указ Президента України від 15.05.2017 № 133/2017. URL: https://

www.president.gov.ua/documents/1332017-21850 (дата звернення: 24.11.2021).

4. Про забезпечення функціонування української мови як державної : Закон України від 25.04.2019 № 2704. URL: https://zakon.rada.gov.ua/laws/show/2704-19#Text (дата звернення: 24.11.2021).

5. Про рішення Ради національної безпеки і оборони України від 29.12.2016 «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 24.11.2021).

6. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 24.11.2021).

7. Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 24.11.2021).

8. Про національну безпеку України : Закон України від 21.06.2018 № 2469. URL: https://zakon.rada.gov.ua/laws/show/2469-18#Text (дата звернення: 24.11.2021).

9. Про рішення Ради національної безпеки і оборони України від 14.09.2020 «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/391/2020#top (дата звернення: 24.11.2021).

10. Про рішення Ради національної безпеки і оборони України від 15.09.2021 «Стратегія інформаційної безпеки» : проєкт Указа Президента України. URL: https://mkip.gov.ua/files/pdf/45698712365.pdf (дата звернення: 24.11.2021).

11. Питання Центру протидії дезінформації : Указ Президента України від 14.09.2020 № 187/2021. URL: https://www.president.gov.ua/documents/1872021-38841 (дата звернення: 24.11.2021).

12. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki (дата звернення: 24.11.2021).

Аннотация. В статье сопоставляются основные информационные операции Российской Федерации в отношении Украины с предпринятыми украинскими государством и обществом мерами противодействия. По результатам проведенного анализа дана оценка национальному опыту противодействия информационным влияниям со стороны страны-агрессора и определены дальнейшие направления усовершенствования отечественной системы обеспечения информационной безопасности.

Ключевые слова: гибридное противостояние, информационная безопасность, информационное пространство, информационные влияния.

Abstract. The article compares the main information operations of the Russian Federation targeting Ukraine with the countermeasures taken by the Ukrainian state and society. Based on the results of the analysis, an assessment of the national experience of countering information influences of the aggressor country was given and further directions for improving the domestic information security system were identified.

Key words: hybrid warfare, information security, information space, information influences.