НАЦІОНАЛЬНА БЕЗПЕКА

DOI: https://doi.org/10.32839/2304-5809/2021-5-93-58
УДК 351.86:004.056

Калетнік В.В.
Національний авіаційний університет
Калетнік Н.В.
Громадська організація «Свідома Громадськість»

ІНФОРМАЦІЙНА БЕЗПЕКА І КІБЕРЗАХИСТ ЯК СУЧАСНА ІНТЕЛЕКТУАЛЬНА ЗБРОЯ

Анотація. У статті автори звертають увагу на тому, що в сучасних умовах питома вага кіберзагроз, з боку авторитарних держав та їх посередників, у спектрі загроз національній безпеці країн зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту лише посилюється. Все більш активно застосовується поєднання традиційних та нетрадиційних стратегій і тактик з використанням цифрових інформаційних технологій. Такі умови зумовили визнання кіберпростору разом з іншими фізичними просторами одним з можливих театрів воєнних дій. Розглянуто концепцію інформаційного протиборства Російської Федерації, базовану на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої активно застосовуються в процесі гібридної війни проти України. За результатами розгляду, підкреслено, необхідність формування більш збалансованої та ефективної системи кібероборони, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи безпечне функціонування національного сегмента кіберпростору. Наприкінці авторами сформульовані напрямки подальших досліджень щодо необхідності визначення у відповідних нормативно-правових актах структури системи кібероборони держави, склад, функції і задачі суб'єктів її забезпечення, а також об'єкти кібероборони. Також, актуалізовано необхідність напрацювання належної правової, організаційної, технологічної моделі функціонування та застосування сил кібероборони.

Ключові слова: інформаційна війна, інформаційне протиборство, інформаційна безпека, кібероборона, кіберпростір.

Kaletnik Vasyl
National Aviation University
Kaletnik Nataliia
Non-Governmental organization «The Conscious Community»

INFORMATION SECURITY AND CYBER PROTECTION AS A MODERN INTELLECTUAL WEAPON

Summary. The authors point out that in modern conditions the share of cyber threats from authoritarian states and their intermediaries in the range of threats to national security is growing, and this trend is only increasing with the development of information technology and it's convergence with artificial intelligence technologies. The combination of traditional and non-traditional strategies and tactics with the use of digital information technologies is increasingly used. Such conditions have led to the recognition of cyberspace, along with other physical spaces, as one of the possible theaters of war and encourage leading governments to improve the architecture of national cybersecurity systems, change strategies and tactics to combat cyber threats. The concept of information confrontation of the Russian Federation, based on the symbiosis of combat operations in cyberspace and information operations, the mechanisms of which are actively used in the process of hybrid war against Ukraine, is considered. The common and distinctive features of the Russian understanding of information confrontation and the approach of the American military to information operations are revealed. It is noted that the main mechanisms by which Russian structures inflict damage are divided into information-psychological and information-technical and their content is revealed. It is emphasized that in addition to traditional tools, Russia uses a set of hidden tools of influence, which it calls active measures, the experience of which has remained since Soviet times, has been adapted and improved for use in modern conditions. According to the results of the review, the need to form a more balanced and effective cyber defense system, which will be able to flexibly adapt to changes in the security environment, ensuring the safe functioning of the national segment of cyberspace, was emphasized. Finally, the authors formulate directions for further research on the need to determine in the relevant regulations the structure of the state cyber defense system, the composition, functions and tasks of its subjects, as well as the objects of cyber defense. Also, the need to develop a proper legal, organizational, technological model of functioning and use of cyber defense forces was updated.

Keywords: information war, information confrontation, information security, cyber defense, cyberspace.

Постановка проблеми. В останні роки ліберальні демократії все частіше стають об'єктами не кінетичних нападів з боку країн з авторитарними режимами, особливо в сфері кіберпростору. Всі держави – як демократичні, так і авторитарні – традиційно використовують кіберможливості для збору розвідувальної інформації в інших країнах, проте, сьогодні політична війна малої інтенсивності в кіберпросторі стала набагато більш помітною. На жаль для демократичних

країн, кіберпростір є ідеальним середовищем для підриву демократичних процесів та інститутів за допомогою різних прихованих операцій.

Аналіз актуальних досліджень. Наукове осмислення концептуальних засад та окремих аспектів цієї проблеми здійснили в своїх роботах такі науковці, як: В.В. Бадрак, М. Галеотті, В.П. Горбулін, В.В. Калетнік, В.О. Киселльов, С. Кім, В.Ю. Мікрюков, П. Пернік, Р. Сілі, Б.В. Соколов, К. Шваб та ін.

Виділення не вирішених раніше частин загальної проблеми. Разом із тим, віддаючи належне важливості та науковій цінності наявних досліджень, доводиться констатувати, що даний напрямок потребує подальших досліджень в аспекті вивчення та напрацювання механізмів кіберзахисту.

Метою статті є розгляд інформаційної безпеки і кіберзахисту як сучасної інтелектуальної зброї.

Виклад основного матеріалу. На початку 2000-х років ЗМІ полюбляли цитувати неназваного топ-чиновника із керівництва Пентагону, який якось помітив: «Ми наближаємося до такого рівня розвитку, коли вже ніхто не являється солдатом, але всі – учасники бойових дій. Задача зараз стоїть не в знищенні живої сили, але в підриві цілей, поглядів і світогляду населення, в руйнуванні соціуму» [5]. Так ось, по закінченню всього двох десятків років після цієї заяви науковці констатують, що ми вже давно увійшли і вкоренилися в цій новій реальності, коли кожен з нас, хоче він того чи не хоче, являється учасником війни як в нашій локальній російсько-українській, так і в глобальному світовому протистоянні за ту чи іншу ментальну модель сучасної цивілізації [2].

Більшість науковців сходяться в думці, що задачі інформаційної безпеки повинні вирішуватися в рамках профільності у всіх відомствах національної безпеки, що передбачає організацію системної взаємодії. Координатором в такій моделі може стати Національний координаційний центр кібербезпеки, хоча в особливих випадках деякі питання можуть виноситися на рівень засідання Ради національної безпеки і оборони [11]. Тут, особливо, потрібно налагодити співпрацю і з громадським сектором, з найбільш розвиненими профільними цивільними інститутами, здатними до активних інформаційних заходів, що, до речі, зазначено і в Законі України «Про національну безпеку України».

Кіберзахист держави в значній мірі залежить від вміння використовувати інформаційні технології. А це означає, що персонал повинен бути навчений використанню сучасних засобів зв'язку, IT і кібербезпеки. Також важливо своєчасно залучати і мотивувати перспективну молодь, що навчається на відповідних спеціальностях у вітчизняних навчальних закладах. Особливо, коли мова іде про IT-сектор, сегмент журналістики або організації, які спеціалізуються на формуванні і просуванні у відкритих джерелах інформації специфічного інформаційного контенту [12].

В той же час для неоднорідного українського суспільства варто врахувати високий рівень ризиків інформаційно-психологічного впливу на ту частину населення, яка й досі віддає перевагу не демократії, а «сильній руці», не відрізняючи міф про «сильну руку» від реального авторитарного режиму з жорсткою формою правління правоохоронних органів і спецслужб. Тут доречним може бути порівняння цього періоду з часами 2008–2009 років, коли завданням російських спецслужб була впевнена демонстрація слабкості української влади на фоні штучної героїзації самого Путіна, формування для середньостатистичного сприйняття образу російського президента як лідера наддержави.

З деяких пір кібератаки стали невід'ємною частиною російської інформаційної війни. Для авторитарних режимів це не є новим – вони завжди використовували їх для розширення зон впливу. Поруч з Китаєм, Іраном, Північною Кореєю, Росія намагається удосконалити свої стратегії ведення інформаційних війн, часто використовуючи напрацювання для підривних операцій. До речі, характерною рисою цих держав являється відсутність розподілу часу на мирний та воєнний. Основні російські стратегічні документи (Військова доктрина Російської Федерації від 2014 року і Стратегія національної безпеки Російської Федерації від 2015 року) прямо вказують на використання інформаційних технологій в рамках захисту російських геополітичних інтересів.

Науковий співробітник Естонської академії дослідження проблем безпеки Пірет Пернік справедливо зазначає, що свобода інформації і її середовище – вільний і відкритий інтернет в Західному світі, – стали об'єктами нападу Росії, яка звично і традиційно виставляє себе жертвою нападу [6].

На думку Пірет Пернік, основні механізми за допомогою яких російські структури наносять збитки поділяються на інформаційно-психологічні та інформаційно-технічні. До технічних інструментів вона відносить кібератаки низького рівня (наприклад, несанкціонований доступ до інформаційних ресурсів). Кінцевою метою таких атак являється зміна стратегічної поведінки противника, що досягаються шляхом маніпулювання сприйняттям ним реальності та його свідомістю, за допомогою технологічних і психологічних компонентів протиборства [6].

Психологічні заходи включають в себе все, що може вплинути на цивільне населення і на особовий склад збройних сил. У 2017 році В.А. Киселльов в статті в російському журналі «Военная мысль» роз'яснює, що для Росії цілями психологічної діяльності є здійснення впливу на волю, поведінку і бойовий дух супротивника, а також на більш приховані емоції, які, в свою чергу, впливають на раціональне мислення [4].

Слід зауважити, що відповідно до російської військової доктрини, інформаційна війна в сучасних конфліктах не тільки націлена на прийняття противником ключових рішень, але також і на широке використання «протестного потенціалу населення» [13]. Прикметним є те, що військова доктрина США надає набагато меншого значення психологічному впливу на населення супротивника в цілому. Вона просто вказує, що мета інформаційної війни полягає в тому, щоб посіяти сумніви, спантеличити і обдурити політичне керівництво країни, військову й іншу аудиторію, здійснити на них вплив, але при цьому нічого не говорить про необхідність маніпулювати окремими сегментами населення [9].

Два ключові аспекти різнять російське розуміння інформаційного протиборства від підходу американських військових до інформаційних операцій. З точки зору Росії, інформаційна війна, по-

перше, повинна вестися постійно в мирний час, і, по-друге, це діяльність стратегічного рівня, яка повинна вестися усім суспільством як відповідь відповіді. Такий підхід нагадує радянську концепцію тотальної оборони, згідно з якою для потреб національної оборони використовувалися всі ресурси громадянського суспільства. Експерт з Росії Марк Галеотті в своїй статті, написаній для Європейської ради з міжнародних відносин, описує, як при реалізації цього комплексного підходу Кремль залучає для здійснення конкретних операцій добровольців, організовані злочинні угруповання, представників бізнесу, Російську Православну Церкву, неурядові організації, ЗМІ та інших суб'єктів [8]. У США, навпаки, військові вважають інформаційні операції діяльністю воєнного часу, які проводяться спеціально призначеними установами у межах їх повноважень. У США ця діяльність вважається діяльністю оперативного рівня.

У деяких аспектах американські і російські підходи схожі. Для Росії, як стверджує Кисельов, насильницькі фізичні дії, такі як «викрадення держчиновників противника» або «фізичне знищення майна і цілей противника» також є психологічними інструментами [4]. Аналогічним чином, в США фізичне руйнування включено в число інструментів інформаційних операцій. Обидві країни вважають, що кібератаки належать до набору інструментів інформаційної війни і що пов'язана з інформацією діяльність повинна проводитися одночасно в кібернетичному і фізичному просторі. Також, обидві країни включають оборонні заходи (наприклад, організацію безпеки на оперативному рівні і захист власної інфраструктури, комп'ютерних мереж і військ) до складу інформаційної війни, оскільки вони згодні з тим, що кінцева мета інформаційної війни полягає в досягненні інформаційної переваги. Росія робить упор на інформаційно-психологічні можливості, оскільки контроль над інформацією, включаючи контроль над контентом і фізичною структурою Інтернету, представляється гарантією виживання режиму. США, навпаки, роблять основний упор на інформаційно-технологічні можливості.

Відомий російський експерт з питань інформаційної війни Сергій Модестов, апелює до впливу на когнітивну сферу і підкреслює, що когнітивна сфера як поле бою немає кордонів. Він сприймає і описує сучасну інформаційну війну як таку де кордони розмиті між війною і миром, тактичними, оперативними та стратегічними рівнями операцій, видами воєнних дій (обороною і наступом) і силовим впливом [6].

Тому, щоб зрозуміти і побудувати схему ефективної протидії, доречно також згадати і про досить умовний розподіл інструментів російської зовнішньої політики, представлених у 2017 році Робертом Сілі в RUSI Journal. Мова йде про державне управління, економіку і енергетику, політику і політичне насилля, військову потужність, дипломатію і зв'язки з громадськістю, а також інформаційну сферу і військові наративи [10]. Крім традиційних інструментів Росія також використовує набір прихованих інструментів впливу, які вона називає активними заходами. Досвід використання активних заходів і залякування, що залишився з радянських часів, був пристосований і вдосконалений для застосування в сучасних умовах. [3]. Зрозуміло, що всі ці категорії переплітаються, створюючи важливі умови, коли інформаційне поле окремої або навіть групи держав стає мішенню, дезінформація – класичною інформаційною зброєю, а інтернет – сучасним полем бою.

До того ж, такі асиметричні інструменти можуть бути передані для операцій в руки різних суб'єктів, і ще однією привабливою стороною такої політики для Росії є те, що такий вплив коштує недорого, виконавців багато, ступінь анонімності та прихованості досить висока, ризик ескалації низький, а дестабілізуючий потенціал величезний. І як вважає Сілі, відмінною рисою Росії є те, що різні види асиметричних інструментів щільно взаємопов'язані між собою і скоординовані з конвенціональними операціями на ранніх і підготовчих етапах воєнного конфлікту (наприклад, під час кінетичних операцій в Грузії і в Криму) [10].

Однією з головних загроз, які демократичний світогляд являє для російської моделі правління, це свобода слова, яка реалізується, крім інших можливостей, також через вільний і відкритий Інтернет. Інтернет може розпалювати протести і народні хвилювання – наприклад, «кольорові революції» – і Кремль побоюється, що переворот на зразок «арабської весни» може позбавити його влади. Кремль висловив свій страх перед вільним і відкритим Інтернетом ще в 2014 році, коли Путін назвав його «проектом ЦРУ», від якого Росія повинна захиститися. З цієї причини модель, при якій Інтернетом керують численні зацікавлені суб'єкти, сприймається Росією і іншими авторитарними режимами як небезпечна. Ці режими мають намір посилити свій контроль за контентом і фізичною інфраструктурою кіберпростору, а також за програмним і апаратним забезпеченням. В оборонних або наступальних цілях, або ж їх поєднання, Росія використовує кіберпростір для проведення дій з надання політичного впливу на стратегічному рівні проти багатьох членів ЄС і НАТО, а також проти країн Західних Балкан, Південного Кавказу та Центральної Азії [2].

Не слід забувати про те, що Всесвітня мережа – це всього лише середовище, універсальна площадка для реалізації операцій і акцій контентного інформаційно-психологічного впливу. В цілому, інформаційна зброя Кремля являється древнім знаряддям і від того добре відточеним і небезпечним, а традиції створення ефективних методів інформаційно-психологічного впливу або, говорячи сучасною мовою, проведення успішних інформаційних операцій, формувалися в Росії ще у часи активного «збирання земель».

Центр досліджень армії, конверсії та розброєння у своєму дослідженні «Інформаційний фронт Кремля» запропонував відокремити поняття «кібероперації» і «інформаційно-психологічні акції» російських спецслужб та агентів їх впливу, а також, виділити для вивчення та всебічного аналізу такі інформаційні операції:

– російські інформаційні провокації і дезінформація, що проводяться за участі недержавних структур або ЗМІ;

– інформаційні операції, що проводяться науково-дослідними установами Росії;

– інформаційно-психологічні операції, що проводяться офіційними структурами РФ, в тому числі першими особами держави;

– інформаційні операції, що проводяться слідом за спеціальними заходами та провокаціями за участі силових (військових) структур Росії;

– інформаційно-психологічні операції, що проводяться політиками або громадськими діячами («лідерами думок» для конкретних фокус-груп);

– інформаційно-психологічні операції, що проводяться на рівні міжнародних організацій і міжнародних конференцій;

– інформаційно-психологічні операції з використанням специфічних комунікаційних каналів: книг, фільмів, спеціально побудованих телепередач, монументів і вигідних образів минулого;

– інформаційно-психологічні операції, що ґрунтуються на створенні і просуванні рейтингів політиків, партій, армій і т. п.;

– великі комплексні інформаційно-психологічні операції, що проводяться штучно створеними «лідерами думок» [1].

Дійсно, якщо ми чуємо заяву Володимира Путіна про те, що «в Україні проживають сімнадцять мільйонів росіян» [14] і пов'язані з цим неоднозначні натяки на територіальні претензії, то це ніщо інше, як чітко спланована інформаційна операція. Час від часу ситуація синхронно повторюється. Так, 18 липня 2020 року Путін публікує статтю в американському журналі The National Interest, присвячену Другій світовій війні (тільки на наступний день стаття під назвою «75 лет Великой Победы: общая ответственность перед историей и будущим» з'явилася на сайті президента Росії і була надрукована в «Российской газете»).

У свою чергу, московський професор Борис Соколов звертає увагу на те, що The National Interest, цілковито субсидійований з Росії, фактично також являється російським пропагандистським органом, де періодично з'являються різні цікаві статті про російську «чудо-зброю», яка краща за будь-яку в світі і яку всі бояться [7]. Тобто, в підсумку, все це відноситься до інформаційної зброї.

Однак, повернемося до технологічного питання – протидії кібервійні. Кіберпростір інколи навіть визначають «п'ятою сферою ведення збройної боротьби» поряд з чотирма традиційними – «Земля», «Море», «Повітря» і «Космос». Тому, не дивно, що на сьогодні дискусії про застосування державами кібервійськ і кіберзброї сприймаються як щось цілком звичайне.

На практиці Україна зіштовхнулася з російською агресією в кіберпросторі з початку гібридної війни в 2014 році. Хоча об'єктивно визнання кібероборони (складової оборони держави) відбулося в Україні лише в березні 2016 року після Указу Президента України про введення в дію Стратегії кібербезпеки України. В ній визначено, що «основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України» [15]. В цьому документі вперше для Міністерства оборони України і Генерального штабу ЗС України були визначені нові задачі, серед яких підготовка держави до відбиття агресії в кіберпросторі і забезпечення, у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України, кіберзахисту власної інформаційної інфраструктури.

До речі, один із ключових нюансів оформлення системи кіберпротидії – визначення місця в секторі безпеки держави, а можливо, створення єдиного підрозділу із забезпечення кібербезпеки і кіберзахисту ЗС України на стратегічному, оперативному і тактичному рівнях. Тоді ж, в березні 2016 року, було створено і Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України, до задач якого належить нарощування кібероборонних можливостей держави, в тому числі і за рахунок військово-технічного співробітництва.

Уже в жовтні 2017 року вступив у силу Закон України «Про основні засади забезпечення кібербезпеки України» в якому визначено дещо інший, аніж у Стратегії, за пріоритетністю і складу перелік основних суб'єктів національної системи кібербезпеки. Перш за все, Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, а далі не лише Міністерство оборони України, але й Генеральний штаб Збройних Сил України, а також розвідувальні органи і Національний банк України [16].

Втім, Закон про кібербезпеку уже чітко розподілив задачі між цими суб'єктами. Наприклад, Державній службі спеціального зв'язку та захисту інформації України довірений кіберзахист об'єктів критичної інфраструктури, а також попередження, виявлення і реагування на кіберінциденти і кібератаки та усування їх наслідків. Національна поліція займається захистом прав і свобод людини і громадянина, інтересів суспільства від злочинних посягань у кіберпросторі; здійснює заходи з попередження, виявлення, припинення і розкриття кіберзлочинів. Служба безпеки України проводить, між іншим, контррозвідувальні і оперативно-розшукові заходи, направлені на боротьбу з кібертероризмом і кібершпіонажем. Для Міністерства оборони України і Генерального штабу Збройних Сил України в рамках Стратегії кібербезпеки України основні задачі наведені без змін. А також передбачений кіберзахист критичної інформаційної інфраструктури в умовах правового режиму воєнного чи надзвичайного стану.

Правда, тільки через півтора роки після цього, на початку січня 2019 року, уряд вніс підготовлені Міністерством оборони України зміни в Положення про Міністерство оборони України. А вкінці січня 2019 року було затверджено Положення про Генеральний штаб ЗС України, який, насамперед повинен взяти на себе розгортання, управління і функціонування єдиної системи захисту інформації і кіберзахисту в інформаційно-телекомунікаційних системах Міністерства оборони України і ЗС України.

Варто зазначити, що заходи з забезпечення кібероборони і нарощення кібероборонних можливостей держави поки відсутні в Стратегічному оборонному бюлетені і в державних програмах з розвитку Збройних Сил України, їх озброєння і воєнної техніки. А затверджені урядом щорічні плани заходів з реалізації Стратегії кібербезпеки України до 2020 року не містили заходів із забезпечення Міністерством оборони України та Генеральним штабом Збройних Сил України кібероборони держави. До речі, на 2019 і 2020 роки такі плани уряду взагалі не затверджувалися, хоча, на початку лютого

2020 року в ЗС України було створено нове Командування Військ зв'язку та кібербезпеки ЗС України, а також призначено його командувача. В той же час кидається в очі те, що «кібернетична безпека» не зовсім відповідає такій задачі Міністерства оборони України і Генерального штабу ЗС України, як забезпечення кібероборони держави.

14 травня 2021 року Рада національної безпеки та оборони України ухвалила Стратегію кібербезпеки України на 2021–2025 роки.

Варто зазначити, що в ній відсутній перелік суб'єктів національної системи кібербезпеки, але зазначається, що до вирішення завдань щодо забезпечення кібербезпеки в національному масштабі крім основних суб'єктів національної системи кібербезпеки, на яких спиралася на початковій стадії формування національної системи кібербезпеки (тобто, іде відсилання до Стратегії кібербезпеки України на 2016–2020 роки), залучається широке коло суб'єктів забезпечення кібербезпеки, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України.

Ключову об'єднувальну та координаційну роль у цьому процесі, вже визначено, що відіграватиме Національний координаційний центр кібербезпеки [11].

Прикметним є те, що серед стратегічних цілей у формуванні потенціалу стримування (С) до 2026 року, які необхідно досягти, в ній визначено дієву кібероборону (ціль С.1). Для реалізації зазначеної цілі передбачається утворення у складі Збройних Сил України окремого роду військ – сил кібероборони, забезпечивши його належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору [11]. Це свідчить про те, що формування кібероборони в державі, хоч із запізненням, але почалося.

Інформаційна протидія і кібероборона, без сумніву, являються важливими компонентами сучасної оборони держави. А документи оборонного планування України повинні визначати цілі, задачі і заходи як з розвитку сил (військ) кібероборони, так і їх підготовку для відбиття інформаційної агресії.

В даній області існує досвід НАТО. Так на саміті Альянсу у Варшаві в липні 2016 року кіберпростір був визнаний новою сферою проведення операцій. А в лютому 2017 року був схвалений оновлений План кібероборони і дорожня карта з освоєння нової сфери проведення операцій [17; 18].

Так чи інакше, військово-політичному керівництву держави є над чим працювати. Складається враження, що кібероборона і кіберзахист держави як поняття (і в силу нових загроз) потребують деякого подальшого переосмислення у питаннях виділення організації протидії цим загрозам у самостійний сегмент сектору безпеки держави, не виключено, що зі структурним об'єднанням, коли в організаційній конструкції з'являться підрозділи кіберзахисту і інформаційної протидії контентно-психологічним операціям. Такі підрозділи логічно мати в структурах спецслужб, військового відомства, Генерального штабу ЗС України, як і в структурі Державної служби спеціального зв'язку та захисту інформації України. Скоріш за все вони виявляться різними за складом і реалізацією задач, однак координація діяльності в області кіберпротидії повинна здійснюватися з єдиного центру [2].

На жаль, в нормативно-правових актах залишаються невизначеними структура системи кібероборони держави, склад, функції і задачі суб'єктів її забезпечення, а також об'єкти кібероборони. Виконання основних задач із забезпечення кібероборони держави відповідно до законодавства покладено на Міністерство оборони України та Генеральний штаб ЗС України, які повинні разом вживати заходів з кібероборони для захисту суверенітету держави і забезпечення її обороноздатності, запобігання збройного конфлікту і відбиття збройної агресії. Ще більше запитань виникає до формування і діяльності підрозділів, які відповідають за інформаційно-психологічні контентні операції і за протидію активності ворога в цій сфері. Тому, наразі назріла необхідність щодо створення профільних підрозділів в структурах розвідки, Служби безпеки України, Міністерства оборони України, Державній службі спеціального зв'язку та захисту інформації України. В цілому вони повинні складати сили (війська) інформаційної протидії і кібероборони.

Варто прийняти до уваги, що складові інформаційно-психологічної протидії, кібератак і кібероборони суттєво відрізняється від кінетичної зброї, а, отже, концепція їх застосування мало підходить для поєднання з концепцією використання конвенційної зброї. Важливо підкреслити, що активна інформаційна війна не лише можлива за межами загальноприйнятої, конвенційної війни, але й протікає у мирний час (поряд з воєнним). Сфера застосування інформаційних засобів впливу на порядок ширша, ніж зони воєнних конфліктів.

І найголовніше: в інформаційній війні участь приймають не лише військові, але й значна частина цивільного суспільства. Більше того, вдало організована для цілей протидії агресії інформаційна зброя складає вагому частину загального імунітету нації, робить її неприступною в силу ідеологічної стійкості і обов'язкового зерна національної ідеї. Без останнього взагалі не може бути ефективної протидії і успішної оборони держави. І якщо битви ведуть не армії, а народи, то таке ментальне сприйняття війни являється формоутворюючим для створення і закріплення нації.

Висновки і перспективи подальших досліджень. Підводячи підсумок, варто зазначити, що Росія не застосовує якусь одну універсальну стратегію кібернападу до всіх об'єктів; навпаки, вона творчо підходить до вивчення різних можливостей щодо нових об'єктів у міру їх появи. В руках авторитарних держав кібератаки є ідеальною зброєю для поширення їх національного впливу і підтримки інших видів діяльності з метою надання політичного впливу. Кібератаки можуть використовуватися для стримування і здійснення тиску, для чого необхідно:

– розробити більш ефективну теорію міжнародних відносин в кіберпросторі, щоб пояснити, як саме кібератаки можуть служити факторами стримування або тиску;

– об'єднати кількісні і якісні методи і аналітичні викладки на оперативному і стратегічному рівнях, щоб розробити нові теоретичні та концептуальні рамки для розуміння цього середовища, яке швидко еволюціонує, і того, як авторитарні держави можуть його використовувати в своїх цілях.

Оцінка сучасного стану забезпечення інформаційної безпеки та кіберзахисту в Україні,

в аспекті напрацювання науково обґрунтованих пропозицій з цього питання, актуалізувала необхідність формування:

– збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачати нові можливості для цифровізації всіх сфер суспільного життя;

– належної правової (визначивши структуру системи кібероборони держави, склад, функції і задачі суб'єктів її забезпечення, а також об'єкти кібероборони у відповідних нормативно-правових актах), організаційної, технологічної моделі функціонування та застосування сил кібероборони.

Список літератури:

1. Бадрак В.В. Інформаційний фронт Кремля. *Комунікаційно-контентна безпека в умовах гібридно-месіанських агресій путінської Росії* : праці Міжнародного форуму з кризових комунікацій (Київ, 9-10 червня 2016 року). Київ : ВІКНУ, 2016. С. 35–44.
2. Горбулин В.П. Как победить Россию в войне будущего. Киев, 2020. 256 с.
3. Калетнік В.В. Проблема правового забезпечення в контексті протидії «активним заходам». *Гілея: науковий вісник*. 2020. Вип. 154. № 3. С. 269–275.
4. Киселев В.А. К каким войнам необходимо готовить Вооруженные Силы России. *Военно-теоретический журнал «Военная мысль»*. 2017. № 3. С. 37–46. URL: https://vm.ric.mil.ru/upload/site178/Gaz78Z3wGB.pdf (дата звернення: 20.05.2021).
5. Микрюков В. Новое лицо войны. Наука о вооруженном противоборстве требует корректировки. *Независимое военное обозрение*. 2017. № 02. С. 8–10. URL: https://nvo.ng.ru/nvo/2017-01-20/1_933_face.html (дата звернення: 20.05.2021).
6. Перник П. Хакерство как инструмент влияния. Кибератаки являются ключевым элементом российской информационной войны. *Журнал по проблемам безопасности и обороны Европы «per Concordiam»*. 2020. Том. 10. № 1. С. 46–52. URL: https://www.marshallcenter.org/sites/default/files/files/2020-10/pC_V10N1_RUS.pdf (дата звернення: 20.05.2021).
7. Соколов Б. Війна Володимира Путіна. *Газета «День»*. 2020. № 115. URL: https://m.day.kyiv.ua/ru/article/podrobnosti/voyna-vladimira-putina (дата звернення: 20.05.2021).
8. Galeotti M. Controlling Chaos: How Russia Manages Its Political War in Europe. *European Council on Foreign Relations*: Policy Brief (London, August 2017). London, 2017. URL: https://ecfr.eu/archive/page/-/ECFR228_-_CONTROLLING_CHAOS1.pdf (дата звернення: 20.05.2021).
9. Kime, Steve F. A 21st-Century Military Doctrine for America. *Joint Force Quarterly*. 2018. № 88. P. 58–63. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88.pdf (дата звернення: 25.05.2021).
10. Seely R. Defining Contemporary Russian Warfare. Beyond the Hybrid Headline. *Publication of the Royal United Services Institute for Defence and Security Studies «The RUSI Journal»*. 2017. Vol. 162. № 1. P. 50–59. URL: https://www.tandfonline.com/doi/abs/10.1080/03071847.2017.1301634 (дата звернення: 25.05.2021).
11. Проект Стратегії кібербезпеки України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 25.05.2021).
12. Schwab K. Shaping the Fourth Industrial Revolution. *World Economic Forum*. Geneva, 2018. 274 p.
13. Об утверждении Военной доктрины Российской Федерации: утверждено президентом Российской Федерации 25 декабря 2014 года № Пр-2976. *Российская газета*. 2014. № 298(6570). URL: https://rg.ru/2014/12/30/doktrina-dok.html (дата звернення: 25.05.2021).
14. Путин пересчитал всех русских в Украине. URL: https://ukraine.segodnya.ua/ukraine/putin-perecchital-vcekh-rucckikh-v-ukraine-211788.html (дата звернення: 25.05.2021).
15. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016 / Президент України. *Офіційний вісник Президента України*. 2016. № 10. С. 39. Ст. 198.
16. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII / Верховна рада України. *Відомості Верховної Ради України*. 2017. № 45. С. 42. Ст. 403.
17. Основні рішення Варшавського саміту. *Бюлетень*. (Варшава, 8-9 липня 2016 року). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160923_1609-factsheet-warsaw-summit-key-ukr.pdf (дата звернення: 25.05.2021).
18. Press conference: by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defense Ministers. URL: https://www.nato.int/cps/en/natohq/opinions_141340.htm (дата звернення: 25.05.2021).

References:

1. Badrak V.V. (2016) Informatsiinyi front Kremlia [The Kremlin's information front]. Proceedings of the *Mizhnarodnoho forumu z kryzovykh komunikatsii: Komunikatsiino-kontentna bezpeka v umovakh hibrydno-mesianskykh ahresii putinskoi Rosii (Ukraine, Kyiv, June 9-10, 2016)* (eds. Balabin V.V.), Kyiv: VIKNU, pp. 35–44.
2. Horbulyn V.P. (2020) Kak pobedyt Rossyiu v voine budushcheho [How to defeat Russia in the war of the future]. Kyiv: Bright Books. (in Ukrainian)
3. Kaletnik V.V. (2020) Problema pravovoho zabezpechennia v konteksti protydii «aktyvnym zakhodam» [The problem of legal supply in the context of the action against «active measures»]. *Hileia: naukovyi visnyk*, vol. 154, no. 3, pp. 269–275.
4. Kiselev V.A. (2017) K kakim voynam neobhodimo gotovit Vooruzhennyie Silyi Rossii [What wars should the Armed Forces of Russia be prepared for]. *Voenno-teoreticheskiy zhurnal «Voennaya myisl»* (electronic journal), no. 3, pp. 37–46. Available at: https://vm.ric.mil.ru/upload/site178/Gaz78Z3wGB.pdf (accessed 20 May 2021).
5. Mikryukov V. (2017) Novoe litso voynyi. Nauka o vooruzhennom protivoborstve trebuet korrektirovki [The new face of war. The science of armed confrontation needs adjustment]. *Nezavisimoe voennoe obozrenie* (electronic journal), no. 2, pp. 8–10. Available at: https://nvo.ng.ru/nvo/2017-01-20/1_933_face.html (accessed 20 May 2021).

6. Pernik P. (2020) Hakerstvo kak instrument vliyaniya. Kiberataki yavlyayutsya klyuchevyim elementom rossiyskoy informatsionnoy voynyi [Hacking for influence. Cyber attacks are key to Russian information warfare]. *Zhurnal po problemam bezopasnosti i oboronyi Evropyi «per Concordiam»* (electronic journal), vol. 10, no. 1, pp. 46–52. Available at: https://www.marshallcenter.org/sites/default/files/files/2020-10/pC_V10N1_RUS.pdf (accessed 20 May 2021).
7. Sokolov B. (2020) VIyna Volodimira PutIna [Vladimir Putin's war]. *Gazeta «Den»* (electronic newspaper). Available at: https://m.day.kyiv.ua/ru/article/podrobnosti/voyna-vladimira-putina (accessed 20 May 2021).
8. Galeotti M. (2017) Controlling Chaos: How Russia Manages Its Political War in Europe. *European Council on Foreign Relations:* Policy Brief (London, August 2017). Available at: https://ecfr.eu/archive/page/-/ECFR228_-_CONTROLLING_CHAOS1.pdf (accessed 20 May 2021).
9. Kime, Steve F. (2018) A 21st-Century Military Doctrine for America. *Joint Force Quarterly* (electronic journal), no. 88, pp. 58–63. Available at: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88.pdf (accessed 25 May 2021).
10. Seely R. (2017) Defining Contemporary Russian Warfare. Beyond the Hybrid Headline. *Publication of the Royal United Services Institute for Defence and Security Studies «The RUSI Journal»* (electronic journal), vol. 162, no. 1, pp. 50–59. Available at: https://www.tandfonline.com/doi/abs/10.1080/03071847.2017.1301634 (accessed 25 May 2021).
11. Proekt Strategiyi kiberbezpeki Ukrayini. Available at: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (accessed 25 May 2021).
12. Schwab K. (2018) Shaping the Fourth Industrial Revolution. *World Economic Forum*. Geneva, 274 p.
13. Ob utverzhdenii Voennoy doktrinyi Rossiyskoy Federatsii: utverzhdeno prezidentom Rossiyskoy Federatsii 25 dekabrya 2014 goda № Pr-2976 [Decree of the President of the Russian Federation on the approval of the Military Doctrine of the Russian Federation No. Pr-2976 (2014, December 25)]. *Rossiyskaya gazeta*, 2014, no. 298(6570). Available at: https://rg.ru/2014/12/30/doktrina-dok.html (accessed 25 May 2021).
14. Putin pereschital vseh russkih v Ukraine [Putin counted all Russians in Ukraine]. Available at: https://ukraine.segodnya.ua/ukraine/putin-perecchital-vcekh-rucckikh-v-ukraine-211788.html (accessed 25 May 2021).
15. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 15 bereznia 2016 roku № 96/2016 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cyber Security Strategy of Ukraine» № 96/2016 (2016, March 15)]. *Ofitsiinyi visnyk Prezydenta Ukrainy*, 2016, no. 10, p. 39, art. 198.
16. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05 zhovtnia 2017 roku № 2163-VIII [Law of Ukraine on the Basic Principles of Cyber Security of Ukraine № 2163-VIII (2017, October 5)]. *Vidomosti Verkhovnoi Rady Ukrainy*, 2017, no. 45, p. 42, art. 403.
17. Osnovni rishennia Varshavskoho samitu. [The main solutions of the Warsaw Summit] *Biuleten (Poland, Warsaw, July 8-9, 2016).* Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160923_1609-factsheet-warsaw-summit-key-ukr.pdf (accessed 25 May 2021).
18. Press conference: by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defense Ministers. Available at: https://www.nato.int/cps/en/natohq/opinions_141340.htm (accessed 25 May 2021).