УДК 681.324 DOI: 10.37701/dndivsovt.14.2022.11

Ю.Ф. Кучеренко[1], О.В. Александров[1], А.М. Носик[2], Д.О. Камак[3]

[1] *Харківський національний університет Повітряних Сил ім. Івана Кожедуба, Харків*
[2] *Національний технічний університет "Харківський політехнічний інститут", Харків*
[3] *Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси*

МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРАЇНИ З УРАХУВАННЯМ УМОВ СУЧАСНОГО ПЕРІОДУ ЇЇ ДЕРЖАВОТВОРЕННЯ

У статті наведені методологічні основи інформаційної безпеки держави як однієї з складових національної безпеки України. Детально розкриті складні умови сучасного періоду процесу державотворення в Україні, що визначаються впливом низки негативних зовнішніх та внутрішніх факторів, а саме: процесом формування нової політичної географії у світі; поширенням впливу національних рухів на відносини між країнами та в середині суспільства; здійснення повномасштабного військового вторгнення з боку російської федерації; загострення міждержавних економічних та територіальних суперечностей; зростання кількості внутрішніх конфліктів етнічного і релігійного характеру на території країни; зріст злочинності та корупції в державі; боротьба різних партій та громадських організацій за лідерство між собою; неконтрольоване розповсюдження зброї; низький економічний стан країни та зниження рівня життя більшості населення країни тощо.

Представлена система інформаційної безпеки держави, визначені основні її складові та розкриті джерела, що класифіковані за групами впливу на її базову основу, яка представляє собою інформацію. Розкритий механізм необхідності адаптації системи захисту інформаційної сфери від зміни зовнішніх та внутрішніх факторів впливу на неї.

Показано, що запобігання впливу на інформаційний простір нашої країни та її електронні ресурси, а також системи державного управління, в тому числі і автоматизовані системи управління військового призначення особливо в умовах ведення повномасштабної збройної агресії з боку російської федерації є першочерговим завданням, вирішення якого забезпечить дотримання відповідного рівня національної безпеки держави, в частині однієї з її основних складових (інформаційної безпеки) на належному рівні.

Результати досліджень доцільно використовувати науковцями і педагогічному складу, які займаються питаннями інформаційної безпеки держави на системному рівні, при розробці концепції та програми створення адаптивної системи захисту інформаційної сфери, що впливає на загальний стан національної безпеки України на сучасному періоді її знаходження.

Ключові слова: *агресія, безпека, війна, гібридна війна, державотворення, захист, інформація, інформаційна безпека, інформаційна сфера, психологічна операція, система захисту, фактор впливу.*

Вступ

Постановка проблеми. Умови сучасного процесу державотворення в Україні визначаються впливом низки зовнішніх (геополітична обстановка у світі, міждержавні стосунки України з іншими державами і перш за все із країнами сусідами, націоналістичні рухи в країнах світу, міжнародний тероризм, недостатня ефективність існуючих структур і механізмів забезпечення міжнародної безпеки та глобальної стабільності, територіальні суперечки між країнами та здійснення повномасштабного військового вторгнення росії на територію України тощо) факторів впливу на цей процес та внутрішніх факторів (політичного, економічного, соціального характеру), що діють в країні. Дані фактори створюють різні умови, які можуть як позитивно так і негативно впливати на стан національної безпеки (НБ) держави. Виділимо основні з них, що впливають на сучасний процес державотворення в Україні, в частині НБ (рис.1.), це: релігійна боротьба різних конфесій у світі; розвиток процесу формування нової політичної географії у світі, що призводить до виникнення територіальних претензій (суперечок) між державами, а іноді і до конфліктів; поширення впливу національних рухів на відносини між країнами та в середині суспільства; формування нових політичних еліт в країнах світу; здійснення широкомасштабної військової агресії з боку російської федерації (рф) від 24.02.22 року і як наслідок цього, ведення бойових дій в 14 областях України та

здійснення ракетних ударів по всій території країни, знищення її цивільної та військової інфраструктури; загострення міждержавних економічних суперечностей (проведення взаємної торгівельної блокади по багатьом товарам між країнами, в тому числі і з рф); зростання кількості внутрішніх конфліктів етнічного і релігійного характеру на території країни (боротьба конфесій Московського та Київського патріархату щодо впливу на свідомість своїх вірян та за їх кількість); непродумані вибухонебезпечні дії лідерів національних меншин, які можна розцінювати як загрозу стабільності і територіальній цілісності держави перед вторгненням російських військ на територію України; зріст злочинності та корупції в державі на всіх рівнях державного управління; боротьба різних партій та громадських організацій між собою за рейтинг і голоси виборців; неконтрольоване розповсюдження зброї; низький економічний стан країни та зниження рівня життя більшості населення країни, нелегальна міграція і таке інше. В останній час значно посилюється вплив таких явищ, як міжнародний тероризм та ведення інформаційних операцій з метою дестабілізації ситуації в країнах на користь агресора, а також здійснення застосування методів "гібридної" війни для вирішення своїх корисних інтересів, в тому числі і до нашої країни з боку рф, що відбувалось задовго до вторгнення її військ в нашу країну – коли все частіше залучаються до участі у буцімто внутрішніх конфліктах держави недержавні суб'єкти іншої держави, а саме інформаційні засоби, електронні ресурси, неконституційні військові формування, радикальні елементи та кримінал [1].

Російська федерація, проводячи проти України "гібридну" війну до 24.02.22 року, стверджувала мировій спільноті, що в Україні присутній "внутрішньо український конфлікт" або є в наявності ознаки "громадянської війни", а тому вона не є стороною конфлікту, але при цьому вона виконувала ворожі дії, які не притаманні широкомасштабному військовому вторгненню, здійснювала придушення свого опонента використовуючи скриті операції підривного характеру, влаштовуючи диверсії, захоплення інформаційного простору нашої держави, здійснювала кібератаки на державні та військові системи і електронні ресурси, а також забезпечувала всіляку військову та економічну підтримку незаконно проголошеним республікам, а після 24.02.22 року рф проводить широкомасштабну військову агресію прикриваючись лозунгом проведення "спецоперації". При цьому рф продовжує нав'язувати мировій спільноті свою думку про події, що відбуваються на Сході нашої країни (буцімто боротьбу з нацистами та захист російськомовного населення) застосовуючи для цього медіа простір, різні інформаційні засоби (методи) впливу на свідомість громадян, в першу чергу Європейського Союзу (ЄС). Вона здійснює проведення психологічних операцій, виконання заходів економічного тиску та політичного шантажу на країни ЄС, а також проводить різноманітні інформаційні операції для створення сприятливих умов щоб загальмувати процеси політичного, економічного і соціального розвитку України та остаточно загальмувати процес вступу її до ЄС через своїх лобістів. Зараз рф за рахунок впливу на інформаційну сферу (ІС) України (медіа простір, державні електронні ресурси та різні системи державного управління, в тому числі і військові системи управління) своїми інформаційними засобами (методами), здійснює всі можливі зусилля для забезпечення надійного контролю та впливу на неї під час ведення повномасштабної збройної агресії. Не можна відмітити, що останнім часом, використовуючи дестабілізуючи моменти, які впливають на міцність нашої держави, окремі країни здійснюють втручання у внутрішні справи, поширюють певні заяви, чутки й акції (ведення недружелюбної пропаганди, підтримка сепаратистських рухів, ведення переговорів с агресором без України і таке інше), які є результатом проведення спецоперацій рф у країнах ЄС та взагалі у світі, метою якою є здійснити розкол країн у питанні підтримці України в боротьбі з рф.

В цих умовах Україна мусить формувати і проводити гнучку та зважену орієнтовану на відповідні країни зовнішню політику з урахуванням найбільш суттєвих дестабілізуючих чинників і умов, які здатні викликати загострення двосторонніх відносин та відстоювати свої національні інтереси. Поглиблювати співпрацю з країнами парламенти, яких визнали то, що здійснює рф в Україні, як геноцид українського народу та проводити заходи щодо формування громадської думки в інших країнах щодо визвольної боротьби українського народу, який захищає зараз ціною життів своїх громадян європейські цінності та і сам ЄС, з метою впливу на рішення своїх держав щодо втілення економічних санкцій проти рф та здійснення економічної та військової допомоги нашій країні.

Тому, на сьогодні, одним з першочергових завдань є забезпечення інформаційної безпеки (ІБ) держави в умовах ведення інтенсивного інформаційного протиборства та повномасштабної збройної агресії з боку рф.

В такому складному і важкому періоді здійснення процесу державотворення України дуже важливе значення, на наш погляд, має виконання низки заходів, що направлені на зміцнення сектору національної безпеки і оборони держави та захист ІС країни від впливу інформаційно-психологічних та інформаційно-технічних засобів і методів агресора (інших недружелюбних до нас країн), який веде не тільки війну в Україні але і "гібридну" війну за лідерство у геополітичному просторі та за більш вагомий давно втрачений вплив на міжнародній арені [2].

Тому, роль ІБ держави на сучасному періоді державотворення країни, особливо під час ведення повномасштабної збройної агресії рф, як складової частини НБ України значно підвищується і поглиблене вивчення її як об'єкту дослідження з системних позицій стосовно визначення системи її захисту має дуже актуальне значення.

Метою статті є розгляд методологічних основ системи інформаційної безпеки України та визначення системи захисту інформаційної сфери країни з врахуванням сучасних умов, в яких здійснюється процес її державотворення

Аналіз останніх досліджень і публікацій. В наведеній літературі [1–16] розглядаються питання щодо особливостей сучасних війн [3–4], в тому числі ведення гібридних та інформаційних війн [1; 4–6], національної та інформаційної безпеки держави, світового впливу на процеси державотворення, функціонування державних та військових систем управління, медіа простору та таке інше [2; 7–16], але розгляду питань щодо адаптованості системи захисту ІС України до сучасних умов, в яких здійснюється процес її державотворення в них уваги майже не приділялось.

Виклад основного матеріалу

З набранням чинності: Указу Президента України №392/2020 від 14 вересня 2020 року Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України" [7], в якому визначено пріоритети національних інтересів України, забезпечення національної безпеки, цілі та основні напрями державної політики у сфері національної безпеки, загрози національній безпеці та національним інтересам України; Указу Президента України №121/2021 Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України" [8], в якому визначено систему поглядів на глобальні, регіональні та національні аспекти безпекового середовища у контексті воєнної безпеки України та визначені цілі, пріоритети і завдання реалізації державної політики у воєнній сфері, а також наголошено, що головним безпековим аспектом у воєнній сфері на національному рівні залишається розв'язана рф гібридна війна проти України; Указу Президента України №685/2021 від 28 грудня 2021 року Про рішення Ради

національної безпеки і оборони України "Про Стратегію інформаційної безпеки" [9], в якому визначено виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, що спрямовані на протидію визначеним загрозам, захист прав осіб на інформацію і захист персональних даних; Указу Президента України № 447 від 26 серпня 2021 року Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" [10], в якому визначено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України – держава отримала програмні документи щодо будівництва та укріплення національної безпеки держави і її основних складових, а також визначення основних аспектів НБ держави (рис.1).

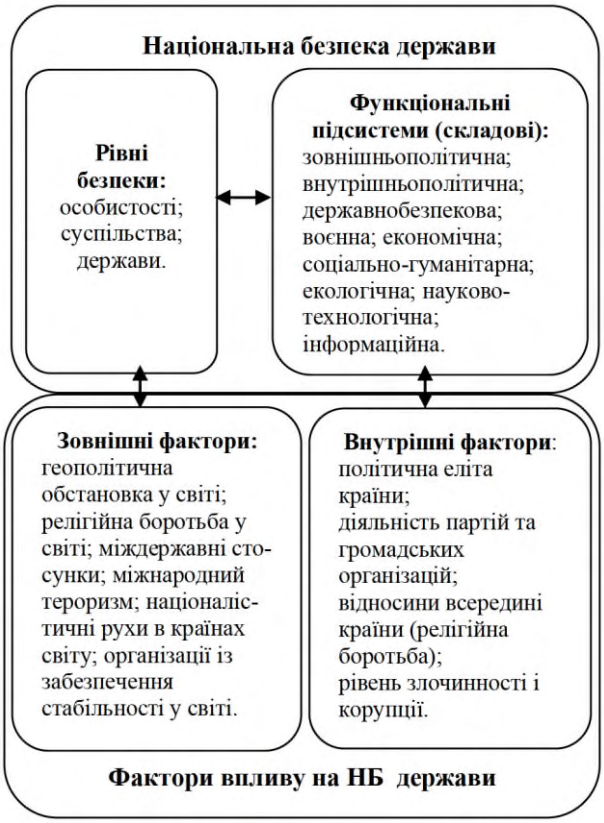

Рис.1. Методологічні аспекти національної безпеки держави
Джерело: розроблено авторами

В широкому аспекті під виразом "національна безпека" розуміється, стан захищеності життєва важливих інтересів особистості, суспільства та держави, а також обрису життя та національних інтересів (життєва важливих матеріальних, духовних і інтелектуальних цінностей Українського народу, визначальних потреб суспільства і держави), від широкого спектру зовнішніх та внутрішніх загроз (політичних, економічних, воєнних, екологічних, психологічних, інформаційних та інших [7–11]. Вона, як організаційна система, має три взаємопов'язаних рівня: безпека особистості, безпека суспільства і безпека держави. Складається з низки функціональних підсистем (складових), що характеризують відповідну сторону національної безпеки за відповідними сферами державного управління, я саме: зовнішньополітичною, внутрішньополітичною, державнобезпековою, воєнною, економічною, соціально-гуманітарною, екологічною, науково-технологічною та інформаційною (рис.1).

Основним завданням інформаційної безпеки на всіх рівнях її національної безпеки, бачиться захист ІС держави, через яку здійснюється вплив на свідомість як окремих громадян (особистостей, політиків. керівників всіх рівнів державного управління) так і населення країни

в цілому від інформаційних сил і засобів інших країн (організацій, груп і таке інше).

Тому, вивчення питання щодо побудови системи інформаційної безпеки (СІБ) держави та її адаптованості, тобто відповідності сучасним викликам (загрозам), що динамічно змінюються на сучасному періоді процесу державотворення в Україні потребує системного дослідження.

З методологічної точці зору ІБ, як одна з основних складових національної безпеки держави (рис.1.) визначає стан захищеності національних інтересів в ІС, що визначається сукупністю збалансованих інтересів особистості, суспільства та держави від навмисних та ненавмисних впливів інформаційного характеру, захищеність інформаційного середовища (медіа простору (МП), інформаційної інфраструктури (ІІ) від цих загроз та негативних впливів зовнішніх та внутрішніх факторів. Тому, в сучасних складних умовах державотворення, в яких опинилась Україна, у зв'язку із посиленням дії впливу політичного, силового, інформаційного та психологічного характеру на неї з боку рф, що розв'язала повномасштабну військову агресію, роль СІБ країни значно підвищується. А тому, її функціонування необхідно розглядати та досліджувати як сукупність взаємопов'язаних організаційних компонентів (керівний та підлеглий склад відповідних державних органів, служб, організацій), а також засобів, методів та заходів, що синхронізовано діють з метою забезпечення інформаційного суверенітету України у відповідності до проявів зовнішніх та внутрішніх факторів впливу на НБ безпеку України.

В сучасних умовах державотворення боротьба в ІС (в якій проводяться інформаційні операції з боку рф, що спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві та дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні) за контроль над ІІ, МП, державними електронними ресурсами (ДЕР) стає не менш важливою, чим боротьба Збройних Сил України з військами рф на полі бою (на землі, в морі або в повітряно-космічному просторі) і вестися вона буде не тільки під час ведення бойових дій, а і після їх завершення у мирний час. У подальшому слід очікувати, що ця боротьба перейде в площу кіберпростору, а це вже ознаки нової ери – ведення мережецентричних війн, в яких інформаційний вплив на свідомість людей і ІІ країни та її ДЕР буде відігравати основну роль для просування (нав'язування) своїх інтересів ("денацифікація", "демілітаризація").

З цього прикладу витікає висновок, що роль ІБ у подальшому, в загальній системі національної безпеки держави, буде тільки збільшуватись, а той хто забезпечить захист ІС та суспільства від негативних дій іншої сторони (сторін), зможе відстоювати інформаційний суверенітет країни на належному рівні.

У методологічному аспекті ІБ можливо представити двома складовими: інформаційно-психологічною та інформаційно-технічною, що направлені на захист ІС та населення держави від дії інформаційних сил і засобів інших країн (організацій, груп).

Інформаційно-психологічна безпека визначає стан захищеності громадян, окремих груп та населення країни від негативних інформаційно-психологічних впливів.

Інформаційно-технічна безпека визначає стан захищеності інформаційно-технічного середовища від програмних, силових, розвідувальних, радіоелектронних та інших впливів, що направлені на знищення, спотворення (втрату) інформації, вивід з ладу інформаційно-технічних об'єктів (ІТО), інформаційної інфраструктури держави, включаючи систему державного та воєнного управління (СД та ВУ).

Аналізуючи складові ІБ та їх призначення можливо припустити, що забезпечення ІБ у основному пов'язане з захистом ДЕР, її ІТО та ІІ (СД та ВУ, МП, Інтернету та інших

інформаційних систем), а також свідомості громадян, і в першу чергу основи, що їх об'єднує (пов'язує) в інформаційному аспекті – інформації. Інформація, в широкому аспекті її розуміння, має всеохоплююче значення для всіх сфер державного управління, бо є основою для забезпечення діяльності (виконання своїх функцій) людини, суспільства, держави, особливо в частині здійснення прийняття управлінських рішень, накопичення інформації, її обміну, а також для функціонування різних програмно-технічних засобів, комплексів і систем, а тому, вона пронизує в інформаційному розумінні всі складові ІБ, впливаючи на рівень їх функціонування. Тому, її необхідно надійно захищати від дії зовнішніх та внутрішніх організаційних елементів та інформаційних засобів (методів) негативного впливу.

В гуманітарному аспекті певна інформація, що сформована за відповідними правилами (алгоритмами, програмами) діє на структуру міркувань людини з метою забезпечення зміни її поведінки, яка протилежна її інтересам. В технічному аспекті в основі функціонування елементів інформаційної сфери (ДЕР, ІТО, МП, Інтернет, СД та ВУ та інших інформаційних систем (рис.2.) знаходиться інформація і її спотворення (нав'язування хибної) призводить до руйнування роботи цих елементів, що наносить значних збитків державі та її інформаційній безпеці.

Таким чином, в основу ІБ держави повинно бути положено захист інформації, що належить країні та суспільству, тоді аналіз джерел, які являють загрозу для неї (з точки зору негативного впливу) і їх класифікація по групах з метою визначення заходів щодо боротьби з ними, є першочерговим завданням для здійснення захисту ІС держави. Джерела, які можуть впливати на інформацію, можливо класифікувати за наступними групами: організаційні елементи (окремі люди, групи людей за національними ознаками (інтересами), державні організації (в тому числі силові), громадські утворення, релігійні конфесії та інші); інформаційно-технічні та програмні засоби (різні інформаційні джерела, технічні засоби впливу на інформацію, моделі та програми, що здійснюють вплив на інформацію (знешкодження, спотворення, несанкціоноване копіювання та інше); психологічні методи та програми впливу на свідомість громадян держави (рис.2).

До сучасних засобів інформаційного впливу (інформаційної зброї) входить сукупність спеціально організованої інформації та інформаційних технологій, що дозволяє цілеспрямовано змінювати, знешкоджувати, копіювати, блокувати інформацію, долати системи захисту, здійснювати дезінформацію, пошкоджувати функціонування носіїв інформації та інформаційних систем, здійснювати вплив на свідомість людей.

Засоби інформаційної боротьби, за характером інформаційного впливу (на об'єкти впливу) умовно, за функціональними ознаками, можна класифікувати за наступними групами:

– засоби масової інформації (радіо, преса, телебачення, агітаційно-пропагандистські), як вид інформаційної зброї масового ураження (морально-духовного життя населення, світогляду тощо);

– психотронні засоби (спеціальні генератори, спеціальна відеографічна та телевізійна інформація), що призначені для дистанційного зомбування населення та військовослужбовців;

– електронні засоби (оптико- та радіоелектронні засоби, спеціальні передавальні пристрої та випромінювачі електромагнітних хвиль і імпульсів, "комп'ютерні віруси", програмні закладки та інше), що призначені для придушення і ураження радіоелектронних і оптико електронних засобів (комплексів) та інформаційних систем;

– лінгвістичні засоби (мовні одиниці, мовні звороти та спеціальна термінологія), що призначені головним чином для використання висококваліфікованими фахівцями при веденні міжнародних переговорів, підписанні та виконанні договірних зобов'язань (бо мають семантичну неоднозначність при перекладі на інші мови);

– психотропні засоби (спеціально структуровані ліки, психофармакологічні та психодислептичні засоби, транквілізатори, галюциногени, алкоголь, наркотики та інші), що призначені для впливу на психіку людини, в тому числі на генному чи хромосомному рівні.

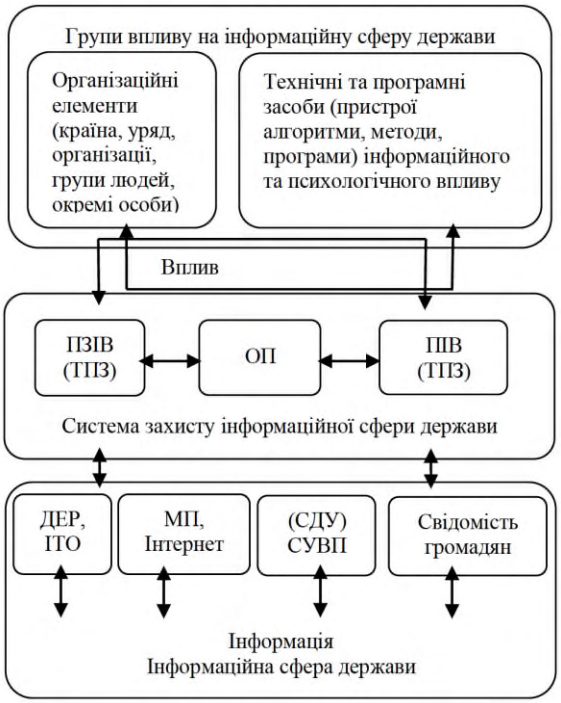

Рис.2. Інформаційна сфера держави, групи впливу не неї
та складові системи захисту інформаційної сфери держави у взаємозв'язку
Джерело: розроблено авторами.

Багато країн прагнуть до домінування у світовому інформаційному просторі і витиснення України із зовнішнього та внутрішнього інформаційного ринку, а тому розроблюють концепції ведення інформаційних війн. Дані концепції передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн, порушення функціонування інформаційної інфраструктури країн та одержання доступу до їх електронних ресурсів.

З метою протидії цим засобам та заходам необхідно мати систему захисту інформаційної сфери (СЗІС) держави (рис.2), яка повинна бути адаптованою до характеру та динаміці зміни методів ведення інформаційної боротьби у інформаційному просторі.

В загальному плані інформаційну боротьбу у ІС можливо представити як процес виконання відповідного комплексу взаємопов'язаних заходів інформаційного впливу на державу з боку інших країн (міжнародних організацій, різних груп людей і окремих осіб в тому числі і в середині країни, а також захист елементів ІС своєї держави (ДЕР, ІТО, МП, Інтернет, СД та ВУ, свідомості громадян (СГ)) від цього впливу, який проводиться з метою нанесення шкоди (в міжнародному, політичному, психологічному сенсі) та матеріальних збитків державі. Тоді СЗІС повинна складатись з наступних функціональних підсистем, які повинні протистояти певним загрозам в ІС (рис.2). До них слід віднести:

1. Організаційну підсистему (ОП), яка здійснює управління застосуванням відповідних сил (організаційних елементів (відповідних підрозділів), що відповідають за захист елементів ІС) і програмно-технічних (психологічних) засобів (методів), спрямованих на захист інформації та свідомості громадян своєї країни та здійснення організації протидії загрозам, що виникли у інформаційній сфері. Дія її повинна бути направлена на: здійснення прогнозування, виявлення та оцінку появі зовнішніх і внутрішніх загроз, дестабілізуючих чинників і конфліктів, які будуть негативно впливати на стан її елементів, а також причин їх виникнення

та наслідків їх прояву; розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту елементів ІС; організацію і зосередження зусиль технічних та програмних засобів (ТПЗ) для захисту елементів ІС; вдосконалення методів боротьбі з інформаційно-технічними (психологічними) засобами, що визивають дані загрози і організацію взаємодії з іншими підсистемами СЗІС.

2. Підсистему захисту від інформаційного впливу (ПЗІВ), що забезпечує виконання ряду заходів щодо захисту елементів інформаційної сфери держави від негативної дії технічних та програмних засобів інформаційного і психологічного впливу, з метою блокування їх дії на політично-соціальну, воєнну, економічну сфери діяльності держави та свідомість громадян. Дія її направлена в першу чергу на збереження ефективності функціонування всіх елементів ІС в умовах впливу на них інформаційних (психологічних) засобів за рахунок контролю в першу чергу за медіа простором, Інтернетом, за інформаційними потоками в державних та військових системах управління та забезпечення надійного захисту електронних ресурсів держави.

3. Підсистему інформаційного впливу (ПІВ), що забезпечує адекватний вплив на дії, які спричинили виникненню певних загроз в ІС держави за рахунок адаптивного застосування необхідних методів (програм та засобів) психологічного впливу на організаційні елементи та технічного впливу на функціонування різних інформаційних засобів (комплексів, систем), а також інформаційного простору недружелюбних сторін впливу, що визивають дані загрози для ІБ держави. Дія її повинна бути направлена на запобігання та усунення впливу виявлених загроз і дестабілізуючих чинників на ІС держави, блокування розповсюдження різних фейків та дезінформації підривного характеру. У кризових ситуаціях вона повинна забезпечувати виконання заходів щодо руйнування організаційно-технічної структури державних систем управління і в першу чергу систем управління військами та бойовими засобами противника, здійснювати виконання заходів дезінформації на всіх етапах інформаційного забезпечення управління в країні противника та його силових відомствах. Вона є основною ударною складовою для забезпечення завоювання та утримання інформаційної переваги над противником при боротьбі в інформаційній сфері.

Функціонування даних підсистем повинно бути тісно взаємопов’язаним поміж собою. Якісне виконання заходів ОП дозволяє виявити неправдиву інформацію, дію відповідних сил і засобів недружелюбної сторони, що визивають певні загрози, оцінити їх можливості щодо здійснення інформаційного впливу на елементи ІС, забезпечити планування своєчасного нарощування своїх сил і засобів захисту елементів ІС на відповідних напрямках. Це дозволяє ПІВ здійснити своєчасне виконання адекватних заходів впливу на ІС недружелюбної сторони (агресора) та нанести їй спрямовані дії, що направлені на усунення певних загроз, що в свою чергу підвищує ефективність роботи ПЗІП та послаблює вплив інформаційно-технічних засобів на функціонування елементів ІС нашої країни. Таким чином комплексне і своєчасне виконання заходів вказаних підсистем щодо захисту ІС, які повинні відбуватися за єдиним задумом (сценарієм) у відповідності до динаміці зміни обстановки в ІС повинно забезпечити відповідний рівень ІБ держави, що є одним з основних напрямів забезпечення НБ держави на сучасному етапі її державотворення. На сучасному етапі розвитку країни, для забезпечення адаптації системи ІБ країни умовам ведення проти неї повномасштабної збройної агресії, одночасно з методами ведення “гібридної” та інформаційної війни з боку рф, а також іншим негативним проявам інформаційного впливу з боку певних країн, необхідно, приділити увагу вдосконаленню та впровадженню перспективних методів, механізмів та засобів забезпечення інформаційно-технічної безпеки, що значно впливають на функціонування СЗІС держави, а саме:

– вдосконалення методів аналізу комп'ютерних програм на наявність вразливості і не декларованих можливостей;

– вдосконалення антивірусних технологій;

– впровадження перспективних методів та механізмів ідентифікації и аутентифікації користувачів з застосуванням електронних ключів і інших засобів їх впізнавання;

– забезпечення екранування і фільтрації інформації (позбавлення від непотрібної та надлишкової інформації);

– вдосконалення методів логічного розмежування доступу користувачів до певної інформації;

– вдосконалення засобів моніторингу стану функціонування елементів інформаційної сфери з метою вияву аномальних ситуацій при їх функціонуванні;

– впровадження нових методів шифрування і дешифрування інформації;

– впровадження перспективних засобів перевірки цілісності інформації на носіях і таке інше.

Стосовно протидії інформаційно-психологічним методам (алгоритмам, програмам, заходам), які здійснюють інформаційний вплив на масову свідомість з метою внесення змін в пізнавальна-розумову функцію людей з тим, щоб одержати відповідні зміни в структурі їх поведінки для прийняття ними і в першу чергу керівництвом держави (держслужбовцями всіх рівнів управління) неправильних соціальних, економічних, політичних та воєнних рішень і створення сприятливих умов для здійснення дестабілізації ситуації в середині країни,. необхідно приділити увагу вдосконаленню та впровадженню перспективних методів та механізмів боротьби з ними, а саме:

– розробки перспективних методів з елементами штучного інтелекту щодо аналізу інформації структура якої може негативно впливати на свідомість людини;

– вдосконалення методів (технологій) захисту від дії небезпечних заходів психологічного впливу на свідомість, почуття і дії громадян (суспільства);

– розробки перспективних методів щодо формування та впровадження потрібної нашим національним інтересам міжнародної громадської думки стосовно дії негативних загроз та дестабілізуючих чинників (факторів впливу) на процес державотворення в нашій країні;

– підготовки спеціальних інформаційних агентів для проведення заходів інформаційно-психологічного характеру (впливу на суспільство (громадські організації, громадян) на території недружелюбної країни);

– розширення можливостей служб радіо- і телевізійного мовлення (і в першу чергу, за рахунок використання вітчизняних супутників зв'язку та пересувних високотехнологічних радіо- і телевізійних станцій) для цілодобового ведення передач національного характеру як у самій країні, так і за її межами.

Таким чином, сучасна світова геополітика проводиться в умовах жорсткого інформаційного протиборства між великими державами та іншими країнами і характеризується нав'язуванням іншим країнам своїх вимог (поведінки), з метою збереження лідерства у геополітичному просторі та на міжнародній арені. Тому, захист національних інтересів в ІС, яка є основною інформаційною складовою НБ держави, повинен бути головним пріоритетним напрямом на сучасному етапі здійснення процесу державотворення в Україні.

Висновки

За підсумками проведених досліджень щодо методологічних основ ІБ України з врахуванням сучасних умов, в яких здійснюється процес її державотворення та з метою

запобігання впливу на медіа простір нашої країни, а також її державні ресурси, ІІ, в тому числі СД та ВУ та на свідомість громадян з боку інших сторін, і в першу чергу рф, першочерговим завданням є захист ІС держави, вирішення якого можливо за допомогою створення та постійного вдосконалення адаптованої системи захисту ІС, яка забезпечить дотримання відповідного рівня НБ держави та її складової – ІБ на належному рівні.

Даний матеріал, з практичної точки зору, буде доцільним використовувати при розробці вимог до перспективних засобів та методів адаптивної СЗІС держави та її елементів в умовах ведення жорсткої інформаційної, гібридної та повномасштабної війни проти нашої держави.

Список літератури

1. Кушнір О.І., Давикоза О.П., Кучеренко Ю.Ф. Аналіз впливу "гібридної" війни на розвиток автоматизованої системи управління авіацією та ППО Збройних Сил України. *Наука і техніка Повітряних Сил Збройних Сил України*. 2017. № 2(27). С. 116–120. https://doi.org/10.30748/nitps.2017.27.22.

2. Саганок Ф.В., Фролов В.С., Павленко В.І. та ін. Сектор безпеки і оборони: стратегічне керівництво та військове управління: монографія / за ред. д.військ.н. проф. І.С. Руснака. Київ: ЦЗ МО та ГШ ЗС України, 2018. 230 с.

3. Кучеренко Ю.Ф., Гузько О.М. Деякі особливості сучасних локальних війн. *Збірник наукових праць Харківського університету Повітряних Сил*. 2008. № 2(17). С. 20–23.

4. Алімпієв А.М., Пєвцов Г.В. Особливості гібридної війни рф проти України. Досвід, що отриманий Повітряними Силами Збройних Сил України. *Наука і техніка Повітряних Сил Збройних Сил України*. 2017. № 2(27). С. 19–25. https://doi.org/10.30748/nitps.2017.27.03.

5. Странніков А.М. Інформаційна боротьба у воєнних конфліктах другої половини XX століття. Альтерпрес, 2006. 191 с.

6. Медведєв В.К., Кучеренко Ю.Ф., Гузько О.М. Сучасна інформаційна війна та її обрис. *Системи озброєння і військова техніка*. 2008. № 1(13). С. 52–54.

7. Про Стратегію національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020.

8. Про Стратегію воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021.

9. Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021.

10. Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021.

11. Бжезинський З. Україна і Європа. *Національна безпека і оборона*. 2000. № 7. С. 11–20.

12. Huntington S.P. The Clash of Civilizations. 2000. 400 с.

13. Ярош С.П. Теоретичні основи побудови та застосування розвідувально-управляючих інформаційних систем протиповітряної оборони. Харків: ХУПС, 2012. 512 с.

14. Худов Г.В., Таран І.А. Методика синтезу раціональної структури підсистеми розвідки системи протиповітряної оборони з використанням генетичного алгоритму. *Наука і техніка Повітряних Сил Збройних Сил України*. 2016. № 2(23). С. 25–31.

15. Ковалевський С.М., Пєвцов Г.В., Худов Г.В. Пропозиції щодо створення скритого маловисотного радіолокаційного поля в умовах ведення сучасних мережецентричних та гібридних війн. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. № 1(18). С. 77–81.

16. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка. Харків: ФОП Федорко М.Ю., 2021. 558 с. ISBN 978-617-7664-71-9.

Надійшла до редколегії 17.11.2022
Схвалена до друку 12.12.2022

Відомості про авторів:

Кучеренко Юрій Федорович
кандидат технічних наук
старший науковий співробітник
провідний науковий співробітник
Харківського національного університету
Повітряних Сил ім. Івана Кожедуба,
Харків, Україна
https://orcid.org/0000-0001-9937-371X

Information about the authors:

Yurii Kucherenko
PhD in Engineering
Senior Research
Leading Research Associate
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/ 0000-0001-9937-371X

Александров Олександр Валерійович
кандидат технічних наук
старший науковий співробітник
начальник науково-дослідного відділу
Харківського національного університету
Повітряних Сил ім. Івана Кожедуба,
Харків, Україна
https://orcid.org/0000-0001-6405-9456

Носик Андрій Михайлович
кандидат технічних наук
старший науковий співробітник доцент
Національного технічного університету
"Харківський політехнічний інститут"
Харків, Україна
https://orcid.org/0000-0002-4171-1875

Камак Дмитро Олександрович
начальник науково-дослідного відділу
Державного науково-дослідного інституту
випробувань і сертифікації озброєння
та військової техніки,
Черкаси, Україна
https://orcid.org/0000-0003-0348-5456

Oleksandr Aleksandrov
PhD in Engineering
Senior Research
Head of Scientific Research Department
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0001-6405-9456

Andrii Nosyk
PhD in Engineering
Senior Research Associate Professor
of National Technical University
"Kharkiv Polytechnic Institute",
Kharkiv, Ukraine
https://orcid.org/0000-0002-4171-1875

Dmytro Kamak
Head of the Scientific-Research Department
of State Scientific Research Institute
of Armament and Military Equipment
Testing and Certification,
Cherkasy, Ukraine
https://orcid.org/0000-0003-0348-5456

METHODOLOGICAL FOUNDATIONS OF COUNTRY'S INFORMATION SECURITY CONSIDERING THE CONDITIONS OF THE CURRENT STAGE'S DEVELOPMENT

Y Kucherenko, O Aleksandrov, A Nosyk and D Kamak

The article provides methodological foundations of information security in the state as one of the Ukrainian national security components. The complex conditions in the modern period of the Ukrainian state-building process are revealed in detail. These conditions are determined by the influence of a number negative external and internal factors, namely: the process of a new political geography formation in the world; the spread of national movement's influence on relations between countries and within society; the embodiment of a full-scale military invasion by the russian federation; aggravation of interstate economic and territorial contradictions; an increase in internal conflicts of ethnic and religious nature in the country; growth of crime and corruption in the state; the struggle of different parties and social organizations for leadership among themselves; the uncontrolled proliferation of weapons; the low economic state of the country and the decline in the living standard of the majority country's population and more.

The system of the state information security is presented. Its main components are determined and the sources are classified according to the groups of influence on its foundation which represents the information. It reveals the mechanism for adapting the system to protect the information sphere from changes in external and internal factors affecting it.

It is shown that prevention of influence on information space of our country and its electronic resources and also the state management's system including the military automated control systems, especially in conditions of conducting full-scale armed aggression from the side of the russian federation is the priority task which solution will provide observance of an appropriate national state's security level, regarding one of its basic components (information security) at a proper level.

The results of research is advisable to use by researchers and teaching staff dealing with information security of the state on a systemic level when developing the concept and program of creating an adaptive system protection in the information sphere affecting the overall state of Ukrainian national security at the present period of its location.

Keywords: *aggression, security, war, hybrid warfare, statehood, protection, information security, information security, information sphere, psychological operations, protection system, influence factor.*