залучені до врегулювання конфліктів в обох країнах та значну критику діяльність організації, стверджується про доцільність комплексного вивчення ролі ОБСЄ у вирішенні обох конфліктів, а саме її нормативно-правової основи, роботи інституцій та оперативної діяльності на місцях. Доведено, що досвід роботи вже закритої місії ОБСЄ в Грузії може стати корисним при розробці плану врегулювання кризи в Україні. Серед досягнень функціонування місій ОБСЄ у Грузії та Україні виокремлено її нейтральний статус, що дозволяє залучити до переговорів велику кількість учасників. У випадку Грузії та України ОБСЄ стала платформою для ведення переговорів з Росією, як однією зі сторін конфлікту і без погодження з якою неможливе вирішення кризи. Наголошено на такому досягненні організації як залучення сторін конфлікту до переговорів та зменшення інтенсивності військових дій, враховуючи й той факт, що у своїй діяльності ОБСЄ дотримується багатофункціонального підходу у вирішенні кризи у суспільстві, який містить гуманітарний підхід у роботі з населенням та моніторинг прав людини. Виокремлено виклики у роботі ОБСЄ, до яких віднесено складний процес прийняття рішень, відсутність механізму примусу щодо виконання домовленостей, що призводить до порушення угод та невирішеності конфлікту, часту відсутність спостерігачів на місці, де трапляються збройні інциденти тощо. Доводиться необхідність реформування процесу прийняття рішень, особливо у випадку, коли сторони конфлікту долучені до прийняття важливих рішень; впровадження механізму примусу, чи то економічного, чи то політичного, який міг би впливати на сторони конфлікту задля виконання домовленостей; оснащення місій ОБСЄ новим обладнанням та засобами безпеки задля усунення ризиків для міжнародних спостерігачів та кращого моніторингу в зоні конфлікту.

Ключові слова: *ОБСЄ, спеціальна моніторингова місія ОСБС, конфлікт у Грузії, конфлікт на Сході України, міжнародна безпека.*

УДК 351.862.4:316.776

М.А. Еделєва

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

В XXI столітті людство отримало стрімкий розвиток науково-технічного потенціалу завдяки швидкому поширенню інформації та впровадженню сучасних інформаційних технологій (ІТ) в повсякденне життя суспільства. Виявлено, що розвиток ІТ призведе до принципово нового витка розвитку людства, що може привести до корінних змін в багатьох сферах суспільства, зокрема в політичній та економічній. Автором з'ясовано, що в новому столітті відмічається попит на інформацію як новий стратегічний ресурс, що відкриває нові можливості для країн, що розвиваються як в економічному, так і політичному секторі. Також встановлено, що з розвитком інформаційного суспільства зростають інформаційні загрози, з'являється необхідність забезпечення інформаційної безпеки держави, суспільства та особистості. В період модернізації політичної системи держави владою повинні бути визначенні основні напрямки державної інформаційної політики в сфері забезпечення інформаційної безпеки.

Ключові слова: *інформаційна політика, інформаційна безпека, кібербезпека, хакери.*

В останні роки, питання забезпечення інформаційної безпеки в контексті реалізації державної інформаційної політики стають все більш актуальними. Влада розуміє існування проблем і складність завдань, при вирішені питань з забезпечення інформаційної безпеки в країні. На сьогодні необхідно провести комплексне дослідження стану забезпечення інформаційної безпеки та знайти можливі шляхи удосконалення.

Робиться спроба виділити конкретні виміри, за межами яких дія цих чинників перетворюється на загрозу життєдіяльності суспільства, і сформулювати належний формат та інструменти за сприянням яких адекватно приймати і реагувати на наявні та потенційні загрози національної безпеки через реальний стан державної інформаційної політики України.

Питання інформаційної безпеки вітчизняні вчені досліджували і раніше, але комплексних, системних досліджень в контексті державної інформаційної політики не багато. В українській вітчизняній науці питання забезпечення інформаційної безпеки вивчалися такими вченими як В. Гурковський, О. Довгань, В. Козубський, О. Крюков, Є. Макаренко, В. Остроухов, В. Петрик, Г. Почепцов та інші.

Аналіз нормативних документів провідних, розвинутих демократичних країн з інформаційної безпеки, які були прийняті ще в 90-х роках ХХ століття, показав, що американські та європейські уряди вже тоді розуміли складність інформаційних систем, а з тим і складність забезпечення інформаційної безпеки.

Інформаційна безпека є предметом дослідження вчених різних галузей: політології, соціології, філософії, державного управління, юридичних наук. Ця проблема є дискусійною, як серед вчених, так серед представників громадськості, політиків, військових тощо.

Метою даної статті є аналіз проблемних питань в сфері інформаційної безпеки та пошук напрямків вдосконалення інформаційної політики держави.

У двадцятому столітті внаслідок великого попиту на інформацію як з боку держав так і суспільства, зросла її роль як ресурсу. Інформація стала не тільки стратегічним ресурсом, який створюється у величезних масштабах, зберігається і передається, обробляється і використовується, а й великою потребою для населення всієї земної кулі. Владі треба усвідомити, що: по-перше, засоби масової комунікації (ЗМК) відіграють провідну роль у формуванні відносин між владою та суспільством; по-друге, суспільство наразі значно інформоване ніж раніше. На сьогодні існує «цілий комплекс проблем, які пов’язані з гуманітарною складовою національної безпеки як окремого індивіда, так і проблеми управління суспільною свідомістю нації» [5, с. 8].

З ростом попиту населення на інформацію, держава повинна прораховувати виклики та проблеми, швидко проводити модернізацію в стратегічних областях державного сектору. Отож, в сучасному суспільстві, яке здійснює модернізацію, виникає потреба переглянути існуючі економічні, політичні, соціально-культурні концепції розвитку та інформувати суспільство про ці зміни.

В той же час, розвиток інформаційних технологій, що необхідне для накопичення і ефективного використання інформаційних ресурсів, стає стратегічним чинником забезпечення національної безпеки. Для державної інформаційної політики забезпечення інформаційної безпеки держави стає принциповим, влада розуміє, що загрози в інформаційній сфері заважають ефективному розвитку політичної системи країни та демократизації суспільства.

На сьогодні, на жаль, як ніколи для Української держави стають актуальними поняття «інформаційна безпека», «інформаційна війна», «кібертероризм». Зупинимося на характеристиці цих явищ детальніше.

У сучасних умовах інформаційна війна розглядається військовими теоретиками як якісно новий вид бойових дій, активна протидія в інформаційному просторі, а інформація при цьому - як потенційна зброя та зручна ціль [1, с. 7]. Раніше інформація слугувала для населення засобом інформування про події, що відбуваються в країні та світі. Сьогодні під час ведення інформаційної війни, інформацію використовують як новий вид зброї для дестабілізації політичної системи в країні та підриву демократичних цінностей.

Для України представляє науковий та практичний інтерес стратегія розвитку національної безпеки розвинутих країн світу, зокрема США. Для США питання національної безпеки в інформаційній сфері завжди були пріоритетами розвитку держави.

У підготовлений Комітетом збройних сил США документі «Єдина доктрина протиборства в галузі управління та зв'язку» термін «інформаційна війна» визначається як сукупність заходів, що приймаються з метою досягнення інформаційної переваги над противником шляхом впливу на його інформаційні системи, процеси, комп'ютерні мережі, громадськість і індивідуальну свідомість та підсвідомість населення, також особового складу збройних сил, при одночасному захисті свого інформаційного середовища [12, с. 7].

Можна стверджувати, що при наявності такої великої кількості аналітичних досліджень, присвячених способам та методам ведення інформаційної війни, тільки їх ігнорування при розробці інформаційної політики держави могло привести до негативних наслідків в 2014 р. (АТО та анексія Криму).

Ще в 2005 році Козубський В.О. звернув увагу на проблеми та загрози стабільності в кримському регіоні, які пов'язані з недосконалістю інформаційної політики. Автор наголошує, що тривала аналітична діяльність у сфері кримського сегменту національного інформаційного простору усе більше переконує не тільки в тім, що кардинальні рішення просто відсутні, але й у тім, що конструктивний шлях стабілізації автономії лежить насамперед у послідовній і кропіткій роботі з суспільною думкою» [5, с. 4].

Дійсно, державна інформаційна політика України в кримському регіоні була вкрай слабкою, вплив російської інформаційної політики на формування настроїв населення Криму був сильніший, ніж української.

З початком формування в Україні інформаційного суспільства та входженням до світового інформаційного простору у держави з'явилося ряд нових завдань, які потребують нагального вирішення. Особливої актуальності набуває вирішення проблем інформаційної безпеки в сучасному суспільстві.

В умовах існуючих нових загроз інформаційній безпеці, держава повинна впроваджувати і нові методи захисту інформації. Новизна дослідження як раз і полягає в тому, щоб систематизувати загрози в інформаційному просторі, порівняти вже існуючі методи боротьби з ними та запропонувати нові ефективні методи протидії інформаційним загрозам в контексті реалізації державної інформаційної політики.

На думку науковців, інформаційна безпека – це стан захищеності об'єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), при якому досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів [9, с. 136].

В. Фомін та А. Рось, зауважують, що суть інформаційної безпеки в системі національної безпеки держави полягає в наступному: прагненням кожної держави реалізувати та захистити власні національні інтереси, що направлені на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів [11, с. 24]. Звичайно, розвинутим країнам світу свій

інформаційний простір значно простіше захистити, ніж тим країнам, що є менш розвиненими. Захист інформаційного простору вимагає не тільки великих матеріальних затрат, але і достатньої кількості висококваліфікованих спеціалістів в цій галузі. Чи зацікавлені розвинуті країни світу в наданні допомоги країнам з менш розвинутим технологічним забезпеченням, з тим щоб впровадити сучасні технологій глобальної міжнародної інформаційної безпеки? Очевидно, розвинуті країни світу будуть виходити з своїх власних інтересів, враховувати ситуацію, що склалася в світі, прораховувати всі виграші і програші при наданні такої допомоги.

Як зауважує Є. Макаренко, проблеми глобальної безпеки посідають особливе місце в структурі міжнародної інформаційної політики, визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня і гостроти, що можуть поставити під загрозу забезпечення світопорядку, реалізацію стратегій становлення глобального інформаційного суспільства, навіть саме існування цивілізації [7, с. 20].

Геополітичне розташування України багато в чому визначало політичний курс різних політичних сил, що перебували при владі в Україні в різні часи, а з тим і систему управління щодо забезпечення інформаційної безпеки. Нині вектор розвитку політичної системи України спрямований на демократизацію суспільства та впровадження європейських цінностей.

Сьогодні існують численні проблеми в сфері інформаційної безпеки України, одна із головних – це збереження інформації, яка може бути використана з метою руйнування цілісності держави, або проти інститутів влади, від функціонування яких залежить стабільність, розвиток українського суспільства.

Наприклад, США розуміючи всі загрози в інформаційній сфері та пов’язуючи її з стратегічною сферою інтересів держави, розробили ряд послідовних кроків, які мають запобігти загрозам безпеці в кіберпросторі. Перш за все кадрові призначення повинні бути відповідальними та зваженими, адже успіх у вирішенні цієї проблеми залежить від професіоналізму, кваліфікованості працівників в цій сфері. «Президент США Барак Обама оголосив інформаційну інфраструктуру Америки «стратегічним національним активом» і призначив Говарда Шмідта, колишнього начальника служби безпеки корпорації Майкрософт, начальником з кібербезпеки США» [13, с. 4]. Також, «У травні 2010 року Пентагон створив свій новий відділ по боротьбі з кіберзлочинцями «Cyber Command» (Cybercom) на чолі з генералом Кітом Олександром, директором Агентства національної безпеки (NSA). В його обов’язки входить, проводити спеціальні операції так званого «повного спектру», тобто захищати американські військові мережі та здійснювати несанкціоновані напади на електроні системи інших країн, як і за якими правилами залишається таємницею» [13, с. 4]. Отже, дбаючи про власну кібербезпеку США (як і інші країни) не виключають спеціальних операцій щодо електронних систем інших країн, незважаючи на те, що 22 липня 2000 року провідними країнами світу була підписана «Окінавська Хартія глобального інформаційного суспільства», в якій зазначалося, що «Зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, повинні супроводжуватися погодженими діями по створенню безпечного і вільного від злочинності кіберпростору» [8, с. 6].

Слід визнати, що за той час, що пройшов з моменту підписання угоди світ змінився, інформаційний простір країн став ще більш уразливим, атаки в кіберпросторі стали носити системний характер.

Особливе місце в системі забезпечення інформаційної безпеки займає кібертероризм. Від традиційного цей вид тероризму відрізняється використанням сучасних інформаційних технологій, зловмисним створенням інформаційних загроз життєво важливим інтересам особистості і суспільства. Ця обставина обумовлює застосування більшої кількості способів досягнення цілей.

В 2017 році в ході хакерської атаки від комп'ютерного вірусу Petya значно постраждала інформаційна інфраструктура України. Внаслідок чого понесли збитки національні стратегічні об'єкти, комерційні установи та громадяни України. Ця хакерська атака стала можливою через недостатній рівень захищеності інформаційних ресурсів та нехтування правил кібербезпеки. Метою атаки була дестабілізація політичної системи України, створення хаосу в інформаційному просторі країни.

Кібервійни в мережі Інтернет породжують складні, різнобічні та потенційно дуже небезпечні загрози. Сучасні суспільства все більше залежать від комп'ютерних систем, з'єднаних з Інтернетом, що надає ворогам більше можливостей для нападу.

В журналі The Economist, зазначається, що «як і в разі контролю над ядерним та звичайним озброєнням, великі країни повинні почати говорити про те, як зменшити загрозу кібервійни, мета - обмежити напади, перш ніж буде занадто пізно [13, с. 1].

Отож, нині, кіберпростір став ще однією сферою, в якій розгортаються бойові дії після землі, морського та повітряного простору.

Нині служби безпеки (держави, приватного сектора) постійно працюють над захистом інформації та вдосконалення систем захисту даних. Подія жовтня 2013 року (Агентство національної безпеки США прослуховувало особистий телефон Канцлера Німеччини) показала, що недостатній захист інформації приводить до того, що незахищеними від прослуховувань є і особисті телефоні переговори політичних лідерів країн [3, с. 106]. Це призводить до погіршення відносин між країнами партнерами та загострення відносин на міжнародній арені.

У XXI ст. виникла ціла низка нових проблем в сфері безпеки. Процеси глобалізації привели не тільки до позитивних наслідків, але породили серйозні негативні явища, до яких світова спільнота виявилася не готовою. Як зауважує, О. Крюков, «Виклики, пов'язані з глобалізацією, завдали колосальних збитків майже всім країнам» [6, с. 3].

Відомий експерт в сфері державної інформаційної політики Г. Почепцов відмічає, що «на сьогодні величезні обсяги фінансування виділяють на те, щоб закрити інформаційний простір від чужих, оскільки там містяться секрети, а в комунікативний простір вкладаються гроші, щоб розміщена там інформацій поширилася якомога більше» [10, с. 198].

Наступна проблема в системі забезпечення інформаційної безпеки, яка існує в нашому суспільстві, це проблема доступу до інформації громадськості. Ця проблема певною мірою пов'язана з проблемою захищеності інформаційного простору від несанкціонованих атак та ведення інформаційної війни в площині українського інформаційного простору. Тобто, варто відмітити, що в будь-якій державі є секретна інформація, доступ до якої може бути дозволений через багато років, тоді, коли знімається гриф секретності. Це, в першу чергу, та інформація, розповсюдження, оприлюднення якої, може завдати шкоди як державі, так і суспільству. В свою чергу, як відмічається в монографії «Інформаційна політика України: європейський контекст» (2007), «інформаційна безпека – це завжди балансування між інформаційною відкритістю та закритістю**,** між прагненнями максимально розширити доступ громадян до невтаємниченої публічної інформації (державної, комерційної, наукової, освітньої, персональної тощо) й максимально захистити інформацію корпоративного і приватного змісту» [4, с. 120].

Певно, для громадськості важливий вільний, максимально розширений доступ до інформації, але якщо мова йде про державу, то для неї в пріоритеті є конфіденційність, обмежений доступ до інформації, що повинно регулюватися законами, які визначають рівень доступу.

Варто відзначити, що на сьогодні українська влада підтримує курс на євроінтеграцію та взяті зобов'язання дотримуватися практики вільного доступу

громадян до інформації та забезпечувати відкритість прийняття рішень. В умовах реалізації демократичних принципів та конституційних прав громадян на вільний доступ до інформації зросли потреби соціально активної частини суспільства в розширенні інформаційної взаємодії влади і громадськості.

Однак, сьогодні, коли держава намагається побудувати демократичне, відкрите суспільство, слід враховувати зростаючу роль таких явищ як «інформаційна війна» та «інформаційні протиборства», а також кібертероризм, який має чітку мету отримати секретні данні держав задля створення хаосу в певних країнах.

З одного боку, існують права і свободи людини, в тому числі право на інформацію та право на захист інформації, що є невід'ємними правами громадян демократичних країн, з іншого боку, коли проти України ведеться інформаційна війна, то заради безпеки людини в умовах існування міжнародного кібертероризму держава змушена закривати деякі Інтернет ресурси, які можуть розповсюджувати інформацію, яка направлена на дестабілізацію політичної системи країни. Метою таких дій є і попередження підготовки терористичних актів. Такі попереджувальні дії держави звичайно ж викликають занепокоєння щодо збереження демократичних принципів.

Сьогодні ніде в світі людина не може відчувати себе в безпеці – ні в розвинутих країнах, ні в тих, що розвиваються. Уявлення про «безпечні» країни дуже змінилися.

Слід зважати на те, що з кібертероризмом боротися дуже важко. «Інформаційна зброя», яку використовують кібертерористи, специфічна. Якщо відносно інших видів озброєння час від часу держави ведуть переговори щодо їх скорочення, то щодо використання «інформаційної зброї» вести переговори важко, якщо взагалі можливо. Це робить цю сферу ще більш небезпечною. Аналітики не можуть прогнозувати те, яку владу можуть отримати кібезлочинці в сучасному світі та передбачити їх наступну мішень, а тому держави, в тому числі й Україна, мають бути готовими до захисту від кібератак в будь-який момент часу.

Питання національної безпеки України в інформаційній сфері поєднано з питанням безпеки міжнародної. Якщо в цілому світ став небезпечним, не може в окремій державі бути безпечно.

Для України є актуальним питання взаємодії органів державної влади щодо гарантування інформаційної безпеки держави. В. Гурковській наголошує, що від органів державної влади очікується вдосконалення не тільки технічного захисту власних систем безпеки комп'ютерних, інформаційних мереж, а й розробки нових підходів та організаційно-правових заходів щодо взаємодії з іншими державними органами, здатними розв'язувати зазначені проблеми на національному рівні [2, с. 3].

Потребує вдосконалення також правова база інформаційної політики. Закон повинен чітко регламентувати права держави і не заперечувати основним правам і свободам громадян. Наприклад, Інтернет не є державною мережею, що ускладнює контроль з боку влади, а є мережею, яка в основному належить приватному сектору. Але між владою та приватним сектором були укладені домовленості щодо забезпечення безпеки інформаційного простору країни. У 2017 р. були внесені зміни в законодавчі акти, що стосуються медіа сфери, захисту інформаційного простору та кіберпростору. Була введена заборона інтернет-провайдерам щодо надання послуг з доступу користувачам мережі Інтернет до ресурсів, які несуть загрозу Українській державі в умовах «гібридної війни».

Важливим кроком в напрямку посилення державної безпеки є економічне забезпечення ефективної державної інформаційної політики. Довгі роки не проводилася модернізація національних систем захисту інформації. Той комплекс засобів захисту інформаційних мереж, який дістався Україні після розпаду Радянського Союзу застарів, частина була зруйнована, а частина модернізована. Його нині не вистачає для того, щоб

Україна зайняла гідне місце в світі в сфері захищеності мереж. Для цього потрібно: відповідне фінансування; запровадження технологій, які використовують передові держави сфері в інформаційної безпеки; кваліфіковані кадри в сфері захисту інформації держави від несанкціонованого доступу.

Також важливо створити механізм протидії попадання в інформаційний простір країни недостовірної інформації з метою дестабілізації суспільства. Метою державної інформаційної політики є боротьба з фейковими новинами за допомогою механізмів протидії цьому феномену. Пересічному громадянину дуже складно розібратися в інформаційному контенті, який він споживає, для цього потрібно розробити урядову програму для школярів та менш захищених верств населення (пенсіонерів, інвалідів) по медіаграмотності. Уряд повинен працювати на випередження, тобто він повинен передбачити вкидання інформації до того моменту коли ця інформація потрапить в суспільство.

Отже, сьогодні проблема інформаційної безпеки в процесі глобалізації та міжнародних інтеграційних процесів набувають особливого значення. Країни з потужним потенціалом в інформаційному просторі мають змогу впливу на країни з низьким рівнем захищеності інформаційного простору та кіберпростору. За останні три роки Україною в інформаційному просторі, мережі Інтернет та кіберпросторі було здійснено більше заходів щодо забезпечення інформаційної безпеки ніж за всі попередні роки незалежності країни.

Законодавча база щодо інформаційної сфери в Україні одна із передових, але комплексне вивчення дає змогу побачити відставання від розвинутих демократичних країн, що гальмує інтеграцію в світовий інформаційний простір.

Таким чином, перед владою стоїть завдання ліквідувати наступні загрози, які підривають інформаційну безпеку держави: послаблення уваги до питань інформаційної безпеки; недосконала правова база; застарілі технології захисту мереж; відсутність кваліфікованих кадрів в сфері захисту інформації; економічна, соціальна та політична нестабільність в країні та інше.

Багато чого також можна досягти шляхом більш тісної співпраці між урядом та приватним сектором. Більшу частину роботи щодо забезпечення того, щоб звичайні комп'ютерні системи не використовувались злочинцями або «кібервоїнами», можуть виконати постачальників послуг Інтернету, які керують мережею. Вони можуть взяти на себе більшу відповідальність за виявлення заражених комп'ютерів та виявлення атак. Всі ці заходи, звичайно, не приведуть до припинення злочинів в інформаційній сфері, шпигунства чи воєн в кіберпросторі, але це може зробити світ трохи безпечнішим.

Нейтралізувати вплив інформаційних загроз покликана єдина державна система інформаційної безпеки, якої на сьогодні в Україні ще не створено.

Список використаної літератури:

1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – Київ : Інтертехнологія, 2009. – 164 с. ; Horbulin V. P. Informatsiini operatsii ta bezpeka suspilstva: zahrozy, protydiia, modeliuvannia: monohrafiia / V. P. Horbulin, O. H. Dodonov, D. V. Lande. – Kyiv : Intertekhnolohiia, 2009. – 164 s.

2. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : автореф. дис. … канд. наук з держ. управ. : спец. 25.00.02 / Володимир Ігорович Гурковський; Нац. акад. держ. управ. при Президентові України. – Київ, 2004. – 23 с. ; Hurkovskyi V. I. Orhanizatsiino-pravovi pytannia vzaiemodii orhaniv derzhavnoi vlady u sferi natsionalnoi informatsiinoi bezpeky : avtoref. dys. … kand. nauk z derzh. uprav. : spets. 25.00.02 / Volodymyr Ihorovych Hurkovskyi; Nats. akad. derzh. uprav. pry Prezydentovi Ukrainy. – Kyiv, 2004. – 23 s.

3. Еделєва М. А. Проблеми інформаційної безпеки в сучасному суспільстві / М. А. Еделєва // Соціальне прогнозування та проектування майбутнього країни: миротворення у гібридних війнах : матер. VI Міжнар. наук. конф., м. Запоріжжя, 25 березня 2016 р. – Запоріжжя, 2016. – С. 105 – 107 ; Edelieva M. A. Problemy informatsiinoi bezpeky v suchasnomu suspilstvi / M. A. Edelieva // Sotsialne prohnozuvannia ta proektuvannia maibutnoho krainy: myrotvorennia u hibrydnykh viinakh : mater. VI Mizhnar. nauk. konf., m. Zaporizhzhia, 25 bereznia 2016 r. – Zaporizhzhia, 2016. – S. 105 – 107.

4. Інформаційна політика України: європейський контекст : моногр. / Л. В. Губерський, Є. Є. Камінський, Є. А. Макаренко та ін. – Київ : Либідь, 2007. – 360 с. ; Informatsiina polityka Ukrainy: yevropeiskyi kontekst : monohr. / L. V. Huberskyi, Ye. Ye. Kaminskyi, Ye. A. Makarenko ta in. – Kyiv : Lybid, 2007. – 360 s.

5. Козубський В. О. Інформаційна безпека держави: Кримський регіон : автореф. дис. … канд. політ. наук : спец. 23.00.02 / Валентин Олексійович Козубський; Тавр. нац. універ. ім. В. І. Вернадського. – Сімферополь, 2005. – 19 с. ; Kozubskyi V. O. Informatsiina bezpeka derzhavy: Krymskyi rehion : avtoref. dys. … kand. polit. nauk : spets. 23.00.02 / Valentyn Oleksiiovych Kozubskyi; Tavr. nats. univer. im. V. I. Vernadskoho. – Simferopol, 2005. – 19 s..

6. Крюков О. І. Інформаційна безпека держави в умовах глобалізації [Електронний ресурс] / О. І. Крюков // Державне будівництво. – 2007. – №. 2. Режим доступу : http://nbuv.gov.ua/UJRN/DeBu_2007_2_12 ; Kriukov O. I. Informatsiina bezpeka derzhavy v umovakh hlobalizatsii [Elektronnyi resurs] / O. I. Kriukov // Derzhavne budivnytstvo. – 2007. – №. 2. Rezhym dostupu : http://nbuv.gov.ua/UJRN/DeBu_2007_2_12

7. Макаренко Є. А. Міжнародна інформаційна політика: структура, тенденції, перспективи : автореф. дис. … д-ра політ. наук : 23.00.04 / Євгенія Анатоліївна Макаренко; Київський національний ун-т ім. Т. Шевченка. – Київ, 2002. – 66 с. ; Makarenko Ye. A. Mizhnarodna informatsiina polityka: struktura, tendentsii, perspektyvy : avtoref. dys. … d-ra polit. nauk : 23.00.04 / Yevheniia Anatoliivna Makarenko; Kyivskyi natsionalnyi un-t im. T. Shevchenka. – Kyiv, 2002. - 66 s.

8. Окинавская Хартия глобального информационного общества [Электронный ресурс] // Режим доступа : http://www.iis.ru/library/okinawa/charter.ru.html ; Okinavskaya Khartiya globalnogo informatsionnogo obshchestva [Elektronnyy resurs] // Rezhim dostupa : http://www.iis.ru/library/okinawa/charter.ru.html

9. Остроухов В. В. До проблеми забезпечення інформаційної безпеки України / В. В. Остроухов, В. М Петрик //Політичний менеджмент. – 2008. - № 4. – С. 135-141 ; Ostroukhov V. V. Do problemy zabezpechennia informatsiinoi bezpeky Ukrainy / V.V. Ostroukhov, V. M Petryk //Politychnyi menedzhment. – 2008. - № 4. – S. 135-141

10. Почепцов Г. Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття / Г. Г. Почепцов. – Київ : Видавничий дім «Києво-Могилянська академія», 2017. – 260 с. ; Pocheptsov H. H. Vid pokemoniv do hibrydnykh viin: novi komunikatyvni tekhnolohii KhKhI stolittia / H. H. Pocheptsov. – Kyiv : Vydavnychyi dim «Kyievo-Mohylianska akademiia», 2017. – 260 s.

11. Фомін В. О. Сутність і співвідношення понять «інформаційна безпека», «інформаційна війна» та «інформаційна боротьба» / В. О. Фомін, А. О. Рось // Наука і оборона. – 1999. - № 4. - С. 23-32 ; Fomin V. O. Sutnist i spivvidnoshennia poniat «informatsiina bezpeka», «informatsiina viina» ta «informatsiina borotba» / V. O. Fomin, A.O. Ros // Nauka i oborona. – 1999. - № 4. - S. 23-32

12. National security strategy [Electronic resource]. – Mode of access : www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

13. Cyberwar [Electronic resource] // The Economist. – 2010. - July 3. - Mode of access : http://www.economist.com/node/16481504

Стаття надійшла до редакції 04.10.2017 р.

M. Edelieva

PROVISION OF THE INFORMATIONAL SECURITY IN THE CONTEXT OF REALIZATION OF GOVERNMENTAL INFORMATIONAL POLITICS

In the XXI century humanity has received a rapid development of the scientific-technologic potential thanks to the fast spread of information and involving of the modern informational technologies (IT) in the everyday life of the society. It is revealed that IT development leads to the principally new branch of humanity development that can lead to the drastic changes in many spheres of the society including political and economic. The author has defined that in the modern society there's a request for information as a new strategic resource that opens new opportunities for the developing countries in the economic as well as in the political sector. It is also established that with the development of the informational society increases the risk of informational threats, appears the need of the informational security provision of the country, society and an individual. In the period of modernization of the political system of the country by the government it is important to define the main branches of the governmental and informational politics in the sphere of informational security provision.

The goal of this article is analysis of the problematic questions in the sphere of informational security and search of the directions for the improvement of the informational politics of the government.

With the increase of request of the population for information government should calculate the requests and problems, rapidly carry out the modernization of in the strategic regions of the governmental sector. Thus in the modern society with carrying out of the modernization appears the need to review the existing economic, political and socio-cultural concepts of the development and inform the society about these changes.

This way government has a task of liquidate the following threats that derange informational safety; decreased attention to the questions of the informational safety; incomplete law base; out of date technologies of web protections; absence of the qualified human resources in the sphere of informational security; information protection; economic, social and political instability in the country etc.

***Key words**: informational politics, informational security, cybersecurity, hackers.*

УДК 323.1(4)

О.Я. Івасечко, М.В. Здоровега

КРИЗА ПОЛІТИКИ МУЛЬТИКУЛЬТУРАЛІЗМУ В ЄВРОПІ: ПРИЧИНИ ТА НАСЛІДКИ

У статті розглянуто особливості розвитку сучасних західноєвропейських держав в умовах зростання критики політики мультикультуралізму, механізмів та проблем імплементації відповідної політики провідними країнами Європи на національному рівні. Визначено, що упродовж останніх років політика мультикультуралізму все частіше є викликом та загрозою національній ідентичності держав-членів ЄС. Труднощі пов'язані із втіленням ідеології мультикультурного суспільства у європейських реаліях полягають у необхідності формування спільної європейської ідентичності, яка задовольняє інтереси далеко не всіх мешканців ЄС. Проаналізовано етапи становлення політики мультикультуралізму, її моделі та основні напрями. Розкрито способи імплементації політики мультикультуралізму у провідних державах Європи. Зазначено, що криза