УДК 316.6:659.9]:004.7

О. В. Курбан, кандидат наук із соціальних комунікацій, доцент, Київський університет імені Б. Грінченка, м. Київ

ОСНОВИ СУЧАСНОЇ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Визначено ключові проблемні аспекти сучасної системи національної інформаційної безпеки України, серед яких — геополітичне питання, радянський спадок та брак належної уваги держави. Розглянуто історію дослідження порушеної теми в працях провідних українських фахівців у практичному та теоретичному аспектах. Проаналізовано юридичні аспекти забезпечення реалізації державної національної інформаційної безпекової стратегії України, зокрема визначено достатньо значну кількість профільних нормативно-правових актів, які є переважно декларативними. Визначено основні напрями подальшого розвитку системи інформаційної національної безпеки України та надано прикладні рекомендації щодо способів досягнення визначеної мети та практичних завдань, серед яких: необхідність залучення профільних фахівців, ресурсів та співпраця з євроатлантичними структурами.
Ключові слова: інформаційна безпека, інформаційна війна, соціальні мережі.

А. В. Курбан, кандидат наук по социальным коммуникациям, доцент, Киевский университет имени Б. Гринченка, г. Киев

ОСНОВЫ СОВРЕМЕННОЙ НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ

Определены ключевые проблемные аспекты современной системы национальной информационной безопасности Украины, среди которых — геополитический вопрос, советское наследие и отсутствие должного внимания государства. Рассмотрена историография поднятой темы в работах ведущих украинских специалистов в практическом и теоретическом аспектах. Проанализированы юридические аспекты обеспечения реализации государственной национальной информационной стратегии безопасности Украины, в частности достаточно значительное количество профильных нормативно-правовых актов, которые имеют в большинстве случаев лишь декларативный характер. Определены основные направления дальнейшего развития системы информационной безопасности Украины и представлены прикладные рекомендации относительно путей достижения цели и практических задач, среди которых: необходимость привлечения профильных специалистов, ресурсов и сотрудничество с евроатлантическими структурами.
Ключевые слова: информационная безопасность, информационная война, социальные сети.

O. V. Kurban, Candidate of Sciences in Social Communications, Associate Professor, BorysтGrinchenko Kyiv University, Kyiv

FOUNDATIONS OF MODERN NATIONAL INFORMATION SECURITY OF UKRAINE

The paper explores the key aspects of the current problems of the national information security of Ukraine, including geopolitical issues, the Soviet legacy and the lack of focus on the part of the state. The history of the study in the works of the leading Ukrainian specialists in the practical and theoretical aspects is considered. The author analyzes the legal aspects of implementing the state national information security strategy of Ukraine, in particular defines sufficiently large number of relevant normative acts that are in most cases only declarative. The paper defines the main directions for the development of the national security information of Ukraine and recommendations on how to achieve a particular purpose and solve practical problems, including: the need to involve specialized experts, resources and cooperation with Euro-Atlantic structures.
Key words: information security, information warfare, social networks.

Постановка проблеми. Події останніх років, зокрема російсько-український конфлікт, наочно засвідчили, які серйозні проблеми в системі державної інформаційної безпеки загалом та конкретно в онлайновому мережевому просторі має нині Україна. Серед чинників, що призвели до цього, виокремимо такі:

- геополітичне положення країни — розташування в зоні політичних, економічних та військових інтересів світових країн-лідерів;
- радянський спадок — старі кадри та традиції, що гальмують суспільний розвиток;
- недостатній розвиток громадянського суспільства;
- слабкість системи державної влади та її залежність від олігархічно-кланового капіталу;
- брак ґрунтовних профільних наукових та прикладних розробок.

Відповідно до визначених ключових аспектів актуальності порушеної теми, **мета статті** — вивчити сучасний стан національної системи інформаційної безпеки України та перспективи її подальшого вдосконалення в контексті гібридної агресії зі сторони Російської Федерації. У форматі зазначеної мети передбачається вирішення таких завдань:

- огляд попередніх розробок у питанні національної інформаційної безпеки України;
- аналіз ситуації та ключових аспектів системи національної інформаційної безпеки України (правові, організаційні тощо);
- розробка рекомендацій щодо поліпшення ситуації та подальшого розвитку національної системи інформаційної безпеки в Україні.

Аналіз останніх досліджень і публікацій. Серед тих, хто першим порушив питання про інформаційну безпеку на початку становлення незалежності України, був фахівець зі стратегічних комунікацій Г. Г. Почепцов. Він розглядав специфіку інформаційних атак, яких зазнавала Україна від своїх сусідів, та їх контентної складової [13–21]. З точки зору традиційних інструментів міжнародних конфліктів і внутрішньої політики питання інформаційної безпеки розглядав відомий державний діяч та науковець В. П. Горбулін [2; 3].

Психологічні аспекти інформаційних конфліктів у контексті національної безпеки вивчав В. В. Зеленін [6; 7; 8]. Інноваційні аспекти інформаційних війн у межах порушеної теми досліджували А. Кемаль та Є. Магда, зокрема щодо гібридних агресій та соціальних мереж [10; 12].

У контексті подій останніх років, зокрема російсько-українського військово-політичного конфлікту навколо Криму й окремих районів Донбасу, питання національної інформаційної безпеки досліджували Т. Березовець, Д. Тимчук, Ю. Карін, К. Машовець, В. Гусаров [1; 22].

Виклад основного матеріалу дослідження. Зміст і специфіка інформаційної та будь-яких інших національних загроз, ризиків та викликів залежать від розвиненості й цивілізованості суспільства, його міжнародних зв'язків. При цьому рівень національної безпеки визначається здатністю до реальної оцінки й оптимальної протидії [4, с. 246].

Розвинуті незалежні громадські або державні аналітично-дослідницькі інституції в демократичних суспільствах є чутливими індикаторами зовнішніх та внутрішніх загроз. Саме конкурентне експертне середовище формує ефективну систему діагностики, аналізу і прогнозування.

Серед пріоритетів зовнішньої та внутрішньої політики будь-якої держави завжди одне з провідних місць посідає інформаційна безпека як чинник і гарантія національної незалежності та стабільності. За базовим визначенням, інформаційна безпека — це рівень захищеності держави, який унеможливлює або максимально мінімізує здійснення спеціальних інформаційних операцій, актів зовнішньої інформаційної агресії, інформаційного тероризму, незаконного отримання інформації, комп'ютерні злочини й інший деструктивний інформаційний вплив [5, с. 247].

Традиційно визначають три базові рівні інформаційної безпеки [5, с. 250]:

- рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);

- суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні ЗМІ, які належать вітчизняним власникам);
- державний рівень (інформаційно-аналітична робота органів, інформаційне забезпечення внутрішньої та зовнішньої політики на міждержавному рівні, система захисту інформації, протидія правопорушенням в інформаційній сфері).

У Законі України «Про основи національної безпеки» однією з головних інформаційних загроз визначено спробу маніпулювати суспільною свідомістю, зокрема поширення недостовірної, неповної або упередженої інформації. Серед інших важливих загроз визначено:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення державної таємниці [5, с. 250].

В Указі Президента України «Про Доктрину інформаційної безпеки України» (2009 р.) серед інших виокремлено такі загрози інформаційній безпеці України [23]:

- поширення викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- зовнішні деструктивні інформаційні впливи на суспільну свідомість;
- деструктивні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності України;
- прояви сепаратизму в ЗМІ, мережі інтернет за етнічною, мовною, релігійною та іншими ознаками.

Створена у 2015 р. Експертною радою при Міністерстві інформаційної політики України «Концепція інформаційної безпеки України» враховує як останні досягнення в галузі соціальних комунікацій, так і реалії сучасної України — передусім результати російської інформаційної агресії 2014–2016 рр. [23].

Зазначена Концепція визначає інформаційну безпеку як стан захищеності життєво важливих інтересів людини і громадянина, суспільства й держави, при якому запобігається завданню шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [9].

Аналізуючи поточну ситуацію і специфіку сучасних світових викликів та інформаційних загроз, автори Концепції запропонували таке поняття, як інформаційний суверенітет України. Під цим терміном розуміється виключне право України, відповідно до Конституції й законодавства України та норм міжнародного права, самостійно та незалежно, з дотриманням інтересів особи, суспільства й держави, визначати та реалізувати внутрішні й геополітичні національні інтереси в інформаційній сфері, державну внутрішню та зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави [9].

Серед принципово нових понять у Концепції є такі, що відбивають тенденції останніх років, зокрема пов'язаних з російсько-українським протистоянням. Ці визначення принципово важливі в умовах сучасних інформаційних конфліктів, у яких особливого значення набувають питання створення контенту та управління інформаційними процесами. До таких належать національний інформаційний продукт, що визначається як аудіовізуальний, друкований чи інший продукт, призначений для задоволення інформаційно-комунікативних потреб громадян України, суспільства й держави, створений громадянами або юридичними особами України згідно з чинним законодавством [9].

Стратегічні протистояння на міждержавному рівні відбуваються також завдяки створенню та застосуванню стратегічного контенту, який визначено в Концепції як національний інформаційний продукт, який має на меті забезпечити політичну, культурну та духовну цілісність і розвиток політичної нації [9].

В умовах сучасної інформаційної та гібридної війни важливе значення має система управління інформаційними процесами. Це питання в Концепції узагальнюється поняттям інформаційна інфраструктура, що визначено як сукупність організаційних структур і систем, які забезпечують функціонування та розвиток інформаційного простору, засобів інформаційної взаємодії та доступу користувачів до інформаційних ресурсів [9].

Окреме питання — юридичне формулювання та прикладне визначення інформаційних процесів, що відбуваються в кіберпросторі. У цьому контексті Концепція пропонує таке поняття, як кібернетична безпека (кібербезпека) — стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [9].

Інформаційні процеси, що відбуваються у віртуальному просторі, безпосередньо стосуються використання соціальних онлайн-мереж, які є частиною кіберпростору. Кіберпростір визначено в Концепції

як середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем.

Інформаційні протистояння та конфлікти в кіберпросторі доволі часто втілюються у вигляді т. зв. кібертероризму, що визначено в Концепції як терористична діяльність у кіберпросторі або з його використанням.

Відповідно до реалій сучасності, перед українською системою національної державної безпеки постають принципово нові виклики. Серед них можна визначити комунікативні загрози, ті, що стосуються реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації. Мають місце технологічні загрози, у сфері функціонування й захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що становлять матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору [9].

Принципово новий формат вирішення питань інформаційної безпеки передбачає застосування механізмів громадського контролю та державно-громадського партнерства. Так, згідно зі ст. 13 Концепції, структурами громадського контролю при органах державної влади мають стати експертні ради. Склад таких рад формується з науковців, освітян, представників органів самоорганізації населення та громадських організацій (за напрямом конкретної державної програми) [9].

Отже, аналіз суспільного розуміння державного впливу та нормативно-правового забезпечення питань національної інформаційної безпеки свідчить про необхідність посилення роботи в цьому напрямі. Зазначимо, що це є компетенцією не тільки органів державної влади, а й громадських інституцій, і стосується профільних недержавних організацій та різноманітних експертних центрів, що продукуватимуть незалежні думки й погляди, а також системно й неупереджено аналізуватимуть ситуації.

Щодо можливостей та компетенції державних структур, то нагальною є необхідність посилення системної роботи та надання певних матеріальних ресурсів для поліпшення ситуації. Передусім, необхідно закцентувати на створенні системи підготовки фахівців з питань інформаційної безпеки. На це мають спрямовуватися зусилля військових, правоохоронних і цивільних вищих навчальних закладів у співпраці з відповідними державними структурами та громадськими організаціями.

Серед напрямів, за якими мають досліджуватися означені питання, можна визначити щонайменше три.

Перший напрям (прикладний) — розробка та впровадження стандартів і алгоритмів ведення мережевих інформаційних війн, які допомагатимуть швидко реагувати на певні виклики та компенсувати в певних обставинах брак досвіду та власних інструментів.

Другий напрям (кадровий) — налагодження системної роботи з підготовки відповідних фахівців, яка базуватиметься на чіткій методологічній базі та практичних методиках навчання.

Третій напрям (науковий) — створення мережі незалежних наукових центрів та стимулювання роботи окремих науковців, котрі досліджуватимуть проблематику інформаційно-психологічних війн у мережевому онлайновому просторі.

Як засвідчили події останніх років — Євромайдан, анексія Росією Автономної республіки Крим та її гібридна агресія на Сході України — вітчизняна інформаційна сфера, в її безпековому аспекті, потребує суттєвих структурних змін. Зазначені зміни мають спрямовуватися на:

- удосконалення систем моніторингу й контролю інформаційних потоків, як у межах країни, так і в міжнародному масштабі;
- уніфікацію та модернізацію засобів і методів управління інформаційними потоками, що мають базуватися на гнучких схемах роботи;
- розробку та практичне впровадження національної стратегії інформаційно-комунікаційної безпеки, що відповідає сучасним викликам гібридної й інформаційно-психологічної війн другого покоління;
- формування профільної нормативно-правової бази, що дозволятиме оперативно реагувати на сучасні виклики та загрози в контексті інформаційно-психологічних війн у соціальних онлайн-мережах;
- створення та широке застосування ефективної системи підготовки фахівців у галузі інформаційно-психологічних війн із відповідними знаннями та рівнем практичної підготовки;
- активне залучення широких верств громадськості до питань національної безпеки на волонтерських засадах;
- формування ефективного ментального бар'єру свідомості громадськості проти іноземних впливів;
- створення національного конкурентоспроможного середовища медіа-проектів;
- вивчення іноземного досвіду, стратегій, тактики ведення інформаційно-психологічних війн;

- інтеграцію України загалом та її профільних фахівців до євроатлантичних структур, що діють у сфері інформаційної безпеки.

За умови реалізації зазначених вище завдань та широкої інтеграції України в європейський інформаційний простір суспільство може нарешті досягнути стабільності та перейти від режиму перманентних суспільно-політичних криз і революцій до стабілізації та подальшого сталого розвитку.

Висновки. Підбиваючи підсумки дослідження, маємо зазначити, що нині в українській системі національної інформаційної безпеки сформувалася парадоксальна ситуація — існує значна регулююча нормативно-правова база, проте реальні механізми її застосування фактично відсутні, як і дієві структури та досвідчені фахівці. І це — серйозна проблема, яку потрібно вирішувати, передусім у прикладній площині, створюючи альтернативні інформаційно-аналітичні ресурсні центри та вдосконалюючи існуючі. Важливими напрямами роботи є підготовка профільних фахівців, розбудова відповідної системи.

Саме на вирішенні цих аспектів у найближчий час мають спрямовуватись зусилля як фахівців-практиків, так і науковців.

Список використаних джерел

1. Березовець Т. Анексія: Острів Крим. Хроніки «гібридної війни» / Т. Березовець. — Київ : Брайт Стар Паблішінг, 2015. — 392 с.
2. 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.
3. Горбулин В. «Гибридная война» как ключевой инструмент российской геостратегии реванша [Электронный ресурс] // Зеркало недели [сайт], 23.11.2015. Режим доступа: http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html. — Загл. с экрана.
4. Гриняев С. Н. Интеллектуальное противодействие информационному оружию / С. Н. Гриняев. — М. : Изд-во «СИНТЕГ», 1999. — 232 с.
5. Дергачов О. П. Партнерський потенціал України: становлення і реалізація / О. П. Дергачов. — Київ : Парламентське видавництво, 2009. — 496 с.
6. Зеленін В. В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни / В. В. Зеленін. — Вінниця : Віндрук, 2014. — 384 с.
7. Зеленін В. В. Сучасні агітаційно-пропагандистські технології в регіональних виборчих кампаніях: дайджест навчально-методичних рекомендацій / В. В. Зеленін. — Київ : ЦСВТ, 2013. — 116 с.
8. Зеленін В. Політична пропаганда як засіб партійного будівництва / В. Зеленін, П. Бублик, Б. Мотузенко, Д. Рождественська. — Донецьк :

Інноваційний центр соціально-політичних і гуманітарних наук ДонНТУ, ФППР, 2003. — 180 с.
9. Концепція національної безпеки України [Електронний ресурс] // Міністерство інформаційної політики України [сайт]. — Режим доступу: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20%28%D0%A2%D0%B5%D0%BA%D1%81%D1%82%29%20-%2030.09.15.pdf. — Назва з екрана.
10. Кемаль А. Кибервойна. Как Россия манипулирует миром / А. Кемаль. — М. : Алгоритм, 2015. — 208 с.
11. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. — Київ : КНТ, 2006. — 280 с.
12. Магда Є. Гібрида війна. Вижити і перемогти / Є. Магда. — Київ : Віват, 2015. — 304 с.
13. Почепцов Г. Г. Теория и практика информационных войн / Г. Г. Почепцов. — Ровно : «Волинські обереги», 1999. — 124 с.
14. Почепцов Г. Г. Теория и практика коммуникации (от речей президентов до переговоров с террористами) / Г. Г. Почепцов. — М. : Центр, 1998. — 352 с.
15. Почепцов Г. Г. Психологические войны / Г. Г. Почепцов. — М. : Рефл-бук; Київ : Ваклер, 2000. — 576 с.
16. Почепцов Г. Г. Информационные войны. Основы военно-коммуникативных исследований / Г. Г. Почепцов. — М. : Рефл-бук, Киев : Ваклер, 2000. — 576 с.
17. Почепцов Г. Від Facebook'у і гламуру до Wikileaks: медіа-комунікації / Г. Г. Почепцов. — Київ : Спадщина, 2012. — 464 с.
18. Почепцов Г. Анатомия гибридной войны [Электронный ресурс] / Украина криминальная. — Режим доступа: http://cripo.com.ua/?sect_id=8&aid=199931. — Загл. с экрана.
19. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Mediasapiens [сайт]. — Режим доступа: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/ — Загл. с экрана.
20. Почепцов Г. Г. Пропаганда и контрпропаганда / Г. Г. Почепцов. — М. : Центр, 2004. — 252 с.
21. Почепцов Г. Г. Информационные войны. Новый инструмент политики / Г. Г. Почепцов. — М. : Алгоритм, 2015. —256 с.
22. Тымчук Д. Вторжение в Украину: хроника российской агрессии / Д. Тымчук, Ю. Карин, К. Машовец, В. Гусаров. — Киев : Брайт Стар Паблишинг, 2016. — 240 с.
23. Про доктрину інформаційної безпеки України: Указ Президента України [Електронний ресурс] // Верховна Рада України [сайт]. — Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009. — Назва з екрана.

References

1. Berezovets T. Aneksiia: OstrivKrym. Khroniky «hibrydnoiviiny» / T. Berezovets. — Kyiv :Brait Star Pablishinh, 2015. — 392 s.
2. Horbulin V. P. Informatsiinioperatsii ta bezpekasuspilstva: zahrozy, protydiia, modeliuvannia: monohrafiia / V. P. Horbulin, O. H. Dodonov, D.V. Lande. — Kyiv :Intertekhnolohiia, 2009. — 164 s.
3. Gorbulin V. «Gibridnayavoyna» kakklyuchevoy instrument rossiyskoy geostrategii revansha [Elektronnyyresurs] // Zerkalonedeli [sayt]. 23.11.2015. Rezhim dostupa: http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html. — Zagl. sekrana.
4. Grinyayev S. N. Intellektualnoye protivodeystviye informatsionnomu oruzhiyu / S. N. Grinyayev. — M. : Izd-vo «SINTEG», 1999. — 232 s.
5. Derhachov O. P. Partnerskyi potentsial Ukrainy: stanovlennia i realizatsiia / O. P. Derhachov. — Kyiv : Parlamentske vydavnytstvo, 2009. — 496 s.
6. Zelenin V. V. Po toi bik pravdy: neirolinhvistychne prohramuvannia yak zbroia informatsiino-propahandyskoi viiny / V. V. Zelenin. — Vinnytsia : Vindruk, 2014. — 384 s.
7. Zelenin V. V. Suchasni ahitatsiino-propahandyski tekhnolohii v rehionalnykh vyborchykh kampaniiakh: daidzhest navchalno-metodychnykh rekomendatsii / V. V. Zelenin. — Kyiv : TsSVT, 2013. — 116 s.
8. Zelenin V. Politychna propahanda yak zasib partiinoho budivnytstva / V. Zelenin, P. Bublyk, B. Motuzenko, D. Rozhdestvenska. — Donetsk : Innovatsiinyi tsentr sotsialno-politychnykh i humanitarnykh nauk DonNTU, FPPR, 2003. — 180 s.
9. Kontseptsiia natsionalnoi bezpeky Ukrainy [Elektronnyi resurs]. // Ministerstvo informatsiinoi polityky Ukrainy [sait]. — Rezhym dostupu: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20%28%D0%A2%D0%B5%D0%BA%D1%81%D1%82%29%20-%2030.09.15.pdf. — Nazva z ekrana.
10. Kemal A. Kibervoyna. Kak Rossiya manipuliruyet mirom / A. Kemal. — M. : Algoritm, 2015. — 208 s.
11. Lipkan V. A., Maksymenko Yu. Ye., Zhelikhovskyi V. M. Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii: navch. posib. / V. A. Lipkan, Yu. Ye. Maksymenko, V. M. Zhelikhovskyi. — Kyiv : KNT, 2006. — 280 s.
12. MahdaYe.Hibrydnaviina.Vyzhyty I peremohty / Ye. Mahda. — Kyiv : Vivat, 2015. — 304 s.
13. Pocheptsov G. G. Teoriya I praktika informatsionnykh voyn / G. G. Pocheptsov. — Rovno : «Volynski oberehy», 1999. — 124 s.
14. Pocheptsov G. G. Teoriya I praktika kommunikatsii (ot rechey prezidentov do peregovorov steroristami) / G. G. Pocheptsov. — M. :Tsentr, 1998. — 352 s.
15. PocheptsovG. G. Psikhologicheskiyevoyny / G. G. Pocheptsov. — M. : Reflbuk ; Kiïv : Vakler, 2000. — 576 s.

16. Pocheptsov G. G. Informatsionnyye voyny. Osnovy voyenno-kommunikativnykh issledovaniy / G. G. Pocheptsov. — M. : Refl-buk. Kiyev :Vakler, 2000. — 576 s.
17. Pocheptsov G. Vid Facebooku I hlamurudo Wikileaks: media-komunikatsii / G. G. Pocheptsov. — Kyiv : Spadshchyna, 2012. — 464 s.
18. Pocheptsov G. Anatomiya gibridnoy voyny [Elektronnyy resurs]. / Ukraina kriminalnaya. —Rezhim dostupa: http://cripo.com.ua/?sect_id=8&aid=199931. — Zagl. sekrana.
19. Pocheptsov G. Novyye podkhody v sfere «zhestkikh» infovoyn [Elektronnyy resurs] / // Mediasapiens [sayt]. — Rezhim dostupa: http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/ — Zagl. sekrana.
20. Pocheptsov G. G. Propaganda ikontrpropaganda / G. G. Pocheptsov. — M. : Tsentr, 2004. — 252 s.
21. Pocheptsov G. G. Informatsionnyye voyny. Novyy instrument politiki / G. G. Pocheptsov. — M. : Algoritm, 2015. — 256 s.
22. Tymchuk D. Vtorzheniye v Ukrainu: khronika rossiyskoya gressii / D. Tymchuk. Yu. Karin. K. Mashovets. V. Gusarov. — Kiyev : Brayt Star Pablishing, 2016. — 240 s.
23. Pro doktrynu informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy [Elektronnyi resurs] / // Verkhovna Rada Ukrainy [sait]. — Rezhym dostupu: http://zakon2.rada.gov.ua/laws/show/514/2009. — Nazva z ekrana.

UDC 316.6:659.9]:004.7

Kurban O. V., Candidate of Sciences in Social Communications, Associate Professor, BorysGrinchenko Kyiv University, Kyiv
bairam1970@gala.net

FOUNDATIONS OF MODERN NATIONAL INFORMATION SECURITY OF UKRAINE

The purpose of the article is to explore the current state of the national information security system of Ukraine and the prospects for its further improvement against the background of a hybrid of aggression by the Russian Federation.

Research Methodology. The research presented the results of historiographical research method, the analysis of the legal framework and practical experience, comprehensive public entities in terms of ensuring the information security of Ukraine.

Results. The paper explores the key aspects of the current problems of the national information security of Ukraine, including geopolitical issues, the Soviet legacy and the lack of focus on the part of the state. The history of the study in the works of the leading Ukrainian specialists in

the practical and theoretical aspects is considered. The author analyzes the legal aspects of implementing the state national information security strategy of Ukraine, in particular defines sufficiently large number of relevant normative acts that are in most cases only declarative. The paper defines the main directions for the development of the national security information of Ukraine and recommendations on how to achieve a particular purpose and solve practical problems, including: the need to involve specialized experts, resources and cooperation with Euro-Atlantic structures.

Novelty. The paper is the first attempt for raising the issue to attract the innovative methods and approaches for an effective system of the national information security of Ukraine.

The practical significance. The paper presents practical recommendations to implement the effective national policy on the information security.

Key words: information security, information warfare, social networks.

Надійшла до редколегії 08.01.2017 р.