УДК 341.51:343.98:621.396(477)

З. Коваль

ДИНАМІКА СВІТОВОЇ УПРАВЛІНСЬКОЇ РЕАКЦІЇ НА КІБЕРЗАГРОЗИ: УРОКИ ДЛЯ УКРАЇНИ

Проаналізовано актуальну тему аналізу динаміки світової управлінської реакції на кіберзагрози та шляхи забезпечення державного управління інформаційною безпекою України в умовах системних кіберзагроз. З досвіду управління протидією кіберзагрозам передових країн світу та з позицій системного аналізу, в загальних рисах визначено шляхи вдосконалення інформаційної безпеки України.

Ключові слова: кіберпростір, кібернетика, кіберборотьба, кіберкомандування, системи кібернетичної безпеки, хакерські атаки, кібервійна, кіберзагроза.

Забезпечення державного управління інформаційною безпекою України в умовах кіберзагроз все ще знаходиться у невизначеному стані. Україна все більше потерпає від комплексу наявних та прихованих кіберзагроз. Чітку концепцію, ключові правові механізми державного управління інформаційною безпекою України в умовах кіберзагроз не сформовано, а досвід передових країн світу вчасно не запроваджується.

Зазначена проблематика обговорюється в друкованих виданнях та в мережі Інтернет, її розвивали українські військові та цивільні аналітики: доктор технічних наук, академік Ю. Даник, кандидати технічних наук, доцент В. Фарушев, народні депутати України В. Олійник, Ю. Самойленко, О. Кузьмук, дослідники І. Іжутова, С. Олександров, Б. Буткевич, В. Яковенко, Т. Наритник, І. Сергієнко, М.Константинов, Ю.Пастернак, закордонні фахівці Е. Касперський, І. Морозовіцкій, Р. Халілов та інші.

Підходи до забезпечення державного управління інформаційною безпекою України в умовах кіберзагроз все ще не розгорнуті, бачення їх фрагментарні та неузгодженні. У цьому сегменті національної безпеки в України стан справ все ще один із найгірших серед країн СНД.

Мета статті – на досвіді оперативної управлінської реакції щодо протидії кіберзагрозам передових країн світу та з позицій системного аналізу, зробити спробу в загальних рисах визначити шляхи вдосконалення інформаційної безпеки України.

Навколо нас світ невпинно глобалізується з одночасним загостренням міжнародної конкуренції. Центральною ареною зіткнень і суперництва різноманітних національних інтересів став інформаційний простір. При переході до інформаційного суспільства віртуальний простір Інтернету стає стратегічним полем битви, міняючи при цьому політичні, геополітичні та воєнні пріоритети. Головною метою нової інформаційної війни є інформаційне домінування. Інформаційна та технологічна першість, які опираються на мережу, зумовлюють мережево-центричну війну, або кібервійну. Головний зміст нової теорії війни епохи Інтернету в тому, що війна стає мережевим явищем, а військові дії – різновидом мережевих процесів. Виникає потреба у формуванні інформаційних військ, що переростуть у

інформаційну армію. В умовах кібервійни цивільне населення і військові частини об'єднані в єдину мережу, якою циркулює інформація.

Саме створення такої мережі і складає суть мережево-центричної війни майбутнього. Мета мережево-центричної війни – комплексна. Це встановлення абсолютного контролю над всіма учасниками віртуального простору шляхом контролю за інформаційними потоками; досягнення гегемонії в реальному фізичному середовищі через кібератаки, інциденти з комп'ютерними вірусами, маніпуляції в соціальних мережах. Мережево-центрична війна перманентна по часу і стирає межу між ворогом, нейтралом та іншими. Першою кібервійною стала "Буря в пустелі" (1991 р.).

У кібер-епоху відпадає потреба застосовувати зброю, коли є можливість послабити чи завдати помітної шкоди, за допомогою сучасних ІТ-технологій безпеці конкурентної країни, яка не має міцної і надійної системи захисту від негативних інформаційних впливів. Тому вирішальним чинником зміни типу та методів ведення збройної боротьби стали досягнення у сфері інформаційно-комунікативних технологій.

Доречно згадати, що термін "кібернетика" як мистецтво управління з'явився ще у стародавній Греції. Початок сучасної кібернетики належить до 1948 р., пов'язаний з появою наукової праці Н. Вінера "Кібернетика, або керування й зв'язок у тварині й машині", де вона обґрунтована як наука про загальні закономірності процесів управління і передачі інформації в живих організмах, суспільстві та машинах. Отже, визначення "кібернетики" зводиться до того, що це наука, яка визначає загальні закономірності будови складних систем керування й протікання в них процесів управління. Військова кібернетика розробляє для органів управління основні положення єдиної теорії та практичні рекомендації для управління збройними силами.

У процесі розвитку високих технологій виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережекомп'ютерної складової. Кіберпростір одночасно виступає як суб'єкт та об'єкт впливу. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кіберборотьба набула стратегічного управлінського спрямування. Вона проводиться без міжнародних правових обмежень у просторі та часі і характеризується високою ефективністю щодо досягнення воєнно-політичної мети. Все більш вирішальним чинником досягнення успіху у світовому протиборстві стає інформаційно-технічна дезорганізація систем державного і воєнного управління та інформаційно-психологічна деморалізація населення країн, насамперед складу їх збройних сил. Кіберпростір став невід'ємною частиною інформаційного простору та п'ятою сферою ведення збройної боротьби. Сама збройна боротьба, завдяки інформаційному чиннику, набула високого ступеня керованості.

За таких умов зростає роль оперативності та адекватності реагування на форми та методи ведення кібервійни. На сьогодні світ контролює той, хто контролює кіберпростір. Контроль над кіберпростором означає не тільки збір інформації, але й масовані акції психологічного впливу, аж до контролю та опосередкованого управління поведінкою противника. Стратегічний паритет у кіберпросторі, на відміну від ядерного та звичайних озброєнь, залишається не сформованим. У кіберпросторі діють не тільки визнані суб'єкти міжнародного права, а й громадські і терористичні організації. За різними оцінками, в усьому світі

втрати від діяльності кіберзлочинності становлять щорічно від 290 до 750 млрд євро. Трансграничність загроз спонукає країни вступати в тісну міжнародну взаємодію [1].

Кібервійна дає можливість здійснювати атаки тим, хто має з'єднання з мережею Інтернет та відповідну підготовку, вона не передбачає великих витрат і зусиль. Кібервійна не заміщає собою війну звичайну – вона є іншою ареною ведення більш масштабної війни. І ті країни, які першими оволодіють мистецтвом кібервійни, зможуть отримати фундаментальну перевагу вже на її початкових стадіях.

Для Hard-версії кібервійни першочергове значення має домінування в аерокосмічному просторі, яке досягається за рахунок супутникового зв'язку, крилатих ракет та авіації. Застосування стратегії Hard Power у кібервійні із застосуванням авіації та аерокосмічної підтримки справа надто затратна. Тому основні учасники кібервійни досягають поставлених результатів, застосовуючи нову стратегію "Soft Power". Її основу становить створення шкідливих вірусів для ефективної кібератаки з метою отримання необхідної засекреченої інформації, тотального контролю над соціальними мережами або для організації атаки на комп'ютерні центри управління цивільної, фінансової та воєнної інфраструктури. Вартість такої атаки не перевищує 100 млн дол., а збитки – мільярдні. Так США у 2013 р. зазнали збитків на 300 млрд дол. від кібератак та шпіонажу [2].

Як свідчить статистика, кібернетичні командування та системи кібернетичної безпеки були створені у десятках країн світу з ідентичними складовими. До їх типової структури належать підрозділи: мережевих операцій; інформаційних операцій та інформаційної безпеки; підтримки і забезпечення операцій у кіберпросторі; радіоелектронної боротьби; операційні (командні) центри (центри управління у кризових ситуаціях) тощо. Основними складовими кібернетичної безпеки є кіберрозвідка, кіберзахист та кібернетичні впливи. Досвід іноземних країн щодо захисту від кібернетичних загроз свідчить про комплексний підхід до впровадження заходів зі створення ефективних систем захисту національного сегменту кібернетичного простору та інфраструктури від кібернетичних загроз [3].

Деякі країни, з метою захисту свого кіберпростору, почали просування проектів регулювання (правил поведінки) у кіберпросторі (або за визначенням деяких відповідних документів – "сфері міжнародної інформаційної безпеки"). Основна концептуальна відмінність, що вирізняє ці альтернативні проекти від американських ініціатив, – фактична відсутність розрізнення кібербезпеки від більш широкого поняття "інформаційно-психологічна безпека".

Для прикладу, у 2011 р. у Румунії була прийнята Національна система кібербезпеки інформаційних систем. Це документ, який нормативно забезпечує захист державних органів, установ наукових кіл, бізнес-асоціацій та професійних організацій, координуючи їхні дії по компоненту національної безпеки в кіберпросторі. Також для реалізації стратегії кібербезпеки уряд Румунії прийняв рішення про створення центру національної кібербезпеки, який повинен складатися з 41 підрозділу й управляти системою раннього попередження кіберінцидентів у режимі реального часу. На базі міністерства зв'язку 20 червня 2011 р. був створений центр реагування на загрози кібербезпеки. Він співпрацює з національними органами, відповідальними за запобігання та усунення комп'ютерних загроз [4].

У 2013 р. свої стратегії кібербезпеки прийняли Нідерланди, Іспанія, Туреччина, Угорщина, Польща, Індія. У Росії 29.11.2013 р. у Раді Федерації

відбулися парламентські слухання, де була представлена концепція кіберстратегії. У Таллінні ще у 2008 р. Спільний центр передового досвіду з кіберзахисту був акредитований як Центр передового досвіду НАТО. Він проводить дослідження та навчання у сфері кіберзахисту. У січні 2013 р. у Гаазі почав роботу Європейський центр із боротьби з кіберзлочинністю [5].

Достеменно відомо, що у 18-му спеціальному центрі ФСБ Росії працює майже 1500 тис. людей, які щодня здійснюють дезінформації та провокації, щоб створити і використати паніку в соціальних мережах. Кібервійська створено в НАТО, США, Японії, Китаї, Північній Кореї. Розпочато цю справу і в Росії.

Війна в кіберпросторі спричиняє нові кіберзагрози. Кіберзагрози – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини та громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Кабінет Міністрів України 6 березня 2013 р. схвалив законопроект народних депутатів України В. Олійника, Ю. Самойленка, О. Кузьмука "Про кібернетичну безпеку України". Серед основних загроз кібернетичній безпеці України в законопроекті визначено: використання кіберпростору у воєнних цілях, створення іншими державами кібервійськ, кіберпідрозділів у традиційних родах військ; розроблення іноземними державами нових видів кібернетичної зброї; існування в інших країнах планів наступальних та розвідувальних військових операцій у кіберпросторі; освоєння іноземними спеціальними службами методів розвідувально-підривної діяльності у кіберпросторі, методів маніпулювання суспільною свідомістю за допомогою кіберпростору; можливість втягування України у збройні конфлікти чи у протистояння з іншими державами через використання національного сегмента кіберпростору; спроби втручання у внутрішні справи держави з використанням соціальних мереж, поширення у національному сегменті кіберпростору культу насильства, жорстокості, порнографії; активізація проявів кібертероризму; поширення кіберзлочинності; критична залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції, поширення фактів включення у програмно-технічні засоби скритих шкідливих функцій; зростання ризиків виникнення надзвичайних ситуацій техногенного спрямування через зниження рівня захищеності об'єктів критичної інформаційної інфраструктури держави.

Із названих загроз дві, а саме: освоєння іноземними спеціальними службами методів маніпулювання суспільною свідомістю за допомогою кіберпростору та спроби втручання у внутрішні справи держави з використанням соціальних мереж, поширення у національному сегменті кіберпростору культу насильства, жорстокості, порнографії мають чітко виражений інформаційно-психологічний напрям [6].

Події в Україні, що пов'язані з "євромайданом", стали причиною широкомасштабних дій у кіберпросторі. Як зазначено в ЗМІ, кібератаки проти противників здійснювались з обох сторін барикад. Особливо гостро проявляв себе рух Anonymous у Facebook своїми хакерськими атаками на сайти органів державної влади [7].

Скандал навколо Сноудена, за оцінками експертів, може стати початком цифрових війн як між державами, так і між урядами та громадянами. Зростає загроза нового етапу комп'ютерного тероризму. У звіті сенату США йдеться про те, що втручання у цифрові мережі комунальних служб, держорганів, атомних станцій чи

воєнних баз може призвести до катастрофічних наслідків. Комп'ютеризація всіх систем у США і ЄС зробила їх вразливими для нового типу загроз. У світлі цього комп'ютерна безпека стає все більш актуальною і для України. На сьогодні є основний напрямок бойових дій у кіберсфері: блокування серверів і Інтернет-ресурсів за допомогою DDoS-атак [8].

В українських корумпованих реаліях незахищеність баз інформації, можливий їх продаж, загрожує попаданню до рук злочинців. За інформацією журналу "Український тиждень", на чорному ринку та в Інтернеті за 1,5 – 2 тис. доларів легко можна купити базу даних будь-якого державного органу – від Податкової служби до Реєстру майнових прав громадян. Персональні дані мільйонів українців стали розмінною монетою та перебувають під очевидною загрозою. Основними причинами такого загрозливого стану речей із персональними даними українців стали: погано напрацьована законодавча база (чинний Закон України "Про захист персональних даних") і недостатня кількість регулюючих підзаконних правових актів; тотальна необізнаність людей у питанні захисту персональних даних; відсутність реальної роботи офіційного регулятора галузі – Державної служби України з питань захисту персональних даних. Весь напрям роботи із захисту персональних даних громадян залишився суто декларативним для імітації діяльності перед брюссельськими чиновниками. Тим часом, якщо громадянин навіть дізнається про викрадення особистих даних, йому нікуди писати заяву з цього приводу. До того ж, він не має шансів домогтися якогось покарання для компанії чи державного органу, який це допустив [9].

Свою "боєздатність" кібертерористи продемонстрували 29 липня 2014 р., коли сайт Президента України протягом кількох годин був підданий потужній DDoS-атаці і прес-служба Глави Держави була змушена розсилати власну інформацію через інформагентства. Відповідальність за атаку взяли на себе хакери з так званої групи "Кіберберкут", заявивши у своєму повідомленні про намір і в подальшому здійснювати такі акції.

До речі, завдання, які виконуються із застосуванням кіберзброї, фахівці розподіляють на три рівні: тактичний, стратегічний та спеціальний. Тактичний рівень включає ускладнення чи вибіркове призупинення діяльності телекомпаній, операторів стільникового зв'язку, провайдерів Інтернету, відомих локальних обчислювальних мереж тощо. Це призводить до дезорганізації діяльності систем управління транспортом, енерго- й газопостачання, порушення діяльності систем управління об'єктами критичної інфраструктури, включно з банківською сферою, підприємствами атомної, хімічної, нафтопереробної промисловості. Стратегічні можливості хакерського втручання: розкриття державних кодів і шрифтів, перехоплення й дешифрування листування вищих посадових осіб держави, несанкціонований доступ до державних баз даних, розкрадання, навмисне спотворення або знищення інформації, завдання програмної або апаратної шкоди комп'ютерним системам стратегічного рівня. Спеціальні завдання, які здатна виконувати кіберзброя, мають чітко виражене військове спрямування. Насамперед йдеться про несанкціонований доступ до систем управління зброєю та імітацію примусового запуску окремих елементів ракетної чи іншої зброї, блокування систем управління військами, передачу у війська хибних наказів та директив [10].

Як Україні захистити себе у світі, переповненому безкомпромісною кіберборотьбою? Фахівці вказують на необхідність йти шляхом створення національної операційної системи та необхідних пакетів прикладних програм,

зокрема й вітчизняного антивірусу, створення (відновлення) вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази. Автоматизовані робочі місця, інформаційно-телекомунікаційні системи, у яких циркулює критична інформація, повинні бути суто внутрішніми та не мати прямого виходу до світової мережі Інтернет. Матеріально-технічну базу інформаційно-аналітичних систем, автоматизованих робочих місць доречно формувати виключно через вітчизняних постачальників. Потрібно суттєво підвищити рівень свідомості дій та операцій усіх без винятку безпосередніх учасників роботи з критичною інформацією в умовах автоматизованого робочого місця, інформаційно-аналітичної системи. Працівники повинні усвідомлювати можливі наслідки певних дій, бути обізнаними з засобами забезпечення несанкціонованого витоку інформації та шляхами запобігання цьому [11].

Необхідно усвідомити, що запровадження дієвої комплексної національної системи кіберзахисту вимагає нових підходів до організації державного управління, відповідної підготовки управлінців. Прагнення побудови інформаційного суспільства докорінно змінюють поняття “безпеки” та методи управління нею. Україна повинна мати комплекс своїх, суто національних, інструментів кіберзахисту, які здатні адекватно реагувати на існуючі та нові загрози й виклики у цій сфері, з ефективною системою управління ними. Для прикладу, доречно навести діяльність приватної кампанії “лабораторії Касперського” в Росії, голова якої поставив перед собою патріотичне завдання, яке успішно виконує: захистити системи, які відповідають за життєзабезпечення людей [12].

Так, нещодавно “Лабораторія Касперського” оголосила про розкриття надскладної та надефективної глобальної мережі кібершпіонажу “Маска”, за якою стоять іспаномовні зловмисники. Виявлені сліди вказують на те, що операція ведеться як мінімум з 2007 р. Дії зловмисників були спрямовані, насамперед, на державні організації, дипломатичні офіси і посольства, енергетичні та нафтогазові компанії, дослідницькі організації і політичних активістів. Жертвами цього стали користувачі з 31 країна у всьому світі, включаючи Близький Схід, Європу, Африку й Америку. Головною метою атакуючих був збір цінної інформації із заражених систем, включаючи різні документи, ключі шифрування, налаштування VPN тощо. Такий масштаб діяльності змушує припустити, що організацію та підтримку надавала ціла держава. Зараження користувачів відбувалося через розсилку фішингових листів, що містять посилання на шкідливі ресурси. На цих сайтах розташовувалася низка експлойтів, які, залежно від конфігурації системи відвідувача, використовували різні способи атаки його комп’ютера. У разі успішної спроби зараження, шкідливий сайт перенаправляв користувача на нешкідливий ресурс [13].

До заслуг української науки в управлінні кіберсферою доречно віднести науково-практичну роботу, виконану творчим колективом Державного університету інформаційно-комунікаційних технологій, зі створення принципово нової системи ефективного управління Національною інформаційно-комунікаційною інфраструктурою України. Порівняно з аналогічними світовими системами управління, вітчизняна система має такі переваги: оптимізовано структуру і параметри системи управління внаслідок упровадження архітектури, яка має властивості адаптивності; наявна можливість безпосереднього вимірювання параметрів послуги на основі створеної наскрізної системи управління якістю; упроваджено режим прогнозування управляючої дії [14]. Також в Україні створено

сучасну телекомунікаційну мережу спеціального призначення, яка повинна унеможливити будь-які спроби невмотивованого втручання у сферу державних інтересів [15]. Розроблено методи побудови процесорів на базі нейроструктур для обробки супутникової інформації, систему автоматизації ефірного мовлення, програмні та апаратні засоби швидкої обробки відеоінформації на семи телерадіокомпаніях, телевізійних центрах та студіях України і Росії [16].

Обсяг, швидкість і якість обробки інформації впливають на методи управління соціальними та економічними процесами. Перевага найбільш розвинених країн у сфері програмних матеріалів та електронних продуктів гарантує їм домінування в інформаційній сфері. Інформаційна складова, дедалі набуваючи ваги, стає визначальним елементом національної безпеки.

Україні необхідно створити ключові механізми державного управління інформаційною безпекою в умовах кіберзагроз у вигляді спеціалізованих центрів, інститутів та експериментувати з операціями щодо ведення інформаційної війни, фінансувати експертні дослідження у сфері інформаційних операцій і створювати структури для наукових досліджень і та дослідно-конструкторських розробок. На порядку денному стоїть завдання поетапно сформувати індустрію програмного забезпечення; пришвидшити роботи щодо створення української національної мережі суперкомп'ютерних комплексів, об'єднаних високошвидкісними оптико-волоконними каналами передачі даних; сформувати чітку інформаційну політику з просування вітчизняних ІТ-компаній за кордоном; об'єднати інтереси освіти, науки та ІТ-бізнесу; визначити базові вищі навчальні заклади, на основі яких сформувати кластери, що дадуть змогу вирішувати питання кадрової підготовки фахівців ІТ-технологій.

Україна здійснює заходи із захисту ресурсів та інформації, що на них розміщена. Уряд досягнув домовленості із провідними глобальними Інтернет-серверами для запобігання блокуванню інформації про злочини терористів на українській території. Кабінет Міністрів України 24 липня 2014 р. затвердив робочий варіант Стратегії забезпечення кібернетичної безпеки України. У цьому документі дано визначення кібервійни як дій спеціальних збройних підрозділів іноземної держави проти інтересів України в кібернетичному просторі.

Висновки

Успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кіберборотьба набула стратегічного управлінського спрямування. Вона проводиться без міжнародних правових обмежень у просторі та часі і характеризується високою ефективністю щодо досягнення воєнно-політичної мети. Кіберпростір став невід'ємною частиною інформаційного простору та п'ятою сферою ведення збройної боротьби. Сама збройна боротьба, завдяки інформаційному чиннику, набула високого ступеня керованості.

На сьогодні світ контролює той, хто контролює кіберпростір. Контроль над кіберпростором означає не тільки збір інформації, але й масовані акції психологічного впливу, аж до контролю та опосередкованого управління поведінкою противника. Стратегічний паритет у кіберпросторі, на відміну від ядерного та звичайних озброєнь, залишається не сформованим. У кіберпросторі діють не тільки визнані суб'єкти міжнародного права, а й громадські і терористичні організації. Завдання, які виконуються із застосуванням кіберзброї, фахівці розподіляють на три рівні: тактичний, стратегічний та спеціальний.

Оскільки застосування стратегії “Hard Power” у кібервійні із застосуванням авіації та аерокосмічної підтримки – справа надто затратна, тому основні її учасники досягають поставлених результатів, застосовуючи нову стратегію “Soft Power”. Її основу становить створення шкідливих вірусів для ефективної кібератаки з метою отримання необхідної засекреченої інформації, тотального контролю над соціальними мережами або для організації атаки на комп’ютерні центри управління цивільної, фінансової та воєнної інфраструктури.

Узагальнюючи досвід передових країн світу, кіберзахисту України необхідно йти шляхом створення національної операційної системи та необхідних пакетів прикладних програм, зокрема й вітчизняного антивірусу, створення (відновлення) вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази. Матеріально-технічну базу інформаційно-аналітичних систем, автоматизованих робочих місць доречно формувати виключно через вітчизняних постачальників.

Забезпечення кібернетичної безпеки та ефективне державне управління нею у провідних країнах світу реалізовується з позицій системного підходу шляхом упровадження комплексу нормативно-правових, організаційних, функціональних, фінансових, технічних, навчально-тренувальних заходів та дій і цю практику Україні доречно перейняти. Також необхідно підняти рівень особистої кібербезпеки, тобто відповідальності кожного громадянина перед своєю країною.

Література

1. Іжутова І. Європа переймається кібербезпекою / І. Іжутова // Військо України [Текст]. — 2013. — лип. – серп. — С. 44—47.
2. Форосовец С. Войны будущего идут уже сегодня / С. Форосовец // Комментарии [Текст]. — 2014. — № 35. — 19 сент. — С. 19.
3. Даник Ю. Полігон протистояння – кіберпростір / Ю. Даник // Народна армія [Текст]. — 2011. — 9 груд. — С. 4.
4. Олександров С. ЗС Румунії: за стандартами НАТО / С. Олександров // Військо України [Текст]. — 2013. — листоп. – груд. — С. 69—71.
5. Константинов М. Кібернетичні технології / М. Константинов // Оборонний вісник [Текст]. — 2013. — № 12. — С. 12—17.
6. Олійник В. Проект Закону України “Про кібернетичну безпеку України” [Електронний ресурс] / Олійник В., Самойленко Ю., Кузьмук О. — Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=47240&pf35401=264705.
7. Халилов Р. Бойцы невидимого фронта / Р. Халилов // Комментарии [Текст]. — 2013. — № 48. — 13 груд. — С. 6.
8. Морозовицкий И. Игры патриотов И. / Морозовицкий // Фокус [Текст]. — 2014. — 10 янв. — С. 20, 21.
9. Буткевич Б. Відкритий доступ / Б. Буткевич // Український тиждень [Текст]. — 2013. — № 41(309). — 11 – 17 жовт. — С. 4, 5.
10. Ступак І. Українська реальність: неоголошена кібервійна / І. Ступак // Народна Армія [Текст]. — 2014. — 12 серп. — С. 7.
11. Фурашев В. Інформаційний простір та безпека / В. Фурашев // Камуфляж [Текст]. — 2010. — № 10. — С. 14, 15.
12. Милкус А. Евгений Касперский рассказал, как и от чего он собирался спасти мир / А. Милкус // Комсомольская правда в Украине [Текст]. — 2013. — 19 сент. — С. 9, 10.

13. Росія, ІП “Софтодром”: “Лаборатория Касперского” раскрыла глобальную сеть кибершпионажа” [Электронный ресурс]. — Режим доступа : http://news.softodrom.ru/ap/b19173.shtml.

14. Яковенко В. Україна в глобальному інформаційному просторі: здобутки вітчизняних вчених / В. Яковенко, Т. Наритник // Урядовий Кур’єр [Текст]. — 2013. — № 170. — 19 верес. — С. 19.

15. Пастернак Ю. Нова система спецзв’язку хакерам буде не по зубах / Ю. Пастернак // Урядовий кур’єр [Текст]. — 2012. — № 152. — 12 серп. — С. 10.

16. Сергієнко І. Імідж країни спирається на сучасні комп’ютери // Урядовий кур’єр [Текст]. — 2012. — № 165. — 13 верес. — С. 11.

Z. Koval

DYNAMICS OF THE WORLD GOVERNMENT REACTION TO CYBER THREATS: LESSONS FOR UKRAINE

The article analyzes the dynamics of the world government reaction to cyber threats and the ways the public administration provides information security of Ukraine under systematic cyber threats. Taking into account the experience of the world’s leading countries in managing counteraction to cyber threats, and, from the point of view of systems analysis, the ways to improve information security of Ukraine are outlined.

Key words: cyberspace, cybernetics, cyber wrestling, cyber command, cyber security systems, hacker attacks, cyberwar, cyber threat.