

УДК 355.40:004.9

Віталій Кацалап, старший науковий співробітник Центру воєнно-стратегічних досліджень, Національний університет оборони України імені Івана Черняхівського, Україна, м. Київ

Олександр Устименко, канд. наук з державного управління, старший науковий співробітник Центру воєнно-стратегічних досліджень, Національний університет оборони України імені Івана Черняхівського, Україна, м. Київ

Створення, розвиток та захист кібернетичного простору воєнної сфери України

Розглянуто питання створення та розвитку інформаційного простору держави для інформаційного забезпечення процесів військового управління, причому не лише в контексті протидії кібертероризму та негативному інформаційному впливу на суспільство та інфраструктуру держави, а в розрізі отримання і циркуляції інформаційних ресурсів задля забезпечення функціональної діяльності суб'єктів воєнної сфери в інтересах оборони держави.

Ключові слова: інформаційна безпека, інформаційна боротьба, інформаційний простір, кіберпростір воєнної сфери

Vitaliy Katsalap, Aleksandr Ustimenko. Создание, развитие и защита кибернетического пространства военной сферы Украины.

Рассмотрены вопросы создания и развития информационного пространства государства для информационного обеспечения процессов военного управления, причем не только в контексте противодействия кибертерроризму та негативному информационному воздействию на общество та инфраструктуру государства, но и в разрезе получения и циркуляции информационных ресурсов с целью обеспечения функционирования субъектов военной сферы в интересах обороны государства.

Ключевые слова: информационная безопасность, информационная борьба, информационное пространство, киберпространство военной сферы.

Vitaliy Katsalap, Aleksandr Ustimenko. Creation, development and defence of cybernetic space of military sphere of Ukraine

The question of creation and development of informative space of the state is considered for the informative providing of processes of military management. Thus not only in the context of counteraction of cyberterrorism and to negative informative influence on society and infrastructure of the state, and in the cut of receipt and circulation of informative resources for the sake of providing of functional activity of subjects of military sphere in interests of defensive of the state.

Keywords: informative safety, informative fight, informative space, cyberspace of military sphere.

Існуючі світові концептуальні і доктринальні документи щодо забезпечення інформаційної безпеки та ведення інформаційної боротьби спрямовані виключно на захист інфраструктури, зокрема військової, від різноманітних інформаційних впливів, а також на створення умов і засобів для такого впливу на іншу сторону. Зміст цих документів відображає основну сутність політики розвитку засобів інформаційного протиборства в світі в інтересах інформаційної безпеки в сучасних умовах [1].

В той же час, зазначена концептуальність забезпечення інформаційної безпеки держав є неповною, що полягає у відсутності закріплення на концептуальному рівні потреби створення та розвитку інформаційних інфраструктур (у державах), які продукують необхідні інформаційні ресурси (ІР), тобто створення інформаційного простору для інформаційного забезпечення різноманітних процесів управління (іншими словами – кіберпростір), в тому числі у воєнній сфері (те, що може бути об'єктом негативного впливу та потребує захисту).

Свого часу ми зазначали, що в Україні відсутні підрозділи в органах державної влади, які б відповідали за здійснення оперативних і стратегічних заходів з метою попередження та нейтралізації негативного інформаційно-психологічного впливу [2]. На жаль за цей час істотних зрушень, щодо вирішення піднятих проблем, не відбулося.

На сьогоднішній день питання захисту ІР надзвичайно важливе, зважаючи на те, що прискорений розвиток комп'ютерних технологій не тільки значною мірою сприяє підвищенню ефек-

тивності їхнього функціонування, але і відкриває додаткові можливості для навмисного на них деструктивного впливу. Новітні технології дозволяють проводити атаки у кіберпросторі. Особливо швидкими темпами цей сегмент інформаційного протистояння розвивається у Китаї та США. Про це, у тому числі, свідчить і розслідування, що проводиться Міністерством юстиції США, про факти розголошення тасмної інформації стосовно проведеної американцями скритої кібератаки на іранські ядерні об'єкти [3].

На нашу думку сьогодні проблема забезпечення інформаційної безпеки, зокрема у воєнній сфері, повинна розглядатись не лише як проблема протидії кібертероризму та негативним інформаційним впливам на інфраструктуру держави. Це надзвичайно складна проблема, котра охоплює усі процеси отримання і циркуляції IP з метою забезпечення функціональної діяльності суб'єктів воєнної сфери в інтересах оборони держави.

Метою статті є висвітлення складових процесу створення та розвитку інформаційного простору держави для інформаційного забезпечення процесів військового управління (кіберпростору воєнної сфери).

Забезпечення інформаційної безпеки України у воєнній сфері, на нашу думку, повинно здійснюватись шляхом вирішення комплексу завдань за такими основними напрямками:

створення та розвиток єдиного інформаційного простору України у воєнній сфері (кіберпростору воєнної сфери);

захист єдиного інформаційного простору України у воєнній сфері (кіберпростору воєнної сфери).

Забезпечення інформаційної безпеки України у воєнній сфері в сучасних умовах має пов'язуватись із перспективною моделлю ведення війни, яка передбачає вплив на противника у ході воєнного конфлікту за кібернетичним принципом (рис.1), для чого і повинен створюватись (підтримуватись) єдиний інформаційний простір воєнної сфери (кіберпростір воєнної сфери) [4].

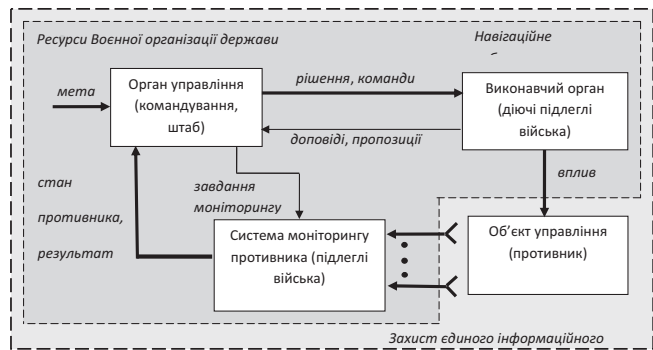


Рис. 1. Кібернетична модель ведення збройної боротьби з противником

Фундаментальним завданням створення та розвитку єдиного інформаційного простору України у воєнній сфері (кіберпростору воєнної сфери) є еволюційна побудова та підтримка дієздатності основного (бойового) інформаційного простору України у воєнній сфері, який гарантує формування, використання та розповсюдження IP в інтересах досягнення інформаційної переваги над противником та управління ним в ході воєнного конфлікту. Основний (бойовий) інформаційний простір України у воєнній сфері утворюється в інтересах діяльності Збройних Сил України та інших військових формувань Воєнної організації держави, а його достатність забезпечується результатами виконання необхідного переліку заходів такого змісту [5].

1. Забезпечення формування IP органів військового управління.

Реалізується шляхом глибокої інформатизації суб'єктів Воєнної організації держави, створення та ефективного функціонування Єдиної АСУ Збройних Сил України, поєднаної через Інтранет– та Інтернет-технології із локальними АСУ, електронними архівами і базами даних інших суб'єктів Воєнної організації держави; створенням потужної бази імітаційного моделювання процесів збройної боротьби; досягненням необхідного рівня професіоналізму персоналу (особового складу) органів військового управління.

2. Забезпечення інформаційного обміну між органом(ми) військового управління і виконавчим органом, яким є підлеглі війська (з їх органами управління), що здійснюють силовий вплив на противника або його ураження, а також формування IP органів управління цих підлеглих військ.

Реалізується можливостями Єдиної АСУ Збройних Сил України, засобами імітаційного моделювання, створенням сучасної системи зв'язку і обміну даними між усіма ланками військового управління, а також досягненням необхідного рівня професіоналізму в органах управління підлеглих військ (сил).

3. Забезпечення формування IP системою моніторингу противника, а також інформаційного обміну між органом(ми) військового управління і цією підлеглою системою.

Реалізується можливостями Єдиної АСУ Збройних Сил України, створенням сучасної системи зв'язку і обміну даними, а також еволюційним створенням комплексу взаємопов'язаних моніторингових систем:

системи інформаційної підтримки процесів прогнозування і превентивного аналізу глобальних і регіональних конфліктів та прикордонних кризових ситуацій з метою формування статичного IP (системи первинних даних) для вироблення рішень щодо нейтралізації загроз воєнного характеру методами дипломатії або іншими діями суб'єктів Воєнної організації держави;

стаціонарної загальнодержавної цивільно-військової радіолокаційної системи контролю повітряного простору мирного часу з метою формування динамічного IP для інформаційного забезпечення управління діями авіації, обслуговування повітряного руху та чергових сил з протиповітряної оборони об'єктів держави від терористичних атак з повітря;

мобільної системи інформаційного забезпечення міжвидового (оперативного) угруповання військ Збройних Сил України на основі комплексного застосування методів радіоелектронної розвідки з метою стійкого формування динамічного IP про стан та дії противника (у повітрі, на морі і суші) для управління ним у ході воєнного конфлікту силовими та несиловими методами;

системи висвітлення обстановки (повітряної, надводної, підводної, радіоелектронної) в Азово-Чорноморському басейні з метою формування динамічного IP для забезпечення цивільно-військової діяльності на морському напрямі.

4. Забезпечення формування динамічного IP засобами дистанційного спостереження у складі зброї.

Реалізується у складі зброї (засобів вогневого або іншого фізичного ураження) і забезпечується на основі удосконалення елементів контуру наведення (самонаведення) на ціль конкретного її зразка.

5. Забезпечення формування та використання спеціальних IP з метою інформаційного впливу на противника шляхом заходів оперативного маскування, застосування технологій мас-медіа для інформаційно-психологічного впливу на противника, а також інформаційних технологій для порушення роботи його інформаційних систем.

Реалізується лише в умовах участі України у воєнному конфлікті і забезпечується на основі розробки теорії інформаційної операції та її впровадження в практику у ході подальшого реформування Збройних Сил України.

6. Здійснення навігаційного забезпечення сил та засобів, що належать суб'єктам Воєнної організації держави (збройним силам).

Реалізується шляхом створення системи навігаційного забезпечення Збройних Сил України як складової загальнодержавної навігаційної системи на основі комплексного використання технологій геоінформаційних систем, засобів автономної навігації рухомих об'єктів та можливостей космічної радіонавігації з мережею контрольно-коригуючих наземних станцій на території України.

Невід'ємним завданням створення та розвитку єдиного інформаційного простору України у воєнній сфері є запровадження та удосконалення системи (середовища) статичних IP сектору ресурсного забезпечення суб'єктів Воєнної організації держави (матеріально-технічного, фінансового, кадрового, медичного) в інтересах інформаційної підтримки процесів створення (реформування), оновлення та ефективної діяльності її військових формувань. Реалізується шляхом виконання заходів такого змісту:

поглиблення інформатизації усіх суб'єктів Воєнної організації держави, створення відомчих та міжвідомчих електронних бібліотек (фондів, архівів, баз даних, інформаційних масивів тощо), у тому числі структурованих тематично;

створення автоматизованої Єдиної системи управління адміністративно-господарськими процесами Збройних Сил України;

створення нормативно-правових та технічних умов регламентованого вертикально-горизонтального доступу до статичних IP суб'єктів Воєнної організації держави.

Наявність вищезазначених складових та їх інтеграція визначають достатність (повноту) кіберпростору воєнної сфери, без чого він є неповноцінним та малоефективним за функціональною ознакою. Тому, з точки зору придатності за призначенням кіберпростору воєнної сфери, потрібно одночасно розглядати як питання його достатності (повноти), так і всебічного захисту, основні завдання якого наводяться нижче.

Основні завдання захисту єдиного інформаційного простору України у воєнній сфері (кіберпростору воєнної сфери) полягають в наступному:

створення національної системи конфіденційного (спеціального) зв'язку, розгалуженої до елементів інформаційної інфраструктури Военної організації держави;

створення і впровадження комплексних систем захисту інформації на об'єктах автоматизації та в інформаційно-телекомунікаційних мережах суб'єктів Военної організації держави, зокрема на об'єктах Єдиної АСУ Збройних Сил України, шляхом виконання нормативно-правових, організаційних та технічних заходів;

створення потужної системи державної експертизи, ліцензування та сертифікації технічних компонентів іноземного походження, або готових національних виробів на їх основі, призначених для інформаційної інфраструктури Военної організації держави;

підвищення ефективності засобів активної локації (радіо-, гідро-, оптичної), призначених для функціонування в умовах навмисних завад, за рахунок збільшення їх мобільності, енергетичного потенціалу та передових методів обробки сигналів;

посилення взаємодії Военної організації держави із засобами масової інформації України з метою забезпечення дієвості національної мас-медійної галузі у сфері оборони держави, зокрема стійкості роботи транскордонного телебачення та радіомовлення, національного сегменту мережі Інтернет, а також стабільності поширення друкованої продукції за межі країни, в умовах інформаційної війни (боротьби);

передбачення заходів щодо оборони важливих об'єктів інформаційної безпеки держави у военній сфері від ураження високоточною зброєю противника, у тому числі самонавідною;

розроблення та впровадження в життя комплексної державної політики виховання патріотизму у громадян України справедливою і дієвою поведінкою влади, методами матеріального та морального стимулювання, впливом національного телебачення, радіо, кіно, Інтернет-технологій, тематичними публікаціями газет і журналів, творами мистецтва та літератури тощо;

збереження та примноження освітнього потенціалу нації, залучення до інформаційної сфери держави найбільш зорієнтованих та інтелектуально підготовлених її представників, створення належних умов для їх професійного навчання, саморозвитку та самореалізації, зокрема в інформаційному середовищі Военної організації держави.

Список використаних джерел

1. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 09.01.2007 р. № 537-V.

2. Устименко О. В. Пропозиції щодо забезпечення інформаційної безпеки держави у ході ведення інформаційної війни / О.В. Устименко // Збірник наукових праць "Труди Академії". – 2008. – №5(85). – С. 75–81.

3. Скандал в Пентагоні: генерала підозревають в утечці секретних даних о кібератаках США [Електронний ресурс]. – Режим доступу : <http://mytime.net.ua/news/2013/06/2013-06-28-10.htm>.

4. Сніцаренко П.М., Вещицький І.В. Витоки і сутність інформаційної безпеки України у военній сфері та проблемні питання її забезпечення. – К.: ІПНБ, 2009, Вип. 5(24). – С. 23–33.

5. Звіт про НДР «Обґрунтування комплексного підходу до вирішення проблеми забезпечення інформаційної безпеки України у военній сфері», шифр «Комунікатор». – К.: НАОУ, 2009. – 46 с.

* * *