УДК355.45

к.т.н., доц. **Пампуха І.В.** (ВІКНУ)
Адаськов О.І. (ВІ КНУ)
Місяць О.О. (ВІКНУ)

РЕКОМЕНДАЦІЇ ЩОДО ЗБІЛЬШЕННЯ МОЖЛИВОСТЕЙ ОПЕРАТИВНОГО КОМАНДУВАННЯ ПРИ ПРОВЕДЕННІ ДІЙ В КІБЕРПРОСТОРІ В ІНТЕРЕСАХ СТАБІЛІЗАЦІЙНОЇ (АНТИТЕРОРИСТИЧНОЇ) ОПЕРАЦІЇ

Кіберскладова інформаційної війни між Російською Федерацією та Україною охоплює справжні "війни" між російськими та українськими користувачами різних соціальних мереж, здійснюються практично щоденні DDoS-атаки на різні інформаційні ресурси, в обох країнах намагаються спотворити офіційну інформацію. Щоденно відмічаються факти злому тих чи інших ресурсів з конфіденційною інформацією, приватних облікових записів електронної пошти, аккаунтів соціальних мереж тощо. Це потребує розробки рекомендацій щодо збільшення можливостей оперативного командування при проведенні дій в кіберпросторі в інтересах стабілізаційної (антитерористичної) операції, які полягають у збільшенні можливостей Оперативного командування щодо проведення дій в кіберпросторі шляхом встановлення постійної взаємодії та залучення до виконання завдань патріотично налаштованих громадських організацій, які займаються діяльністю в кіберпросторі.

Ключові слова: інформаційна війна, гібридна війна, оперативне командування.

Постановка проблеми. За словами генерал-майора Франка ван Каппена: "Держава, яка веде гібридну війну, укладає оборудку з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок із якими формально повністю заперечується. Ці виконавці можуть робити такі речі, які сама держава робити не може, тому що будь-яка держава зобов'язана дотримуватися Женевської конвенції та Гаазької конвенції про закони сухопутної війни, домовленості з іншими країнами".

Певний інтерес становить роль інформаційних заходів в гібридній війні. З впевненістю можна сказати, що саме інформаційні заходи є визначальними для даного типу війни.

Сьогодні з боку Російської Федерації проводиться потужна інформаційна кампанія, спрямована на дестабілізацію суспільно-політичної обстановки та деморалізацію населення України. Під впливом цієї інформаційної кампанії радикалізувались сепаратистські настрої в окремих регіонах України і сформувались умови для проведення спеціальних операцій щодо розгортання рухів опору та диверсійно-розвідувальної (особливо) в Донецькій та Луганській областях. Одночасно з цим керівництвом Росії здійснюється потужний інформаційний вплив на населення Російської Федерації з метою його переконання у правильності та необхідності власних дій та на міжнародну спільноту з метою зменшення тиску країн світу на Росію, а також, виправдання власних дій.

Під впливом російської пропаганди збуджувалися маси населення в Криму та на Сході України, формувалися та поширювалися сепаратистські настрої, тобто формувалася основа для появи нерегулярних збройних формувань.

В подальшому під впливом інформаційних заходів відповідні настрої в регіонах конфлікту закріплювались та поширювались, загострювались протиріччя між населенням даних регіонів з одного боку, державною владою та силовими структурами України – з іншого.

Постійно проводяться інформаційні заходи щодо залякування особового складу наших військ та населення. Офіційними російськими ЗМІ та бойовиками розповсюджується інформація про значні втрати серед українських силових структур, власні ж – применшуються; про неминучість краху української держави, про некомпетентність керівництва, неспроможність чинної влади врегулювати ситуацію тощо.

Крім інформаційно-психологічної складової, окремо слід виділити кіберскладову інформаційної війни між Російською Федерацією та Україною. Вона охоплює справжні "війни" між російськими та українськими користувачами різних соціальних мереж; практично

щоденні DDoS-атаки, які здійснюються на різні інформаційні ресурси в обох країнах; намагання спотворити офіційну інформацію (наприклад щодо результатів виборів). "Війна в кіберпросторі" між Росією та Україною ведеться з застосуванням нових шпигунських програмних засобів (наприклад – хробак Уроборос) та іншого шкідливого програмного забезпечення. Щоденно відмічаються факти злому тих чи інших ресурсів з конфіденційною інформацією, приватних облікових записів електронної пошти, аккаунтів соціальних мереж тощо.

Безпосередньо в районі конфлікту відмічається посилена робота засобів контролю радіо простору та радіоелектронної розвідки. Прослуховуються практично всі радіомережі, включаючи мережі стільникового та супутникового зв'язку. Виявлена інформація відразу ж застосовується для організації вогневого ураження, диверсій, засідок тощо.

Таким чином, постає задача розробки рекомендацій щодо збільшення можливостей оперативного командування при проведенні дій в кіберпросторі в інтересах стабілізаційної (антитерористичної) операції.

Виклад основного матеріалу. Завдання, які потребують проведення дій у кіберпросторі в інтересах стабілізаційної операції Оперативного командування Збройних Сил України можна визначити за напрямами:

Моніторинг кіберпростору, розвідка та інформаційно-аналітична діяльність має здійснюватися постійно з метою виявлення, оцінювання та прогнозування розвитку інформаційних загроз проведенню стабілізаційної операції Оперативного командування; виявлення інформації, важливої для проведення стабілізаційної операції; виявлення дезінформації; аналізу ефективності проведених інформаційних заходів.

Дії щодо захисту власного кіберпростору:

1. Інформування Командування оперативне командування (ОК) про виявлені інформаційні загрози;

2. Організація нейтралізації інформаційних загроз, пов'язаних з проведенням противником заходів інформаційно-психологічного впливу на Командування ОК;

3. Організація нейтралізації інформаційних загроз, пов'язаних з дезінформуванням противником Командування ОК;

4. Організація захисту інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем ОК;

5. Організація захисту особового складу Збройних Сил України від негативного інформаційно-психологічного впливу, який реалізується в кіберпросторі;

6. Організація захисту об'єктів систем управління військами від фізичного (вогневого) ураження та радіоелектронного подавлення, які можливі при проведенні противником комплексу заходів інформаційної боротьби;

7. Організація комплексу заходів протидії технічним видам розвідки противника;

8. Організація технічного та криптографічного захисту інформації в інформаційно-телекомунікаційна система (ІТС) ОК; антивірусного захисту об'єктів інформаційної діяльності ОК.

Інформаційні дії щодо активного впливу на кіберпростір противника та світовий:

1. Інформаційно-психологічний вплив на керівний склад противника, вороже налаштованих лідерів політичних, релігійних та громадських організацій, лідерів незаконних збройних формувань з метою їх деморалізації, залякування, провокування, спонукання до потрібних дій, переконання, дискредитації, компрометації тощо;

2. Підготовка та розповсюдження дезінформаційних матеріалів з метою введення противника в оману в інтересах виконання бойових завдань військ (сил) Збройних Сил України, інші військові формування та правоохоронні органи;

3. Порушення нормального функціонування (виведення з ладу) інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем противника шляхом проведення кібератак та спеціальних заходів технічного впливу;

4. Порушення конфіденційності, доступності та цілісності інформації в інформаційно-телекомунікаційних системах противника шляхом проведення кібератак та розповсюдження спеціального апаратного та програмного забезпечення;

5. Інформаційно-психологічний вплив на особовий склад військ противника, незаконних збройних формувань, вороже налаштоване цивільне населення в районі виконання бойових завдань з метою їх деморалізації, внесення розколу (дезінтеграції), виклику відчуття паніки та безперспективності власних дій;

6. Інформаційна робота з нейтрально та дружньо налаштованим цивільним населенням в районі виконання бойових завдань з метою їхньої підтримки та заспокоєння, інформування про зміст та сутність політики держави (особливо стосовно регіону, де проживає це населення), залучення до заходів цивільно-військового співробітництва (відновлення інфраструктури, спільна охорона громадського порядку і забезпечення законності, підтримка діяльності органів місцевої влади, організація розповсюдження гуманітарної допомоги тощо), залучення до виявлення та збору інформації в інтересах виконання бойових завдань; попередження та нейтралізації пропаганди противника;

7. Блокування роботи (захоплення, виведення з ладу, знищення) телевізійних та радіо засобів пропаганди противника, виявлення та вилучення друкованих засобів пропаганди противника, нейтралізація інформаційних ресурсів противника в Інтернет;

8. Організація фото, відео документування результатів виконання бойових завдань, заходів цивільно-військового співробітництва, порушення противником норм міжнародного гуманітарного права (вбивства цивільного населення, захоплення та катування заручників, насильство над дітьми, жінками та особами похилого віку, знищення історичних пам'яток, об'єктів культури, пошкодження цивільної інфраструктури тощо);

9. Організація роботи засоби масової інформації (ЗМІ) з метою висвітлення позитивної інформації про власні дії, негативної – про дії противника; попередження витоку негативної та критично важливої інформації;

10. Розповсюдження в світовому інформаційному просторі позитивної інформації про власні дії, негативної – про дії противника.

11. Визначення критично важливих об'єктів інформаційної інфраструктури противника (вузли зв'язку, комутатори, інформаційні центри, телерадіоцентри, засоби радіоелектронної розвідки та боротьби тощо) та внесення їх до планів вогневого ураження та радіоелектронного подавлення.

Перераховані завдання відносяться до завдань інформаційної боротьби, яка відповідно до перспективних поглядів на систему застосування Збройних Сил України може вестися у формі інформаційної операції.

Рекомендація: дії у кіберпросторі в інтересах стабілізаційної операції ОК проводити узгоджено з інформаційною операцією Збройних Сил України.

Рекомендації щодо організації управління діями в кіберпросторі в штабі Оперативного командування.

В структурі Оперативного командування штатний орган управління, функції якого стосуються організації дій в кіберпросторі, відсутній. Частково завдання захисту інформації та забезпечення безпеки інформаційно-телекомунікаційних систем вирішуються органами захисту інформації та криптології, а також, органами безпеки зв'язку. Однак, покласти на ці органи весь спектр завдань дій в кіберпросторі неможливо, тому що ці дії безпосередньо стосуються не тільки завдань захисту власного кіберпростору Оперативного командування, а й моніторингу та активного впливу на кіберпростір (при проведенні заходів виявлення та перевірки інформації, важливої для проведення стабілізаційної операції; інформаційно-психологічного впливу на противника; інформування населення в операційній зоні; цивільно-військового співробітництва; блокування інформаційних ресурсів противника; збору та висвітлення фактів порушення противником норм міжнародного гуманітарного права тощо).

Ці завдання вирішуються центрами (загонами) інформаційно-психологічних операцій, військовими ЗМІ та регіональними медіацентрами, групами цивільно-військового співробітництва, органами морально-психологічного забезпечення, військовими частинами (підрозділами) радіоелектронної боротьби.

Рекомендація: в штабі ОК створити під керівництвом начальника штабу позаштатний орган управління заходами інформаційної боротьби, до складу якого включити представників:

Управління (відділу) розвідки;

Центру (загону) інформаційно-психологічних операцій (ІПсО), який виконує завдання в операційній зоні Оперативного командування;

Прес-центру (прес-служби) Оперативного командування;

Групи цивільно-військового співробітництва;

Відділу по роботі з особовим складом;

Відділу зв'язку;

Відділу захисту інформації та криптології;

Відділу радіоелектронної боротьби.

Можливості Оперативного командування щодо проведення дій в кіберпросторі можуть бути суттєво збільшені за рахунок організації взаємодії з відповідними державними структурами та громадськими організаціями.

Так, тільки одна з подібних організацій, "Українські кібервійська" в інтересах антитерористичної операції на Сході України регулярно проводить заходи щодо:

блокування сайтів противника в Інтернет;

блокування доступу до "електронних гаманців" в платіжних системах WebMoney, PayPal та інших, на які збираються кошти для незаконних збройних формувань;

перехоплення управління маршрутизаторами на території противника (самопроголошених ДНР та ЛНР, частково – на території РФ);

перехоплення управління та висвітлення інформації з Web-камер, розміщених на тимчасово окупованих територіях Донецької, Луганської областей та АР Крим;

отримання доступу до електронної пошти та облікових записів соціальних мереж терористів.

Рекомендація: збільшити можливості Оперативного командування щодо проведення дій в кіберпросторі шляхом встановлення постійної взаємодії та залучення до виконання завдань патріотично налаштованих громадських організацій, які займаються діяльністю в кіберпросторі.

Висновки.

1. Дії у кіберпросторі в інтересах стабілізаційної операції ОК повинні проводитись в постійній взаємодії з управлінням (відділом) військово-цивільної адміністрації в операційній зоні, відповідальним за реалізацію державної інформаційної політики та забезпечення інформаційної безпеки.

2. Для управління діями в кіберпросторі в штабі ОК необхідно створити під керівництвом начальника штабу позаштатний орган управління заходами інформаційної боротьби, до складу якого включити представників управління (відділу) розвідки; центру (загону) ІПсО, який виконує завдання в операційній зоні Оперативного командування; прес-центру (прес-служби) Оперативного командування; групи цивільно-військового співробітництва; відділу по роботі з особовим складом; відділу зв'язку; відділу захисту інформації та криптології; відділу РЕБ.

3. Збільшити можливості Оперативного командування щодо проведення дій в кіберпросторі можливо шляхом встановлення постійної взаємодії та залучення до виконання завдань патріотично налаштованих громадських організацій, які займаються діяльністю в кіберпросторі.

ЛІТЕРАТУРА:

1. Концепція забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України, затверджена Наказом МО України від 20.08.2013 № 450.

2. Концепція інформаційної операції Збройних Сил України, затверджена спільним Наказом МО України та ГШ ЗС України від 31.12.2014 № 948.

3. Проект Закону України "Про кібернетичну безпеку України".

4. Fahrenkrug T. D. Cyberspace Defined / T. D. Fahrenkrug [Електронний ресурс]. - Режим доступу: http://www.au.af.mil/au/awc/ awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm;

5. Cyber Atlantic 2011 [Електронний ресурс]. - Режим доступу: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011.

6. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. - К. : НІСД, 2014. - 328 с.

7. National Military Strategy for Cyberspace Operations [Електронний ресурс]. - Режим доступу: http://www.dod.gov/pubs/foi/ ojcs/07-F-2105doc1.pdf.

8. Woolley P. Defining Cyberspace as a United States Air Force Mission /P. Woolley [Електронний ресурс]. - Режим доступу: http:// www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA453972& Location=U2&-doc=GetTRDoc.pdf.

9. Securing Cyberspace for the 44th Presidency / ed. by A. J. Lewis [Електронний ресурс]. - Режим доступу: http://csis.org/files/media/ csis/pubs/081208_securingcyberspace_44.pdf.

10. Cyberpower and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. - Washington, D.C. : Potomac Books, 2009. - 642 p.

11. Ліна Вежель Мережевий код російської інформаційної війни // Телекритика. – 2014, 11.07.2014.

12. Інформаційна безпека держави у воєнній сфері. – навчальний посібник /Рось А.О., Биченок М.М., Шемаєв В.М., Дзюба Т.М. та інші. – К.: НУОУ, 2011.

13. Військовий стандарт 01.004.004 (Видання 1) Воєнна політика, безпека та стратегічне планування: Інформаційна безпека держави у воєнній сфері. – К.: ЦУМС ЗС України, 2014.

14. Проект Закону України "Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України".

15. NSA leak: Source believes exposure, consequences inevitable // Washington Post [Електронний ресурс]. - Режим доступу: http:// www.washingtonpost.com/video/thefold/nsa-leak-source-believes-exposure-consequences-inevitable/2013/06/07/fb15c0fe-cf94-11e2-8845-d970ccb04497_video.html.

Рецензент: д.військ.н., проф. Шарий В.І., Військовий інститут Київського національного університету імені Тараса Шевченка

к.т.н., доц. Пампуха И.В., Адаськов А.И., Месяц А.А.

РЕКОМЕНДАЦИИ ОТНОСИТЕЛЬНО УВЕЛИЧЕНИЯ ВОЗМОЖНОСТЕЙ ОПЕРАТИВНОГО КОМАНДОВАНИЯ ПРИ ПРОВЕДЕНИИ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ В ИНТЕРЕСАХ СТАБИЛИЗАЦИОННОЙ (АНТИТЕРРОРИСТИЧЕСКОЙ) ОПЕРАЦИИ

Киберсоставляющая информационной войны между Российской Федерацией и Украиной охватывает настоящие «войны» между российскими и украинскими пользователями различных социальных сетей, осуществляются практически ежедневные DDoS-атаки на различные информационные ресурсы, в обеих странах пытаются исказить официальную информацию. Ежедневно отмечаются факты взлома тех или иных ресурсов с конфиденциальной информацией, частных учетных записей электронной почты, аккаунтов социальных сетей и тому подобное. Это требует разработки рекомендаций по увеличению возможностей оперативного командования при проведении действий в киберпространстве в интересах стабилизационной (антитеррористической) операции, заключающиеся в увеличении возможностей оперативного командования по проведению действий в киберпространстве путем установления постоянного взаимодействия и привлечения к выполнению задач патриотически настроенных общественных организаций, которые занимаются деятельностью в киберпространстве.

Ключевые слова: информационная война, гибридная война, оперативное командование.

Ph.D. Pampukha I.V., Adaskov O.I., Misyats O.O.

RECOMMENDATIONS FOR INCREASING THE OPPORTUNITIES OPERATIONAL COMMAND AT CARRYING OUT ACTION IN CYBERSPACE FOR STABILIZATION (ANTI-TERRORIST) OPERATIONS

Cyber component information war between the Russian Federation and Ukraine is covered by this "war" between the Russian and Ukrainian users of different social networks, carried out almost daily DDoS-attacks on various information resources in both countries are trying to distort the official information. Daily notes the hacking of various resources of confidential information, private e-mail accounts, social networking accounts and the like. This requires the development of recommendations to increase the capacity of operational command during the action in cyberspace in the interests of stabilization (anti-terrorism) operations is to increase the capacity of operational command for the action in cyberspace by establishing a permanent cooperation and involvement in tasks patriotic public organizations, which are engaged in activities in cyberspace.

Keywords: information warfare, hybrid warfare, the operational command.