ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
КАФЕДРА ФІНАНСОВО - ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

МІЖДИСЦИПЛІНАРНА КУРСОВА РОБОТА

на тему:

«ІНФОРМАЦІЙНІ ВІЙНИ У СУЧАСНИХ УМОВАХ»

Студента 1 курсу магістратури
ФЕБзм – 11 групи
Галузі знань 1801 – специфічні категорії
Спеціальності 8.18010014 «Управління фінансово-економічною безпекою»
Козака І.В.
Керівник доцент кафедри фінансово - економічної безпеки та інтелектуальної власності, к.ю.н. Москалюк Н.Б.

Національна шкала _____
Кількість балів:_____ Оцінка ECTS _____
Члени комісії _____ _____
_____ _____

м. Тернопіль – 2016 рік

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В сучасних умовах проблеми інформаційних воєн актуалізувалися у зв'язку з глобалізацією інформаційних процесів, бурхливим розвитком і пануванням інформаційних технологій, що дозволяють політикам експлуатувати інформаційний простір, процес взаємодії масових комунікацій і їх аудиторії.

Поняття «інформаційна війна» увібрало в себе в ході історичної еволюції цілий ряд явищ, що виявляються в житті громади при взаємодії мас, народів, соціальних груп.

Дане поняття - «інформаційна війна» - відповідно до цілей впливу на людей отримувало позначення як пропаганда, контрпропаганда, спецпропаганда, психологічна війна, техніка дезінформації і т.п.

В умовах становлення інформаційного суспільства, суспільства масової культури, в ході глобалізації інформаційних процесів та демократизації суспільства, тобто участю в соціальному житті все більших людських спільнот, стало очевидним відокремлення такого явища, як інформаційна війна.

Інформаційна війна є важливою складовою сучасного глобалізаційного процесу і без розуміння її сутності неможливо в повній мірі оцінити наслідки глобалізаційного тиску.

В даний час відбувається процес докорінного переосмислення сформованого образу інформації а також сутності інформаційних воєн, її цілей та методів. Це особливо важливо для вироблення нового підходу до розуміння загального зв'язку явищ і реальних кроків в напрямку формування більш конструктивних взаємин всередині людського співтовариства і забезпечення інформаційної безпеки на усіх рівнях і для усіх суб’єктів.

Тема дослідження є актуальною, оскільки для сучасного глобалізованого світу характерні інформаційні війни, провідною метою яких є маніпуляція суспільною свідомістю, тобто навмисна підміна в масовій свідомості змісту явища, коли при збереженні ідентичних зовнішніх ознак, явище набуває деструктивного сенсу або асоціюється з ним. Складність ідентифікації

маніпуляційних технологій полягає в можливості неоднозначних інтерпретацій результатів їх застосування, труднощі виявлення всіх елементів маніпуляційної програми, складність доведення навмисності тієї чи іншої маніпуляції.

У розроблюваних на Заході концепціях інформаційної війни значна увага приділяється поширенню по інформаційних каналах противника або в світовому інформаційному просторі дезінформації або тенденційної інформації дня впливу на оцінки, наміри і орієнтацію населення і осіб, що приймають рішення, з метою формування громадської думки, вигідної для конкретного суб'єкта.

Інформаційні війни в сучасному світі в істотній мірі є формами соціальної взаємодії різних суб'єктів глобалізації, які керуються в своїх діях стандартами відповідних моделей світу. Саме тому дія і життєздатність процесів глобалізації передбачає класифікацію агресивних інформаційних впливів з урахуванням їх характеру, спрямованості та адресності.

Ступінь наукової розробки даної тематики в Україні є вкрай незадовільним, що ще раз вказує на його актуальність.

Отже, **метою дослідження є**: на основі всебічного системного та критичного аналізу дослідити інформаційні війни у сучасних умовах, їх стратегії і тактики, інструменти і зброю.

Основні завдання дослідження:

- проаналізувати стратегії і тактики ведення інформаційних воєн;
- дослідити інформаційну зброю в сучасних інформаційних протиборствах;
- проаналізувати застосування глобальної мережі Інтернет в інформаційних війнах.

Об'єктом дослідження є суспільні відносини, що виникають в процесі здійснення впливу на свідомість людей під дією інформаційних воєн.

Предметом дослідження є інформаційні війни у сучасних умовах.

Методологічна та теоретична основа дослідження. При проведенні дослідження було використано комплекс загальнонаукових і приватних методів, включаючи системно-структурний, історико-правовий, порівняльно-правовий, логічний та інші методи пізнавальної діяльності.

Практичне значення одержаних результатів полягає в тому, що висновки, зроблені в процесі дослідження, можуть бути використані для подальшого розвитку вчення про інформаційні війни. Вони могли б стати методологічним підґрунтям і теоретичною базою для подальших наукових пошуків із цієї тематики: у правотворчості – в процесі врегулювання деяких норм інформаційного законодавства України; в науково-методологічній роботі – при підготовці підручників, навчальних посібників тощо.

1. СТРАТЕГІЇ І ТАКТИКИ ВЕДЕННЯ ІНФОРМАЦІЙНИХ ВОЄН

Розвиток світової спільноти наочно демонструє, що останнім часом критично важливим державним ресурсом, що надає все більший вплив на національну безпеку, стає інформація, що циркулює в автоматизованих системах управління і зв'язку. Дані системи є невід'ємним компонентом структури управління державою, економікою, фінансами і обороною. Прискорений розвиток комп'ютерних технологій не тільки в значній мірі сприяло підвищенню ефективності їх функціонування, а й відкрило додаткові можливості для навмисного деструктивного впливу на них протилежної сторони [7].

У нинішній ситуації ряд розвинених західних держав, і в першу чергу США, на початку 90-х років впритул приступили до вивчення і опрацювання проблем, пов'язаних з протиборством в інформаційній сфері, або так званої «інформаційною війною» (ІВ). За твердженням американських фахівців, окремі положення концепції «інформаційна війна» вже протягом тривалого часу реалізуються США на політичному рівні в основному в формі психологічної війни, яка внесла свій вклад в розвал СРСР і Організації Варшавського Договору [9].

У США під цим терміном розуміється комплексний вплив на систему державного і військового управління протилежної сторони, її політичне і військове керівництво, яке вже в мирний час призводило б до прийняття сприятливих для Сполучених Штатів рішень, а в ході війни повністю паралізувало структуру управління супротивника [4]. Одночасно з наступальним впливом інформаційне протиборство передбачає забезпечення надійного захисту національної інформаційної інфраструктури США.

В даний час розроблена Пентагоном концепція ведення інформаційної війни реалізується на двох рівнях: державному та військовому.

На державному рівні мета інформаційного протиборства в широкому сенсі слова полягає в ослабленні позицій конкуруючих держав, підриві їх національно-державних підвалин, порушення системи державного управління

за рахунок інформаційного впливу на політичну, дипломатичну, економічну і соціальну сфери життя суспільства, проведення психологічних операцій, підривних та інших деморалізуючих пропагандистських акцій.

Інформаційні операції (ІС) на даному рівні можуть вирішувати завдання захисту національних інтересів США, попередження міжнародних конфліктів, захід провокаційних і терористичних акцій, а також забезпечення безпеки національних інформаційних ресурсів.

На військовому рівні інформаційні операції являють собою комплекс заходів, що проводяться в масштабах збройних сил країни, їх видів, об'єднаних командувань в зонах, і є складовою частиною військових кампаній (операцій) [17]. Вони спрямовані на досягнення інформаційної переваги над противником (в першу чергу в управлінні військами) і захист своїх систем управління. Для цього можуть використовуватися будь-які військові та технічні сили і засоби, наявні в розпорядженні, при формальному дотриманні правових, моральних, дипломатичних, політичних і військових норм. Перед ВС вперше поставлена задача впливу на противника ще в загрозливий період (до початку активних бойових дій) з тим, щоб забезпечити вигідну для США спрямованість процесів управління і прийняття рішень протистоїть стороною.

Такий розподіл завдань, за оцінкою американських експертів, має забезпечити необхідну ефективність проведення заходів в рамках інформаційного протиборства, яке в теорії і практиці військового будівництва в Сполучених Штатах стало розглядатися в якості особливої форми міждержавних відносин після аналізу підсумків війни в зоні Перської затоки.

У грудні 1992 року основні положення концепції інформаційного протиборства стосовно діяльності ВС були сформульовані в загальному вигляді в директиві міністра оборони США № TS-3600.1 «Інформаційна війна» [9]. У ній ставилися завдання об'єднаному штабу КНШ і штабам видів збройних сил з розробки нової концепції. Ця робота була завершена до кінця 1993 року і знайшла своє відображення в директиві голови КНШ МОР № 30-93. У ній ідеї інформаційного протиборства були трансформовані для ВС в концепцію «боротьби з системами управління» (БСУ). У директиві КНШ БСУ визначалася

як «комплексне проведення за єдиним задумом і планом психологічних операцій, заходів з оперативної маскування, радіоелектронної боротьби і фізичного знищення пунктів управління і систем зв'язку з метою позбавлення противника інформації, виведення з ладу або знищення його систем управління при одночасному захисті своїх від аналогічних дій » [9].

Директива МОР № 30-93 фактично виділила боротьбу з системами управління в самостійний вид оперативного забезпечення бойової діяльності військ. Теорія боротьби з системами управління отримала свій подальший розвиток в Єдиному статуті КНШ № 3-13.1 1995 року «Спільні дії різнорідних сил по боротьбі з системами управління супротивника».

В подальшому, в міру розвитку комп'ютерних технологій і в зв'язку з окреслилися тенденціями до підвищення ролі інформації у всіх сферах життя сучасного суспільства, в тому числі і у військовій справі, американське командування було змушене більш широко поглянути на проблему інформаційної війни.

У документі КНШ ЗС США «Єдина перспектива-2010», який визначив основні напрямки розвитку оперативно-стратегічних концепцій застосування збройних сил в XXI столітті, підкреслювалося, що головною рисою збройної боротьби в наступному столітті буде перенесення акценту в сферу інформаційного протиборства і досягнення «інформаційного панування» стане обов'язковою умовою перемоги над будь-яким супротивником. Ці ж положення містить і виготовлений у 2000 році черговий документ КНШ «Єдина перспектива-2020»

Подальше свій розвиток концепція інформаційного протиборства отримала в інструкції КНШ 3210.01 А «Концепція інформаційних операцій 3 об'єднаних угруповань збройних сил» від 1996 року, Єдиному статуті КНШ № 3-13 «Доктрина спільних дій з проведення інформаційних операцій», директивах, статутах і настановах штабів видів збройних сил 1998 го. У цих документах йдеться про те, що інформаційні операції є більш широким поняттям, ніж боротьба з системами управління (БСУ), але не підміняють його. Завдання БСУ як самостійного виду бойового забезпечення - боротьба з системами управління

і зв'язку як з цільовими об'єктами, а мета проведення інформаційних операцій - вплив на інформаційні системи противника і циркулює в них інформацію або знищення їх При організації інформаційних операції дії по БСУ централізовано інтегруються в них і стають їх невід'ємними елементами.

У перерахованих документах визначені цілі, завдання та основні принципи інформаційного протиборства, обов'язки керівних органів і посадових осіб за їх організації і планування в мирний час і в умовах кризової обстановки. Крім того, в них перераховані вимоги до роботи з розвідувальною інформацією інформаційних операцій, а також до підготовки особового складу, що забезпечує їх планування та проведення.

Військове керівництво США вважає, що ефективне інформаційне протиборство має забезпечити командирам (командувачем) можливість нав'язати протистоїть стороні хибне бачення обстановки, примусити її до ведення військових дій в невигідних для неї умовах. Це досягається в основному завдяки проведенню комплексу заходів, що дозволяють, з одного боку, порушити процес прийняття рішень супротивником, а з іншого - обробляти інформацію по циклу прийняття рішень в своїй системі управління ефективніше і швидше, ніж це може зробити командувач протистоїть угрупованням військ

Практична реалізація концепції інформаційного протиборства здійснюється шляхом проведення інформаційних операцій, які представляють собою комплекс заходів, що мають на меті вплинути на інформацію та інформаційно-керуючі системи (ІКС) противника при одночасному захисті своєї інформації і інформаційних систем [5]. Вони є важливим фактором у досягненні і утриманні інформаційної переваги в ході операцій об'єднаних угруповань ВС. Інформаційна війна являє собою відповідну операцію, проведену в період кризової ситуації або конфлікту (включаючи війну) для досягнення специфічних цілей над специфічним противником або противниками. Стосовно до інформаційних операцій термін «противник» розглядається в більш широкому сенсі. Під ним маються на увазі організації, групи осіб або окремі особи, які приймають рішення або здійснюють дії,

спрямовані на зрив виконання завдань, поставлених перед командуванням об'єднаних збройних сил.

Підготовка та проведення інформаційних операцій пов'язані з узгодженням і дозволом на рівні національного військово-політичного керівництва країни комплексу питань законодавчого та політичного характеру. ІВ проводяться на всіх рівнях військових дій, межі між якими найчастіше носять умовний характер.

На стратегічному рівні такі операції проводяться за рішенням військово-політичного керівництва країни і покликані забезпечити досягнення національних стратегічних цілей. В ході їх здійснюється вплив на всі елементи державного устрою потенційних супротивників (політичні, військові, економічні та інформаційні) при одночасному захисті своїх державних структур. Для досягнення цілей ІВ на цьому рівні повинна забезпечуватися висока ступінь координації між військовими органами та урядовими установами і відомствами США, а також союзниками і партнерами по коаліції.

На оперативному рівні ІС проводяться для забезпечення успішного ходу операції або кампанії в цілому або рішення головних завдань операції. Їх мета - вплив на лінії зв'язку, системи тилового забезпечення і бойового управління збройними силами противника при одночасному захисті аналогічних систем, як своїх ЗС, так і союзників. Інформаційні операції, що проводяться на цьому рівні, можуть сприяти досягненню стратегічних цілей.

Інформаційні операції на тактичному рівні проводяться з метою забезпечення вирішення тактичних завдань. Вони зосереджені на впливі на інформацію та інформаційні системи, такі, як системи зв'язку, бойового управління, розвідки та інші, які безпосередньо забезпечують ведення бойових дій сполуками і частинами противника при одночасному захисті як систем своїх, так і союзників.

В основу концепції інформаційного протиборства закладена обопільна залежність (вразливість) США і їх потенційних супротивників від інформації і інформаційних систем. У зв'язку з цим при її реалізації розглядаються два аспекти діяльності - вплив на інформаційну інфраструктуру противника і

захист своєї власної інформаційної середовища [14]. Відповідно всі інформаційні операції поділяються на наступальні і оборонні.

Наступальні інформаційні операції являють собою комплексне проведення за єдиним задумом і планом заходів по оперативної маскування, радіоелектронної боротьби, програмно-математичного впливу на ІКС, фізичного знищення (виведення з ладу) об'єктів інформаційної інфраструктури, а також психологічних і спеціальних ІВ. В ході таких операцій вживаються заходи, що впливають на свідомість людей і спрямовані на зрив процесу прийняття рішень, а також дії з метою порушення роботи або знищення елементів інформаційної інфраструктури. Новим елементом наступальних інформаційних операцій в порівнянні з концепцією боротьби з системами управління є спеціальні ІС і заходи щодо програмно-математичного впливу на комп'ютерні мережі противника.

Оборонні інформаційні операції являють собою взаємопов'язані процеси щодо захисту інформаційного середовища, розкриття ознак нападу, відновлення боєздатності та організації дій у відповідь на агресію (напад). Їх основними елементами є: забезпечення фізичної безпеки інформаційної інфраструктури, безпеки інформації та скритності дій військ (сил); розтин заходів по оперативної маскування противника; контрпропаганда; контррозвідка; радіоелектронна захист і спеціальні інформаційні операції.

Оборонні інформаційні операції повинні забезпечувати своєчасність і точність передачі даних, гарантований доступ до них користувачів в умовах інформаційного впливу противника. В ході їх передбачається проведення заходів щодо відновлення боєздатності інформаційних систем.

Наступальні і оборонні інформаційні операції можуть проводитися за єдиним задумом і планом і взаємно доповнювати один одного. Вони орієнтовані на одні і ті ж об'єкти впливу, в якості яких можуть виступати:

- Органи управління держави і його збройних сил;
- ІКС цивільної інфраструктури (телекомунікаційні, включаючи засоби масової інформації, транспортні, енергетичного комплексу, фінансового та промислового секторів);

- Керуючі елементи військової інфраструктури (системи зв'язку, розвідки, бойового управління, тилового забезпечення, управління зброєю);
- Лінії, канали зв'язку і передачі даних;
- Інформація, що циркулює або зберігається в системах управління;
- Суспільство в цілому (як цивільне населення, так і особовий склад збройних сил), його державні, економічні та соціальні інститути;
- Керівний склад та персонал автоматизованих систем управління, який бере участь в процесі прийняття рішень [18].

В період проведення миротворчих операцій об'єктами впливу можуть бути також воєнізовані, партизанські і політичні організації, релігійні та соціальні групи, окремі особи, відкрито чи таємно виступають проти присутності збройних сил США або союзників і перешкоджають виконанню ними своєї місії.

За оцінкою американських експертів, ефект цільового інформаційного впливу на противника порівняємо із застосуванням зброї масового знищення і загроза піддатися такому впливу може стати важливим фактором стримування потенційного агресора [7]. На їхню думку, ефективність цієї загрози прямо пропорційна рівню технологічного розвитку та масштабам використання комп'ютерної техніки в системах управління державою.

Будучи за своїм характером комплексним процесом, інформаційна операція являє собою інтегроване, узгоджене з часу використання різних засобів і методів, орієнтованих на досягнення певної спільної мети.

Основу досить багатого і постійно вдосконалюється арсеналу методів ведення інформаційної війни в ЗС США складають як історично добре зарекомендували себе заходи, пов'язані з використанням традиційних видів оперативного (бойового) забезпечення військ (сил), так і нові способи подібного впливу на супротивника.

При проведенні наступальних інформаційних операцій основними традиційними методами є психологічні операції і заходи щодо оперативної маскування, здавна застосовувалися для здійснення впливу на свідомість людей

в процесі прийняття ними рішень, а також такі дії, як радіоелектронне придушення і використання засобів фізичного знищення, спрямовані на порушення функціонування або знищення елементів інформаційної інфраструктури. До досить новим методам в даному випадку можна віднести програмно-математичне вплив на комп'ютерні мережі противника і спеціальні інформаційні операції. Існує також безліч інших способів і дій, які можуть інтегруватися при проведенні різного роду операцій. Деякі з них носять наступальний характер, інші - оборонний. На думку американських фахівців, їх спільне використання вкрай важливо для досягнення успіху в ході проведення як оборонних, так і наступальних операцій.

Психологічні операції являють собою заходи щодо поширення спеціально підготовленої інформації з метою здійснення впливу на емоційний стан, мотивацію і аргументацію дій, прийняті рішення та поведінку окремих керівників, організацій, соціальних або національних груп і окремих особистостей іноземних держав в сприятливому для США та їхніх союзників напрямку. Вони можуть бути стратегічними, оперативними і тактичними за своїми масштабами і їх проведення може забезпечуватися заходами оперативного маскування.

На стратегічному рівні психологічні операції можуть проводиться в формі пропаганди певних політичних чи дипломатичних позицій, офіційних заяв або повідомлень керівників держави.

На оперативному рівні такі операції можуть проводитися у вигляді поширення листівок, за допомогою радіо- і телемовлення, мовлення з використанням засобів гучномовного зв'язку, а також інших засобів для передачі інформації, що містить заклики, які спонукають особовий склад збройних сил противника до масового саботажу, дезертирства, втечі або капітуляції.

На тактичному рівні проведення психологічних операцій передбачає використання гучномовного зв'язку та інших засобів для нагнітання страху, розпалювання розбіжностей і зростання непокори в рядах противника.

Вплив на політичних і військових лідерів, а також на керівників (найбільш помітних представників) ЗМІ, культури і мистецтва протилежної сторони є важливим аспектом інформаційного протиборства в цілому і психологічних операцій зокрема. У зв'язку з цим в США особлива увага приділяється створенню колективних та індивідуальних моделей поведінки представників вищої та середньої ланки державного і військового керівництва, зокрема складання психологічних портретів на керівників (у військах - до командира з'єднання включно).

Для вивчення воєначальників потенційного противника і складання їх психологічних портретів широко використовуються відкриті джерела, агентурні дані, а також заходи в рамках військового обміну, масштаб якого військово-політичне керівництво США наполегливо прагне розширити.

Заходи по оперативної маскування (в США цим терміном позначається дезінформація і введення противника в оману - прим. Ред.) Проводяться під керівництвом командувачів об'єднаними угрупованнями військ (сил). Їх змістом є надання впливу на органи прийняття рішень супротивника через його системи збору, аналізу і розподілу інформації шляхом надання їм завідомо неправдивої інформації та приховування ознак реальної діяльності військ (сил). Мета цих заходів полягає в тому, щоб заплутати, дезінформувати розвідувальні органи противника, змусити їх робити неправильні висновки і, як наслідок, домогтися від військового керівництва супротивника невірних дій [21]. Ці заходи дозволяють також випередити противника в ухваленні рішення, що є ключем до успіху будь-якої операції.

Оперативна маскування передбачає застосування таких способів:

- Дезінформація - поширення завідомо неправдивої інформації про склад, стан, дислокації, боєготовності своїх військ, їх угрупованнях, характер і способи вирішення завдань, плани, призначення і стан військової техніки та об'єктів;

- Імітація - відтворення правдоподібних демаскуюхх ознак, характерних для реальної діяльності військ (об'єктів), створення радіоелектронної

обстановки з використанням імітаторів, радіотехнічних пристроїв, помилкових споруд і об'єктів, макетів військової техніки і т. Д .;

- Демонстративні дії - навмисний показ противнику спеціально виділеними силами і засобами активної діяльності з метою його дезорієнтації і приховування справжніх намірів організаторів;

- Забезпечення скритності дій - визначення ознак, які розпізнаються розвідувальними системами противника і дозволяють йому на основі їх аналізу отримувати особливо важливу і своєчасну інформацію; вибір і проведення заходів, які забезпечували б приховування цих ознак і тим самим знижували б до прийнятного рівня вразливість союзників від дій розвідки противника [19].

Заходи по оперативної маскування зазвичай проводяться одночасно з іншими, що забезпечують дії об'єднаних сил. Планування цих заходів здійснюється зверху - вниз з тим, щоб плани по введенню супротивника в оману підлеглих ланок підтримували і забезпечували аналогічні плани вищого командування. У вищому ланці воно передбачає використання частин і підрозділів самого нижнього рівня, хоча самі їх командири і їх безпосередні начальники можуть не знати змісту загального плану заходів. Тому в таких випадках важливим є координація планів заходів щодо введення противника в оману командирів нижчестоящих частин і підрозділів зі старшим начальником.

Успіх проведення заходів з оперативної маскування у визначальній мірі залежить від ефективності розвідувального забезпечення. Розвідка в цьому випадку здійснює розтин об'єктів супротивника, щодо яких замишляє ці дії, надає допомогу в розробці правдоподібною версією, пропонованої для дезінформації, виборі найбільш перспективних об'єктів для реалізації дезінформації та оцінює ефективність проведених заходів.

Радіоелектронна боротьба підрозділяється на радіоелектронне придушення, радіоелектронну захист і радіоелектронне забезпечення. Радіоелектронне придушення є дії наступального характеру, що починаються з метою дезорганізувати, нейтралізувати або знизити можливості противника по ефективному використанню їм радіоелектронних систем в різних ланках управління збройних сил. Радіоелектронна захист передбачає такі дії, як захист

своїх радіоелектронних засобів (РЕЗ) від перешкод, створюваних противником, і здійснення контролю (нагляду) за роботою (РЕЗ) союзників, з метою виключення їх взаємного впливу один на одного. Радіоелектронне забезпечення являє собою дії, спрямовані на виявлення, ідентифікацію та визначення місця розташування РЕЗ противника, які можуть бути як джерелами отримання розвідданих, так і джерелами інформаційних загроз.

При прийнятті рішення про використання коштів радіоелектронного придушення враховуються не тільки цілі кампанії або операції, але також і ризик від можливих дій у відповідь противника. Для досягнення максимального ефекту операції обов'язковою умовою є тісна координація дій сил і засобів РЕБ з іншими заходами щодо забезпечення інформаційних операцій, що проводяться розвідкою і зв'язком.

Фізичне знищення елементів інформаційної інфраструктури розглядається як проводяться в ході ІС дії щодо застосування засобів вогневого ураження і фізичного знищення з метою виведення з ладу ключових елементів системи управління і зв'язку супротивника.

Програмно-математичний вплив на комп'ютерні мережі (комп'ютерна атака) визначається як дії із застосуванням апаратно програмних засобів, спрямовані на використання, спотворення, підміну або знищення інформації, що міститься в базах даних комп'ютерів і інформаційних мереж, а також на зниження ефективності функціонування або висновок з ладу самих комп'ютерів і комп'ютерних мереж.

Способи програмно-математичного впливу з цілком зрозумілих причин не є надбанням широкої гласності і описуються в спеціальній грифовані літературі, призначеній для обмеженого кола зацікавлених осіб. Що стосується коштів такого впливу, а роботи в області їх створення ведуться в США з 1990 року, то їх можна поділити на такі:

- «Логічні бомби» - приховані керуючі програми, які за певним сигналом або у встановлений час приходять в дію, знищуючи або спотворюючи інформацію, забороняючи доступ до тих чи інших важливих фрагментів керованого інформаційного ресурсу або дезорганизуя роботу технічних засобів.

В АСУ військами і зброєю подібне втручання навіть протягом короткого часу може докорінно вплинути на хід і результат бою, операції.

- Комп'ютерні віруси, що представляють собою спеціалізовані програмні продукти, які здатні відтворювати «логічні бомби» (маючи при цьому ще більшою руйнує силою) і впроваджувати їх дистанційно в інформаційні мережі противника. Крім того, віруси здатні самостійно розмножуватися, тобто копіювати себе на магнітних носіях.

- Програмні продукти типу «троянський кінь» - програми, впровадження яких дозволяє здійснювати прихований несанкціонований доступ до інформаційного масиву противника для добування розвідданих.

- Нейтралізатори тестових програм, що забезпечують збереження природних і штучних недоліків програмного забезпечення.

- Навмисно створені, приховані від звичайного користувача інтерфейси для входу в систему. Вони, як правило, свідомо вводяться в програмне забезпечення програмістами-розробниками з корисливими чи диверсійно-підривними цілями.

- Малогабаритні пристрої, здатні генерувати електромагнітний імпульс високої потужності, що забезпечує виведення з ладу радіоелектронної апаратури [18].

Крім того, велика увага приділяється створенню нових засобів впливу на системи зв'язку, збору і обробки інформації. Так, з початку 90-х років здійснюється перехід до використання невиявлюваних перешкод інтелектуального впливу (блокування ключових елементів повідомлення, наприклад, назв і координат пунктів, часу дії з одночасним введенням помилкових ключових елементів). Такі системи базуються на автоматизованому аналізі структури повідомлень, відстеження ключових слів, синтезуванні мови в реальному масштабі часу [3].

До дій, що забезпечує проведення інформаційних операцій, відносяться і заходи щодо організації зв'язку з цивільною адміністрацією і населенням, а також по зв'язку з громадськістю, що проводяться відповідними службами збройних сил.

Підрозділи по зв'язку з цивільною адміністрацією безпосередньо орієнтовані на дії, що забезпечують взаємну підтримку при проведенні психологічних операцій.

Декларативно завдання служби зі зв'язків з громадськістю полягають в наступному: оперативне доведення точної та своєчасної інформації про проведеної кампанії (операції) до зацікавлених організацій і громадськості; роз'яснення цілей і завдань, що вирішуються збройними силами; надання командуванню каналів ЗМІ для інформування противника (потенційних супротивників) про наміри та можливі дії союзних військ. При цьому стверджується, що всі ці дії не можуть застосовуватися для введення противника в оману або для дезінформації громадськості. На практиці, однак, можливості цієї служби широко використовуються для формування світової громадської думки в вигідному для США щодо за рахунок вибіркової і дозованої подачі інформації.

В цілому концепція інформаційного протиборства в тому вигляді, в якому вона реалізується в ЗС США, не є новим поняттям для національного військового мистецтва. Теоретичні основи інформаційного протиборства досить повно розкриті в військовій науці через поняття «боротьба з системами управління супротивника», «радіоелектронна війна», «завоювання панування в ефірі», «психологічна війна», «дезінформація», «військова хитрість» і т. п . «Новизна» американського підходу до теорії інформаційного протиборства полягає в комплексному використанні військово-теоретичних розробок з даної тематики і своїх технологічних досягнень в області інформатики.

В даний час США, володіючи значною перевагою в сфері розробки і використання новітніх радіоелектронних систем і комп'ютерних технологій і ґрунтуючись на постулатах нової концепції, прагнуть закріпити за собою домінуючу роль не тільки в політичній, економічній і військовій сферах, а й у світовій інформаційній інфраструктурі.

2. ІНФОРМАЦІЙНА ЗБРОЯ В СУЧАСНИХ ІНФОРМАЦІЙНИХ ПРОТИБОРСТВАХ

При демократії суспільство контролює вибір засобів, які використовують люди в процесі своєї діяльності, в тому числі і засобів збройної боротьби. Тільки в тому випадку, якщо наміри людей мають під собою як моральну основу, так і технологічну, цей вибір буде розумний. Але якщо про моральність не замислюються, то виникає ефект доміно: втрачається підтримка з боку суспільства, не використовуються передові досягнення технології, і в результаті збройні сили залишаються без засобів збройної боротьби.

Зараз вже є засоби, що дозволяють створити інформаційну зброю, і так як інформаційна зброя є такою потужною зброєю, як військова, так і цивільне населення повинні бути захищені від нього. До впливу інформаційної зброї уразливі всі. Уряд має прийняти рішення - розробляти засоби інформаційної зброї або переслідувати в судовому порядку тих, хто розробляє такі засоби. Це рішення повинно бути прийнято на підставі ретельного аналізу всіх деталей і з розумінням моральних і етичних ризиків інформаційної зброї. Крім врахування всіх ризиків при прийнятті рішення про створення інформаційної зброї, люди повинні розуміти принципи дії цих коштів і теорію їх використання до того як вони почнуть застосовуватися.

Під інформацією розумітимемо вміст або значення повідомлення. Метою засобів збройної боротьби є вплив на інформаційні системи ворога. У широкому сенсі інформаційні системи включають в себе всі засоби, за допомогою яких противник отримує знання або висуває гіпотези [8]. Для військових інформаційні системи являють собою засоби, за допомогою яких противник отримує інформацію про стан бойових дій і керує військами. У сукупності інформаційні системи є об'єднанням знань, гіпотез, процесів прийняття рішення та систем противника. Результатом інформаційних атак на будь-якому рівні є дати противнику інформацію, що змушує його припинити збройні дії.

З якої причини противник може припинити бойові дії? Існує ряд можливих причин: неможливість управляти збройними силами, деморалізація, отримання інформації (істинної чи імовірною) про те, що війська знищені, або про те, що більш вигідно припинити війну, ніж продовжувати воювати. Ці «повідомлення» про припинення війни можуть відрізнятися як по змісту, так і за змістом, як наприклад: «Ваша контратака провалилася» або «Ваші власні люди не підтримують вас у війні, в якій вбивають дітей». Хоча методи передачі повідомлень, що змушують припинити війну, можуть змінюватися, сенс повідомлень залишається незмінним - припинити війну.

У силу розвитку соціальних інститутів інформаційні системи ускладнювалися, а процеси прийняття рішення ставали все більш складними. Фінансово-промислові організації, що виникли на базі домінантних політичних структур збільшували складність систем у міру збільшення своєї діяльності. З'явилися мережі інформаційних взаємозв'язків між працівниками розумової праці - найсучасніша форма інституційної структури, і їх кількість, а також доступність засобів інформаційної технології різко збільшилася.

У міру розвитку інформаційної технології інформаційні системи привели до появи знання, або ноу-хау, яке дозволяло робити інші інституціональні форми більш ефективними.

Через розвиток соціальних інститутів удосконалювалися і способи збройної боротьби між людьми. Страхітливі звуки барабана, прапори і гонги часів Су Цзи при інформаційній технології стали витонченими психологічними операціями.

Метою війни стало не знищення, а управління, згідно Джону Аркуілле і Давиду Ронфельдт. Інформаційна технологія в наш час робить можливим «управління» при мінімальному насильстві і кровопролитті [2]. На перший погляд це здається хорошим. Але при уважному розгляді це може виявитися небезпечним. Ретельний аналіз допоможе визначити, що це насправді.

Що таке збройне зіткнення? Збройна сутичка - це ряд смертоносних і не призводячих до смерті процесів, що вживаються для придушення ворожих дій противника.

У цьому сенсі збройне зіткнення не є синонімом «війні». Збройна сутичка не вимагає оголошення війни, або існування умови, що розуміється людьми як «стан війни». Збройна сутичка організовується групами людей, контрольованими державою, фінансуються державою або діючими самостійно. Збройна сутичка - це ворожі дії по відношенню до ворога. Метою збройного зіткнення не обов'язково є вбити ворога. Мета збройної сутички - просто підкорити ворога. Фактично верхом майстерності є підкорення ворога без його смерті. Противник покірний, коли він веде себе таким чином, що його дії відповідають тим, які ми, агресор або обороняється, чекаємо від нього.

Намагаючись підпорядкувати собі волю ворога, ми повинні мати чітке уявлення про те, яку неворожу поведінку ми від нього очікуємо, і якої ворожої поведінки ми хочемо уникнути.

Коли збройні сили однієї держави стикаються з збройними силами іншої держави, уряд визначає, яка неворожа поведінка очікувалося від ворога. Коли в збройному конфлікті стикаються два угруповання - клани або партизанські загони - лідер групи вирішує, яка неворожа поведінка бажана. В обох випадках лідерами груп приймаються рішення щодо визначення цілей, методів і бажаного постконфліктного стану.

Тому є міфом, хоча і поширеним і зручним, що в збройній сутичці беруть участь держави або групи.

Рішення організувати збройний конфлікт, включаючи рішення припинити збройний конфлікт, приймається лідерами держави або групи [8].

Аналогічно, саме ворожі наміри ворожих лідерів повинні бути придушені, щоб збройне зіткнення було успішним. Члени груп або громадяни держави, можуть вплинути на рішення лідера, але придушуватися повинна ворожість саме верхівки. Якщо лідерство переходить до іншої людини або групи людей, то повинна бути пригнічена ворожість саме цієї групи. Інформаційна війна може допомогти відібрати ореол «обранців небес» у ворожих лідерів.

Найбільшим відкриттям, яке призвело до початку інформаційної ери, було розуміння того, що все в навколишньому світі може бути представлено у вигляді комбінації нулів і одиниць. Ці комбінації можуть бути передані в

електронному вигляді як дані і зібрані на приймальному кінці, утворюючи інформацію.

На думку Аркуілли і Ронфельдт, інформація - це щось більше, ніж вміст або зміст повідомлення. Швидше, інформація - це «будь-яке розрізнення, яке створює відмінність» [24]. Інформаційна війна - це форма конфлікту, в якій відбуваються прямі атаки на інформаційні системи як засіб для впливу на знання або припущення противника.

Інформаційна війна може проводитися як частина більшого і більш повного набору військових дій - мережевої війни (netwar) або кібервійни (cyberwar) - або виступати в якості єдиної форми ведення військових дій. Більшість видів зброї - слова, що використовується для опису смертельних і несмертельних засобів ведення збройного конфлікту - може бути застосована тільки проти зовнішніх ворогів. А кошти ведення інформаційної війни, хоча найчастіше і застосовуються проти зовнішніх ворогів, можуть бути використані і проти внутрішніх противників. Наприклад, держава або група зазвичай не використовує гармати або бомби проти своїх громадян або членів; тим не менш, засоби ведення інформаційної війни можуть бути використані, використовувалися, і будуть використовуватися як проти зовнішніх, так і проти внутрішніх ворогів. Інформаційна зброя в Третьому Рейху, наприклад, було всеспрямованим.

Інформаційна війна - це збройні дії, спрямовані проти будь-якої частини систем знань або припущень ворога. «Противник» - Це будь-який, чиї дії суперечать цілям лідера. Поза держави це може бути «образ ворога» або «не ми».

Всередині, ворогом може бути зрадник чи мандрівник, будь-хто, хто протистоїть або недостатньо підтримує лідера, який управляє коштами інформаційної війни. якщо члени групи не підтримують цілі лідера в ході бойових дій, внутрішня інформаційна війна (включаючи такі речі, як пропаганда, брехня, терористичні акти і чутки) можуть бути використані в спробі змусити їх бути більш лояльними до цілей лідерів.

Збройна сутичка і його зв'язок з тим, що ми знаємо або припускаємо.

Незалежно від того проти якого ворога вона оголошена, інформаційна війна має кінцевою метою використовувати інформаційні засоби для впливу (маніпулювання або атаки) на системи знання і припущень деякого зовнішнього ворога. В ході війни, наприклад, для зовнішнього ворога корисно знати, чи, принаймні, припускати, що інша держава або група об'єдналися проти нього. Інформаційна війна, яка ведеться як для того, щоб громадяни держави діяли узгоджено, так і для того, щоб зовнішні вороги вважали, що їх ворог воює з ними єдиним ладом, використовується для доведення цього знання до умов лідерів супротивника.

Слабкість знань і припущень

Системи знань - це системи, які створені і діють для виявлення верифікованих феноменологічних індикаторів або десігнаторів, трансляції цих індикаторів в сприйняту реальність, і використання цих первинних відчуттів для прийняття рішення і дій [19]. Системи знань організовуються відповідно до наукових принципів і підкріплюються науковим методом. Тобто, системи знань створені, щоб збирати емпіричні дані шляхом спостережень для висунення гіпотез, проводити тести, що підтверджують або відкидають ці гіпотези, і використовувати ці відкриття як основу подальших дій. Системи припущень - це такі системи, які прямо або побічно орієнтовані на використання як емпіричних даних у формі верифікованих спостережень, так і даних іншого сорту або недостовірних даних (кошмари, фобії, психози, неврози, і всі інші породження підсвідомості, і колективне несвідоме), які не підтверджуються, або які, по крайней мере, нелегко підтвердити.

Згідно Джону Бойду на процес або акт орієнтації (то що Бойд називає великим Про в циклі спостереження-орієнтація-прийняття рішення) також можуть вплинути генетичну спадковість або культурні традиції [21]. Тому орієнтація американських лідерів відрізняється від орієнтації, скажімо, японських або китайських лідерів. Орієнтація капіталістів і їх лідерів відрізняється від орієнтації соціалістів і їх лідерів.

На відміну від систем знань системи припущень є дуже індивідуальними.

Чому? Вони включають в себе елементи несвідомого і підсвідомого, про які їх носій може і не підозрювати.

Хоча метою інформаційного зброї і є уми лідерів ворога, буде помилкою думати про ворога як про один розумі. Насправді ворог - це багато окремих ворогів, і у кожного свій розум. Але це тільки злегка ускладнює проблему.

Наприклад, якщо ворог розосереджений, то окремі уми можуть бути атаковані окремо, використовуючи факт ізоляції в свою користь атакуючими. якщо ж ворог сконцентрований (і більше половини людей планети буде жити в містах до 2020 року і буде доступна впливу великого числа інформаційних атак), атаки повинні проводитися проти великої групи людей.

Навіть якщо так, метою збройної боротьби є придушити ворожі наміри лідерів та осіб, котрі приймають рішення. Це може бути зроблено за допомогою прямих атак, які впливають на знання або припущення лідерів або маніпуляцію з ними, або непрямих атак, спрямованих на знання або припущення тих, на кого лідери покладаються при прийнятті рішення. Лідерів та осіб, котрі приймають рішення, зазвичай легко виявити в будь-якій організації. Коли організація має засоби збройної боротьби, як правило у цій організації є ієрархічна характеристика.

Тому знання і припущення осіб, котрі приймають рішення, є ахіллесовою п'ятою ієрархій.

Системи знань, так як вони більш науковими, є менш схильними до культурним і ірраціональним чинникам, ніж системи припущень, але як системи знань, так і системи припущень входять до складу кожної системи прийняття рішення, де є люди.

Те, що відомо, включаючи методи, за допомогою яких воно стало відомо, може бути перевірено в зв'язку з чим-небудь ще і визначено як або вірне, чи неправильне, правдиве або помилкове. Гадки не піддаються всім цим перевіркам. Більш того, припущення не менш значущі, ніж емпірично отримані знання. Як знання, так і припущення впливають на прийняття людиною рішення. Так як метою збройної боротьби є вплинути на поведінку

супротивника шляхом впливу на прийняття ним рішення, інформаційні атаки повинні бути спрямовані як проти систем знань, так і проти систем припущень.

Якщо противник є коаліцію кількох центрів, в цій коаліції може існувати кілька систем припущень. Всі вони можуть бути переможені. Коаліція не обов'язково повинна бути групою держав або об'єднанням груп людей. Коаліція може бути утворена людьми всередині держави або будь-якої групи. Клаузевіц був прав, коли зробив висновок про потенційну слабкості союзів і коаліцій [24].

Більш того, лідери і особи, які приймають рішення, є більш вигідну ціль для прямих або непрямих атак.

Система - мета інформаційної війни може включати будь-який елемент в епістеміології противника. Епістеміологія включає в себе організацію, структуру, методи і достовірність знань. На стратегічному рівні мета кампанії інформаційної війни - вплинути на рішення супротивника, і як наслідок, на його поведінку таким чином, щоб він не знав, що на нього впливали [19]. Навіть тоді, коли цієї мети важко досягти, вона все-таки залишається кінцевою метою кампанії на стратегічному рівні. Успішна, хоча і незавершена інформаційна кампанія, проведена на стратегічному рівні, призведе до рішень супротивника (а отже і його дій), які будуть суперечити його намірам чи заважати їх виконання.

Успішна інформаційна кампанія, проведена на оперативному рівні, буде підтримувати стратегічні цілі, впливаючи на можливість ворога приймати рішення оперативно і ефективно. Іншими словами, метою інформаційних атак на операційному рівні є створення таких перешкод процесу ухвалення рішення ворогом, щоб супротивник не міг діяти чи вести війну координовано і ефективно. В інформаційній війні метою є гармонізація дій на оперативному рівні з діями на стратегічному рівні, щоб об'єднані, вони змушували супротивника приймати рішення, які б приводили б до дії, які допомагали досягати нам наших цілей і заважали б супротивнику домагатися виконання своїх.

На стратегічному рівні лідерів, продумує план ведення інформаційної кампанії, потрібно знати відповіді як мінімум на три питання:

По-перше, як і зв'язок інформаційної кампанії з глобальними цілями кампанії? По-друге, що ми хочемо, щоб ворожі лідери знали або передбачали по завершенню кампанії? Тобто, який бажаний епістеміологічний стан і отже критерій успіху операції? По-третє, які кошти ведення інформаційної війни є кращими для досягнення встановленого критерію успіху? Тобто як будуть пов'язані кошти з результатом?

На операційному рівні нашим лідерам також потрібно мати відповіді на ряд питань.

Чи буде заборонено атакувати деякі цілі і застосовувати деякі засоби в інформаційних атаках? Досяжний чи бажаний епістеміологічний стан взагалі і всюди, або тільки існують проміжні стани, досяжні в специфічних географічних районах, у специфічній послідовності, або в специфічних секторах інформаційних бойових дій. Крім того слід відповісти на питання про управління і сигналах. Крім того, лідерам на оперативному рівні потрібно знати, коли будуть завершені атаки і засоби, за допомогою яких буде переданий сигнал про припинення атаки. Це важливі питання, так як інформаційна зброя може викликати непрямий руйнування систем знань і припущень у атакуючих.

У гіршому випадку відповідь противника може включати контратаки проти дружніх інформаційних систем, що за великим рахунком не відрізняється від побічних руйнувань «вогневої підтримки».

Чим більше залежимо противник від інформаційних систем при ухваленні рішення, тим більше він уразливий до ворожого маніпулювання цими системами. Програмні віруси впливають тільки на ті системи, в яких є програми. Засоби радіоелектронної боротьби можуть бути застосовані тільки проти збройних сил, що використовують радіо і електроніку. Так як інформаційна війна може вестися проти всієї епістеміології ворога в цілому, то і примітивні суспільства уразливі в інформаційній війні. По-друге, індустріальні суспільства можуть придбати більшу частину їх телекомунікаційної структури у більш розвинених постіндустріальних суспільств.

У державах або групах з високим рівнем розвитку техніки набір цілей атак на стратегічному рівні дуже багатий: телекомунікації та телефонія, космічні супутники, автоматизовані засоби ведення фінансової, банківської та комерційної діяльності; енергосистеми; культурні системи; і весь набір обладнання та програм, на підставі яких ворог отримує знання. Стратегічні інформаційні системи в високотехнологічних державах часто дублюються на оперативному рівні. Всі вони уразливі для атаки. Інформаційна війна не повинна відкладатися до тих пір, поки ворожість не стане відкритою. Лідери противника не захочуть воювати, якщо вони припускають одне з наступного: що насильство - це погано, або що у них не буде союзників, або що на них будуть накладені санкції, що перешкоджають продовженню війни, або що їх індустріальна база не зможе забезпечити перемогу в тривалій війні, або що їхні збройні сили не готові.

Чим вище технологічні можливості держави і чим більше число його взаємодій з іншими групами (включаючи внутрішні групи) або державами, тим більше держава вразливе в інформаційній війні. Ця вразливість буде зростати в міру збільшення розмірів мереж або числа і обсягу транзакцій.

Демократії не є менш вразливими, ніж тоталітарні режими, хоча демократичні соціальні системи, такі як групи, можуть бути трохи більш стійкими до виведення з ладу. Але апарат управління її економікою вразливий. Банки, фінанси, торгівля, подорожі і управління повітряним рухом стають все більш залежними від інформаційної технології.

У міру того, як зростає залежність від інформаційних систем, збройні конфлікти, що організовуються терористами, релігійними екстремістами, ворожими бізнесменами, проти інформаційних систем становитимуть реальну загрозу. Інформаційна зброя в їх руках може бути направлено на енергосистеми або засоби зв'язку, які обслуговують кінцеву мету. Одночасні атаки на різні вузли можуть мати стратегічний ефект. Тобто вони можуть впливати на знання і волю лідерів.

3. ЗАСТОСУВАННЯ ГЛОБАЛЬНОЇ МЕРЕЖІ ІНТЕРНЕТ В ІНФОРМАЦІЙНИХ ВІЙНАХ

Інтернет-протиборства даний час Інтернет все активніше і масштабніше використовується в інтересах інформаційного протиборства сторін, які є учасниками різних конфліктів. Він надає широкі можливості в плані надання впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації).

Активне використання мережі Інтернет для ведення інформаційного протиборства обумовлено наявністю ряду її істотних переваг перед звичайними засобами і технологіями.

Оперативність. Розміщення і регулярне оновлення інформації на окремих сторінках, в Інтернет-виданнях і різного роду новинних розсилках, форумах і конференціях не вимагають значного часу на підготовку матеріалів в електронному вигляді. При цьому користувачі отримують її в режимі реального часу (на відміну, наприклад, від читачів періодичних видань). Крім того, цілеспрямований вплив на інформаційні ресурси протилежної сторони може здійснюватися не тільки в заздалегідь запланований час, а й у міру виникнення необхідності.

Економічність. Є наслідком залучення невеликої кількості персоналу і матеріальних засобів для вирішення поставлених завдань. Так, наявності мінімально підготовленого користувача персональної ЕОМ, підключеної до телефонної лінії, нерідко буває цілком достатньо. Крім того, застосування комп'ютерних технологій для виведення з ладу систем управління протилежної сторони в певних умовах може призвести до більш значного ефекту при значно менших витратах в порівнянні з використанням традиційних засобів (вогневого ураження, радіоелектронної боротьби).

Скритність джерела впливу. Як правило, акт агресії в глобальній мережі важко відрізнити від дії звичайних комп'ютерних хуліганів. Підготувати та провести кібератаку з використанням Інтернету може досить широке коло осіб -

від військових і розвідувальних структур іноземних держав до партизанських формувань, злочинців, промислових конкурентів, хакерів або просто озлоблених людей. Відстежити ж джерело досить складно [10].

Дистанційний характер впливу на комп'ютерні системи в різних регіонах світу. В оглядах порушень мережевої безпеки регулярно повідомляється про виявлені наслідки ефективних дистанційних впливів на комп'ютерні мережі різних країн. Так, навесні 2001 року було зафіксовано проникнення в комп'ютерну систему одного з каліфорнійських операторів, контролюючого підключення до електричних мереж в західній частині країни і керуючого розподілом навантаження на значній території штату. Напад почався 25 квітня, але було виявлено тільки через 17 днів. Розслідування показало, що атака здійснювалася з території однієї з провінцій Китаю через американські веб-сервери, розташовані в трьох містах США [15].

Масштабність можливих наслідків. Крім впливу на формування громадської думки, на позиції офіційних осіб, які беруть найважливіші рішення, використання глобальної мережі для деструктивних впливів може призвести до порушення нормальної роботи або тривалого виведення з ладу життєво важливих об'єктів і систем в окремих районах, країнах або регіонах. «Посадіть мене в кімнаті разом з 12 комп'ютерними фахівцями, і я завдам більше шкоди інфраструктурі противника, ніж бомбардувальник В-1 або весь 7-й флот» [7], - стверджує Френк Джонс, президент компанії «Кодекс систем», що займається розробкою програмної продукції в інтересах військових і розвідувальних структур.

Комплексність подачі інформації та її сприйняття. На Інтернет-сторінках розміщується як текстова, так і графічна інформація в найбільш зручному для сприйняття вигляді, а її обсяг може бути в багато разів більше, ніж у будь-якого друкованого видання, радіопередачі або телевізійної програми. Використання ж сучасних мультимедійних технологій, що дозволяють демонструвати документальні свідчення, фото- і відеоматеріали при спеціально підібраному супроводі (коментарі, музика), надає на налаштовувати спеціальне емоційний вплив.

Доступність інформації. Будь-який користувач може розмістити власну інформацію (нерідко безкоштовно) на серверах, зареєстрованих в інших державах, або організувати розсилання повідомлень по всьому світу. Такою можливістю, наприклад, скористалися оператори югославської радіостанції «B92» після застосування урядом перешкод для «глушіння» підготовлених ними програм, зробивши подальше радіозаглушення безглуздим.

Деякі напрямки використання глобальної комп'ютерної мережі Інтернет в інтересах інформаційного протиборства розглядаються нижче.

Поширення спеціально підібраною інформації (дезінформації). Воно здійснюється шляхом: розсилки електронних листів e-mail; організації новинних груп; створення сайтів для обміну думками; розміщення інформації на окремих сторінках або в електронних версіях періодичних видань та мережевого мовлення (трансляції передач радіо- і телестанцій).

Так, в ході конфлікту в Косово комп'ютерна мережа Інтернет використовувалася для здійснення комплексу заходів інформаційно-пропагандистського та психологічного характеру. Югославської стороною широко застосовувалася розсилання електронних листів. Поштові скриньки більше 10 тис. Користувачів, різних агентств новин і урядовців (в основному в США) регулярно заповнювалися посланням з описом результатів бомбардувань і ракетних ударів по цивільних об'єктах, числа жертв серед мирного населення, а також страждань пересічних громадян, примушуючи тим самим сумніватися в правильності офіційної пропаганди [17].

У свою чергу, дії НАТО вперше супроводжувалися найпотужнішою інформаційною підтримкою в Інтернеті, для чого використовувалося безліч висвітлювали військову операцію сайтів. Більшість з них було створено безпосередньо американськими фахівцями з комп'ютерних технологій або з їх допомогою. Протягом лише перших двох тижнів операції в Косово американське інформаційне агентство CNN підготувало понад 30 статей, розміщених потім у всесвітній мережі. В середньому в кожній з них близько 10 разів зустрічалися слова «біженці», «етнічні чистки», «масові вбивства». Про ретельну підготовку змісту публікацій говорить також той факт, що до складу

спеціальної групи, безпосередньо працювала в CNN, були включені п'ять військовослужбовців 3-го батальйону підготовки та поширення матеріалів 4-ї групи психологічних операцій (ПСО) ВС США.

Під час військової кампанії в Іраку ВС Сполучених Штатів також активно використовували глобальну мережу для надання інформаційно-психологічного впливу на супротивника. Так, на початку січня 2003 року було проведено широкомасштабну акцію за допомогою електронної пошти. Розсилалися послання на арабській мові іракським генералам із закликами не виконувати накази С. Хусейна. Крім того, в електронних повідомленнях, складених американськими військовими психологами, містилися звернення до громадян Іраку допомогти запобігти використанню зброї масового знищення. В електронних листах також звучав заклик позначати місцезнаходження складів хімічної, біологічної та ядерної зброї «світловими сигналами» [14].

Слід зазначити, що широкомасштабне адресне звернення до іракського військового керівництва - порівняно новий момент в психологічних операціях, що проводяться в даний час ЗС США. Вищим офіцерам внушалась думка про те, що «іракці зазнають величезних втрат, якщо не приєднаються до боротьби проти Саддама або, по крайней мере, не відмовляться піднімати зброю проти вторгнення».

Активно і цілеспрямовано використовують можливості Інтернету і чеченські сепаратисти для пропаганди своїх позицій, поширення дезінформації, збору коштів на свою підтримку і залучення нових найманців. Безліч сайтів, розміщених організаціями та приватними особами на серверах різних країн, містять статті «прочеченская» спрямованості, фото- і відеоматеріали з відповідними коментарями, закликами, а також посилання на повідомлення найбільших світових інформаційних агентств, в яких критикується політика Росії і її дії в регіоні . Багато сайтів дублюються на різних мовах.

Найбільш поширеним напрямком використання глобальної мережі в інтересах вищезгаданого протиборства є заміна інформаційного змісту сайтів, яка полягає в підміні сторінок або їх окремих елементів в результаті злому. Такі дії робляться в основному для залучення уваги до атакуючої стороні,

демонстрації своїх можливостей або є способом вираження певної політичної позиції. Крім прямої підміни сторінок широко використовується реєстрація в пошукових системах сайтів протилежного змісту за однаковими ключовими словами, а також перенаправлення (підміну) посилань на іншу адресу, що призводить до відкриття спеціально підготовлених протистоїть стороною сторінок.

Особливо слід виділити так звані семантичні атаки, які полягають у зломі сторінок і подальшому акуратному (без помітних слідів злому) розміщенні на них завідомо неправдивої інформації. Подібним атакам, як правило, піддаються найбільш часто відвідувані інформаційні сторінки, змістом яких користувачі повністю довіряють.

Ще одним напрямком використання Інтернету в інтересах інформаційного протиборства є виведення з ладу або зниження ефективності функціонування структурних елементів мережі. Найбільш часто вживаними способами зниження ефективності функціонування її окремих елементів є наступні:

По-перше, «бомбардування» мережі електронними листами. Даний спосіб вважається однією з форм «віртуальної блокади», оскільки відправка великої кількості електронних послань в одну адресу протягом короткого часу ускладнює або робить неможливим отримання (виділення) адресатом «легальних» листів із загального їх масиву, а іноді може привести і до порушення роботи обслуговуючих серверів. Так, під час конфлікту в Косово обидві сторони регулярно піддавали «поштової бомбардуванню» різні урядові організації. Скоординована розсилка американськими хакерами протягом декількох днів понад 500 тис. Листів привела до повного виведення з ладу урядового сайту Югославії. У той же час представник НАТО Джимі Ши відзначав, що їх поштовий сервер тривалий час отримував щодня понад 2 тис. Послань тільки від одного відправника.

По-друге, DOS-атаки, проведення яких по суті аналогічно технології масової розсилки електронних листів одному адресату і полягає в генерації величезної кількості звернень до вибраного сайту. Це призводить до

уповільнення роботи обслуговуючого сервера або повного припинення зовнішнього доступу до нього.

По-третє, впровадження комп'ютерних вірусів. У ведеться в мережі інформаційному протиборстві використовуються всілякі способи впровадження різних видів вірусів і їх модифікації. Розробляються спеціальні «бойові» різновиди комп'ютерних вірусів. Так, військове відомство Тайваню створило близько 1 тис. Подібних вірусів, які в разі кризової ситуації можуть вивести з ладу комп'ютерні системи КНР. Їх здатність проривати телекомунікаційну мережу «противника» була перевірена в ході навчань.

Таким чином, розвиток глобальної мережі Інтернет супроводжується все більш широким використанням наданих нею можливостей для здійснення інформаційного протиборства, зростанням координації, масштабів і складності дій її учасників, в якості яких виступають як держави або їх коаліції, так і окремі організовані групи, в тому числі терористичні . Об'єктом інтернет-атак все частіше стають інформаційні ресурси, виведення з ладу або утруднення функціонування яких може завдати протистоїть стороні значних економічних збитків або викликати великий суспільний резонанс.

ВИСНОВКИ

Наступ інформаційної ери призвело до того, що інформаційний вплив, що існував споконвіку у взаєминах між людьми, в наші дні все більш очевидно набуває характеру військових дій.

В даний час накопичений значний досвід наукових досліджень у галузі інформаційного протиборства та інформаційно-психологічних війн. Який би зміст у поняття "інформаційна війна" не вкладався, воно народилося в середовищі військових і позначає, перш за все, жорстку, рішучу і небезпечну діяльність, яку можна порівняти з реальними бойовими діями.

Військові експерти, які формулювали доктрину ІВ, чітко уявляють собі окремі її грані і види, стратегії і тактики. Громадянське ж населення поки не готове в силу причин соціального та психологічного характеру в повній мірі відчути всю небезпеку неконтрольованого застосування НКТ в інформаційній війні.

Інформація дійсно стала реальною зброєю. Вона йде вже в третьому поколінні. Сергій Гриняв, доктор технічних наук дає наступну класифікацію:

1-е покоління інформаційної війни - це РЕБ (радіоелектронна боротьба). Дротова, частотна, стільниковий зв'язок, підслухачкою, глушилки, блокування, перешкоди і т.д.;

2-е покоління інформаційної війни - це РЕБ плюс партизанська і контрпартизанських пропаганда. Так було в Чечні в 90-х. У сепаратистів-бойовиків були свої пропагандистські сайти в Інтернеті, вони поширювали газети і бойові листки, організовували інтерв'ю для співчуваючих їм західних журналістів. Контрпропаганда велася доступними федерального центру засобами як на території конфлікту і суміжних територіях, так і на більш широку громадськість.

3-е покоління інформаційної війни - це глобальна інформаційна війна, фахівці називають її так само "війною на ефектах". Інформаційна війни навколо подій в Південній Осетії - саме війна третього покоління.

В епоху інформаційного суспільства ключове значення набули ЗМІ, Інтернет-канали і контроль над інформпотоками. З представленого матеріалу очевидно, що Україна в цьому відношенні значно відстає від провідних країн світу. Для формування нового багатополярного світового порядку в Україні необхідно робити рішучі дії для прориву в інформаційній сфері і боротьбі із інформаційними війнами у практичному аспекті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Афанасьєв В. Соціальна інформація та управління суспільством. - М.: Знание, 2005, - 119 с.
2. Блек С. Паблик рилейшнз. Що це таке? М.: Наука, 2007, - 256 с.
3. Вершинін М.С. Політична комунікація в інформаційному суспільстві. М.: Ягуар, 2006, - 256 с.
4. Волковский Н.Л. История информационных войн. В 2 ч. Часть 1. / Н.Л.Волковский. СПб.: ООО «Издательство «Полигон», 2003.
5. Володин А.Г., Широков Г.К. Глобализация: истоки, тенденции, перспективы//Полис. №5. 1999.
6. Глобализация и мультикультурализм. Отв. Ред. П.С.Карабаев.М.: Изд-во РУДН, 2005.
7. Глоссон Р. Природа войны // Война и геополитика. Выпуск 3. Время мира. Новосибирск, 2003.
8. Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства. — Зарубежное военное обозрение. № 8, 2001.
9. Звіринців А.Б. Комунікаційний менеджмент: Робоча книга менеджера PR: 2-е вид., Испр. - СПб.: Союз, 2007, - 288с.
10. Информационная безопасность систем организационного управления. Теоретические основы [Текст]: в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А.Кузнецов, В.В.Кульба] ; Ин-т проблем передачи информации РАН. — М.: Наука, 2006.
11. Каландара К.Х. Управління суспільною свідомістю. Роль комунікативних процесів. М.: Наука, 2006, - 154 с.
12. Крутских А., Федоров А. Про міжнародної інформаційної безпеки. М.: Слово, 2008, - 234 с.
13. Малькова Т.В. Маси. Еліта. Лідер. М.: Яуар, 2006, - 232 с.

14. Масова інформація в радянському промисловому місті: Досвід комплексного соціологічного дослідження / Під загальною редакцією Б.А. Грушина, Л.А. Оконнікова. - М.: 2006, - 347 с.
15. Новиков, Д.А. Рефлексивные игры [Текст] / Д.А.Новиков, Г.А.Чхартишвили — М.: СИНТЕГ, 2003.
16. Панарин И. Н. Информационная война и геополитика [Текст] / И. Н. Панарин — М.: «Поколение», 2006.
17. Почепцов Г.Г. Інформаційні війни. М.: ВЦ Гарант, 2008, - 453 с.
18. Расторгуєв С.П. Інформаційна війна. М.: Наука, 2008, - 235 с.
19. Рютінгер Р. Культура підприємництва. - М.: Лідер, 2006, 672 с.
20. Танскотт Д. Електронно-цифрове суспільство. Плюси і мінуси мережевого інтелекту. М.: Прогрес, 2006, - 673 с.
21. Техніка дезінформації та обману. - М.: Слово, 2008, - 139 с.
22. Тоффлер Е. Третя хвиля. М.: Пале, 2007, - 458 с.
23. Фірсов Б. Телебачення очима соціолога. - М. Слово, 2008, - 418 с.
24. Хаббард Л.Р. Проблеми роботи. - СПб.: Знання, 2008, - 342 с.
25. Хейне П. Економічний образ мислення. - М.: Слово, 2006, - 457 с.