УДК 32.019.51:654.19

ОСНОВНІ ЗАСОБИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА ТА ІНФОРМАЦІЙНОЇ ВІЙНИ ЯК ЯВИЩА СУЧАСНОГО МІЖНАРОДНОГО ПОЛІТИЧНОГО ПРОЦЕСУ

І. М. Харченко,
к.т.н, доц.
С. О. Сапогов,
к.фіз.-мат.н.
В. М. Шамраєва,
д.політ.н., доц.
Л. В. Новікова,
к.ю.н., доц.
Харківський національний університет імені В.Н.Каразіна
kharchenko@karazin.ua

Останні тенденції розвитку сучасних міжнародних відносин обумовили і перехід від класичного міждержавного силового протистояння до протистояння в інформаційній сфері. Практичними засобами його реалізації є інформаційна зброя. Але розвиток сучасних технологій зробив її доступною значно ширшому колу гравців і сприяє їх залученню у процеси захисту інформації та досягнення інформаційної переваги. Основною метою даної публікації став ретроспективний аналіз основних засобів практичного ведення інформаційного протиборства та інформаційних війн як достатньо нового явища у міжнародних відносинах.

Ключові слова: міжнародні відносини, інформаційна війна, інформаційне протиборство, інформаційна безпека держави.

ОСНОВНЫЕ СРЕДСТВА ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА И ИНФОРМАЦИОННОЙ ВОЙНЫ КАК ЯВЛЕНИЯ СОВРЕМЕННОГО МЕЖДУНАРОДНОГО ПОЛИТИЧЕСКОГО ПРОЦЕССА

Последние тенденции развития современных международных отношений обусловили и переход от классического межгосударственного силового противостояния к противостоянию в информационной сфере. Практическим средством его реализации стало информационное оружие. Однако развитие современных технологий сделало его доступным более широкому кругу игроков и способствует их привлечению в процессы защиты информации и достижения информационного преимущества. Основной целью данной публикации стал ретроспективный анализ основных способов практического ведения информационного противоборства и информационных войн как достаточно нового явления в международных отношениях.

Ключевые слова: международные отношения, информационная война, информационное противоборство, информационная безопасность государства.

THE MAIN METHODS OF INFORMATION WARFARE AND INFORMATION WAR AS A PHENOMENON OF MODERN INTERNATIONAL POLITICAL PROCESS

The recent trends in the development of contemporary international relations have led to the transition from classical interstate military the confrontation to confrontation in the information sphere. Information weapons became A practical means of its implementation. However, the development of modern technology has made it accessible to a wider range of players and promotes their involvement in the protection of information and processes to achieve the benefits of information. The main purpose of the article is to analyse of the main ways of conducting practical information warfare and information warfare, as a fairly new phenomenon in international relations.

Keywords: international relations, information warfare, information warfare, information security of the state.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими або практичними завданнями. Проблематика інформаційних воєн достатньо широка та має кілька логічних підтем. Однією з них стала й інформаційна зброя. Нажаль сьогодні ще не сформовано чітких визначень та підходів до концепту «інформаційна зброя». Багато фахівців розходяться в оцінках, що саме вважати такою, а що відносити до новітніх але звичайних озброєнь. Тому необхідно продовжувати і далі наукову дискусію щодо визначення поняття інформаційна зброя та виокремлення її основних класифікацій.

Аналіз останніх досліджень та публікацій, в яких розглянута дана проблематика і на які спирається автор, виокремлення невирішених раніше частин загальної проблеми, яким присвячена дана стаття. Дана публікація спирається на дослідження іноземних політологів, таких як Т. Гарден, Р. Анжел [5, 6] та ін. Великий внесок у дослідження проблеми внесли і вітчизняні дослідники, такі як В. Богуш, О. Юдін, М. Рижков та ін. [1, 4] В той же час проблематику практичних засобів ведення війни в умовах формування інформаційного суспільства та особливо визначення концепту інформаційна зброя не можна вважати розкритою.

Мета та визначення завдань. Основною метою даної публікації став ретроспективний аналіз основних засобів практичного ведення інформаційно-

го протиборства та інформаційних війн як достатньо нового явища у міжнародних відносинах.

Виклад основного матеріалу дослідження. Інформаційна перевага є одним із центральних понять у сфері інформаційного протиборства. Вона являє собою здатність системи управління держави забезпечити стійкий процес своєчасного одержання достовірної інформації та доведення її до відповідних споживачів при одночасному отриманні можливості використання у своїх інтересах такої ж системи ймовірного противника або пониження ефективності роботи останньої. При цьому під такою системою розуміють особовий склад та компоненти збирання, обробки, аналізу, кореляції, зберігання в пам'яті ЕОМ, відображення на дисплеях, записи на магнітних та інших носіях інформації, систематичного оновлення та уточнення, розподілу за пріоритетністю, передачі інформації споживачам.

Для створення умов для досягнення інформаційної переваги необхідно вирішити п'ять взаємопов'язаних завдань. Перше завдання — створити інтегровану автоматизовану систему управління, зв'язку, розвідки та спостереження, що повинно значно підвищити фундаментальні можливості вирішення наступних завдань.

Другим завданням є забезпечення примусового циркулярного доведення до виконавців важливої інформації в реальному масштабі часу та отримання конкретної інформації за запитами виконавців із баз даних вищих інстанцій.

Третє завдання спрямоване на вирішення питань адекватного співробітництва у розподілі інформації, тобто на забезпечення командного складу штабів і військ за погодженою домовленістю необхідними засобами сполучення, отримання та розподілу інформації.

Після вирішення четвертого завдання збройні сили одержують можливість спільного та узгодженого сприйняття та відображення різними командними інстанціями реальної оперативної ситуації, що дає можливість полегшити прийняття рішень, що відповідали б реальній ситуації, організацію та підтримку взаємодії під час операції.

Вирішення п'ятого завдання, що полягає у можливості використання систем в інтересах радіоелектронної війни, зокрема усіх засобів боротьби з системами бойового управління противника, в цілому повинне дати можливість досягнення інформаційної переваги при проведенні інформаційних операцій за рахунок побудови та функціонування автоматизованих складних саморегулюючих систем.

Переходячи до аналізу інформаційної зброї, слід підкреслити, що до неї належить широкий клас засобів і способів інформаційного впливу на противника від дезінформації і пропаганди до засобів радіоелектронної боротьби [2, 3].

Інформаційну зброю від звичайної відрізняють: прихованість — можливість досягнення мети без видимої підготовки та оголошення війни; масштабність — можливість завдавати невиправні збитки, не визнаючи державних кордонів і суверенітетів, без обмеження простору в усіх середовищах; універсальність — можливість багатоваріантного використання країною, що нападає, проти як воєнних, так і цивільних об'єктів країни ураження.

Сфера застосування інформаційної зброї включає як воєнну галузь, так і інші галузі потенційного використання з метою:

• дезорганізації діяльності управлінських структур, транспортних потоків та засобів комунікації;

• блокування діяльності окремих підприємств та банків, а також цільових галузей промисловості шляхом порушення технологічних зв'язків та системи взаєморозрахунків і т.ін.;

• ініціювання техногенних катастроф на території противника через порушення управління технологічними процесами та об'єктами;

• масового поширення у свідомості людей певних уявлень, поведінкових стереотипів; виклик невдоволення або паніки, а також провокування деструктивних дій різноманітних груп.

Слід відзначити, що основними об'єктами застосування інформаційної зброї як у мирний, так і у воєнний періоди можуть виступати: комп'ютерні та телекомунікаційні системи, які використовуються при виконанні своїх управлінських функцій; воєнна інформаційна інфраструктура, яка виконує завдання управління військами та засобами збору і обробки інформації; інформаційні та управлінські структури економічних суб'єктів; засоби масової інформації, в першу чергу, електронні.

За галузями застосування інформаційну зброю можна поділити на інформаційну зброю воєнного та невоєнного призначення. Інформаційна зброя, використання якої можливе у воєнних умовах, включає засоби з такими функціями:

• ураження звичайними боєприпасами за цілевказівками засобів радіо та радіотехнічної розвідки;

• ураження високоточними боєприпасами — інтелектуальними боєприпасами з самостійним пошуком цілі та самонаведенням на її уразливі елементи;

• радіопридушення засобів зв'язку маскувальними завадами;

• створення завад імітації, синхронізацію в каналах передачі даних, що ініціюють функції перезапиту та дублювання повідомлень;

• придушення за допомогою засобів силової радіоелектронної боротьби;

• виведення з ладу радіоелектронних компонент за рахунок впливу великих рівнів електромагнітних або іонізуючих випромінювань;

• силовий вплив імпульсом високої напруги через мережі живлення;

• порушення властивостей середовища поширення радіохвиль (зрив короткохвильового радіозв'язку шляхом модифікації параметрів іоносфери);

• за допомогою спеціальних методів впливу на ЕОМ систем зв'язку;

• засоби генерації природної мови конкретної людини.

Особливу небезпеку інформаційна зброя становить для комп'ютерних систем органів державної влади, управління військами, фінансами, а також для людей при інформаційно-психологічному впливі на них з метою управління їх поведінкою. При цьому за результативністю інформаційна зброя прирівнюється до зброї масового ураження.

До інформаційної зброї, застосування якої можливе як у воєнний, так і у мирний час, можуть бути віднесені засоби ураження інформаційних комп'ютерних систем та засоби ураження людей.

Засоби ураження інформаційних комп'ютерних систем є сукупністю спеціально організованої інформації та інформаційних технологій, яка дає змогу цілеспрямовано змінювати (знищувати, спотворювати), долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, що застосовуються в ході інформаційної війни.

За метою використання така інформаційна зброя поділяється на інформаційну зброю атаки та інформаційну зброю забезпечення.

Інформаційна зброя атаки — це інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, обробляється і передається в інформаційно-обчислювальних мережах (ІОМ) і порушуються інформаційні технології, що застосовуються в ІОМ.

У складі інформаційної зброї атаки виокремлюють чотири основні види засобів інформаційних впливів: засоби порушення конфіденційності інформації; засоби порушення цілісності інформації; засоби порушення доступності інформації; засоби психологічного впливу на абонентів ІОМ. Застосування інформаційної зброї атаки спрямоване на зрив виконання ІОМ цільових завдань.

Інформаційна зброя забезпечення — інформаційна зброя, за допомогою якої здійснюється вплив на засоби захисту інформації об'єкта атаки. До складу інформаційної зброї забезпечення входять засоби комп'ютерної розвідки та засоби подолання системи захисту інформаційної системи.

Успішне застосування інформаційної зброї забезпечення дозволяє здійснювати деструктивні впливи на інформацію з використанням інформаційної зброї атаки.

За способом реалізації інформаційну зброю поділяють на три великих класи: інформаційна алгоритмічна зброя; інформаційна програмна зброя; інформаційна апаратна зброя.

Інформаційна алгоритмічна зброя — вид інформаційної зброї, до якого відносять: алгоритми, що використовують сполучення санкціонованих дій для здійснення несанкціонованого доступу до інформаційних ресурсів; алгоритми застосування санкціонованого програмного забезпечення і програмні засоби несанкціонованого доступу для здійснення незаконного доступу до інформаційних ресурсів.

До інформаційної програмної зброї відносять програми з потенційно небезпечними наслідками своєї роботи для інформаційних ресурсів мережі обміну інформацією. Програми з потенційно небезпечними наслідками — це окремі програми, які спроможні виконувати множину таких функцій:

• приховування ознак своєї присутності в програмно-апаратному середовищі мережі обміну інформацією;

• здатність до самодублювання, асоціювання себе з програмами і перенесення фрагментів в інші ділянки оперативної або зовнішньої пам'яті;

• руйнування (спотворення) кодів програм в оперативній пам'яті;

• збереження фрагментів інформації з оперативної пам'яті в окремій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);

• спотворення, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм або масивів даних, що уже знаходяться у зовнішній пам'яті;

• придушення інформаційного обміну в телекомунікаційних мережах, фальсифікація інформації в каналах державного й воєнного управління;

• нейтралізація роботи тестових програм і захисту інформаційних ресурсів.

Програми з потенційно небезпечними наслідками умовно поділяють на такі класи:

• (бойові) комп'ютерні віруси;

• засоби несанкціонованого доступу;

• програмні закладки.

Комп'ютерні віруси — це спеціальні програми, які здатні самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приєднання до них для наступного одержання управління та відтворення нових копій.

Після запуску заражених програм вірус може виконувати різні небажані дії, що порушують цілісність інформації та (або) режим роботи засобів обчислювальної техніки: псування файлів та каталогів, модифікування програмного забезпечення, спотворення результатів обчислень, засмічування або стирання пам'яті, створення завад при роботі ЕОМ.

Програми вірусів складаються в основному мовою програмування «асемблер» і при виконанні не створюють ніяких аудіовізуальних відображень у комп'ютерній системі.

Для бойових комп'ютерних вірусів принципове значення мають такі класифікаційні ознаки: об'єкт впливу (зараження); спосіб зараження об'єкта; принцип маскування; деструктивні можливості.

За видом об'єкта зараження комп'ютерні віруси поділяються на завантажувальні віруси, файлові віруси, завантажувально-файлові віруси, макровіруси. За способом зараження комп'ютерні віруси поділяються на резидентні і нерезидентні. За спосо-

бом маскування — на поліморфні віруси, віруси-невидимки та комбіновані віруси. За деструктивними можливостями — на безпечні віруси й віруси, що виконують деструктивні функції.

Особливістю комп'ютерних вірусів є їхня неспрямованість на конкретні програми та властивість самодублювання. Самодублювання програми з потенційно небезпечними наслідками — це процес відтворення програмою з потенційно небезпечними наслідками свого власного коду в оперативній або зовнішній пам'яті персональної ЕОМ.

Комп'ютерні віруси можуть розмножуватися, інтегруватися у програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити з ладу системи управління і т.ін.

Засоби несанкціонованого доступу належать до класу програм з потенційно небезпечними наслідками, які виконують такі функції:

• руйнування (спотворення) кодів програм в оперативній пам'яті;

• збереження фрагментів інформації з оперативної пам'яті в окремій ділянці зовнішньої пам'яті прямого доступу;

• спотворення довільним чином, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті;

• нейтралізація роботи тестових програм і систем захисту.

До засобів несанкціонованого доступу відноситься всіляке позаштатне програмне забезпечення МОІ, яке противник може використати для порушення цілісності операційної системи або обчислювального середовища. Часто цей тип програмного забезпечення використовується для аналізу систем захисту з метою їхнього подолання й реалізації несанкціонованого доступу до інформаційних ресурсів мереж обміну інформацією.

Відмітною ознакою засобів несанкціонованого доступу є наявність функцій подолання захисту.

Програмні закладки належать до таких програм з потенційно небезпечними наслідками, для яких обов'язковим є виконання таких функцій:

• руйнування (спотворення) кодів програм в оперативній пам'яті;

• збереження фрагментів інформації з оперативної пам'яті в окремій ділянці зовнішньої пам'яті прямого доступу;

• спотворення, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, що уже знаходяться у зовнішній пам'яті.

Виділяють декілька видів програмних закладок: троянські програми; логічні бомби; логічні люки; програмні пастки; програмні черв'яки.

До троянських програм належать програмні закладки, які мають законний доступ до системи, але виконують і приховані функції.

Впровадження троянських програм в автоматизовані системи управління противника здійснюється такими способами: використанням віддалених атак; створення програмних закладок в операційні системи та програмне забезпечення, що поставляються на експорт; агентурним шляхом.

Логічна бомба — це така програмна закладка, що здійснює зловмисні дії при виконанні низки певних логічних умов. Вноситься таємно в програмне забезпечення ЕОМ і виконується внаслідок збігу певних обставин або у визначений момент часу (часова бомба) з метою спотворення, знищення, модифікування або викрадення даних.

Логічний люк — механізм усередині операційної системи, який дозволяє програмі зловмисника одержати привілейовану функцію або режим роботи. Логічними люками можуть бути різноманітні помилки, що свідомо вводяться зловмисником у програмне забезпечення об'єкта.

Програмна пастка становить програмну закладку, яка використовує помилки або неоднозначність у програмному забезпеченні.

Програмний черв'як — це програмна закладка, яка маскується під системні засоби пошуку вільних ресурсів у мережі.

Усі програмні закладки можна також класифікувати відповідно до мети створення та за способом доставки в систему.

Як засоби інформаційної зброї програмні закладки мають достатньо специфічну форму реалізації процедури нападу, виконання функцій і дослідження систем захисту елементів обчислювального середовища.

Інформаційна апаратна зброя включає апаратні засоби, призначені для виконання функцій інформаційної зброї. Прикладом інформаційної апаратної зброї можуть бути апаратні закладки, які впроваджуються в ПЕОМ, що готуються на експорт, та їхнє периферійне обладнання. Апаратні закладки маскуються під звичайні пристрої мікроелектроніки і застосовуються для збирання, оброблення й передачі конфіденційної інформації.

Наприклад, так званий «Троянський кінь» створюється на основі певних логічних зв'язків в електронних колах апаратних засобів комп'ютерної техніки для автоматичного виконання несанкціонованих маніпуляцій за аналогією з програмною реалізацією «Троянського коня».

Інформаційна зброя, що належить до різних класів, може застосовуватися спільно, а деякі види інформаційної зброї можуть мати риси декількох класів.

Засоби впливу на людей та їхню психіку розрізняють залежно від мети їхнього застосування в психологічній війні. До таких цілей відносять: спотворення інформації, яку одержує політичне керівництво, командування та особовий склад збройних сил противника, та нав'язування їм фальшивої або беззмістовної інформації, яка лишає їх можливості

правильно сприймати події або поточну ситуацію та приймати правильні рішення; психологічне оброблення військ та населення; ідеологічні диверсії та дезінформація; підтримка сприятливої суспільної думки; організацію масових демонстрацій під фальшивими лозунгами; пропаганду та поширення фальшивих чуток; змінювання та управління індивідуальною і колективною поведінкою.

Поряд з використанням традиційних засобів (друковані та електронні ЗМІ) ідуть активна розробка та апробація спеціальних засобів впливу на людину як через ЗМІ, так і через комп'ютерні мережі: засоби інформаційно-психологічного впливу, психогенного впливу, психоаналітичного впливу, нейролінгвістичного впливу, психотронного впливу.

Висновки. На основі проведеного аналізу застосування інформаційної зброї в інформаційній війні можна скласти перелік особливостей, що характеризують основні риси застосування інформаційної зброї.

Низька вартість. На відміну від традиційних воєнних технологій, розробка інформаційної зброї не потребує значних фінансових ресурсів — достатньо мати досвід роботи в інформаційних системах і доступ у глобальні та відомчі мережі.

Відсутність традиційних кордонів. Відмінності між суспільним і особистим, воєнною і кримінальною поведінкою, а також географічні кордони, які історично складалися між націями, розмиваються зростаючим взаємозв'язком інформаційних інфраструктур.

Нові завдання перед органами розвідки. Неправильне розуміння ролі, можливостей і цілей інформаційної зброї знижує ефективність традиційної розвідувальної діяльності — необхідні нові форми розвідки, що концентруються на інформаційній стратегічній зброї.

Складність оцінки загроз і формування системи попередження. На даний час не існує систем попередження, які дозволили б відрізнити стратегічну атаку з використанням інформаційної зброї від інших форм діяльності в інформаційному просторі, включаючи шпіонаж і випадкові помилки.

Труднощі при створенні й підтримці коаліцій. Коаліції тільки збільшують уразливість їхніх учасників від інформаційної поразки.

Уразливість власних територій. Оскільки інформаційні технології не обмежені в географічному плані, то інформаційною зброєю можуть уражатися цілі як на віддаленому театрі воєнних дій, так і усередині країни.

Література:

1. Богуш В. М. Інформаційна безпека від А до Я / В. М. Богуш, А. М. Кудін. — К. : МОУ, 1999. — 456 с.

2. Гриняев С. Н. Национальная информационная стратегия как основа внешней и внутренней политики США в 21 веке. Защита информации / С. Н. Гриняев // Конфидент. — № 5. — 2002. — С. 26-31; № 6. — 2002. — С. 12-22.

3. Цыганков В. Д. Психотронное оружие и безопасность России. Серия «Информатизация России на пороге XXI века» / В. Д. Цыганков, В. Н. Лопатин — М. : СИНТЕГ, 1999. — 152 с.

4. Юдін О. К. Інформаційна безпека держави / О. К. Юдін, В. М. Богуш. — К. : Консум, 2005. — 576 с.

5. Angell R. N. The Great Illusion : A Study of Relation of Military Power to National Advantages / R. N. Angell — London, 2010 — 672 p.

6. Garden T. The Technology Trap : Science and the Military. / T. Garden — McLean, VA : Brassey's Defense Pubishers, 2009. — 238 p.