**Американська концепція інформаційних операцій**

Вперше термін «інформаційна війна/information warfare» було вжито Томасом Рона у звіті «Системи зброї і інформаційна війна», підготовленому ним в 1976 році для компанії «Боїнг». Автор, зокрема, вказав, що інформаційна інфраструктура стає ключовим компонентом американської економіки, але вона одночасно перетворюється на уразливу ціль як у воєнний, так і в мирний час. Публікація звіту Т. Рона послужила початком активної кампанії в ЗМІ.

Офіційно термін «information warfare» (інформаційна війна, інформаційна боротьба) було введено в обіг Міністерством оборони США після операції «Буря в пустелі» 1991 року.

У 1998 році Міністерством оборони США затверджено Об’єднану доктрину інформаційних операцій, в якій ***інформаційна війна*** визначається як комплексний вплив (сукупність інформаційних операцій) на систему державного та військового управління супротивника, на його військово-політичне керівництво, що вже у мирний час сприяв б прийняттю бажаних для сторони-ініціатора інформаційного впливу рішень, а під час конфлікту повністю паралізував функціонування структури управління супротивника.

Отже, боротьба відбувається в інформаційному середовищі.

*Інформаційне середовище* – це сукупність окремих осіб, організацій і систем, які збирають, обробляють, поширюють інформацію.

Інформаційне середовище включає три виміри:

* Фізичний
* Інформаційний
* Когнітивний

*Фізичний вимір* – це системи управління та відповідна інфраструктура, що дає змогу індивідам та організаціям проводити операції у повітрі, на землі, морі та космосі. Сюди відносяться комп’ютери, комунікаційні мережі та підтримуюча інфраструктура.

*Інформаційний вимір* – це середовище, де інформація збирається, обробляється, зберігається, поширюється, захищається. Сюди відноситься зміст та потоки інформації.

*Когнітивний вимір* включає свідомість осіб, які приймають рішення та цільової аудиторії. Це середовище прийняття рішень. Найбільш важливий вимір. Сюди відносяться сприйняття, емоції, обізнаність, розуміння.

За американською концепцією, інформаційна війна реалізується на двох рівнях: державному та військовому.

На державному рівні мета інформаційного протиборства полягає у послабленні позицій конкуруючих держав, порушенні системи державного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери суспільного життя, здійснення психологічних операцій, підривних та інших пропагандистських акцій.

На військовому рівні інформаційна війна є складовою частиною військових кампаній й спрямовані на досягнення інформаційної переваги шляхом впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації, інформаційних систем та інфраструктури.

Поступово військове керівництво США перестало використовувати в офіційних документах термін «information warfare», віддавши перевагу терміну «information operation».

В американській Доктрині інформаційних операцій 2006 року **інформаційна операція** визначається як інтегроване використання можливостей електронної боротьби (вплив на обладнання супротивника за допомогою спрямованих електромагнітних хвиль), комп’ютерних мережевих операцій (CNO), психологічних операцій (PSYOP), операцій з військової дезінформації та операцій безпеки (OPSEC) з метою здійснення впливу, порушення процесу прийняття рішень супротивником при одночасному захисті власного (рішення).

Інформаційні операції передбачають насамперед здійснення впливу на рішення і процес прийняття рішень.

Кінцевою стратегічною метою інформаційних операцій є стримування потенційного або явного супротивника чи інші цільові аудиторії від вживання дій, які шкодять національним інтересам держави.

**Психологічні операції** - заходи з поширення спеціально підготовленої інформації з метою впливу на емоційний стан, мотивацію й аргументацію дій, прийняття рішень й поведінку окремих керівників, організацій, соціальних або національних груп й окремих особистостей іноземних держав у сприятливому для країни-ініціатора та її союзників напрямку.

ПсО відіграє ключову роль у здійсненні ІО.

Згідно з Польовим статутом армії США, психологічні операції - це планова пропагандистська і психологічна діяльність, розрахована на іноземні ворожі, дружні або нейтральні аудиторії, з метою впливу на їхнє ставлення і поведінку у сприятливому напрямі для досягнення як політичних, так і військових національних цілей США.

***Пропаганда*** - це систематичне, цілеспрямоване поширення певних ідей, з метою здійснення впливу на думку, почуття і ставлення або поведінку цільових аудиторій з тим, щоб досягти прямих або непрямих вигод для країни, яка веде пропаганду.

***Психологічні акції*** включають використання ЗМІ та допоміжну діяльність (напр, демонстрація сили, мітинги, демонстрації тощо) у мирний і воєнний час, з метою підриву престижу і впливу супротивника у ворожих, нейтральних або союзних країнах і зміцнення свого впливу і престижу.

**Заходи з введення в оману/оперативне маскування** (Military Deception –MILDEC) – це заходи, призначені для навмисного введення в оману військового керівництва супротивника щодо військових можливостей, намірів та операцій, аби спонукати супротивника до дій, які сприятимуть досягненню поставлених цілей.

MILDEC грунтується на розумінні того, як командування супротивника мислить і планує дії та як використовує інформаційний менеджмент для підтримки своїх зусиль.

Американські спеціалісти розрізняють поняття дезінформація та психологічна операція. Об’єктами ПсО є групи людей, а дезінформації – певні особистості.

**Радіоелектронна боротьба** включає радіоелектронне придушення, радіоелектронний захист.

*Радіоелектронне придушення* (РЕП) полягає у порушенні або ускладненні функціонування електронних засобів супротивника шляхом випромінювання, відбиття електромагнітних, акустичних і інфрачервоних сигналів. РЕП здійснюється автоматично наземними, корабельними і авіаційними системами постановки перешкод.

*Радіоелектронний захист* передбачає такі дії, як захист своїх радіоелектронних засобів (РЕЗ) від перешкод, створюваних супротивником, і здійснення контролю (спостереження) за роботою РЕЗ союзників, з метою уникнення їхнього взаємного впливу один на одного.

**«Мережеві операції»** включають комп'ютерні мережеві атаки, мережевий захист та використання комп'ютерних мереж супротивника у своїх цілях.

*Комп'ютерні мережеві атаки* визначаються як дії, що реалізуються у відповідних мережах для пошкодження або знищення важливої інформації в комп'ютерах та комп'ютерних мережах або ж виведення з ладу самих комп'ютерів супротивника.

Під *мережевим захистом* розуміються заходи, що передбачають моніторинг та аналіз мережевих атак на комп'ютерні об'єкти Міністерства оборони США та захист від них.

**Безпекові операції** (OPSEC) - процес ідентифікації критичної інформації та подальшого аналізу дій, спрямованих на визначення даних, необхідних супротивнику для отримання точної інформації про сили і наміри союзників; заперечення критичної інформації супротивника про сили і наміри союзників; спонукання супротивника недооцінювати доречність відомої йому критичної інформації.

Планування безпекової операції передбачає реалізацію таких кроків:

1. ***Ідентифікація критичної інформації***: визначення інформації, необхідної супротивнику.

2. ***Аналіз загроз***: аналіз розвідувальних, контррозвідувальних та відкритих джерел інформації для виявлення потенційних супротивників планованої операції.

На цьому етапі потрібно відповісти на такі питання:

(a) Хто супротивник? (хто має намір та можливості вжити заходів проти планованої операції?)

(b) Які цілі має супротивник?

(c) Яка стратегія у супротивника? До яких дій може вдатись супротивник?

(d) Якою критичною інформацією володіє супротивник про операцію?

(e) Які розвідувальні можливості має супротивник?

3. ***Аналіз вразливостей***: аналіз кожного аспекту операції для виявлення індикаторів, які можуть розкрити критичну інформацію та порівняння цих індикаторів з розвідможливостями супротивника.

*Індикатори* – це дії та інформація з відкритих джерел, які можуть бути виявлені розвідкою супротивника і інтерпретовані певним чином, щоб отримати критичну інформацію.

(a) Які індикатори критичної інформації невідомі супротивнику можуть бути виявлені внаслідок дій в рамках операції?

(b) Які індикатори може використати супротивник для завдання шкоди військам?

4. ***Оцінка ризику***: визначення можливих заходів захисту для кожної вразливості; відбір конкретних заходів для реалізації, спираючись на результати оцінки ризиків.

OPSEC заходи можуть використовуватися, з метою попередити виявлення супротивником індикатора, забезпечити альтернативний аналіз індикатора та атакувати ворожу систему збору інформації.

*Типові питання на цьому етапі:*

* Які можуть бути ризики для ефективності операції у разі використання конкретного заходу OPSEC ?
* Які ризики виникнуть у разі невикористання заходів OPSEC?
* Які ризики виникнуть у разі провалу заходів OPSEC?

5. ***Застосування відповідних заходів безпеки****.* Під час впровадження вибраних заходів відстежується реакція супротивника та оцінюється ефективність заходів.

До OPSEC заходів відносяться диверсії, камуфляж/маскування, приховування намірів, введення в оману тощо.

MILDEC and OPSEC доповнюють один одного. MILDEC полягає у тому, щоб підштовхнути до неправильного аналізу і змусити супротивника дійти помилкових висновків. OPSEC передбачає заперечення достовірної інформації та запобігання вірної оцінки супротивником планів країни-ініціатора.

**Допоміжними елементами** інформаційних операцій є

* безпека інформації (Information Assurance, IA),
* фізична безпека (Physical security)
* фізична атака (Physical Attack) на критично важливі информационных структур противника і
* контррозвідка (Counterintelligence).

***Безпека інформації*** – це заходи щодо захисту інформації та інформаційних систем шляхом забезпечення їхньої доступності, цілісності, аутентичності, конфіденційності та непідробленості.

IO спирається на IA для захисту інфраструктури, аби розмістити інформацію для впливу на цільові аудиторії.

***Фізична безпека*** – фізичні заходи, спрямовані на захист персоналу, попередження неавторизованого доступу до обладнання, різним об’єктам, документам та захист їх від шпигунства, саботажу, пошкоджень і крадіжки.

Якщо безпека інформації передбачає захист електронної інформації та інформаційних систем, то фізична безпека полягає у захисті фізичних об’єктів, що містять інформацію та інформаційні системи.

***Фізична атака*** може бути використана на підтримку ІО як засіб атаки на системи управління супротивника аби вплинути на його здатність здійснювати управління і впливати на цільові аудиторії.

***Контррозвідка*** – це збір інформації та діяльність, спрямована на захист від шпіонажу, інших дій розвідки, саботажу або вбивств, замовлених або здійснених від імені іноземних урядів, іноземних організацій/особистостей або міжнародних терористичних груп.

Загалом, допоміжні компоненти IO мають військові цілі, відмінні від цілей ІО, але вони або діють в інформаційному середовищі, або впливають на нього.

**Література:**

1. US Joint Publication 3-13 Information Operations. - https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_13.pdf
2. Гриняев С. Информационное противоборство в современную эпоху. - http://psyfactor.org/infowar1.htm
3. Гриняев С.Н. Поле битвы - киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. – http://csef.ru/media/articles/461/461.pdf
4. Жуков В. Взгляды военного руководства США на ведение информационной войны. - http://pentagonus.ru/publ/22-1-0-175
5. Запорожець О.Ю. Інформаційне протиборство у зовнішній політиці США // Актуальні проблеми міжнародних відносин. - 2012. - Вип. 107(1). - С. 157-164.