ІНФОРМАЦІЙНА ВІЙНА, ЯК ФОРМА ВЕДЕННЯ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Васьковська А.О.

Національний авіаційний університет, Київ
Науковий керівник – Мартинюк Г.В., канд. тех. наук, доц.

Анотація. *На сьогодні постійно працюють над розробкою нових непомітних прийомів інформаційних війн, через що багатьом країнам необхідно постійно працювати над різними контрзаходами, щоб убезпечити себе від впливу таких війн. У доповіді представлено основні складові та форми інформаціних війн, проведено аналіз відмінностей між інформаційними та збройними війнами, запропоновано методи захисту від інформаціних війн.*

Інформаційна війна (ІВ) – це форма інформаційного протиборства, що включає управління інформаційно-комунікаційними технологіями (ІКТ) для досягнення конкурентної переваги перед суперником. Фактично – це маніпуляції інформацією з певною метою/без усвідомлення цілі, але в інтересах того, хто веде інформаційну війну. *Головним об'єктом* є громадська думка та свідомість кожної людини.

Інформаційна війна може мати різні форми [1]**:**

✔ телебачення, Інтернет та радіопередачі можуть бути затримані або викрадені для проведення дезінформаційної кампанії;

✔ логістичні мережі можна відключити;

✔ комунікаційні мережі ворога можуть бути відключені або підроблені, особливо в соціальних мережах;

✔ біржові операції можуть бути заблоковані

✔ використання безпілотників або веб-камер спостереження;

✔ управління комунікаціями.

Основні відмінності між інформаційною та збройною війнами.

1. Ризик для партії чи нації, що ініціює кібератаку, істотно нижчий, ніж при традиційній атаці.

2. Цивільні технології можуть бути націлені на кібератаки, а напади можуть бути розпочаті навіть через особисті комп'ютери чи веб-сайти. Таким чином, важче забезпечити контроль над цивільною інфраструктурою, ніж над фізичним простором.

3. Важко визначити, хто несе відповідальність за будь-яку конкретну подію, яка трапиться. Це питання загострюється у випадку з кібератаками, оскільки іноді практично неможливо простежити, хто вчинив напад та хто був його замовником.

Основна зброя інформаційної війни [2]:

1. *Збір інформації* – чим більше інформації є, тим вища обізнаність, що веде до кращої підготовки і до кращих результатів.

2. *Транспортування* інформації – це можливість передачі інформації в руки тих, хто її потребує

3. *Інформаційні маніпуляції* в контексті інформаційної війни - це зміна інформації з метою спотворення картини реальності противника.

4. *Порушення інформації, деградація та заперечення* – використовується для запобігання ворогу отримувати повну, правильну інформацію.

5. *Спуфінг* - це техніка, яка використовується для погіршення та спотворенння якості інформації, що надсилається ворогу.

6. *Джаммінг* - це техніка, яка використовується для досягнення відмови, яка включає перехоплення сигналів, що надсилаються при комунікаціях або між датчиком і ланкою.

7. *Перевантаження* - це техніка, яка застосовується для відхилення інформації противника як у військових, так і в цивільних умовах. Відправляючи данні у систему зв'язку противника, які занадто великі за об'ємом.Ця тактика називається атакою *"відмова в обслуговуванні"***.**

Захист від інформаційних війн. Захист від збору інформації сторонніми особами передбачає захист власної інформації від перехоплення та запобігання потрапляння інформації до засобів збору противника. Це передбачає використання шифрування, підроблення, введення шуму, джаммінгу та перевантаження для мінімізації збору інформації противником, знищення устаткування противника, знання мови противника, використання паролів [2].

Підводячи підсумки, можна зауважити, що ІВ як складна, так і традиційна. Вона включає багато різних стратегій, прийомів, зброї та оборонних засобів. У деякій літературі заперечується той факт, що частина тем, поданих у даній доповіді як інформаційна війна, не залишає важливих загроз національній безпеці, і автор схильний погодитися з такими твердженнями. Але, в той самий час інформаційні війни ще недостатньо розвинені і на сьогодні дуже багато війн ведеться не тільки в інформаційному полі, але й на фізичному полі з застосуванням армії.

Список використаних джерел

1. Я.М. Жарков Інформаційно-психологічне протиборство (еволюція та сучасність) / Я.М. Жарков, В.М.Петрик, М.М. Присяжнюк та ін.: військовий інститут КНУ ім.Т.Г,Шевченка – м. Київ, 2013 рік.

2. Information Warfare: What and How? / Megan Burns, 1999 рік [Електронний ресур], режим доступу https://www.cs.cmu.edu/~burnsm/InfoWarfare.html