Інформаційна зброя, об'єкти її ураження

Виконала: студентка IV курсу
3 групи
Коломієць Яна

Інформаційна зброя (ІЗ) – сукупність спеціалізованих (інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій і служб інформаційної інфраструктури в цілому або окремих її елементів.

До типів ІЗ можна віднести:

- засоби розвідки, отримання інформації з інформаційних, телекомунікаційних і подібних систем;
- засоби впливу на інформацію, яка обробляється в інформаційних системах, наприклад, на програмно-математичне забезпечення цих систем;
- засоби впливу на інформаційну інфраструктуру;
- засоби впливу на людину та суспільну свідомість у цілому.

Під інформаційним зброєю, в найзагальнішому вигляді, можуть розумітися засоби і методи ведення інформаційних війн, здійснення інформаційного тероризму і здійснення інформаційних злочинів.

Термін «зброя» в понятті інформаційна зброя дещо відрізняється від звичного нам поняття, яке зазвичай застосовується до традиційних видів озброєнь. Цей термін використовується скоріше для позначення негативного впливу засобів і методів на інтереси особистості, суспільства і держави в інформаційному просторі, а також для позначення руйнівної спрямованості зазначених засобів і методів по відношенню до інформаційної та комунікаційної структурі держави.

Об’єктами інформаційної зброї є: інформаційно-технічні та інформаційно-аналітичні системи, кожна з яких включає особистість; інформаційні ресурси; системи формування суспільної свідомості і думки, що базуються на засобах масової інформації і нарешті одним з основних об’єктів інформаційно-психологічного впливу зарубіжних держав є психіка і свідомість молоді, майбутнього нації.

Виходячи з аспектів інформаційної безпеки можна виділити два види інформаційної зброї:

1. особливим чином сформульована або оформлена інформація, яка спеціально призначена для психологічної або ідеологічної обробки населення, для підриву моральних і моральних засад суспільства;
2. спеціальні інформаційні або комунікаційні засоби, призначені для негативного впливу на інформаційну чи комунікаційну інфраструктури.

Другий вид інформаційної зброї являє собою досить новий вид. Інформаційна зброя цього виду включає в себе комп'ютерні віруси.

Комп'ютерні віруси являють собою програми, які приєднуються до звичайних прикладним або ігровим комп' ютерним програмам і здійснюють дії, спрямовані на порушення нормальної роботи комп'ютерної системи.

Комп'ютерні віруси характеризуються здатністю самостійно розмножуватися, поширюватися, активізуватися і функціонувати.

Відомі такі види комп'ютерних вірусів:

1) *Логічна бомба* – програмний вірус, який активізується в певний час або після того як виконана певна послідовність дій. Ці програми зазвичай знищують або перезаписують дані у всіх системах, до яких у них є доступ.
2) *Троянські коні* – програми, вбудовані в програмне забезпечення яке часто використовується комп’ютерним оператором. Ця програма скритно руйнує, видаляє, спотворює, або викрадає дані.
3) *Тимчасова бомба* – комп’ютерна програма, яка сконструйована таким чином, що починає діяти після того, як наступають певні умови.
4) *Комп’ютерний хробак* – самовідтворюються програми, які використовують дисковий простір і пам’ять і можуть, в кінцевому рахунку, вивести з ладу комп’ютерну систему.

5) Нове покоління вірусів – *віруси на генетичній основі*. Подібні віруси можуть самовідновлюватися або відтворюватися за образом біологічного організму. Кожне успішне покоління цих вірусів може відтворюватися із зростаючою комплексністю і власною імунною системою і з поліпшеною здатністю уникати виявлення і знищення. Сніффери – програми електронного стеження використовувані, в тому числі, для моніторингу комунікацій або комерційних угод, таких як переказ грошей або передача паролів для секретних інформаційних мереж. Використання снифферов найбільш поширений спосіб проникнення в мережі.

Інформаційну зброю також можна розділити на наступальну зброю, яке використовується для нападу або для заподіяння шкоди, захисну зброя, яка використовується для захисту від нападів і зброя подвійного призначення. Наступальна зброя включає в себе насамперед комп'ютерні віруси. Захисне зброя включає в себе шифрування, аутентифікацію, системи контролю доступу, мережеві екрани, антивірусне програмне забезпечення, пристрої перевірки функціонування системи, програми відстеження проникнень в систему.

Інформаційна зброя застосовується для надання інформаційного впливу, що може бути *інформаційно-технічних* або *психологічним.* Інформаційно-технічне вплив здійснюється переважно з метою порушення роботи й виведення з ладу телекомунікаційних систем та електронних баз даних.

Вплив інформаційного зброї на окремі групи людей організовується головним чином у рамках психологічної війни. Так, передбачається використання інформації з метою впливу на людську психіку, тобто для надання певного психологічного впливу, здатного призвести до зміни поведінки об'єкта в потрібному напрямку. На думку деяких американських фахівців, існує кілька форм психологічної війни: операції проти населення, військ і командування збройних сил противника, а також культурна експансія.

Отже, основними способами і методами застосування інформаційної зброї можуть бути:

1. Нанесення збитків окремим фізичним елементам інформаційної інфраструктури (руйнування мереж електроживлення, створення перешкод, використання спеціальних програм, що стимулюють виведення з ладу апаратних засобів, а також біологічних і хімічних засобів руйнування елементарної бази);
2. Знищення або пошкодження інформаційних, програмних і технічних ресурсів противника, подолання систем захисту, впровадження вірусів, програмних закладок і логічних бомб;
3. Вплив на програмне забезпечення та бази даних інформаційних систем і систем управління з метою їх спотворення або модифікації;
4. Вплив на комп’ютерне обладнання бойової техніки і озброєнь з метою виведення їх з ладу;

5. Загроза або проведення терористичних актів в інформаційному просторі (розкриття і загроза оприлюднення або оприлюднення конфіденційної інформації про елементи національної інформаційної інфраструктури, суспільно значущих і військових кодів шифрування, принципів роботи систем шифрування, успішного досвіду ведення інформаційного тероризму тощо);
6. Захоплення каналів ЗМІ з метою поширення дезінформації, чуток, демонстрації сили та доведення своїх вимог;
7. Знищення і придушення ліній зв'язку, штучна перевантаження вузлів комутації;
8. Вплив на операторів інформаційних і телекомунікаційних систем з використанням мультимедійних та програмних засобів для введення інформації в підсвідомість або погіршення здоров'я людини;

Дякую за увагу !