УДК 004.056.53

Вакуленко Р.В.
Кіровоградський національний технічний університет

Огляд та аналіз методів протидії інформаційним впливам супротивника в умовах інформаційної війни

Інформація на сьогодні стала одним з найнебезпечніших видів зброї. Інформація має досить значний вплив на маси, тобто за умови вдалого маніпулювання свідомістю мас можна досягти практично будь-якої мети: знищити опонента, прибрати з дороги конкурентів чи розпалити війну. Руйнівна потужність інформаційно-психологічного впливу в сучасних умовах настільки велика, що ставить під сумнів не лише незалежність переможеної держави, але і сам факт існування її народу як національної спільноти.

Першим використав термін «інформаційна війна» американський експерт Томас Рона в звіті, який він підготував у 1976 році для компанії Boeing, і який мав назву "Системи зброї і інформаційна війна". Т. Рона вказав, що інформаційна інфраструктура стає ключовим компонентом американської економіки. У той же самий час, вона стає і дуже вразливим місцем, як у воєнний, так і в мирний час. Під поняттям «інформаційна війна» розуміють сукупність методів та способів цілеспрямованого впливу суб'єктів-агресорів в умовах інформаційної відкритості на соціальні відносини (відносини людей між собою, відносини в суспільстві та державі), інформаційні ресурси, інформаційно-аналітичні та інформаційно-технічні системи, системи формування масової свідомості та психіки окремої людини, з використанням усіх властивостей інформації, інформаційних ресурсів та новітніх інформаційно-телекомунікаційних технологій з метою послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Розвиток процесу інформатизації суспільства і масштабне застосування новітніх інформаційних технологій в різноманітних автоматизованих системах управління усіх сфер діяльності людства, в тому числі і у воєнній сфері, а також створення електронних державних ресурсів щодо діяльності різних міністерств та відомств держави і органів виконавчої влади, висувають вимоги до захисту державної інформації від її втрати, несанкціонованого доступу до неї або внесення хибної інформації до державних електронних ресурсів та зменшення можливості інформаційного впливу на різноманітні державні системи управління як в мирний час, так і під час бойових дій в особливий період.

В інформаційній війні виділяються три основних мети: контроль інформаційного простору і забезпечення захисту своєї інформації від ворожих дій; використання контролю над інформаційним простором для проведення інформаційних атак на ворога; підвищення загальної ефективності збройних сил шляхом повсюдного впровадження військових інформаційних функцій. Можна виділити такі методи протидії інформаційним війнам та методи захисту інформаційного простору:

- пряме спростування;
- встановлення та знешкодження потенційних каналів просочування інформації;
- непряме спростування (наприклад, вказати на сумнівність джерела інформації; абсурдизація звинувачень; прив'язка джерела інформації до будь-якої негативної події; введення ще одного негативного факту, який легко піддається спростуванню);
- відвертання уваги. Варіантами можуть бути: відвертання ресурсів противника на інший об'єкт шляхом перенаправлення його на

іншу діяльність (наприклад на відбиття інформаційної атаки на нього або на його протеже); введення в інформаційний простір нового сенсаційного повідомлення та відвертання уваги аудиторії на нову сенсацію; відвертання уваги аудиторії на малозначний факт у рамках поточної проблеми (концентрація уваги аудиторії на не принципових для вас моментах у рамках озвученої супротивником проблеми);

- мовчання у відповідь;

- мінімізація впливу (наприклад, акцентування на тому, що в повідомленні вказано на деякі правдиві події);

- дискредитація (умисні дії, спрямовані на підривання авторитету, іміджу і довіри до джерела негативної інформації). Варіантами можуть бути: обнародування компромату; обнародування віртуального компромату; негативна похвала (така дія має на увазі публічну похвалу об'єкту дискредитації, специфіка полягає в тому, як похвалили або хто похвалив, якщо похвала виходить від негативного у сприйнятті аудиторії об'єкту, то вона матиме також негативний характер); невмотивоване освистування (масове висловлювання негативного судження з приводу інформації або її джерела); громадське обурення (метод, близький до невмотивованого освистування, але зі зверненням до інших соціальних почуттів аудиторії);

- розмиття негативу (генерація нейтральної або позитивної інформації про об'єкт в об'ємах, що перевищують об'єми негативної інформації;

- доведення до абсурду (спосіб, що ґрунтується на виробленні імунітету у аудиторії до негативу про об'єкт).

В залежності від виду операції, що проводиться, інформаційна війна має відповідні складові, а саме: захист своїх соціальних та інформаційних систем від інформаційних засобів впливу противника; боротьба з державними системами управління противника різного призначення; війна в області політичної та економічної інформації; психологічна війна; комп'ютерна війна; кібернетична війна.

Врахування методологічних основ ведення інформаційної війни в сучасних умовах, визначення напрямів застосування інформаційних засобів та аналіз їх впливу на державні системи управління та різні соціальні структури, вивчення особливостей національної культури противника - це підґрунтя при розробці нових методів захисту своїх інформаційно-технічних і соціальних систем від інформаційної зброї противника та послаблення його інформаційного впливу при веденні інформаційної війни і як наслідок цього здобуття перемоги у війні.

Враховуючи надвисокий ступінь небезпеки, що несуть своєю діяльністю суб'єкти інформаційних війн усім державам (зокрема їх органам державної влади), державним структурам та міжнародним організаціям необхідно виробити відповідну нормативно-правову базу з урахуванням усіх можливостей сучасних інформаційно-телекомунікаційних технологій; звернути першочергову увагу на вироблення та розвиток інформаційно-телекомунікаційних технологій у сфері державного управління, підвищення здатності органів державної влади і місцевого самоврядування до використання ефективних технологій управління та організацію конструктивної взаємодії з громадськістю; звернути увагу на недостатній рівень підготовки кадрів в галузі створення та використання інформаційно-телекомунікаційних технологій та розробити низку заходів щодо підвищення зазначеного рівня.

Список використаних джерел

1. *Шаравов И. К вопросу об информационной войне и информационном оружии // Зарубежное военное обозрение – 2002. – Вип. №10. – С. 3-5.*
2. *Кормич Б. А. Правові засади політики інформаційної безпеки України : монографія / Б. А. Кормич. – Одеса : Юридична література, 2003. – 472 с.*
3. *Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К.: КНТ, 2006. – 280 с.*