

***ЦАРЬОВА Ірина Валеріївна,**
завідувач кафедри мовної підготовки,
доктор філологічних наук, професор,
Дніпровський державний університет
внутрішніх справ*

ЛІНГВАЛЬНА РЕПРЕЗЕНТАЦІЯ КОНЦЕПТУ «ІНФОРМАЦІЙНА АГРЕСІЯ»

У науковій літературі є значна кількість різноманітних інтерпретацій і трактувань феномена «інформаційна агресія». Це поняття тісно переплітається з терміном «інформаційна протидія». Тому є предметом досліджень цілої низки наук.

Характеристики інформаційної війни варіюються в дуже широкому діапазоні: пропагандистська діяльність, політичні технології, що застосовуються різними угрупованнями під час політичної боротьби; протиправні дії в інформаційних мережах, пов'язані з розкраданням, спотворенням або знищенням інформації (хакерська активність), порушення працездатності інформаційних систем.

У результаті цифровізації джерел інформації стає дедалі

більше. З одного боку, вона стала доступною, з іншого, у доступі опинилося багато зайвого, іменованого «інформаційним сміттям» – псевдонаукові «факти», непотрібні добірки фото, фільмів тощо, спам, вірусна реклама, тобто непотрібна або неперевірена інформація. Відбувається сенсорне перевантаження людини – інформація передається таким способом, щоб абсолютно забити інформаційні канали [2]. Інформаційний простір стає зашумленим, і людина не може нічого навіть розібрати. Поглинання інформації не завжди здійснюється свідомо, при цьому все, що людина споживає в інформаційному плані (зі своєї волі чи не по своїй – неважливо), стає частиною її особистості.

Усі наші бажання інформаційно зумовлені. Інформація не просто передається людині, а стає засобом маніпуляції її свідомістю, наприклад, коли з певних питань дають уже готові думки в ЗМІ тощо. Подібним чином відбувається вплив на бажання і потреби. Прикладом цьому можуть слугувати різного роду психологічні «хитрощі», які застосовують магазини для збільшення продажів, ретельно продумана реклама тощо. Усе це

подібно до приманки, на яку потенційний покупець повинен «клянути», причому не всі й не відразу це помічають.

Важливим складником інформаційної війни є семантичні атаки (semantic attacks) [3], спрямовані на введення противника в оману шляхом впливу на інформацію противника. Під час семантичної атаки, на відміну від хакерської атаки, комп'ютерна система працює абсолютно правильно, але рішення, які вона видає, неправильні. Семантична атака спрямована на «органічуття» комп'ютерної системи, яка контролює будь-який процес за допомогою датчиків. Обдурити ці датчики або інші засоби введення – значить вивести систему з ладу, нічого в ній не порушивши. Принцип семантичної атаки може бути розглянутий не тільки у зв'язку з комп'ютерними мережами, а і як ефективний інструментарій із впровадження інформації з метою зміни в бажаному напрямком думок, поглядів, настроїв, ціннісних орієнтацій, а також масових настроїв і суспільної свідомості загалом.

Багато організацій вибудовують власні системи інформаційної безпеки, проводять перевірки та аналіз

захищеності даних. Це стосується і персональних даних клієнтів, персоналу, і інформації про поточну діяльність, фінансовий стан. Зазвичай до реалізації заходів захисту належать організаційні заходи, наприклад, призначення відповідальних за інформаційну безпеку осіб, розробку правил та інструкцій для користувачів, впровадження політики резервного копіювання тощо. Сучасні організації використовують вимоги міжнародних стандартів для побудови систем менеджменту інформаційної безпеки та використовують найкращі світові практики.

Історичний досвід, особливо реалії сьогодення, довели, що воєнні протистояння паралельно супроводжуються агітаційними і пропагандистськими діями через усі види ЗМІ, які виступають необхідною умовою досягнення мети у військових операціях. Факт війни – це і факт наявності певного важкого психологічного стану у свідомості людей, що ставить на перше місце розв'язання завдань, спрямованих на зміну, маніпулювання, одним словом, управління нею [1, с. 41].

Тут доречно окремо розглянути таку важливу форму безпеки, як інформаційна. Треба зазначити, що ідеї

інформаційного суспільства, які беруть свій початок у 60-х рр. XIX ст., не тільки змінили структуру, а й збагатили зміст усієї концепції безпеки. Високий рівень інформатизації всіх сфер життя заклав підґрунтя для осмислення нових реалій, що виникли внаслідок зростання загроз і небезпек. Не менш важливо визначити канали негативного інформаційного впливу: боротьба із системами управління, інформаційно-розвідувальні операції, електронна боротьба, «хакерська боротьба» (інформаційний кримінал), економічна інформаційна війна, «кібернетична» і «мережева» боротьба (зокрема інформаційний тероризм), інформаційно-психологічна боротьба. Інакше кажучи, дезінформування, цілеспрямоване розповсюдження і маніпулювання спотвореною інформацією, дії, що знищують інформаційні бази, – це безпосередні загрози інформаційній безпеці.

В інформаційному суспільстві будь-яка сфера – потенційний об'єкт негативних інформаційних впливів. Фахівці вважають, що «об'єктом державної інформаційної політики може стати будь-який компонент або сегмент інформаційно-

психологічного простору, зокрема масова та індивідуальна свідомість громадян, соціально-політичні системи і процеси, інформаційна інфраструктура, інформаційні ресурси, психологічні ресурси» [4].

Сучасна «інформаційна агресія» – це глобальна проблема, розв’язання якої потребує тісної та ефективної співпраці всіх країн. Технології розвиваються в такому темпі, що за ними не встигають не тільки юристи, а й політики. І це об’єктивний розвиток людства.

Список використаних джерел:

1. Царьова І. В. Сучасний дискурс інформаційної війни. «Південний архів» (філологічні науки). 2023. Вип. ХСV. С. 39-44.
2. Tsareva I. Maksymenko O., Kalko R. Philosophical aspect of information warfare. *Philosophy, Economics and Law Review*, Vol. 4, No. 1. 2024. P. 57-66.
3. Libicki M. C. What is Information Warfare? Washington : National defense univ. 1995.
4. Rona T. P. Weapon Systems and Information War. Seattle, WA, 1976 : Boeing Aerospace Co.