Чукут С.А. (м.Київ)
svchukut@gmail.com

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УМОВАХ МЕРЕЖЕВОЇ ВІЙНИ

Наразі в Україні збільшується кількість прихильників ідеї впровадження електронного урядування. З кожним роком зростають вимоги до: якості надання послуг, можливості отримання і доступу до інформації органів державної влади і місцевого самоврядування, залучення громадян до процесу прийняття управлінських рішень тощо. Всі ці питання безумовно є актуальними і необхідними, особливо враховуючи прагнення до інтеграції в Європейський Союз. Позитивних змін в цьому напрямку є достатньо - від створення влітку 2014 року Державного агентства з розвитку електронного урядування до розробки проекту «Зеленої книги розвитку електронного урядування в Україні», презентованої 17 листопада 2014 р.

Однак, те щоб ще рік тому сприймалося як безсумнівна річ і насправді необхідні кроки щодо подальшого розвитку електронного урядування в Україні, в умовах сьогоднішньої військової агресії з боку Росії, не є зовсім однозначним.

Україна наразі перебуває в стані війни. Цю війну можна визначити як мережеву. Як зазначає російський ідеолог мережевої війни О. Дугін [1], сутність мережевої війни полягає у зруйнуванні фундаментальних уявлень людей про сутність їхньої культури, суспільства та держави, для того щоб викликати страх, дезорієнтувати людей та внести хаос у їхню свідомість. Внаслідок чого здійснюється переорієнтація, а потім знищення традиційних духовних і культурних цінностей народу. Метою мережевих війн є встановлення абсолютного контролю над всіма учасниками історичного процесу у світовому масштабі. Це можливо досягнути за допомогою інтеграції зусиль з чотирьох напрямів: фізичного, інформаційного, інтелектуального та соціального.

Бойові одиниці, система зв’язку, інформаційне забезпечення операції, формування громадської думки, дипломатичні кроки, соціальні процеси, розвідка і контррозвідка, етнопсихологія, релігійна і колективна психологія,

економічне забезпечення, академічна наука, технічні інновації тощо – це все взаємозв'язані ланки єдиної мережі, між якими має здійснюватися постійний обмін інформацією. Інформаційна складова відіграє провідну роль у встановленні контролю над державою, яку прагнуть завоювати. Головна мета – зібрати якнайбільше різноманітної інформації з різних джерел, а потім опрацьовуючи її за відповідним алгоритмом, прийняти рішення необхідні для перемоги. У мережевих війнах не є головною умовою безпосередня пряма окупація чи анексія території - достатньо встановити над нею мережевий контроль.

Росією у війні з Україною використовуються не лише «офіційні» засоби пропаганди – російські засоби масової інформації - телебачення, радіомовлення, он-лайн видання, але й розгалужена мережа різноманітних громадських організацій, груп за інтересами тощо, які поширюються в соціальній мережі «Вконтакті» і кількість їх учасників щоденно збільшується.

У запропонованому проекті для обговорення «Зеленої книги з електронного урядування в Україні» зазначається, що «доступ громадян, громадських організацій та бізнесу до публічної інформації, даних, якими володіють органи влади стосовно них, та можливість автоматизованої обробки відкритих даних з державних інформаційних ресурсів є обов'язковими елементами сучасної демократичної держави, а інформаційно-комунікаційні технології дозволять зробити цей процес максимально зручним. Слід розвивати такі інструменти електронної демократії як збір підписів та надсилання петицій на підтримку ініціатив громадян, звернення, консультації та анкетування, електронне голосування тощо.» [2]

Ці питання дійсно є вкрай необхідними для розвитку електронної демократії, однак в умовах мережевої війни, що ведеться проти України, вони можуть мати зовсім протилежний ефект. Прикладом цього є нещодавно проведене у Франції найбільш впливовим виданням Le Figaro опитування громадян щодо продажу Росії «Містралів» [3]. Дослідження стало предметом маніпулювань завдяки масштабному автоматичному голосуванню. Так, із 260

тис. нібито опитаних читачів 180 тис. належало користувачам IP-адрес (ідентифікаційний номер комп'ютерної системи), які мали ознаки роботизованих систем, що розсилають спам. Більшість таких систем мали російську прописку. І хоча технічні працівники намагалися використати відповідні фільтри для блокування спаму, це не завадило шахраям сфальсифікувати результати опитування.

Особливо небезпечним без необхідного захисту є запровадження електронної взаємодії між органами влади і органами місцевого самоврядування. Слід врахувати, що частина іт-компаній, яка може бути залучена до цього процесу, може мати так званий «російський слід». І це не дивно, тому що за часів попередньої влади в Україні активно просувалися саме російські іт-компанії.

В зоні особливого ризику - запровадження електронних послуг, яке потребує створення національної системи електронної ідентифікації. І заслуговує на особливу увагу захист і наповнення різноманітних баз даних, які створюють органи державної влади.

Наразі питань, більше, ніж відповідей. Як зберегти баланс між безпекою держави і захистом приватності, розвитком електронної демократії і перемогою в мережевій війні?

Таким чином, основне завдання для нашої країни використати переваги електронного урядування для перемоги в цій війні і, водночас, захистити найбільш вразливі його складові від іноземного втручання. У даному випадку, краще рухатися повільніше, але у правильному напрямку.

Використані джерела:

1. Сетевые войны. Аналитический доклад А.Дугина при участии В.Коровина и А. Бовдунова. Режим доступа:

http://www.dynacon.ru/content/articles/2319/

2. Зелена книга з електронного урядування в Україні (проект). Режим доступу: http://etransformation.org.ua/2014/11/17/318/

3. Россияне пытались сфальсифицировать опрос Le Figaro относительно

«Мистралей».

Режим доступа: http://www.ukrinform.ua/rus/news/rossiyane_pitalis_sfalsifitsirovat_opros_le_figaro_otnositelno_mistraley_1685395