УДК 351.82

Чукут С.А.

Національний технічний університет України «Київський політехнічний інститут»

ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УМОВАХ МЕРЕЖЕВОЇ ВІЙНИ

Розглянуто сутність та особливості ведення мережевої війни в Україні. Визначені найбільш вразливі складові електронного уряду і електронної демократії. Запропоновані першочергові кроки уникнення негативного впливу мережевої війни на процес впровадження електронного урядування в Україні.

ВСТУП

З кожним роком кількість прихильників впровадження електронного урядування в Україні збільшується. Водночас 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. На рівні керівництва країни відбувається усвідомлення необхідності впровадження електронного урядування, розвитку його основних складових. Особливо підкреслюється важливість врахування досвіду Європейського Союзу в цій сфері, а також потреба у злагодженій дії усіх гілок влади на цьому шляху.

Однак, перш ніж визначати першочергові кроки щодо подальшого впровадження електронного урядування в Україні, необхідно проаналізувати умови, в яких буде відбуватися цей процес.

Ще рік тому, у 2013 році, почали згортатися процеси розвитку електронної демократії на тлі подій, пов’язаних з революцією Гідності. Особливо це стало показовим з прийняттям так званих «драконівських» законів 16 січня 2014 року, сутність яких полягала в обмеженні права громадян на участь в процесах прийняття управлінських рішень, блокуванні розвитку громадянського суспільства, обмеженні свободи мирних зібрань тощо. Одночасно приділялася більша увага впровадженню елементів електронного уряду, які б допомагали державі контролювати громадянське суспільство як на рівні об’єднань громадян, так і на особистому. Особливо активно органи державної влади почали формувати різноманітні реєстри і бази персональних даних без визначення відповідальних осіб за їх збереження.

Після розстрілів на майдані 18-20 лютого 2014 року та подальшої втечі Януковича, Україна опинилася в зовсім іншій реальності й перед новими викликами, які обов’язково слід врахувати при впровадженні електронного урядування в нашій країні. Мережева війна, елементи якої почали закладатися після 2004 року і більш активно поширюватися в 2010-2011 рр., в 2014 році окреслилася як найбільша загроза для національної безпеки України і лише наразі набирає свої оберти.

ОСНОВНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В дослідженні за основу визначення сутності мережевої війни та її основних складових покладено аналітичну доповідь Олександра Дугіна «Мережеві війни» [3]. Це пояснюється тим, що хоча на початку XXI сторіччя сам термін «мереже-центрична війна» та правила її ведення були запропоновані американськими військовими, однак в тих подіях, які спостерігаються наразі в Україні, чітко простежуються російські підходи до розуміння мережевої війни. Зупинимося на аналізі найбільш важливих її аспектів. Так, сутність

мережевого принципу полягає в тому, що головним елементом усієї моделі є обмін інформацією, а саме максимальне поширення форм продукування цієї інформації, доступу до неї, її розподілу, зворотного зв'язку.

Мережева війна – це новий різновид війни, яка ведеться переважно в інформаційній сфері і ґрунтується на використанні ефекту резонансу, коли найрізноманітніші, на перший погляд, не пов'язані між собою, ідеологічні, громадські, суспільні, економічні, етнологічні, міграційні процеси скеровуються зовнішніми операторами для досягнення конкретних цілей. Так, на думку О.Дугіна, сутність мережевої війни полягає у руйнуванні фундаментальних уявлень людей про зміст їхньої культури, суспільства та держави, для того, щоб викликати страх, дезорієнтацію та принести хаос у свідомість людей. Всі ці явища мають місце на окупованих територіях Донецької і Луганської областей. Вони посилюються як під впливом зовнішніх загроз (бомбардувань, переслідувань, нестачі матеріальних ресурсів, безпосередній загрозі життю тощо), так і вмілою маніпуляцією свідомістю громадян за допомогою поширення пліток, фальсифікації документів, панічних настроїв тощо. Внаслідок цього здійснюється переорієнтація, а потім знищення традиційних духовних і культурних цінностей народу.

З цією метою в Росії створена спеціальна група фахівців, до складу якої входять окремі високопосадові, кращі пасіонарні кадри різноманітних спецслужб (як наприклад, Гіркін і Бєзлер), інтелектуали, вчені, інженери, політологи, корпус патріотично налаштованих журналістів і діячів культури. Зокрема, завданням цієї групи є розробка і просування моделі євразійської мережі, яка вже розпочала активно функціонувати в багатьох зарубіжних країнах і відстоювати інтереси «російського світу».

Підтвердженням того, що Росія веде проти України саме мережеву війну, є тактика і стратегія російських військових на окупованих територіях. Ведення бойових дій, їх 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 російської мережі, між якими здійснюється постійний обмін інформацією. Якщо відбудеться збій декількох із них, вся мережа може опинитися під загрозою.

У мережевій війні реальне виступає другорядним по відношенню до віртуального, саме цим пояснюється значний обсяг неправдивої інформації, що циркулює російськими засобами масової інформації, а також використовується і поширюється соціальними мережами. Головний постулат мережевої війни – той, хто контролює інформаційне поле – той, контролює все. Саме тому інформаційний супровід війни стає не другорядним обслуговуючим моментом (як класична пропаганда), а навпаки – сенсом і змістом війни. Так, на початку військових дій Росії в Україні по захопленню Криму важливе значення мала інформація, яку доносила до українських громадян група «Інформаційний спротив». Підтвердженням актуальності цього постулату стали першочергові дії російських найманців на території Криму та Донецькій і Луганських областей щодо захоплення радо-телевізійних передавальних станцій, ретрансляторів зв'язку тощо.

У мережевій війні першочерговим завданням є боротьба за інформаційну перевагу, тому докладаються зусилля з метою: штучно збільшити потребу супротивника в інформації і водночас скоротити для нього доступ до неї; забезпечити широкий доступ до інформації своїх прихильників і агентів за допомогою мережевих механізмів та інструментів зворотного зв'язку, надійно захистивши їх від впровадження супротивника; скоротити власну потребу в

статистичній інформації завдяки обслуговуванню доступу до широкого спектру оперативного і динамічного інформування [5].

Отже, головна мета мережевої війни – зібрати якнайбільше різноманітної інформації з різних джерел, а потім, опрацьовуючи її за відповідним алгоритмом, прийняти рішення, необхідні для перемоги.

Цю обставину слід обов'язково враховувати при впровадженні електронного урядування в Україні, тому що його розвиток неможливий без забезпечення вільного і рівного доступу до різноманітної інформації органів державної влади тощо. Особливо це актуально для такої важливої його складової, як електронна демократія. Саме її зростання в умовах мережевої війни перебуває під загрозою. Це пояснюється тим, що громадянське суспільство, яке формується, є максимально зручною платформою для ведення мережевої війни, оскільки воно в технічному розумінні виступає оптимальним простором для ефективного ведення мережевої війни. Інститути громадянського суспільства не надто жорстко регулюються з боку держави. Відповідно, в умовах мережевої війни ці інститути громадянського суспільства та його сегменти стають найбільш ефективним середовищем, непідконтрольним владі, яке використовується для її руйнування та дискредитації, з метою втрати суверенітету держави.

Різноманітні неурядові організації, фонди, рухи, експертні мережі, наукові співтовариства, групи за інтересами, інститути чи радикальні та інтелектуальні центри можуть використовуватися, а деякі з них вже використовуються, для проведення активної антиукраїнської політики, впливаючи на формування громадської думки в нашій країні.

За даними Державної реєстраційної служби України [4], на кінець 2013 року в нашій країні зареєстровано 199 політичних партій. За даними місцевих органів юстиції, на кінець 2013 року зареєстровано 67155 центральних органів громадських організацій (з них 409 – із всеукраїнським статусом), громадських спілок – 599, професійних спілок – 5746, об'єднань профспілок – 1133 та благодійних організацій – 10482, з яких 86% становили благодійні фонди, 9% – благодійні установи та 5% – благодійні товариства. Загальна кількість членів на обліку громадських організацій, які подали звіти, нараховує 35,5 млн. осіб, з них 6,3 млн. (17,8% від загальної кількості) – члени, що перебували на обліку керівних органів.

Статистична інформація за основними напрямками діяльності Головних управлінь юстиції та територіальних органів юстиції з питань легалізації об'єднань громадян, державної реєстрації друкованих засобів масової інформації за І квартал 2014 року

	Головним управлінням юстиції		Районними, міськими, міськрайонними управліннями юстиції	
	Усього	У т.ч. за 2014 рік	Усього	У т.ч. за 2014 рік
Зареєстровано:				
Громадських організацій	13173	3	31523	856
Осередків всеукраїнських та міжнародних громадських організацій	4008	-	5802	-
Творчих спілок (самостійних)	8	-	15	-
Осередків всеукраїнських творчих спілок	245	-	15	-
Структурних утворень політичних партій	4706	27	153407	41
Благодійних організацій	3111	-	2234	-
Відділень всеукраїнських та міжнародних благодійних організацій	279	-	84	-

З метою уникнення небезпеки подальшого деструктивного впливу різноманітних громадських організацій і об'єднань слід ретельно проаналізувати їх діяльність в Україні, джерела фінансування, особливо звернувши увагу на інформацію, яка поширюється ними в соціальних мережах. Необхідно, не обмежуючи розвиток громадянського суспільства, уникнути поширення громадських організацій і об'єднань, які сприяють дестабілізації в Україні і мають антиукраїнський характер. Прикладом такої громадської організації є утворений і зареєстрований в 2011 році «Союз громадян України», діяльність якого наразі активізувалася і, зокрема, спрямовується на організацію і підтримку так званих «народних республік».

Отже, 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 масово поширюються в російській соціальній мережі «В контакті» як на території України, так і за її межами. Особливістю цих груп в соціальних мережах є те, що складно визначити реальний відсоток людей, які є громадянами України і насправді відстоюють свої переконання. Більшість з учасників антиукраїнських груп є громадянами інших держав, переважно Росії. Значний відсоток учасників цих груп є так званими тролями, суттєво збільшилося використання «чат-ботів», що сприяє дестабілізації ситуації в Україні, підривної діяльності, псування іміджу нашої країни і наших військових сил, сіяння паніки і відчуття безкарності за вчинені злочини. Найбільш яскраво це простежується в створенні й діяльності таких груп на окупованих територіях.

Саме тому, при плануванні подальшого розвитку електронної демократії в Україні, особливо пов'язаного з більш активним залученням громадян до процесів прийняття управлінських рішень, їх впливом на формування державної політики в Україні, необхідно вжити заходів, які б допомогли уникнути перераховані вище загрози. Так, 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» [1].

Як зазначається, за результатами дослідження, проведеного соціологічною службою Центру Разумкова з 12 по 18 вересня 2014 року, більше 60% відсотків українців відвідують урядові сайти, половина з них цікавиться режимом роботи та необхідними документами для отримання адміністративних послуг, інша половина – отриманням консультацій, 24% громадян України хочуть мати можливість впливати через Інтернет-петиції на обов'язковість розгляду того чи іншого питання відповідними органами влади та вносити свої пропозиції до проектів рішень, 19% висловили готовність брати участь у консультаціях, які організовують органи влади на веб-сторінках з питань місцевої регіональної та державної політик, а 11% готові приділяти цьому щомісячно декілька годин свого часу. Приблизно 3% користувачів Інтернету в Україні зацікавлені в обговорені: проектів/звітів щодо виконання державного та місцевих бюджетів, проектів/звітів щодо виконання державних та регіональних цільових програм, прогнозу/аналізу регуляторного впливу, проектів нормативно-правових актів.

Ці питання дійсно є вкрай необхідними для розвитку електронної демократії, однак в

умовах мережевої війни, що ведеться проти України, впровадження їх без належного захисту може призвести до протилежного результату. Прикладом цього є нещодавно проведене у Франції найбільш впливовим виданням Le Figaro опитування громадян щодо продажу Росії «Містралів» [2]. 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.

Окрім того, при впровадженні електронного урядування слід також враховувати вразливість інформаційних ресурсів, баз даних, в тому числі персональних даних громадян України, особливо тих, хто перебуває на окупованих територіях або приймає участь в антитерористичній операції тощо.

Так, у 2013 році в Україні розпочато розробку системи електронної взаємодії державних електронних інформаційних ресурсів (створено дослідний зразок системи), яка зможе об'єднати Єдині та державні реєстри, а також інші інформаційні ресурси для того, щоб спростити та значно прискорити отримання будь-яких дозвільних документів та інших адміністративних послуг. Однак, слід звернути увагу на захист і наповнення цих баз даних і інформаційних ресурсів. Вони в умовах мережевої війни перебувають в особливій небезпеці. Особливо, якщо врахувати, що в цілому в країні функціонує 726 державних інформаційних ресурсів, з них 135 – у центральних органах виконавчої влади. Зокрема, Міністерство юстиції України є держателем та забезпечує функціонування 17 Єдиних та Державних реєстрів – електронних баз даних, що є державною власністю. Ситуація ускладняються також і тим, що наразі відсутній єдиний Національний реєстр державних інформаційних ресурсів. Це призводить до неузгодженості в організації взаємодії між різноманітними державними інформаційними ресурсами, що в свою чергу пояснюється відсутністю обов'язкових вимог та єдиного національного координатора в цій сфері.

Особливо небезпечним, без належного захисту є запровадження електронної взаємодії між органами влади і органами місцевого самоврядування. Слід врахувати, що частина IT-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 IT-компанії.

Надання адміністративних послуг в електронній формі забезпечується через Єдиний державний портал адміністративних послуг (http://poslugi.gov.ua). Зазначимо, що досі залишається нерозв'язаним питанням ідентифікації громадян на порталі. Станом на грудень 2014 року, у розділі «Вхід» від відвідувача вимагається лише введення логіна і паролю. Проте не всі послуги можуть надаватися електронним чином без належної ідентифікації їх споживача. Саме тому подальший розвиток електронних послуг перебуває в зоні особливого ризику. Ця проблема може розв'язатися завдяки розробки і впровадження Національної системи електронної ідентифікації.

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗРОБОК

Україна перебуває в стані мережевої війни, тому кожен крок щодо подальшого впровадження електронного урядування має бути максимально виваженим і вивіреним з точки зору оптимального поєднання з одного боку – безпеки, з іншого – захисту приватності. Однак саме брак довіри до надійності захисту і збереження персональних даних, навіть в

мирний час, стає суттєвою перепоною на шляху розвитку електронного урядування. Вирішення цієї проблеми безпосередньо пов'язане з внесенням змін до відповідних нормативно-правових актів України.

Переважна більшість складових е-урядування є вразливою до зовнішніх і внутрішніх загроз в умовах мережевої війни. Тому слід розставити першочергові акценти, а саме розробити механізми ідентифікації особистості, яка б відповідала сучасним світовим вимогам, на її основі – запровадити Національну систему ідентифікації. Враховуючи обраний Україною напрям щодо європейської інтеграції, доцільно це зробити шляхом імплементації норм Регламенту eIDAS. Позитивним кроком в цьому напрямку є намагання розробити Державним агентством України з питань розвитку електронного урядування «Стратегії впровадження сучасних засобів та схем електронної ідентифікації в Україні». Окрім того необхідно об'єднати зусилля українських провідних технічних університетів (зокрема Національного технічного університету України «КПІ») з метою розробки і запровадження власної соціальної мережі, яка б відповідала національним інтересам тощо.

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

Список використаних джерел

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

2. 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

3. Сетевые войны. Аналитический доклад А.Дугина при участии В.Коровина и А. Бовдунова. Режим доступа: http://www.dynacon.ru/content/articles/2319/

4. Статистична інформація за основними напрямками діяльності ГУЮ та територіальних органів юстиції з питань легалізації об'єднань громадян, державної реєстрації ЗМІ та інформаційних агентств за І квартал 2014. Режим доступу: http://www.drsu.gov.ua/show/12734

5. Burke M. Information Superiority, Network Centric Warfare and the Knowledge Edge. Electronics and Surveillance Research Laboratory, Salisbury, Australia, 2000. DSTO Publications Online. Режим доступу: http://hdl.handle.net/1947/4169

References

1. Zelena knyha z elektronnoho uriaduvannia v Ukraini (proekt) [Green Book on electronic governance in Ukraine (project)]. Available at: http://etransformation.org.ua/2014/11/17/318/ (Accessed 21 December 2014). (In Ukrainian).

2 Rossiyane pytalis' sfal'sifitsirovat' opros Le Figaro otnositel'no «Mistralei» [The Russians tried to rig the poll for Le Figaro "Mistralej"] Available at: http://www.ukrinform.ua/rus/news/rossiyane_pitalis_sfalsifitsirovat_opros_le_figaro_otnositelno_mistraley_1685395/ (Accessed 21 December 2014). (In Russian).

3. Setevye voiny. Analiticheskii doklad A.Dugina pri uchastii V.Korovina i A. Bovdunova [Network war. Analytical report A. Dugina in V. Korovin and A. Bovdunova] Available at:

http://www.dynacon.ru/content/articles/2319/ (Accessed 21 December 2014). (In Russian).

4. Statystychna informatsiia za osnovnymy napriamkamy diialnosti HUIu ta terytorialnykh orhaniv yustytsii z pytan lehalizatsii ob'iednan hromadian, derzhavnoi reiestratsii ZMI ta informatsiinykh ahentstv za I kvartal 2014 [Statistical information on the main activities of MAJ and territorial justice on the legalization of civil associations, State registration of MASS MEDIA and information agencies for the I quarter of 2014]. Available at: http://www.drsu.gov.ua/show/12734/ (Accessed 21 December 2014). (In Ukrainian).

5. Burke M. Information Superiority, Network Centric Warfare and the Knowledge Edge. Electronics and Surveillance Research Laboratory, Salisbury, Australia, 2000. DSTO Publications Online. Available at: http://hdl.handle.net/1947/4169/ (Accessed 21 December 2014).

Чукут С.А. Внедрение электронного управления в условиях сетевой войны

В условиях сетевой войны, которая сейчас ведется в Украине со стороны России, на первый план выступает сбор разнообразной информации, влияние на формирование общественного мнения, максимально деструктивное воздействие на деятельность органов государственной власти и органов местного самоуправления. В статье отмечается, что государство при внедрении электронного управления должно учитывать эти условия. Определяются наиболее уязвимые составляющие электронного управления: разнообразные информационные ресурсы, базы данных, персональные данные граждан Украины (как тех, кто проживает на оккупированных территориях, так и тех, кто принимает участие в антитеррористической операции) прочее. Отмечается, что оказание электронных услуг, где требуется идентификация личности – тоже под угрозой. Особенно раскрывается работа социальных сетей, которые используются не всегда в интересах национальной безопасности и могут негативно влиять на развитие электронной демократии. В первую очередь это относится к различным открытым обсуждениям актуальных проблем государственной жизнедеятельности, опросам общественного мнения, деятельности некоторых общественных и правозащитных организаций.

Делается вывод, что с целью избежания и предотвращения негативного воздействия сетевой войны на развитие и дальнейшее внедрение электронного управления в Украине, необходимо в первую очередь решить вопросы национальной системы идентификации граждан, защиты информации и персональных данных, блокирования негативного воздействия деструктивных факторов.

Ключевые слова: электронное управление, электронная демократия, электронные услуги, сетевая война, защита персональных данных, система идентификации.

Chukut S.A. Implementing of e-Governance under Network war.

Within a network war, which is conducted now by Russia in Ukraine, the principle issue is to collect various information, influence on the forming of public opinion, the most destructive effect on the activities the bodies of State power and bodies of local self-government. The article notes that State is obliged to take to consideration of these conditions under implementing of e-governance. Defined the following most vulnerable components of e-Government: a variety of information resources, databases, personal data of citizens (as those living within the occupied territories and those taking part in the anti-terror operation), etc. Also defined that the providing of electronic services requires personal identification is also under threat. Analyzing the work of social networks, which are not always acting due to the interests of national security and may have adversely effect on the development of e-democracy. This primarily refers to the various

public discussions of current problems of public life, public polls, some of the public and human rights organizations.

It is concluded that in order to avoid and prevent the negative impact of network war on the development and implementation of e-Governance in Ukraine, the first task should be to address issues which are related with the national citizen identity system, the protection of information and personal data, locking the negative impact of the destructive factors.

Keywords: e-Government, e-Governance, e-democracy, e-services, network war, protection of personal data, identification system.