

Дубов Д.В.,
головний консультант, відділу
інформаційної безпеки та міжнародних
інформаційних відносин Національного
інституту проблем міжнародної безпеки
РНБО України

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Розвиток нових форм інформаційно-управлінської діяльності у системі державного управління, зокрема нової форми - *електронного урядування*, виникнення і розвиток якого пов'язаний із розвитком інформаційно-телекомунікаційних технологій, виявляє суттєве значення стану *інформаційної безпеки*, структура і суб'єкти якої змінюються із його впровадженням.

З огляду на важливість інтеграції України до ЄС, питання розвитку електронного простору України набуває особливої актуальності. Важливим кроком у цьому напрямі було започаткування 18 квітня 2002 року довгострокової програми під умовною назвою «Електронна Україна», в межах якої передбачено заходи створення ефективного механізму інформаційної взаємодії органів влади всіх рівнів, впровадження електронного документообігу та забезпечення інформаційної безпеки.

Проблема інформаційної безпеки у тісному взаємозв'язку із широким спектром чинників її виникнення і шляхів забезпечення певною мірою досліджувалась у різних аспектах у працях вітчизняних і зарубіжних науковців. Серед наукових публікацій останніх років можна виділити роботи, присвячені аналізу ведення інформаційно-психологічної боротьби і проблем інформаційно-психологічної безпеки, які при цьому виникають [1], досліджуються характерні риси, шляхи та механізми свідомої чи несвідомої міфологізації суспільної свідомості, а також вплив цих процесів на формування та задоволення духовних і матеріальних потреб людей [15], аналізуються суттєві аспекти інформаційної безпеки у процесі політичної комунікації, зокрема, мовного політичного маніпулювання [3], досліджуються методи та засоби формування друкованими ЗМІ громадської думки в Україні відносно політичних сил держави [13], виявляються засоби ведення і наслідки інформаційних війн [4, 16, 17] та ін.

Однак, невирішеними залишаються питання інтегрованого розгляду проблем *інформаційної безпеки*, які виникають у процесі впровадження і функціонування *електронного урядування*, яке є сукупністю комплексу державних інформаційних систем, інформаційно-технологічної інфраструктури їх взаємодії між собою та інфраструктури доступу до них населення, що забезпечує новий рівень інформаційної відкритості, результативності і ефективності діяльності органів державної влади для найбільш повного задоволення прав громадян [18].

Слід зазначити, що політична комунікація, здійснювана з використанням системи електронного урядування, містить низку латентних проблем, тісно пов'язаних із проблемами інформаційної безпеки:

- система адміністративної влади, яка покликана висловлювати волю громадян, може стати системою «...самопрограмованої, замкнутої циркуляції, керуючи поведінкою виборців» [6], намагатись уникати контролю публічної сфери і диктувати свої взаємовідносини між державою і громадянським суспільством;
- домінанта державної безпеки над безпекою людини та суспільства;
- вимоги сучасного демократичного державотворення можуть викликати потребу відповідного демократичного варіанта втручання у сферу громадянського суспільства з метою прискореного формування його зруйнованих або недостатньо розвинених механізмів [7], що суперечить можливості формування громадянського суспільства «згори» за бажанням або за планом представників влади [8];

- невідповідність задумів модернізації інституту зв'язків державної влади та управління з громадськістю, яке виражається у планах впровадження системи електронного урядування, потребам, інтересам та можливостям громадян може спричинити кризу «проникнення» нових форм комунікацій у суспільство через невідповідний освітній рівень, рівень демократичної та політичної культури;
- розрив між очікуваними та фактичними результатами впровадження елементів електронного урядування.

У аналізі змісту і специфіки впливу впровадження електронного урядування на систему інформаційної безпеки слід розглядати обидва ці явища з точки зору взаємовпливу зазначених систем одна на одну, у їх взаємодії, а також проаналізувати вплив на розглядувані явища інших явищ, подій, процесів.

Інформаційно-технологічна інфраструктура, яка пронизує всі сфери діяльності, включає і систему інформаційного забезпечення всіх структур держави і суспільства, включає сукупність інформаційні системи і ресурси, а також засоби, які забезпечують їх функціонування, взаємодію між собою, громадянами і організаціями. Інформаційна інфраструктура забезпечує загальні умови доступу всіх користувачів до інформації і надає їм можливість використання нових інформаційних технологій.

Одним із елементів розглядуваної проблеми електронного урядування є інфраструктура влади, яка представляє комплекс соціально-політичних і правових органів, закладів, норм, силових, інформаційних та інших структур, на яких базується влада і які сприяють її існуванню, функціонуванню і розвитку. До такого роду інфраструктури включають також громадські рухи, політичні партії, системи відбору і підготовки лідерів, засоби масової інформації, органи політичного маркетингу та ін.

Властивості системи електронного урядування її сутнісні характеристики і параметри детерміновані властивостями *зовнішнього* відносно цієї системи середовища. З одного боку, таким зовнішнім середовищем є *суспільна система* - ті соціально-економічні, політичні та науково-технічні фактори, які об'єктивно діють на даному етапі суспільного розвитку і пред'являють цілком певні вимоги до системи електронного урядування. Система електронного урядування повинна бути чутливою до зовнішніх впливів, своєчасно і з необхідним випередженням реагувати на тенденції, що назрівають у зовнішньому середовищі, давати їм відповідну інтерпретацію з точки зору державної політики і державного управління, оперативно відображати суспільні вимоги (соціальне замовлення) у всіх компонентах подальшої діяльності з державного управління на різних його ступенях з урахуванням їх послідовності і взаємозв'язку. З іншого, система електронного урядування, як чинник, впливає на загальну систему інформаційної безпеки, значною мірою визначаючи вимоги до її об'єктів, суб'єктів, принципів забезпечення, джерел безпеки, виникнення і спрямованості небезпечних інформаційних потоків, створюючи нові підсистеми інформаційної безпеки організаційного, правового, соціального та іншого характеру.

Єдність електронного урядування як системи забезпечується загальною для всіх її складових цільовою спрямованістю на досягнення безперервного розвитку особистості, а також досягненням відносин взаємосприяння, які визначають взаємозв'язок, взаємоузгодженість і взаємну підпорядкованість компонентів, які у неї входять, координацію процесів управління, які у них відбуваються, за їх спрямованістю і призначенням.

Система електронного урядування і система інформаційної безпеки є взаємопов'язаними елементами загальної системи державного управління. Зокрема, очевидними є загальні для обох розглядуваних систем групи інформаційно-технічних небезпек:

- новий клас соціальних злочинів, що ґрунтуються на використанні сучасних інформаційних технологій (махінації з електронними грошима, комп'ютерне хуліганство та ін.);

- електронний контроль за життям, настроями, планами громадян, політичних організацій;
- використання нових інформаційних технологій з політичною метою;
- вплив інформаційної зброї на психіку, свідомість людей.

У процесі розвитку електронного урядування виявлені проблеми можуть актуалізуватись у принципових суперечностях, отже визначення шляхів розв'язання їх у взаємозв'язку із проблемами інформаційної безпеки потребує відповідних досліджень. При цьому виникає завдання окреслити основні об'єкти забезпечення інформаційної безпеки у контексті впровадження системи електронного урядування, виявити чинники загроз, можливі наслідки та шляхи попередження загроз у основних формах взаємодії держави та суспільства у системі електронного урядування - «Уряд-Громадяни», «Уряд-Бізнес», «Уряд-Уряд».

Однією з ключових проблем формування і розвитку відкритого суспільства є *прозорість діяльності влади*, як ознаки демократичного суспільства, чинника його відкритості. Розвиток інформаційно-комунікаційних технологій дає змогу реалізувати принципи відкритості і прозорості шляхом впровадження *системи електронного урядування*, яке можна розглядати як інструмент забезпечення підконтрольності влади та розвитку комунікацій між різними учасниками демократичного політичного процесу, як засіб підвищення активності громадян, їхньої політичної культури, як форму реалізації права громадян на повну і об'єктивну інформацію.

Впровадження електронного урядування - це комплексна суспільно-соціальна, правова, економічна проблема, яка розв'язується в умовах складних фінансових, матеріально-ресурсних та інших обмежень, характерних як для світової практики впровадження електронного урядування, так і для специфічних умов, у яких ці процеси відбуваються в Україні.

Електронне урядування – це процес виконання функцій державного управління, за якого вся сукупність як внутрішніх, так і зовнішніх зв'язків та процесів підтримується та забезпечується відповідними інформаційно-комунікаційними технологіями. Електронне урядування передбачає систематичне використання урядовими установами інформаційних та комунікаційних технологій (таких як локальні мережі, мережа Інтернет, мобільні технології), що дає можливість трансформувати відносини з громадянами, бізнесом та урядом. Основні напрями взаємодії у системі електронного урядування - «Уряд-Громадяни» (G2C - Government-to-Citizen), «Уряд-Бізнес» (G2B - Government-to-Business), «Уряд-Уряд» (G2G - Government-to-Government).

Система електронного урядування виконує такі функції:

- *політичну* - як інструмент державної політики відповідно до встановлених принципів організації та діяльності політичної системи;
- *соціальну*, спрямовану на регулювання і гуманізацію суспільних відносин, пов'язаних із здійсненням державного управління, стимулювання громадянської активності у суспільстві;
- *організаційну* яка полягає у взаємозв'язку системи органів державної влади, визначенні взаємодії між ними відповідно до визначеної компетенції, між галузями влади;
- *іміджеві (презентаційну)*, яка реалізується у тенденції відмови від класичної бюрократії, створенні більш гнучких форм взаємодії між державною і суспільством, встановленні індикаторів якості та ефективності діяльності;
- *зв'язків з громадськістю*, пов'язана з аналітико-прогностичним забезпеченням, реалізується у можливості публічного політичного дискурсу між громадянами і державою з метою забезпечення політичної підтримки рішень уряду;
- *виховну*, яка реалізується у вихованні поваги до необхідності додержання прав і свобод людини і громадянина, суспільства в цілому.

Діяльність з електронного урядування відбувається у таких основних напрямках: забезпечення конституційних прав і свобод людини та громадянина в галузі одержання і

використання інформації; забезпечення прозорості державної політики для громадян; забезпечення зворотного зв'язку між державною та суспільством.

Сучасна інформатизація і медіатизація часто призводять до того, що особисте життя, дозвілля, поведінка, настрої і всі людські прояви виявляються жорстко і примусово унормованими. Новітня індустрія інформатики, як зазначає А.Д.Урсул, «...дає змогу не тільки підключитись до кожного, але і виключити кожного із процесу життя, діяльності і мислення. Проникнення у все суспільство і у життя кожного, влада над фізичним і психічним цілком очевидні» [10].

Розвиток інформаційних технологій є процесом амбівалентним. З одного боку, удосконалення засобів обробки і передачі інформації створює умови для розвитку демократичного суспільства, участі громадян у прийнятті найважливіших рішень, подолання відчуженості тощо. Але інформаційні технології можуть бути використані для створення системи всеохоплюючого, тотального контролю над суспільством взагалі та кожним його членом зокрема - як зазначається у праці відомого футуролога Й.Масуди «Комп'ютопія»: «...існує серйозна небезпека того, що ми рухаємося у напрямі контрольованого суспільства» [11]. Це стає можливим за допомогою «електронного слідкування», «електронного контролю» за діями осіб, партій, рухів, колективів та ін. Отже, у процесі політичної комунікації, яка реалізується у системі електронного урядування, інформаційних відносин органів державного управління із суспільством, суттєво важливою постає проблема *інформаційної безпеки* - стану захищеності життєво важливих інтересів особистості, суспільства і держави, зведення до мінімуму неповноти, невчасності і недостовірності інформації, негативного інформаційного впливу, негативних наслідків функціонування інформаційних технологій. Варто згадати слова Ж.-Ж.Руссо: «Держава повинна закласти собі надійну основу, щоб набутти тривкості і завдяки цьому протистояти тим потрясінням, яких ніколи не бракує, і мати змогу чинити дії, яких настійливо вимагає самозбереження» [9, стор.57].

Безпека - це відсутність загрози або можливість надійно захиститися від неї. Небезпечним слід вважати такий інформаційний вплив, який має дестабілізуючі наслідки, утискає інтереси особистості, суспільства, держави.

Забезпечення інформаційної безпеки спрямоване на два взаємопов'язані, але суттєво самостійні об'єкти, які умовно можна визначити як «соціальний» і «ресурсний». Соціальний об'єкт - людина, суспільство, держава - їх політичні, культурні й моральні риси мають бути об'єктом захисту у сфері інформаційних відносин [5].

Основними параметрами їх інформаційної безпеки, є, перш за все:

- забезпечення свободи слова та доступу громадян до інформації - «комунікація стає політично значущою лише в тому разі, якщо виражає ставлення громадянина або групи до діяльності держави, адміністративної влади» [6];
- збереження системи цінностей, духовного та фізичного здоров'я особи, суспільства;
- запобігання маніпулюванню громадською думкою з боку державної влади, фінансово-політичних кіл.

«Ресурсний» об'єкт пов'язаний, перш за все, із запобіганням проявам кіберзлочинності, спрямований на збереження інформаційних ресурсів та захищеність інформаційної інфраструктури, і характеризується такими основними параметрами:

- захищеність інформаційних мереж, систем управління транспортом, енергетичної та банківської сфер, державного управління, військових формувань та ін.; комп'ютерна злочинність (комп'ютерні «віруси», атаки «хакерів», спотворення, блокування, порушення цілісності, нав'язування фальшивої інформації); радіоелектронне «придушення» ліній зв'язку, систем управління; фізичне руйнування інформаційної інфраструктури, в т.ч. в результаті дій природних факторів
- захист великих масивів конфіденційної інформації про особу, що накопичуються у державних та недержавних структурах; діяльність іноземних розвідок

- високий рівень залежності комп'ютерних мереж від іноземних виробників програмного забезпечення
- вплив за кордон спеціалістів у галузі інформаційних технологій;
- масові порушення прав на інтелектуальну власність.

Основні форми комунікації у системі електронного урядування пов'язані з такими об'єктами як людина, інституціональні структури суспільства, органи державного урядування - їх політичні, культурні риси, а також комерційні інтереси стають об'єктом захисту у сфері інформаційних правовідносин.

Відповідно до розглянутих вище функцій системи електронного урядування (політичної, соціальної, організаційної, виховної та ін.) виникають певні чинники загрози інформаційній безпеці, які можуть мати суттєві негативні наслідки (табл.1.).

Таблиця 1.

Система інформаційної безпеки відносин соціальних об'єктів у межах впровадження електронного урядування

Форми взаємодії	Чинник загрози	Можливий наслідок	Шляхи попередження загроз
«Уряд-громадяни»	Різноманітні, часом діаметрально спрямовані інформаційні впливи, маніпулятивні технології, ігнорування громадської думки при прийнятті важливих політичних рішень	Політичне відчуження громадян, порушення демократичних принципів і норм діяльності держави	Забезпечення конституційного права громадян на доступ до достовірної та оперативної урядової інформації, що сприяє виробленню соціального «імунітету» до маніпулятивних технологій
«Уряд-бізнес»	Складність відносин комерційного характеру (купівля-продаж, інвестиційні контракти, страхування, банківські послуги, різні форми ділового співробітництва та ін.); відсутність доступу до нормативно-правової інформації, Ігнорування повідомлень про факти корупції, зловживань посадових осіб, порушення прав громадян.	«Прозорість» комерційної інформації. Втрата підтримки державної політики з боку підприємницьких структур	Надання органами державної влади інформації громадянам та інституціональним структурам суспільства; забезпечення зворотного зв'язку, виявлення тенденцій і закономірностей розвитку ситуації; регулювання електронного документообігу, підтвердження справжності електронного підпису та інформації у інформаційних продуктах і послугах, створення систем захисту персональної інформації. Відкритість інформації за умов забезпечення встановленої законом конфіденційності комерційної, службової, професійної таємниці, державної таємниці, режиму інформації про громадян
«Уряд-уряд»	Відсутність зв'язків, «розпорошеність» систематизованих у бібліотеках, архівах, службах діловодства	Порушення інформаційних зв'язків і координації інформаційно-управлінських	Підвищення ефективності інформаційного забезпечення державного управління шляхом інтеграції Інтернет-порталів і систем електронного

	та інформаційно-пошукових системах масивів інформації; недостатня розвиненість інформаційної інфраструктури органів державної влади	відносин; відсутність інформаційних моделей фактів, явищ, процесів, які є сферою діяльності органу державного управління; зниження ефективності державного управління в цілому	документообігу з метою доступу до всіх необхідних внутрішніх і зовнішніх джерел інформації
--	---	--	--

Ступінь інформаційної безпеки при впровадженні системи електронного урядування значною мірою визначається рівнем розвитку національної інформаційної інфраструктури захисту інформації (табл.2).

Таблиця 2.

Структура компонентів національної інфраструктури захисту інформації

НАЦІОНАЛЬНА ІНФРАСТРУКТУРА ЗАХИСТУ ІНФОРМАЦІЇ				
<i>Законодавча компонента</i>	<i>Технічна компонента</i>	<i>Організаційна компонента</i>	<i>Економічна компонента</i>	<i>Методологічна компонента</i>
Закон «Про електронний цифровий підпис», «Про електронний документ та електронний документообіг», «Про захист інформації у автоматизованих системах», статті у кримінальному кодексі, закони та підзаконні акти, які регулюють функціонування національної інформаційної інфраструктури	Програмні та апаратні засоби крипто-графічного захисту інформації, розвиток вітчизняної індустрії інформації	Органи, що координують створення і розвиток системи національної інформаційної інфраструктури (Держкомітет, центр електронних ключів та ін.)	Фінансування програм розвитку національної інформаційної інфраструктури, в тому числі розвитку виробництва вітчизняних конкурентоспроможних засобів і систем інформатизації	Концепції і програми розвитку національної інфраструктури захисту інформації, системи ліцензування, сертифікації, системи аудиту безпеки використовуваних технологій, система громадського контролю за розвитком національної інфраструктури захисту інформації

Забезпечення інформаційної безпеки в умовах впровадження електронного урядування - це складне явище, яке включає:

- сукупність інформаційних потреб державного управління у процесі функціонування державної влади і діяльність із забезпечення цих потреб;
- зовнішні та внутрішні загрози інформаційно-технологічному простору електронного урядування - апаратно-програмні (загрози цілісності даних та апаратно-програмних засобів, використання несертифікованих вітчизняних та зарубіжних технологій при створенні й розвитку інформаційної інфраструктури) та суспільно-інформаційні (неправомірне обмеження доступу громадян до відкритих інформаційних ресурсів органів державної влади, незадовільні якісні характеристики інформаційних повідомлень та ін.);
- комплекс нормативно-правових, організаційно-технічних, методичних засобів протидії загрозам інформаційної безпеки.

Необхідність впровадження в Україні системи електронного урядування, спрямованої на підвищення результативності і ефективності задоволення суспільних потреб, нерозривно пов'язана із проблемою інформаційної безпеки у всіх формах взаємодії держави і суспільства.

Інформаційна безпека є системоутворюючим чинником, від якого залежить ефективність реалізації всіх функцій системи електронного урядування - політичної, соціальної, виховної та ін. Громадянське суспільство повинно створити багатофункціональну інфраструктуру для здійснення моніторингу загроз і небезпек, виробити механізм керування ними, реагування на інформаційні загрози особистості, суспільству, державі.

Перспективи подальших розвідок

Ступінь інформаційної безпеки при впровадженні системи електронного урядування значною мірою визначається рівнем розвитку національної інформаційної інфраструктури захисту інформації, її законодавчої, технічної, організаційної, економічної та методологічної компонент, які потребують подальшого визначення, наповнення і накреслення шляхів реалізації.

Література:

1. Леонтьєва Л. Доктринальні погляди на ведення інформаційно-психологічної боротьби//Українська національна ідея: реалії та перспективи розвитку.-2000.-Вип.13.-С.121-126.
2. Шевченко А. Пропаганда возвращается. Каким образом телевидение манипулирует общественным сознанием?//Корреспондент.-2002.-№25.-С.25-27.
3. Петренко В.В. Політична мова як засіб маніпулятивного впливу: Автореф. дис. ...канд.політ.наук/Нац.університет ім.Т.Шевченка.-К., 2003.-17 с.
4. Андрушко А.М. Інформаційні війни: міф чи реальність?//Суспільство. Держава. Армія. Сер.:Суспільні науки.-2003.-Вип.6-7.-С.113-120.
5. Кормич Б.А. Суб'єктно-об'єктний склад інформаційної безпеки//Актуальні проблеми політики.-2003.-Вип.8.-С.130-137.
6. Барматова С. Роль Ю.Габермеса в розвитку універсальної теорії політичної комунікації//Соціологія: теорія, методи, маркетинг.-2003.-№2.-С.60-71.
7. Мартинюк Р.С. Державна влада та громадянське суспільство в сучасній Україні: політико-правовий аспект//Актуальні проблеми вдосконалення чинного законодавства.-2003.-Вип.ХІ.-С.24-36.
8. Банчук М. Громадянське суспільство в Україні: поняття і реальність//Людина і політика.-2003.-№ 1.-С.42-49.
9. Руссо Ж.-Ж. Про суспільну угоду або Принципи політичного права.- К.: «Port-Royal», 2001.-348 с.
10. Урсул А.Д. Информатизация общества и безопасность развития цивилизации //Социально-политические науки.- 1990.- № 10.-С.24-32.
11. Масуда Й. Комп'ютопія//Філософська і соціологічна думка.-1993.-№6.-С.36-50.
12. Тихомирова Є.Б. Транспарентність і відкритість діяльності влади та шляхи їх забезпечення в Україні//Наук. записки Національного університету «Києво-Могилянська академія».-2002.-Т.20: Сер.Політ.науки.-С.39-43.
13. Бадрак В. В. Фактори ефективності впливу друкованих ЗМІ (преси) на електорат/ Автореф. дис.канд. філологічних наук (10.01.08 – журналістика).-Київ, 2000.-19 с.
14. Матвієнків С. М. Політична свідомість: суть та умови її формування в процесі державотворення в Україні// Автореферат дис... канд.політ. наук (23.00.02 – політичні інститути та процеси).- Львів,2001.-19 с.
15. Усов Д.В. Міфологізація свідомості в сучасному суспільстві/Автореферат дис...канд. філос. наук (09.00.03 – соціальна філософія та філософія історії).-Київ, 2002.-19 с.
16. Ожеван М. Двогостра зброя//Підприємництво в Україні .- 2001.-№ 8.
17. Ожеван М. Фронти й тили великих інформаційних війн//Підприємництво в Україні. - 2001.-№ 4-5.
18. Данилин А.В. Предложения по концепции формирования архитектуры «электронного правительства» Российской Федерации[Електрон.ресурс].-Спосіб доступу: URL:http://www.msdb.ru.-Загол. з екрану.