УДК 351.746:007

Сергій Шайхет
аспірант кафедри державної політики та суспільного розвитку
НАДУ при Президентові України

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СЕРВІС НАЛЕЖНОГО ВРЯДУВАННЯ

У статті розглянуто особливості впровадження належного врядування у контексті інформаційної безпеки як сервісу. Доведено, що головною проблемою впровадження принципів належного врядування є відокремленість програмних продуктів, роздробленість та ситуативність їхньої взаємодії. Обґрунтовано необхідність впровадження сервісно-орієнтованого державного управління. Визначено механізми забезпечення інформаційної безпеки клієнтів-громадян з одночасним поєднанням відкритості органів влади.
Ключові слова: належне врядування, електронне врядування, інформаційна безпека, сервісно-орієнтована державна політика.

Sergiy Shaykhet
PhD student of the Public Policy & Social Development Depatment
NAPA under the President of Ukraine

INFORMATION SECURITY AS A SERVICE OF GOOD GOVERNANCE

Problem and relevance. *The main problem in implementing the principles of good governance in life is the isolation of software, situational fragmentation and their interaction. That is why urgent problem for Ukraine is the development and implementation of service-oriented architecture of e-government. One of its main components must be standardized model for describing and implementing business processes, administrative regulations, storage and processing of information management, data reporting, the use of application systems and technologies. Designated milestones allow to update layer «government – citizens», which is still in the shadow of the other two because it is fundamental towards them, and officials and businessmen, primarily a physical (private) persons who actualize themselves not only professional field, but also in private. That is why confidence in the government, the belief that the administrative systems are service oriented, is now an important element in the revival of adequate customer service.*
Formulation purposes of article (problem). *The article is to examine the characteristics of information security in the context of good governance. The subject – existence specifics outlined in the operation of the service information in modern society.*
A brief statement of the nature of the study. *One of the main functions of government is to provide the basic needs of the individual, including the dominant need is security. This is due to the fact that biologically this requirement leads to the survival of individuals, continuing its kind, which means literally «built in» in the human psyche. New time converted the need for security, deepening its meaning, creating unison with the actual conditions in which there is a biological unit - body, namely the peculiarities of existence information. Globalization, besides cooperation of individuals, led to a whole new level of danger in which there are a variety of scams, while creating problem of information security.*
Conclusions. *In our view, the actualization of the objectives is possible through:*
– provide the integrity of information generated networks, transport management, energy and banking sectors, government, military formations; block computer crime (viruses, hacker attacks, distortion, etc. block of electronic services of good governance); tracking muffling electronic signals to conceal information etc.;
– provide and guarantee complete inaccessibility of large amounts of data collected on citizens, to prevent their use by criminals (to prevent fraud with electronic money, computer bullying, etc.);
– provide uninterrupted support to foreign developers of computer networks in order to adequately perform their work and initially defined functions;
– provide at preventing electronic control of their lives, moods, plans of citizens, political organizations, etc. by expanding the legal framework of the outlined issues and careful alignment system requirements for events of national importance, which allow a government intervention (preparation of acts of terrorism, riots, etc. that undermine the very statehood);
– providing information obstruct impact weapons on the psyche, the consciousness of citizens through regular study information channels that can be used with criminal intent (the first turn - the media);
– provide proper ownership and use of state employees new information technologies by improving their skills and developing a system of professional incentives.
Key words: *governance good, governance electronic, security information, customer service.*

Сергій Шайхет
аспирант кафедры государственной политики и общественного развития
НАГУ при Президенте Украины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СЕРВИС ЭФФЕКТИВНОГО УПРАВЛЕНИЯ

В статье рассмотрены особенности внедрения эффективного управления в контексте информационной безопасности как сервиса. Доказано, что главной проблемой внедрения принципов эффективного управления

являются обособленность программных продуктов и ситуативность их взаимодействия. Обоснована необходимость внедрения сервисно-ориентированного государственного управления. Определены механизмы обеспечения информационной безопасности клиентов-граждан в сочетании с открытостью органов власти.
Ключевые слова: *эффективное управление, электронное правительство, информационная безопасность, сервисно-ориентированная государственная политика.*

Постановка проблеми

Основою існування біологічних особин є прагнення до якнайдовшого продовження збереження їхнього гомеостазу (сталості) функціонування всіх органів і систем, з метою відтворення свого буття у горизонті онтологічної реальності. У такому сенсі основоположною для сучасного існування людини можна вважати специфіку взаємодії (як окремого індивідуума, так і суспільства в цілому) із реальністю. Зрозуміло, що такий зв'язок, хоча і має суворо суб'єктивний характер, однак є мимовільно узагальненим, внаслідок своєї побутової (емпіричної) значимості для щоденного життя (грубо кажучи – виживання) будь-якого людського організму [3, с. 100].

Відтак, існування людських особин пов'язане, першою чергою, із забезпеченням базових фізіологічних потреб, які вдало відображені у піраміді потреб А. Маслоу, однією з яких є потреба у безпеці (відсутності загрози або можливості надійно захиститися від неї [4]). Зрозуміло, що в біологічному сенсі безпека постає складником не просто довгого підтримання самості організму в горизонті подій онтологічної реальності, а й чинником його репродуктивної (відтворюючої) функції, що забезпечує збереження виду як такого.

У контексті сучасності продуктивною є актуалізація питання інформаційної безпеки, суть якого в наявності низки інформаційних впливів, які мають дестабілізуючі наслідки, пригнічують або нівелюють інтереси особистості, суспільства, держави [4] тощо. При цьому природним є певний конфлікт між означеними трьома віхами (особистістю, суспільством, державою), закладений у самій свідомості індивідуума: з одного боку – прагнення до кооперації, актуалізації своєї суб'єктності через репрезентацію себе у антропному оточуючому світі, з іншого – жадання до збереження свого «Я», що постійно піддається руйнації у середовищі соціуму, держави тощо. Зрозуміло, що в такому сенсі держава (уряд) постає структурованою системою, головна функція якої, у вузькому розумінні, – забезпечення потреб клієнтів-громадян, – стрижнева мета належного врядування, реалізація ідей якого можлива через запровадження інструментів електронного врядування: інформування громадян та бізнесу про діяльність державних органів на відомчих сайтах; надання управлінських послуг у режимі онлайн: залучення громадян та бізнесу до обговорення та прийняття управлінських рішень; автоматизація діяльності окремих державних органів та міжвідомчої взаємодії; підконтрольність влади суспільству [5, с. 135].

Інформаційна безпека є системоутворюючим чинником, від якого залежить ефективність реалізації всіх функцій системи електронного врядування – політичної, соціальної, освітньої тощо [4]. Таким чином, його (електронне урядування) слід розглядати як засіб актуалізації ідей належного, а значить, – в кінцевому випадку, – як систему сервісів, націлену на забезпечення потреб членів спільноти, на базі і в межах якої воно існує. Так, застосування електронного врядування в містах-метрополіях актуалізується вимогою суспільства щодо підвищення доступу до надання управлінських послуг мешканцям, покращення їх якості, а відтак є ознакою формування громадянського суспільства [11].

Зауважимо, що інформаційні війни та конфлікти можуть виникати не лише між державами. У низці випадків проведення заходів щодо інформаційного захисту може бути потрібним і на регіональному рівні в мирний час. При цьому умовами інформаційних конфліктів є виборчі кампанії, боротьба політичних і економічних еліт за сфери впливу, переділ сфер впливу корупційними та кримінальними елементами і групами, проведення терористичних актів тощо [10].

Аналіз останніх досліджень і публікацій

Останнім часом здійснено ряд досліджень, спрямованих на виокремлення основ інформаційної безпеки держави, створення теоретичних підвалин інформаційного (інформаційно-психологічного) протиборства, що мають дозволити з єдиних методичних позицій розв`язати основні завдання планування і ведення інформаційного протиборства (боротьби) у різних сферах життєдіяльності держави, її оборонних та правоохоронних органів [10]. Так, основоположними є дослідження щодо теми інформаційної безпеки таких вчених, як: І. Ажмухамедова, В. Бабаєва, М. Ваніна, С. Гайдученка, О. Гатман-Голутвіну, О. Гладкіх, В. Дементьєва, Д. Дубова, Н. Дяченко, О. Карпенка, П. Клімушина, А. Колодій, Г. Пітерса, Г. Почепцова, Дж. Розенау, Г. Саймона, А. Серенка, Дж. Стігліца, В. Томпсона, І. Тріфаленкова, С. Щеглюка та інших.

Виділення невирішених раніше частин загальної проблеми

Ефективність роботи органів влади визначається трьома чинниками: ефективністю взаємодії з громадянами та підприємцями, ефективністю внутрішньої роботи кожної установи та ефективністю взаємодії органів державної влади між собою. Очевидно, що успішне подолання зазначених факторів у системі електронного уряду можливе на основі розвитку інфраструктури захисту інформації з використання систем обміну конфіденційною інформацією [9, с. 144]. Однак, окрім обміну такими даними, виникає етичне питання особливостей використання означеної інформації урядом, оскільки: по-перше, вона може стати необхідним джерелом даних, що забезпечить адміністративний апарат низкою важливих відомостей, які стануть надзвичайно цінними у випадку їх централізованої аналітичної, логістичної (тощо) обробки з метою вироблення методології не тільки самої роботи, а і впливу на населення. Окреслена тенденція є амбівалентною, оскільки з одного боку збір і систематизація даних щодо уподобань клієнтів, природно, покращить якість, оперативність тощо їх обслуговування, що лежить в основі роботи належного урядування. З іншого – тут варто говорити вже не про забезпечення існуючих потреб людей, а про витворення штучно сформо-

ваних симулякрів таких потреб, з метою маніпуляції останніми і досягнення бажаних для уряду результатів. Таким чином, інформаційні технології можуть бути використані для створення системи всеохоплюючого, тотального контролю над суспільством взагалі та кожним його членом зокрема [4], що руйнує саму ідею демократичного ладу.

По-друге, варто говорити про певну диференціацію відкритості даних, оскільки такий тип врядування передбачається як інструмент демократизації, вільного волевиявлення удосконалення засобів обробки і передачі інформації й створює умови для розвитку демократичного суспільства, участі громадян у прийнятті найважливіших рішень, подолання відчуженості тощо [4], натомість перетворюючись на привабливу мішень для різного роду шахраїв й авантюристів і тому подібних. Зважаючи на вищезазначене, невирішеною частиною загальної проблеми є відсутність належного науково-теоретичного обґрунтування сфери інформаційної безпеки як сервісу врядування, де ефективна градація даних, викладених у вільному доступі, унеможливлює вразливість електронної інфраструктури у цілому.

Мета

Формулювання цілей статті (постановка завдання). Метою статті є розгляд особливостей інформаційної безпеки у контексті належного урядування. Предметом – специфіка побудови окресленого сервісу в процесі функціонування інформації в сучасному суспільстві.

Виклад основного матеріалу

Розвиток нових форм інформаційно-управлінської діяльності у системі державного управління, зокрема нової форми – електронного врядування, специфіка становлення якого пов'язана із розвитком інформаційно-телекомунікаційних технологій, виявляє суттєве значення інформаційної безпеки, структури і суб'єкти якої змінюються із його впровадженням [4]. Першою чергою, це репрезентується на трьох рівнях, які можна виділити для представлення цього явища: це, по-перше, система «уряд – уряд», яка означує цілісність інформаційно-віртуальної репрезентації даних, що може бути досягнуто у, власне, внутрішньому сполученні адміністративного апарату. Останнє, на наш погляд, є важливою передумовою підвищення якості надання послуг населенню, оскільки ефективна, гнучка, динамічна, чітка взаємодія органів державного управління є запорукою оперативності надання необхідної клієнту інформації. По-друге, система «уряд – бізнес», яка, фактично, безпосередньо є домінантою економічного розвитку, оскільки виступає регулятором частки інвестицій у економіку країни, а відтак – постає важливим чинником розвитку всього регіону. По-третє, система «уряд – громадяни», яка, власне, і є предметом нашого дослідження, а відтак буде докладніше окреслена нижче. Якщо говорити конкретно щодо інформаційної безпеки, то існують певні заходи, ефективні щодо захисту інформації: розробка політики безпеки, проведення аналізу ризиків, планування забезпечення інформаційної безпеки, планування дій в надзвичайних ситуаціях, вибір механізмів і засобів забезпечення інформаційної безпеки [2, с. 108]. Для прикладу візьмемо такий тип представлення даних, як репозитарії, основною особливістю яких є репрезентація наукового доробку певної установи у світі через вільний доступ у мережі Інтернет.

Тут одразу треба зауважити, що забезпечення інформаційної безпеки спрямоване на два взаємопов'язані, але суттєво самостійні об'єкти, які умовно можна визначити як «соціальний» і «ресурсний» [13]. У першому випадку мова іде про людину, тобто, власне, клієнта, побутування якого, а точніше – потреби, що виникають у його (побутування) процесі є об'єктом забезпечення (читайте – діяльності) врядування. Натомість «ресурсний» можна означити як суто техніко-матеріалістичні особливості функціонування інформації: хостинг; сервер, на якому розміщуються дані; структура і природа програмного забезпечення, сполучуваність останнього з іншими програмними продуктами тощо. Репозитарій виступає осередком саме ресурсного типу, оскільки дані, представлені у ньому, не є об'єктом виключно авторського права, це пов'язано з тим, що вони були створені під егідою самої установи, фінансуючись за її кошти, то «соціальний» прошарок не актуалізований у них зовсім. Повертаючись до самої проблеми репозитарію, звернемо увагу на численні спільні риси представленої у ньому інформації з даними, що наявні у вільному доступі, у випадку електронного врядування: по-перше, інформація, що розміщується у вільному доступі не є об'єктом виключного авторського права, а тому – може бути актуалізована за умови відповідно оформленого посилання; по-друге – наявна проблема захисту інформації, вирішувана неоднозначно (відсутня системність і цілісність програмного забезпечення репозитаріїв як інформаційних сервісів; особливо яскраво можна виділити цю тенденцію у контексті електронного врядування, оскільки відмінність «софту» платформи, на якій вибудовується сервіс, продукує відсутність взаємодії одразу двох вищезазначених систем «уряд – уряд» та «уряд – бізнес»). Тобто найбільший ефект від надання управлінських послуг в електронному вигляді може бути отриманий у випадку, якщо актуалізація цих послуг вимагає звернення до різних органів державної влади та органів місцевого самоврядування або їхньої взаємодії між собою, за рахунок інтеграції відомчих інформаційних систем, що підтримують відповідні процеси, та автоматизації процедур інформаційного обміну між ними. Це дозволить втілити в життя принцип «єдиного вікна», за яким звернення до інших органів влади буде здійснювати той орган, до якого звернулись за послугою [1]. Останнє створює низку успішних комунікативних сесій між урядом та урядом, урядом та бізнесом, що забезпечить цілісність, оперативність й доступність отримання необхідних даних.

Головною проблемою технологічного впровадження принципів належного врядування в життя є відокремленість програмних продуктів, роздробленість та ситуативність їхньої взаємодії [6, с. 137]. Саме тому нагальною проблемою для України є розробка і впровадження сервісно-орієнтованої архітектури електронного врядування, за якого взаємодія «уряд – громадяни» актуалізується. Довіра до уряду, переконання в тому, що державне управління є сервісно-орієнтованим, наразі виступає важливим елементом відродження адекватного обслуговування користувачів в України.

Політична комунікація, здійснювана з використанням системи електронного врядування, містить низку латентних проблем, тісно пов'язаних із проблемами інформаційної безпеки: система адміністративної влади

може тяжіти до уникнення контролю державної сфери і диктувати свої взаємовідносини між органами влади і громадськістю; можливе домінування державної безпеки над безпекою людини та суспільства; вимоги демократизації державотворення можуть спричинити втручання громадськості у цей процес, останнє може деструктивно вплинути на цілісність, прогнозованість тощо останнього; розрив між освітнім рівнем громадян та тими каналами, якими вони можуть взаємодіяти з урядом; розрив між очікуваними та фактичними результатами [4] і тому подібне.

Звичайно, що окрім згаданого клієнтоцентризму необхідним є належний рівень захисту конфіденційної інформації: це особливо актуально зараз, оскільки прошарок користувачів інформаційних технологій порівняно невисокий, а значить потрібно впевнити громадян у тому, що інноваційні сервіси, доступні завдяки новому типу моделі врядування, є безпечними й надійними. Так, необхідним ми вважаємо:

- проведення ґрунтовного й достовірного аналізу потреб громадян українського суспільства з метою виявлення «магістральних шляхів» забезпечення найзапитуваніших послуг населення, що дозволить актуалізувати наявні сервіси урядування в контексті сучасного стану суспільства;
- виокремлення можливих шляхів втрати конфіденційних даних клієнтів: апаратно-програмні (загрози цілісності даних та апаратно-програмних засобів, використання несертифікованих вітчизняних і зарубіжних технологій при створенні й розвитку інформаційної інфраструктури) й суспільно-інформаційні (неправомірне обмеження доступу громадян до відкритих інформаційних ресурсів органів державної влади, незадовільні якісні характеристики інформаційних повідомлень тощо) [4];
- розширення нормативно-правової бази й вилучення неточностей трактувань, суперечностей формулювань, подвійності тощо; створення та введення в експлуатацію організаційно-технічних, методичних засобів протидії загрозам інформаційної безпеки [4].

Висновки

Отже, однією з основних функцій органів влади є забезпечення базових потреб особистості, серед яких домінуючою є потреба у безпеці. Це пов'язано з тим, що біологічно ця потреба призводить до виживання особини, продовження її роду, а значить буквально «вмонтована» у психіку людини.

Новий час конвертував потребу у безпеці, поглибивши її смисл, витворивши його суголосно актуальних умов, в яких знаходиться біологічна одиниця – організм, а саме особливостям побудування інформації. Так, глобалізація, окрім кооперації окремих індивідуумів, спричинила абсолютно новий рівень небезпеки, в якому мають місце різноманітні шахрайства електронної сфери, одночасно витворивши проблему захисту інформації, тобто інформаційну безпеку. Значною мірою це питання лягає на органи влади, стрижневою особливістю роботи яких є забезпечення безпеки інформації клієнтів-громадян в одночасному поєднанні з такою необхідною для демократичного суспільства відкритістю останньої. На наш погляд, актуалізація поставлених завдань є можливою через забезпечення механізмів:

- захищеності створюваних інформаційних мереж, систем управління транспортом, енергетичної й банківської сфер, державного управління, військових формувань; блокування комп'ютерної злочинності (вірусів, хакерських атак, спотворення, блокування тощо електронних сервісів належного врядування);
- захисту мега-масивів даних, що накопичені про громадянина, з метою запобігання їхньому використанню зловмисниками (недопущення махінацій з електронними грошима, комп'ютерного хуліганства тощо);
- безперебійної підтримки іноземними та вітчизняними розробниками комп'ютерних мереж з метою адекватної їх роботи та виконання ними первинно заданих функцій;
- недопущення електронного контролю за життям, настроями, планами громадян, політичних організацій тощо шляхом розширення нормативно-правової бази з окресленого питання та ретельного вибудовування системи вимог до подій державного значення, що уможливлюють таке втручання уряду (підготовка терактів, заворушень тощо, що підривають саму державність);
- перешкоджання впливу інформаційної зброї на психіку, свідомість громадян через регулярне дослідження каналів інформації, що можуть бути використані зі злочинним наміром (першою чергою – мас-медіа);
- належного володіння й використання державними службовцями нових інформаційних технологій шляхом підвищення їхньої кваліфікації, а також розроблення системи професійних заохочень.

Перспектива дослідження – у подальшій розробці ролі нових інформаційних технологій у оптимізації роботи органів влади з метою актуалізації їх роботи не тільки в контексті європейських тенденцій діяльності урядовців, а й суголосно розвитку українського суспільства з метою його подальшого розквіту у контексті європейської інтеграції. Таким чином, реалізація взаємодії держави та суспільства в Україні має здійснюватись через застосування механізмів вироблення сервісно-орієнтованої державної політики [7, с. 330, 8 с. 70], в контексті розвитку сфери інформаційної безпеки.

Література.

1. Баранов О. А. Концепція розвитку електронного урядування в Україні: [електронний ресурс] / О. А. Баранов, М. С. Демкова, С. В. Дзюба та ін.; за ред.: А. І. Семенченко // Мастерская е-управления: муниципально-общественный центр электронного управления. – Электрон. данные. – Режим доступа: http://www.e-gov.in.ua/idata/files/140612-121916-2516.doc. – Название с экрана.

2. Гладких А. А. Базовые принципы информационной безопасности вычислительных систем: учеб. пособ. для студентов, обучающихся по специальностям: 08050565, 21040665, 22050165, 23040165 / А. А. Гладких, В. Е. Дементьев. – Ульяновск: УлГТУ, 2009. – 156 с.

3. Довгань А. В. Взаимодействие со смыслом в контексте теории действующих вещей и буддизма / А. В. Довгань // Доклады Национальной академии наук

Республики Казахстан. – 2014. – № 4. – С. 100–104. – Библиогр.: 8 назв.

4. Дубов Д. В. Інформаційна безпека в умовах впровадження електронного урядування: [електронний ресурс] / Д. В. Дубов // Національний інститут проблем міжнародної безпеки. – Електрон. дані. – Режим доступу: http://www.niisp.org.ua/dubov_~1.pdf. – Назва з екрану.

5. Дяченко Н. Прогнозні оцінки динаміки впровадження електронного урядування в Україні / Н. Дяченко // Державне управління та місцеве самоврядування. – 2013. – Вип. 13. – С. 134–142. – Бібліогр.: 8 назв.

6. Карпенко О.В. Механізми впровадження програмного забезпечення в органах державного управління / О.В. Карпенко // Державне управління: теорія і практика [Електронний ресурс]: електрон. наук. фах. вид. – 2006. – №1. – Режим доступу: http://www.academy.gov.ua/ej3/txts/TEXNOLOGIYA/05-KARPENKO.pdf / 2006–1. – Заголовок з екрану.

7. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : Дис... д-ра наук з держ. упр.: спеціальність 25.00.02 «Механізми державного управління» / Карпенко Олександр Валентинович; Нац. Акад. держ. упр. при Президентові України. – К., 2016. – 466 с.

8. Карпенко О. Формування правових засад сервісної діяльності органів державної влади в Україні: комунікативний аспект розвитку / Олександр Карпенко // Актуальні проблеми державного управління: Збірник наукових праць ОРІДУ. – 2013. – Вип. 4(56). – С. 61–71.

9. Клімушин П. С. Електронне урядування в інформаційному суспільстві: монограф. / П. С. Клімушин, А. О. Серенок. – Х.: Вид-во ХарРІ НАДУ «Магістр», 2010. – 312 с.

10. Пєвцов Г. В. Модель регіону України як об'єкту забезпечення інформаційної безпеки: [електронний ресурс] / Г. В. Пєвцов // Харківський університет Повітряних сил. – Електрон. дані. – Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/7598/soi_2010_5_3.pdf. – Назва з екрану.

11. Щеглюк С. Д. Електронне урядування як інструмент модернізації державного управління міським розвитком: [електронний ресурс] / С. Д. Щеглюк // Національна бібліотека України імені В. І. Вернадського. – Електрон. дані. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/regek_2015_2_8.pdf. – Назва з екрану.