УДК 35.077.6

П.С. КЛІМУШИН, А.О. СЕРЕНОК

ЗАСОБИ ОБМІНУ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ В СИСТЕМІ ЕЛЕКТРОННОГО УРЯДУ

***Р**озглянуто проблеми підвищення ефективності державного управління через вдосконалення організаційних, правових і технічних механізмів взаємодії інфраструктур суспільства в системі Електронного Уряду.*

***T**he article is devoted to the problem of effectiveness increase of government by improvement the organizational, legal and technical procedure of society infrastructures' interaction in electronic government system.*

З позиції управління соціальними системами, електронний уряд [4] – це система збору, введення, пошуку, обробки, збереження та надання на вимогу користувача згідно з визначеними критеріями інформаційних ресурсів. Ця система покликана забезпечити надання державними органами всіх гілок влади численних послуг бізнесу та всім категоріям громадян, а також інформування громадян про роботу державних органів. Електронне врядування є не простим технологічним рішенням, а інноваційною концепцією управління державою.

Світовий досвід впровадження електронного врядування дозволяє виділити три етапи:

– інформаційний – надання в Інтернеті інформації про діяльність органів влади (розклад прийомних годин, контактні телефони посадових осіб, інформація про діяльність органу влади, опис процедури одержання необхідних послуг);

– інтерактивний – реалізується зворотній зв'язок користувача з інформаційним ресурсом (електронна приймальня, форум, конференція, заповнення бланків документів на надання певних послуг);

– інтегрований – створення єдиної національної інформаційної системи для надання всього комплексу адміністративних послуг (перерахування через Інтернет плати за надану послугу; контролювання процесу проходження документів; одержання соціальної допомоги; занесення на облік на біржі праці; оформлення паспорту, посвідчення водія, посвідчення про шлюб і народження дитини; занесення на облік авто; подання заяви в правоохоронні органи; отримання консультації від державного службовця; участь в обговоренні законопроекту; рішення питань, пов'язаних з реєстрацією бізнесу, подачею звітності, сплатою податків, оформленням митних декларацій).

Класифікація Євросоюзу передбачає 20 видів основних державних послуг, які повинні надаватися в електронному виді. Усього ж у Євросоюзі більше 80 % суспільно – орієнтованих служб мають інтерактивний "офіс" [6]. Високий рівень розвитку електронного врядування спостерігається у США. Одним із піонерів введення електронного врядування на території колишнього Радянського Союзу

стала Естонія, що впровадила національну інформаційну систему. Вона першою з пострадянських республік навіть надала громадянам можливість голосувати на виборах через Інтернет. Численні посвідчення й документи – паспорт, права водія, амбулаторну картку – естонцеві заміняє персональна ID-карта.

Розвиток електронного врядування в Україні перебуває в стадії трансформації від першого інформаційного етапу до другого – інтерактивного етапу. Концепція розвитку електронного врядування підкріплена відповідними законами, державними програмами й іншими нормативними актами [1; 2]. Усі органи вищої державної влади, міністерства, відомства, комітети, служби, більшість міських рад мають свої представництва у Всесвітній Мережі. Здебільшого, електронне врядування має поки що інформаційний характер, до справжньої інтерактивної взаємодії ще далеко. Проте, вже зараз пересічний користувач Інтернету може порушити питання перед органом влади через електронну приймальню, розрахуватися за комунальні послуги, замовити необхідну покупку через Інтернет – магазин, заповнити і відправити податкову декларацію до податкової інспекції або надати звітні документи до пенсійного фонду.

У зв'язку із цим, актуальне завдання подальшого розвитку інтерактивних схем взаємодії органів влади, бізнесу й громадян у системі електронного врядування. Метою проведених досліджень є підвищення ефективності державного управління за рахунок удосконалювання організаційних, правових і технічних механізмів взаємодії різних інфраструктур суспільства.

Ефективність роботи органів державного управління визначається трьома факторами: ефективністю взаємодії з громадянами та підприємцями, ефективністю внутрішньої роботи кожної установи та ефективністю взаємодії органів державної влади між собою. Очевидно, успішне подолання зазначених факторів у системі електронного уряду можливе на основі розвитку інфраструктури захисту інформації з використанням систем обміну конфіденційною інформацією.

У цілому для корпоративних систем Інтернету існують два основних виду погроз для комп'ютерної інформації:

– порушення конфіденційності інформації, тобто несанкціоноване ознайомлення з нею;

– порушення цілісності інформації, тобто, її несанкціонована модифікація.

Відповідно до перелічених погроз існує ще два основних методи захисту інформації:

– шифрування інформації для забезпечення її конфіденційності;

– застосування електронного цифрового підпису (ЕЦП) для забезпечення її цілісності.

Останнім часом у світі зростає кількість проектів, метою яких є організація обміну конфіденційною інформацією між державними органами в системі телекомунікаційних мереж. Сьогодні цілий ряд країн, таких як США, Англія, Швеція, Франція, Канада, Німеччина, Австралія перейшли на без-паперову технологію обміну документами через Інтернет. Здійснюється перехід до електронного документообігу і в Україні (подання в органи влади бухгалтерської і податкової звітності через Інтернет). Виходячи з об'єктивної закономірності цього переходу, у статті розглянуті проблеми впровадження систем обміну конфіденційною інформацією в Україні.

Із прийняттям законів "Про електронний цифровий підпис" [1], "Про електронні документи та електронний документообіг" [2] в Україні створені законодавчі передумови для розвитку систем електронного документообігу.

Система електронного документообігу є найбільш ефективною на відміну від традиційної системи документообігу (паперової) та більш легко піддається оптимізації. Перевагами системи електронного документообігу є: підвищення швидкості обміну інформацією, скорочення витрат на обробку та зберігання документів.

У звичайній системі документообігу з кожним роком потік документів збільшується на 15 – 20 %, порядку 30 % робочого часу витрачається на пошук й узгодження документів, при цьому 6 % документів безповоротно губляться, кожен внутрішній документ копіюється до 20 разів, у середньому кожен співробітник витрачає 150 годин у рік на пошук загубленої інформації, що в результаті приводить до значного зниження продуктивності праці.

Таким чином, звичайна система документообігу має потребу в удосконалюванні. Найбільш ефективний засіб вирішення цієї проблеми можливий із впровадженням електронного документообігу на основі ЕЦП. Розрахунки показують, що в деяких сферах суспільної діяльності інформатизація дозволяє збільшити продуктивність праці в 3-4 рази [3].

Кінцевою метою даної роботи є виявлення проблем впровадження електронного документообігу в Україні для подальшого вироблення практичних рекомендацій, спрямованих на найбільш ефективний розвиток системи обміну конфіденційною інформацією в органах влади.

Беручи до уваги майбутню інтеграцію України до європейської спільноти, можна виділити такі сучасні українські проблеми [5]:

– невідповідність державних стандартів електронного цифрового підпису міжнародним стандартам і рекомендаціям (країни ЄС використовують близько 35 різних криптографічних алгоритмів, Україна – 4: ГОСТ 28147-89 – симетричне шифрування, ДСТУ 34310-95 і ДСТУ 4145-2002 – цифровий підпис, ДСТУ 34311-95 – кешування, жоден з яких, не є стандартом у країнах ЄС; український стандарт сертифіката ЕЦП відрізняється від європейського);

– наявність великої кількості неурегульованих питань в області впровадження стандартів цифрового підпису, гарантованої цілісності електронних документів, засвідчених ЕЦП;

– значна кількість порушень у практиці застосування технологій цифрового підпису суб'єктами господарської діяльності, спрощення підходу до захисту електронної інформації ЕЦП;

– відсутність судової практики в розгляді справ про цифровий підпис;

– відсутність методик проведення експертизи документів із цифровим підписом;

– не врегульоване питання забезпечення діяльності і розвитку Центрального засвідчуваного органу, а центри сертифікації ЕЦП діють розрізнено без єдиної термінології;

– надзвичайно низькі темпи розвитку інфраструктури сертифікації ЕЦП (за чотири роки після прийняття основних законів про ЕЦП і документообіг створені тільки одиниці ЦСК, серед яких перший акредитований центр з'явився тільки в 2006 р.).

Потрібно також зазначити, що "вставка" (підміна) прийнятих в Україні стандартів криптографічних алгоритмів у західне програмне забезпечення є дуже складним (часто практично неможливим) завданням.

Основна проблема пов'язана зі слаборозвинутою інфраструктурою сертифікації ЕЦП і знаходиться у законодавчому полі.

Для розвитку інфраструктури доцільно використати механізм правового поширення ЕЦП на безкоштовній основі без прирівнювання її до рукописного підпису (з юридичною силою). Доцільність цього висновку доводить досвід впровадження ЕЦП у деяких країнах Євросоюзу, наприклад, Німеччини, а також пілотний проект з подання звітності в податкові органи України, реалізований на безкоштовній основі, де кількість учасників з кожним роком значно росте. Другий шлях реалізується пенсійним фондом України, заснований на сертифікованої, а, отже, платній структурі ЕЦП, де кількість учасників досить обмежено.

У вигляді розрізнених відомчих підходів у створенні структур ЕЦП доцільно заснувати асоціації електронного цифрового підпису на Україні із залученням всіх зацікавлених сторін як організаційного механізму популяризації і ефективного впровадження ЕЦП у всіх сферах суспільного і економічного життя країни.

У цьому зв'язку необхідне спільне виконання таких питань [6]:

– створення і розгортання інфраструктури електронного цифрового підпису та інфраструктури відкритих ключів у цілому в Україні;

– створення і впровадження систем електронного цифрового підпису в інформаційних системах корпоративних замовників, суб'єктів господарської діяльності і фізичних осіб, забезпечення інформаційної взаємодії систем і засобів, які використовують електронний цифровий підпис і шифрування інформації між собою;

– здійснення співробітництва в галузі виконання наукових і науково-практичних питань розробки, створення, упровадження і забезпечення безпеки функціонування захищених інформаційних технологій, систем і засобів криптографічного захисту інформації;

– створення механізмів інвестування розвитку сучасних інформаційних технологій, надання інформаційної, консультативної, методичної і практичної допомоги в питаннях, які мають відношення до ЕЦП;

– взаємодія в накопиченні необхідної інформації, формуванні матеріально-технічної, науково-методичної і нормативної бази даних, що не містить інформації з обмеженим доступом згідно із чинним законодавством, а також проведення наукових досліджень;

– організація і здійснення співробітництва щодо інфраструктур ЕЦП на міжнародному рівні.

Без адекватного рішення вище перерахованих проблем можлива міжнародна ізоляція України в майбутньому.

Нагадаємо, що в листопаді 2005 р. Генеральна асамблея ООН прийняла Конвенцію про використання електронних повідомлень у міжнародних угодах, розроблену Комісією ООН з питань права міжнародної торгівлі. Конвенція розвинула положення, закладені в розробленому раніше "Типовому законі про електронну комерцію" і "Типовому законі про електронний підпис", і визначила правовий

статус електронних повідомлень, що відносяться до висновку чи виконанню угод міжнародної торгівлі.

У свою чергу, Європарламент прийняв програму впровадження до 2010 р. єдиної інформаційної системи митних органів. Документ передбачає формування єдиної бази митних декларацій. Уся система будується на розумінні електронного підпису, цифрових сертифікатів, які несумісні з вітчизняними. Починаючи вже з 2007 р., у випадку, якщо всі документи, пов'язані з міжнародними перевезеннями і поставками, не будуть надаватися в електронному виді, підписані ЕЦП, Україна потрапляє в положення третьої країни (тобто документи вітчизняних суб'єктів господарської діяльності будуть розглядатися за залишковому принципу).

Резюмуючи викладене, можна припустити, що обсяг паперового документообігу, буде наближатися до нуля, а ефективне функціонування системи електронного документообігу є необхідною умовою входження до ЄС.

Організація конфіденційного обміну інформацією в сучасних електронних системах реалізується різними засобами. Найбільш широке поширення одержали системи PGP та PKI, що забезпечують високий ступінь захищеності переданої інформації. Переваги даних систем, на відміну від звичайної системи, полягають у тому, що вони забезпечують не тільки ідентифікацію документа, тобто підтверджують його відношення до певної особи, що поставила підпис, але й підтримують аутентифікацію документа, тобто його цілісність і незмінність.

Відмінності систем PKI і PGP перебувають у найбільш прийнятній структурі організації сертифікації дійсності ключів: у PKI використовується ієрархічна структура сертифікації вповноваженими органами, в PGP – мережна, орієнтована на партнерські відносини.

Крім того, є певне розходження в стандартах розглянутих систем.

В основу PGP покладено стандарт OpenPGP, що містить: відомості про власника сертифіката, відкритий ключ власника сертифіката, ЕЦП власника сертифіката, період дії сертифіката, кращий алгоритм шифрування.

В основу PKI покладено стандарт X.509, що містить: відкритий ключ власника сертифіката, серійний номер сертифіката, унікальне ім'я власника, період дії сертифіката, унікальне ім'я видавця, ЕЦП видавця та ідентифікатор алгоритму підпису.

Аналіз даних стандартів дозволяє зробити низку фундаментальних різниць:

– сертифікат PGP створюється особисто партнером по виду діяльності, сертифікат X.509 може засвідчуватися центром сертифікації;

– сертифікат X.509 містить тільки одне ім'я власника сертифіката;

– сертифікат X.509 містить тільки одну ЕЦП, що підтверджує дійсність сертифіката.

Слід зазначити, що система PGP споконвічно створювалася для потреб приватних користувачів і призначалася для роботи з електронною поштою, надалі PGP стали пристосовувати під потреби захисту електронного документообігу. Названа система може виступити вдалим рішенням для внутрішніх корпоративних цілей, коли завірителем сертифіката є вповноважене адміністрацією установи особа. У свою чергу, система PKI дає можливість завірити дійсність сертифіката сторонньою

вповноваженою установою, що підтверджує особистість відправника. Не зречення як проблема аутентифікації вирішується в даній системі не тільки шляхом чіткої фіксації авторства, але й часу створення документа за допомогою спеціального модуля служби штампів часу (TSA). Використовуючи цей сервіс, можливо, створити систему, що забезпечить не зречення не тільки за іменем творця, але і за часом створення документа.

Аналіз даних систем дозволяє зробити такі висновки: PGP й PKI це дві схожі, але все-таки різні системи. Перша призначена для неструктурованого захищеного обміну даними. PKI забезпечує обмін зашифрованими даними як на локальному, так і на міжмережевому рівні з достатнім ступенем вірогідності. У цей час технологія PGP розвивається убік сумісності з PKI. Однак досвід показує, що для обміну конфіденційною інформацією в органах влади віддається перевага технології PKI.

Придбання одних тільки програм шифрування на основі стандарту X.509 не створює повною мірою саму інфраструктуру PKI. Необхідно використати сертифіковані для України криптопровайдери, а також забезпечити взаємодію з офіційними вітчизняними центрами сертифікації.

Переваги системи PKI відносно забезпечення безпеки, а також забезпечення вірогідності дозволяють говорити про доцільність її впровадження в систему обміну конфіденційною інформацією в органах влади.

У вітчизняному законодавстві визначені суб'єкти ієрархічної інфраструктури сертифікації ключів, їхній статус, права, функції і обов'язки [2], на що орієнтовано систему PKI. Така система включає: центральний (кореневий) центр, що засвідчує, сертифікації ключів і центри сертифікації ключів (ЦСК), а також певний контролюючий орган для забезпечення безпеки і надійності функціонування всієї системи в цілому в особі Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України. Центральний орган, що засвідчує, перебуває під управлінням державного органу з питань інформатизації – Державного департаменту з питань інформатизації. Слід зазначити, що політика сертифікації ЦСК не контролюється з боку держави і ступінь довіри до них є справою його клієнта.

На сьогодні для генерації ключів ЕЦП, формування звітів і проведення контролю, уведених у звіт даних, підписання й шифрування звітів і відправлення їхньому контролюючому органу з наступним повідомленням про їхнє прийняття, необхідно використати спеціалізовані програмні комплекси (автоматизовані робочі місця) залежно від певного відомства. Безсумнівно, таке положення справ знижує технічну доступність й ефективність реалізації систем обміну конфіденційною інформацією.

У цьому зв'язку очевидна необхідність інтеграції всіх систем на єдиній інформаційній і технологічній платформі як основного інформаційного – технічного механізму розвитку інфраструктур засобів конфіденційного обміну інформацією в системі електронного врядування. За основу побудови такої системи може бути прийнятий комплекс "Бест звіт плюс" (на основі інтеграції із широко використовуваними на ринку України інформаційними системами управління підприємствами "Галактика", "1С", "Вітрило").

Таким чином, у результаті проведених досліджень виявлені закономірні етапи розвитку електронного врядування і визначені організаційні, правові та технічні механізми вдосконалювання засобів конфіденційного обміну в системі Електронного Уряду.

Реалізація даних механізмів дозволить оптимізувати систему оберту конфіденційної інформації в органах державної влади і забезпечити ефективність їхнього функціонування в умовах вступу України до ЄС.

Література:

1. Закон України "Про електронний цифровий підпис" від 22 травня 2003 р. № 852-IV // ВВР України. – 2003. – № 36. – Ст. 276.

2. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. № 851-IV // ВВР України. – 2003. – № 27. – Ст. 275.

3. *Гаврилов О.А.* Курс правовой информатики. – М.: НОРМА-ИНФРА, 2000. – С. 38.

4. *Клименко І.В., Линьов К.О.* Технології електронного урядування. – К.: Центр сприяння інституційному розвитку державної служби, 2006. – 192 с.

5. *Степаненко В.* Электронная цифровая подпись // Сети и бизнес. – № 6 (31). – 2006. – С. 82 – 91.

6. Сайт про електронний цифровий підпис. – Режим доступу: http://www.e-signature.com.ua

Надійшла до редколегії 20.08.2008 р.