УДК 35.077.6

П. С. КЛІМУШИН

ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

***В**изначено принципи забезпечення національної інформаційної безпеки в умовах динамічного розвитку міжнародного ділового документообігу.*

***I**n the article the principles of construction of the national informative system of safety at development of international business legally meaningful circulation of documents in the conditions of informative society are definite.*

Останніми роками стрімко змінюється парадигма розвитку людського суспільства, яка направлена на глобалізацію економіки і перехід до інформаційного суспільства [1]. Стрімкий розвиток даних тенденцій призводить до негативних процесів у частині безконтрольного розповсюдження інформації і виникнення кібертероризму, що завдає збитку сучасної цивілізації. Живильним ґрунтом для численних зловживань у кіберпросторі є переважно анонімна логіка розвитку Інтернету. За цих умов міжнародне співтовариство вимушено виробляти адекватні заходи.

Одним з таких заходів є використання електронного цифрового підпису (ЕЦП). Ключова властивість ЕЦП – це додаткова функціональність, можливість зберігання і передачі електронних документів в цілісності і незмінному вигляді із забезпеченням їх юридичної значущості і гарантованою підтримкою авторства в судових інстанціях.

Функціонування цифрового підпису можливо зі створенням інфраструктур, які в міжнародній термінології мають назву "інфраструктури відкритих ключів" або PKI (public key infrastructure). Усі розвинуті країни світу нарощують такі інфраструктури, формуються вони і в Україні [4].

Проблема полягає в тому, що створювані в світі національні інфраструктура PKI, навіть в об'єднанній Європі, слабо взаємодіють один з одним, оскільки не забезпечують необхідну юридичну значущість трансграничних комунікацій. Складність цієї проблеми полягає у ступені міждержавної довіри у сфері національної інформаційної безпеки, оскільки в основі вживаних цифрових підписів лежать різні національні криптографічні алгоритми і стандарти їх сертифікації.

Аналіз останніх досліджень А. Єгорцева, В. Степаненко [6; 7] свідчить, що країни Євросоюзу в загальній сукупності використовують близько 35 різних криптографічних алгоритмів, Україна – 4. Наслідком таких відмінностей є неможливість повноцінно використовувати такий могутній інструмент інформаційного суспільства, як Інтернет, з метою ділового документообігу: міжнародна електронна торгівля, адміністративні послуги, телемедицина, дистанційна освіта, електронне правосуддя, фінансові платежі та інші завдання.

У свою чергу, ключовою вимогою ділового документообігу є його юридична значущість, тобто можливість пред'явлення документів до судових органів у разі

виникнення конфліктної ситуації. При цьому для електронних документів дана вимога представляється особливо актуальною [2].

У зв'язку з цим, актуальне завдання дослідження організаційних, правових і технологічних принципів практичного використовування юридично значущих електронних документів у діловому документообігу.

Метою досліджень, що проводяться, є забезпечення національної інформаційної безпеки в умовах динамічно розвиваючого міжнародного ділового документообігу.

Сьогодні інтенсивно ведеться опрацьовування цієї проблеми, перш за все з технологічних позицій. Одна з можливих технологій, умовно названа "електронний нотаріат", націлена на збереження в різних країнах власного простору довіри при забезпеченні можливості трансграничного обміну електронними документами. Ця технологія атестована у взаємодії країн Євросоюзу.

Проте для практичного застосування такої технології буде потрібно прийняти спеціалізовану Конвенцію про порядок визнання електронних документів або внести зміни в Гаагську конвенцію 1961 р. "Про апостілях" про взаємне міждержавне визнання звичайних паперових документів.

Таким чином, проблема, яка виникла в умовах відсутності меж у глобальному інформаційному просторі, не може бути ефективно вирішена тільки в національному форматі. У цьому напрямку транснаціональні корпорації інвестують величезні фінансові ресурси в розвиток нових систем обміну даними. Так, сучасний мобільний телефон у промисловому виконанні сполучений з персональним комп'ютером при забезпеченні повсюдного доступу в Інтернет. Результатом такої реалізації є необхідність не тільки міжнародного роумінгу мобільній телефонії, що стало вже звичним, але і забезпечення роумінгу інформаційних послуг, де голосовий зв'язок буде одним з багатьох доступних сервісів, у тому числі юридично значущих.

Останнє завдання ефективно може бути вирішеним тільки досягши відповідних міждержавних домовленостей, оскільки стосується питання захисту прав громадян, що знаходяться під юрисдикцією різних національних законодавств. Після цього використовування ЕЦП для аутентифікації учасників юридично-значущих комунікацій стане масовим. Така логіка ринкового попиту і задоволення потреб користувачів. Це стане реаліями світового інформаційного суспільства.

Перша спроба регулювання на рівні міжнародного права питань юридично значущої електронної взаємодії суб'єктів правовідносин відбувається на Генеральній асамблеї ООН 23 листопада 2005 р. з ухваленням Конвенції про використання електронних повідомлень у міжнародних договорах [3].

Проте разом з прогресивними ідеями ця Конвенція має низку суттєвих недоліків. До них слід віднести такі:

1. Конвенція покликана регулювати відносини між суб'єктами підприємницької діяльності. Її дія не розповсюджується на відносини у сфері між держорганами, державою з бізнесом, державою з громадянами, бізнесом з громадянами і між громадянами. Більш того, дія Конвенції обмежена у сфері фінансових і фондових ринків між суб'єктами бізнесу. У результаті сфера застосування Конвенції сильно звужена.

2. У Конвенції повсюдно використано тлумачення "технологічної нейтральності" інформаційно-телекомунікаційних систем. Таке тлумачення не сприяє практичній

побудові міжнародних інформаційно-телекомунікаційних систем і не дозволило стандартизувати інтерфейсну взаємодію національних систем PKI і створити єдиний міжнародний простір довіри, особливо тих, що використовують інформаційно-безпечні рішення.

3. У світі з'явилося спеціалізоване національне законодавство про цифрові підписи, і системи PKI сьогодні практично використовуються в більшості розвинутих країн, але на ці законодавства і системи в Конвенції немає ніяких посилань.

4. Конвенція не формує міжнародне право у сфері взаємного визнання електронних документів, і через це не може представити ефективний механізм використання електронних повідомлень у міжнародних договорах. Звідси існує реальна проблема досягнення інтероперабельності національних PKI, оскільки в різних країнах використовуються несумісні між собою стандарти цифрових підписів.

5. Однією з основних проблем Конвенції є те, що вона робить невдалу спробу правового регулювання "електронних повідомлень", тоді як основою ділового спілкування, що склалося, є поняття "електронного документа".

Для додання електронному повідомленню статусу електронного документа сьогодні є практична можливість використовування механізму цифрових підписів та інфраструктури PKI. Виходячи з цих технологічних реалій, значно продуктивніше здійснювати правове регулювання в кіберпросторі на основі базового поняття "електронного документа". Це представляється актуальним не тільки для ділового документообігу, але і для всіх інших сфер юридично значущого електронного спілкування в усіх ланках: держава – бізнес – громадяни.

Таким чином, дана конвенція має локальний характер, і назріла необхідність запропонувати світовому суспільству новий проект міжнародного права, що знімає відзначені недоліки в таких напрямках: розширення сфери застосування, зміна тлумачення принципу "технологічної нейтральності" і перехід до правового регулювання електронного документообігу замість обміну електронними повідомленнями.

В основу нового проекту доцільно покласти такі концептуальні ідеї:

1. Юридично значуща електронна взаємодія піднімає питання забезпечення прав громадян різних країн, і міжнародне законодавство повинне створювати, в першу чергу, передумови для застосування інформаційних систем, що гарантують захист цих прав.

2. Під забезпеченням захисту прав громадян в електронному просторі доцільно розуміти надання державами своїм громадянам можливості використовування гарантованих юридично значущих інформаційно-безпечних послуг, у тому числі при трансграничній взаємодії.

3. Для всіх демократичних держав завдання із забезпечення і захисту конституційних прав громадян є пріоритетними, і вони повинні знайти адекватне рішення не тільки в традиційному тлумаченні – фізичному, але також і в глобальному електронному просторі, перш за все в мережі Інтернет.

4. Створення міжнародного захищеного інформаційного простору представляється оптимальним на основі національних сегментів довіри з використанням національної інфраструктури відкритих ключів і забезпеченням їх інтероперабельності в єдиному світовому просторі довіри.

Наслідуючи мету – забезпечення інформаційної безпеки – сьогодні людське співтовариство повинне зробити усвідомлений вибір: або погодитися із яких-небудь причин зі станом речей, що склався в криміналізованому кіберпросторі, або спільно виробити заходи з протидії наявним негативним тенденціям.

Найактуальнішим представляється створення цивілізованих сегментів у кіберпросторі для протидії негативним тенденціям. При цьому може виникнути питання про забезпечення свобод громадян за наявності деякого виділеного цивілізованого сегменту Інтернет. Кожний громадянин вільний у своїх рішеннях – знаходитися в кіберпросторі або анонімно, або авторизовано. Інтернет вирішує першу можливість, держави світу своїми сумісними зусиллями повинні забезпечити другу можливість.

Сьогодні в Інтернеті є декілька найпоширеніших ідентифікаційних технологій:

– ідентифікація, заснована на криптографічних алгоритмах (симетричних і асиметричних) перетворення інформації, до яких відноситься і цифровий підпис, – є достатньо дорогою і складною, але при цьому забезпечується математично доказовий ступінь захисту;

– ідентифікація за допомогою доменного імені – у разі фіксованого зв'язку дозволяє визначити місцезнаходження комп'ютера, але не людини, що створила електронний документ, а у разі мобільного зв'язку – не дозволяє і цього;

– ідентифікація за допомогою пароля – є найпоширенішою, але і легко компрометованою;

– ідентифікація за допомогою псевдонімів – тотожна анонімності.

Вибір технології самоідентифікації повинен залишатися, безумовно, за громадянином. Проте держава повинна виразно роз'яснити йому можливі наслідки, що виникають у результаті застосування тієї або іншої технології.

Таким чином, демократичні держави зобов'язані в питаннях безпеки працювати на випередження, створюючи необхідні організаційні, правові і технологічні можливості, для надійного забезпечення і захисту прав громадян у глобальному електронному просторі. Саме на це повинне бути націлено відповідне національне і міжнародне законодавство.

У таких умовах все більше значення набувають технології захисту систем електронних документів як від зовнішніх, так і від внутрішніх загроз.

Основними принципами забезпечення національної інформаційної безпеки в умовах інформаційного суспільства на основі аналізу світового досвіду, є такі:

1. Принцип системності має на увазі необхідність захисту електронних документів на всіх етапах їх життєвого циклу – від створення, обробки і зберігання до передачі по каналах зв'язку і знищення. Такий захист включає як технічні засоби, так і заходи організаційного характеру і повинен бути направлений і на самі документи, і на програмні комплекси електронного документообігу.

Система захисту повинна забезпечувати конфіденційність (гарантію доступу до даних тільки певних осіб), цілісність (захист від випадкових і навмисних спотворень і підмін) і готовність (можливість у будь-який час користуватися документами відповідно до встановленої політики безпеки) об'єктів електронних документів.

2. Принцип рівноміцності всіх ланок ланцюга захисту. Він означає, що слід враховувати всі види ризиків, включаючи вірусне зараження, несанкціонований

доступ до документів, незаконне копіювання, ненавмисні помилки, що ведуть до спотворень, відмови апаратних і програмних засобів та інші.

3. Принцип розмежування прав доступу, що полягає в наданні різним користувачам різних повноважень на виконання конкретних операцій над документами.

4. Принцип багаторівневої і багатокомпонентної аутентифікації. При багаторівневій аутентифікації для доступу до захищеної інформації використовуються багатоступінчаті засоби захисту, наприклад, паролі доступу, ідентифікаційні ключі, біометричні дані користувача і так далі. Багатокомпонентість же означає, що для доступу до критично важливих документів потрібна ідентифікація в системі відразу декількох користувачів. За принципом дії даний підхід можна порівняти з банківською практикою зберігання ключів від різних замків особливо важливого сейфа у різних співробітників. Для відкриття сейфа потрібна їх спільна діяльність, а значить, забезпечується взаємний контроль.

5. Принцип відвертості криптографічних алгоритмів використовується для забезпечення аутентифікації користувачів, цілісності та незмінності документів. Застосовуються як протоколи симетричного шифрування, які вимагають управління великою кількістю ключів, так і асиметричні схеми, що володіють підвищеною ресурсоємкістю. Досить часто використовуються гібридні схеми, що дозволяють максимально використовувати переваги обох підходів.

6. Принцип економічної виправданості полягає в необхідності дотримання розумного балансу між ефективністю системи захисту, витратами ресурсів на її створення і підтримку, зручністю і психологічним комфортом користувачів.

Реалізація розглянутих принципів інформаційної безпеки дозволяє створити максимально захищені системи документообігу. Оптимальним представляється формування в єдиному Інтернет-просторі сегментів довіри на основі національної інфраструктури відкритих ключів із забезпеченням їх інтероперабельності в єдиному світовому просторі довіри.

Література:

1. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" // ВВР України. – 2007. – № 12. – 102 с.

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

3. Генеральна асамблея ООН. Конвенція про використовування електронних повідомлень у міжнародних договорах. Комісія ООН по праву міжнародної торгівлі, за 2005р. – Режим доступу : hhtp//:www.directum-journal.ru.

4. *Клімушин П. С.* Підвищення ефективності діяльності державних підприємств за рахунок автоматизації управлінських технологій / П. С. Клімушин // Актуальні проблеми державного управління : зб. наук. пр. : у 2 ч. – Х. : Вид-во ХарРІ НАДУ "Магістр", 2006. – № 2 (28). – Ч. 1. – С. 90–95.

5. *Клімушин П. С.* Інформаційні представництва органів державної влади України / П. С. Клімушин, А. О. Серенок // Теорія та практика державного управління : зб. наук. пр. – Вип. 1 (16). – Х. : Вид-во ХарРІ НАДУ "Магістр", 2007. – С. 31–36.

6. Сайт об электронной цифровой подписи. – Режим доступу : http://www.e-signature.com.ua.

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

Надійшла до редколегії 10.02.2009 р.