УДК 004.9

Ю.І. ГОРБЕНКО, канд.техн. наук, Ю.В. ГОНЧАРОВА

ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ: ПОНЯТТЯ, ВИЗНАЧЕННЯ, ВИМОГИ

Вступ

Розвиток систем електронної інформаційної взаємодії, інфраструктури електронного документообігу є актуальним завданням для України, що і знайшло відображення у Програмі економічних реформ на 2010 – 2014 роки «Заможне суспільство, конкурентоспроможна економіка, ефективна держава», затвердженій Указом Президента України від 12.03.2013 №128/2013 [2, 5]. У цій програмі міститься низка заходів у напрямку розбудови електронного урядування, зокрема «удосконалення державного регулювання та контролю за додержанням законодавства про електронний цифровий підпис». Побудова електронного інформаційного суспільства, насамперед, спирається на довіру, необхідну для взаємодії всіх об'єктів та суб'єктів інформаційного суспільства. Століттями паперового діловодства створено інфраструктуру довіри, засновану на підписах і печатках. Завдання XXI століття – побудувати досконалішу інфраструктуру в інформаційному суспільстві, тобто у віртуальному світі.

Зважаючи на зазначене, актуальності набуває задача розпізнання особистості, відокремлення її серед безлічі інших. Механізм цього отримав назву ідентифікації, проте й досі Законодавцем не надано коректного визначення цього поняття, що стає причиною постійних понятійних колізій.

Метою цієї роботи є розробка загального визначення поняття «електронна ідентифікація», запропонування його для використання у проекті Закону України «Про внесення змін до Закону України «Про електронний цифровий підпис».

Актуальність роботи: 10 квітня 2013 року Міністерством юстиції було затверджено Концепцію реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг. Основною ціллю її прийняття стала підготовка нормативно-правової бази для повноцінного функціонування електронних довірчих послуг в Україні. Проте, першоджерелом у цьому питанні можна вважати прийняту спочатку Пропозицію, а після і сам проект Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку.

14 червня 2013 року Міністерством юстиції України було опубліковано для обговорення проект Закону України «Про внесення змін до Закону України «Про електронний цифровий підпис». Законопроектом пропонується удосконалити державне регулювання та контролю за додержанням законодавства про електронний цифровий підпис, а також реформувати законодавство у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг у два етапи: внесення змін до існуючого Закону (з 01.01.2014) та викладання Закону України із зміною його назви на Закон України «Про електронний підпис та електронні довірчі послуги» у новій редакції (з 01.01.2017). Станом на 5/02/14 вже існує ще один проект Закону, окремі пункти якого обговорені у цій статті.

Згадані документи, попри існуючу багатоманітність поглядів щодо інтеграції з Європою, можна сміливо вважати першими кроками на шляху розвитку електронних послуг не тільки в Україні, а й в усьому світі:

1. Було вперше запропоновано термін електронної ідентифікації та електронних довірчих (трастових, від англ. to trust – довіряти) послуг;
2. Відокремлено межі функціонування електронних довірчих послуг, а також шляхи їх розвитку, що планується реалізувати протягом п'ятьох років;
3. Висвітлена необхідність формування нової та реформування існуючої нормативно-правової бази, а також необхідність переглянути існуючі акти, особливо щодо електронного цифрового підпису, адже саме ця послуга, реалізуючи механізм електронної ідентифікації, вже налагоджено функціонує в країні.

Поняття електронної ідентифікації

На сьогодні Законодавець надає наступні визначення щодо ідентифікації, які автори продемонстрували у вигляді таблиці для полегшення їхнього порівняння.

Таблиця 1

Термін	Визначення
Ідентифікація користувача	Процедура присвоєння користувачеві набору персональних електронних реквізитів (звичайно використовується пара логін – пароль) або надання йому спеціального електронного ключа, що перебуває в його ексклюзивному користуванні. (Міністерство економіки України, Наказ "Про затвердження Порядку планування, формування, створення, функціонування, супроводження, систематизації електронних інформаційних ресурсів Міністерства економіки України та доступу до них" від 16.07.2010 N 854)
Ідентифікація особи	Встановлення відповідності ідентифікаційних ознак людини, занесених у документи або базу даних, фактичним ознакам самої людини. (Державний комітет ядерного регулювання, Наказ "Про затвердження Правил фізичного захисту ядерних установок та ядерних матеріалів" від 04.08.2006 N 116)
Ідентифікація	Належне встановлення особи. (Концепція реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг, Наказ Міністерства юстиції України 10.04.2013 № 668/5)
Ідентифікація	Процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. (Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29 березня 2006р. №373)

Як можна побачити, визначення ці є дещо розмитими та об’єктивно не відображають зміст поняття:

- перше визначення дещо звужує механізми забезпечення ідентифікації, наголошуючи лише на парі логін-пароль;
- друге визначення є дещо ширшим у розумінні об’єктів, що безпосередньо використовуються у процесі ідентифікації;
- третє визначення, на думку авторів, взагалі не розкриває сутності поняття, хоча воно й надано у Концепції, про яку було згадано раніше;
- четверте визначення, на думку авторів, є найбільш вдалим. Проте у [1] надане визначення, що повною мірою розкриває сенс поняття та механізм його реалізації:

Ідентифікація – процеси присвоєння суб’єкту чи об’єкту унікального позначення імені чи коду, характерної ознаки, наявність якої дозволяє виділити даних об’єкт (суб’єкт) серед множин інших, а також процес пред’явлення суб’єктом чи об’єктом цього ідентифікатора.

Існує дві основні ознаки, за якими розпізнавальні ідентифікатори відрізняють конкретну особу від інших учасників:

- на основі членства в групі об’єктів, тобто з груповим рівнем модульності, у якому об’єкти розглядаються еквівалентно цілям автентифікації (у даному випадку ціла група розглядається як одна особа-комітент, що має один розпізнавальний ідентифікатор);

- на основі індивідуального членства, коли ідентифікується один і тільки один об’єкт.

Проте неможливо додати інформаційний простір як середу використання та поставити знак рівності між наданими визначеннями та визначенням електронної ідентифікації. З метою більше глибокого розуміння цього феномену звернемося до тексту зазначеного раніше Регламенту, в якому було введено наступне визначення:

Електронна ідентифікація означає процес використання персональних даних ідентифікації в електронній формі, які однозначно визначають фізичну або юридичну особу.

У тексті прес-релізу Регламенту зазначено, що електронна ідентифікація (eIdentification) – це процес однозначного визначення ідентичності людини/особи за допомогою використання електронних засобів. Надані визначення та коментарі однозначно відокремлює коло суб’єктів ідентифікації (фізичні або юридичні особи), предмети, за допомогою яких здійсню-

ється ідентифікація (ідентифікаційні дані), а також наголошує на основному функціоналі ідентифікації – саме *однозначне* визначення особи. На думку авторів, цей акцент є дуже важливим та його дійсно бракує в українському варіанті.

Архітектура безпеки OSI (OSI Security Architecture, ISO7498-2) дає визначення двом видам ідентифікації: ідентифікації особи та ідентифікації походження даних

1. Ідентифікація особи здійснюється шляхом перевірки одної автентичної особи іншою. Це є операція, орієнтована на взаємозв'язок осіб між собою. Ідентифікація особи зазвичай відбувається за допомогою використання ідентифікаційного механізму обміну. Суть його становить процес обміну повідомленнями між парою осіб і найчастіше називається протоколом ідентифікації.

2. Ідентифікація походження даних, яка надає будь-якій особі підтвердження того, що джерелом отриманих даних є саме заявлене джерело. Але така система сама по собі не дає захисту від дуплікації або модифікації одиниць інформації. Цифровий підпис є особливою технікою розпізнання, яку можна застосовувати для встановлення походження повідомлення, щоб вирішити спір щодо того, яке повідомлення було надіслано (і чи було воно надіслано взагалі. Виходячи з цього, спробуємо надати визначенні електронної ідентифікації:

Електронна ідентифікація – процес використання унікальних даних предмету (в тому числі персональних даних особи) в електронній формі з метою однозначної ідентичності людини/особи. Ідентифікація забезпечує виконання таких функцій:

- встановлення автентичності та визначення повноважень суб'єкта при допуску його в систему;
- контролювання встановлених повноважень в процесі сеансу роботи;
- реєстрація дій та ін.

Суб'єкт може підтвердити свою автентичність, пред'явивши принаймні одну з наступних сутностей:

• щось, що він знає;
• щось, чим він володіє;
• щось, що є частина його самого.

Алгоритмічно процес ідентифікації можна представити наступним чином:

Рис. 1

Предмети ідентифікації

Авторами прийнято припущення, згідно з яким для гармонійного розвитку ринку доцільним буде окремо ідентифікувати наступні предмети: особи, послуги, товари, продукти, ехнології, системи, засоби, механізми, протоколи (у тому числі криптографічні примітиви та криптографічні протоколи).

Очевидним є той факт, що неможливо розробити унікальний алгоритм для однакової ідентифікації усіх зазначених предметів, саме тому доречним буде розподілити методи на групи залежно від їх застосувань.

Ідентифікаційні дані

У проекті Закону України «Про внесення змін до Закону України «Про електронний цифровий підпис», на жаль, не визначено поняття ідентифікації. Проте Законодавець надає вичерпний перелік даних, які однозначно ідентифікують особу (користувача), а саме:

ідентифікаційними даними підписувачів – фізичних осіб є:

прізвище, ім’я та по батькові підписувача;

унікальний реєстраційний номер підписувача, що надається центром сертифікації ключів, засвідчувальним центром чи центральним засвідчувальним органом під час реєстрації підписувача;

країна, область та місто в якому зареєстроване місце проживання підписувача.

У випадку формування сертифікату ключа для фізичної особи – працівника підприємства, установи, організації у сертифікаті ключа на підставі відповідної заяви підприємства, установи, організації додатково зазначаються найменування підприємства, установи, організації працівником якої є фізична особа – підписувач та його посада.

Ідентифікаційними даними підписувачів – власників автоматизованого засобу електронного цифрового підпису є:

повне (або офіційне скорочене) найменування підписувача;

унікальний реєстраційний номер підписувача, що надається центром сертифікації ключів, засвідчувальним центром чи центральним засвідчувальним органом під час реєстрації підписувача;

країна, область та місто, в якому зареєстрований підписувач.

Проте, на жаль, жодної інформації щодо ідентифікації неживих істот Законодавцем не надано.

Поняття автентифікації

Авторам відомі наступні визначення автентифікації, приведені у табл. 2.

Таблиця 2

Визначення	Джерело
Процедура встановленні належності користувачеві інформації в системі пред’явленого ним ідентифікатора.	Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29 березня 2006р. №373
Процедура встановлення належності працівникові володільця або розпорядника бази персональних даних вкладників – фізичних осіб пред'явленого ним ідентифікатора.	Фонд гарантування вкладів фізичних осіб, Рішення "Про затвердження Порядку обробки персональних даних у сфері забезпечення функціонування системи гарантування вкладів фізичних осіб" від 12.07.2012 N 9
Процедура перевірки відповідності пред'явленого ідентифікатора підписувача на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.	Державна митна служба, Наказ "Про затвердження Тимчасового порядку організації, розповсюдження та використання електронного цифрового підпису в митній службі України" від 08.04.2011 N 298
Шлях встановлення вірогідності інформації, пред'явленої користувачем у разі звернення його до системи та відкриття йому доступу, якщо він має на це право.	КМ України, Постанова КМ "Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи" від 20.01.1997 N 40

В останній редакції проекту Закону України “Про електронний цифровий підпис” надане наступне визначення:

Автентифікація – електронний процес, який дозволяє підтвердити належність ідентифікаційних даних фізичній або юридичній особі, інформаційній системі, походження та цілісність електронних даних під час доступу до інформаційної системи.

Автори пропонують вважати останнє визначення найбільш вдалим, а отже використовувати та впроваджувати саме його. Це визначення наголошує на те, що це є саме процес, який нерозривно пов’язано із електронним середовищем, та встановлює однозначну належність даних.

Класифікація методів ідентифікації та автентифікації

Методи ідентифікації умовно можна поділити на однофакторні та двофакторні. Однофакторні методи поділяються:

- на логічні (паролі, ключові фрази);
- ідентифікаційні (носієм ключової інформації є безпосередньо об’єкти);
- біометричні (в їх основі – аналіз унікальних характеристик об’єкту-істоти).

Під методами ідентифікації будемо розуміти саме механізми використання унікальних даних предмету в електронній формі з метою однозначної ідентичності об’єкту. Традиційна класифікація, що приведена в багатьох наукових працях, побудована в залежності від фізичної реалізації методу, а саме:

1.*Парольна ідентифікація*. Найбільш проста як у реалізації, так й у використанні. Суть її зводиться до наступного: кожен зареєстрований користувач системи одержує набір персональних реквізитів (зазвичай використаються пари логін-пароль). Далі при кожній спробі входу особа повинна вказати свою ідентифікуючу інформацію. Оскільки вона унікальна для кожного користувача, на підставі неї система робить висновок про особистість та ідентифікує її.

Головна перевага парольної ідентифікації – це простота реалізації й використання. Крім того, введення парольної ідентифікації не вимагає жодних витрат: даний процес реалізовано у всіх програмних продуктах, що є в продажу. Таким чином, система захисту інформації виявляється гранично простою і доступною.

На жаль, така система має чимало недоліків. І, мабуть, головний – величезна залежність надійності ідентифікації і від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що більшість людей використають ненадійні ключові слова, які легко підбираються. До них відносяться занадто короткі паролі, що мають зміст слова й т.д. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з безладного сполучення букв, цифр і різних символів, тобто псевдовипадкові послідовності.

2.*Апаратна ідентифікація*. Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предмету фізичного світу, ключу, що перебуває в його ексклюзивному користуванні. На даний момент найбільше поширення одержали два типи пристроїв:

- пасивні (картки з пам'яттю);
- активні (інтелектуальні картки).

Найпоширенішим різновидом токенів є пасивні картки з магнітною смугою, яка зчитується спеціальним пристроєм, що має клавіатуру і процесор. При використанні зазначеної картки користувач вводить свій ідентифікаційний номер . У разі його збігу з електронним варіантом, закодованим у картці, користувач отримує доступ до системи. Це дозволяє достовірно встановити особу, яка отримала доступ до системи і виключити несанкціоноване використання картки зловмисником (наприклад, при її втраті).

До переваг використання карток відносять те, що обробка автентифікаційної інформації виконується пристроєм читання без передачі в пам'ять комп'ютера. Це виключає можливість електронного перехоплення каналами зв'язку.

Недоліки пасивних карток наступні: вони істотно дорожче, ніж паролі, вимагають спеціальних пристроїв читання, їх використання потребує спеціальні процедури безпечного обліку і розподілу. Відомі випадки підробки пасивних карток.

Інтелектуальні картки окрім пам'яті мають власний мікропроцесор. Це дозволяє реалізувати різні варіанти пральних методів захисту: багаторазові паролі, паролі, що динамічно змінюються, звичайні запит-відповідні методи.

До зазначених переваг інтелектуальних карток слід додати їх багатофункціональність. Супутнім недоліком карток є їх висока вартість.

3.Біометрична ідентифікація. Біометрична ідентифікація заснована на унікальності характеристик людського тіла. Вважається, що практично не існує двох людей з однаковими біометричними ознаками, тобто що ймовірність такої події є мізерно малою. Біометрія – це прикладна область знань, що використовує при створенні різних автоматичних систем розмежування доступу унікальні ознаки, що властиві кожній окремій людині. До цих ознак, які називають біометричними характеристиками належать перераховані у табл. 2.

Таблиця 3

Фізіологічні методи	Поведінкові методи
Зняття відбитків папілярного візерунку пальців; Сканування райдужної оболонки ока; Сканування сітківки ока; Геометрія кисті руки; Розпізнавання рисунку та рис обличчя; Термограма особи; (наприклад схема кровоносних судин).	Аналіз підпису; Аналіз тембру голосу; Аналіз клавіатурного почерку.

Законодавець України надав таке визначення цього поняття:

Біометрична ідентифікація – засіб підтвердження особи, належності паспорта його власнику шляхом розпізнавання і зіставлення зафіксованих носіями біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, рис обличчя тощо) з особистими даними власника [3].

Схему роботи біометричної системи автентифікації наведено на рис. 2.

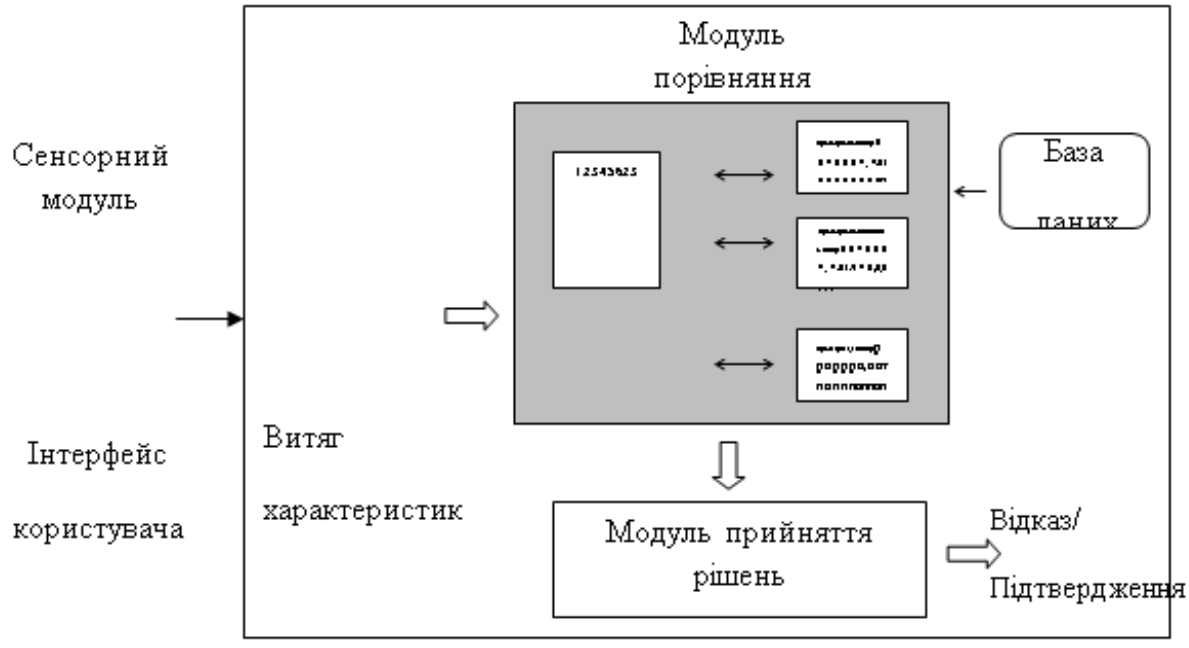

Рис 2. Біометрична система автентифікації

4.Новітнім напрямком автентифікації є доказ достовірності віддаленого користувача за його місцезнаходженням. Цей захисний механізм засновано на використанні системи космічної навігації типу GPS (Global Positioning System). Користувач, що має апаратуру GPS, багаторазово посилає координати заданих супутників, що знаходяться в зоні прямої видимості. Підсистема автентифікації, знаючи орбіти супутників, може з точністю до метра визначити місце розташування користувача. Висока надійність автентифікації визначається тим, що орбіти супутників схильні до коливань, передбачити які досить важко. Крім того, координати постійно змінюються, що зводить нанівець можливість їх перехоплення.

У Європі багато держав-членів забезпечили своїм громадянам електронні ідентифікатори через смарт – карти, мобільні телефони або інші технологій: деякі держави-члени ЄС об'єднали електронну ID з функцією посвідчення особи, що використовується також в якості проїзного документа, деякі мають карту доступу громадянина в громадських місцях онлайн-сервісів, інші працюють з мобільними пристроями, або комбінація карти та телефону [6].

На сьогодні найбільш поширеним методом ідентифікації особи на території нашої держави є електронний цифровий підпис – дані в електронній формі, які додаються особою до інших електронних даних або логічно з ними пов’язуються з метою її *ідентифікації*. Проте пропозиція, що міститься в проекі Регламенту Європейського Парламенту та Ради значно розширює можливості користувачів електронного простору у можливостях обирати механізми реалізації ідентифікації.

Список літератури: 1. *Горбенко, И.Д., Горбенко, Ю.И*. Прикладна криптологія. – Харків : Форт. – 2012, – С. 867. 2. *Закон* України Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки // Відомості Верховної Ради України (ВВР). – 2007. – № 12 .- Ст.102). – Режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16. 3. *Інформаційне* суспільство. – Режим доступу: http://uk.wikipedia.org/wiki/Інформаційне_суспільство. 4. *Постанова* КМ "Про затвердження Концепції створення Єдиного державного реєстру фізичних осіб" від 09.11.2004 N 1500. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/KP041500.html. 5. *Програма* економічних реформ на 2010 – 2014 роки «Заможне суспільство, конкурентоспроможна економіка, ефективна держава» / Указ Президента України від 12.03.2013 №128/2013. – Режим доступу: http://www.president.-gov.ua/docs/Programa_reform_FINAL_1.pdf. 6. *Electronic* identification, signatures and trust services: Questions & Answers . Режим доступу: http://europa.eu/rapid/press-release_MEMO-12-403_en.htm. Дата зверненн: 18/12/13

Харківський національний університет
ім. В.Н.Каразіна

Надійшла до редколегії 11.01.2014