УДК 004.056.55

Д.В. МЯЛКОВСКИЙ, З.А. ОРЄШКО, А.В. ПОТІЙ, д-р техн. наук

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Вступ

Наскрізне проникнення та повсякчасне зростання ступеня впливу інформаційних технологій на сучасне життя особи, бізнесу, суспільства і держави вже сьогодні вимагає чіткого визначення та правильного розуміння і застосування онтологічної моделі забезпечення електронної довіри як до електронних послуг взагалі, так до окремих етапів їх життєвого циклу зокрема.

Довіра до електронної послуги є інтегрованою характеристикою, яка буде наближатися до нижнього рівня кожного разу при встановленні невідповідності визначеним вимогам етапності, сценарію, способу, засобу або використаному джерелу інформації для її надання.

В сучасній українській термінології переважно застосовується термін «гарантія» при перекладі з англійської слова «assurance», хоча б більш правильним доцільно застосовувати термін «запевнення».

В оксфордському словнику цей англомовний термін тлумачиться «як позитивна декларація, спрямована на забезпечення довіри; обіцянка» (a positive declaration intended to give confidence; a promise). Як у звичайному просторі, так і у віртуальному ступінь довіри до об'єкта або процесу складається із сукупності показників довіри до достовірно встановленої або підтвердженої справжності кожного елемента процесу або об'єкта. Тому, чим більше таких підтверджених справжностей, тим більше кожний із нас відчуває себе впевненішим, що він не помиляється у тому, що оцінюваний об'єкт, процес тощо є справжнім, не підміненим, тотожним або є істинним за унікальним набором своїх властивостей, що відповідають або є оригіналом.

У цій статті автори аналізують предметну область електронної ідентифікації з метою уточнення змісту визначень в цій галузі.

Порівняння норм ЗУ «Про електронні довірчі послуги» та Регламент ЄС №910/2014

Алгоритми надання електронних послуг можуть і повинні відрізнятись, проте ключовим моментом тут є електронна ідентифікація. Успішне її проходження забезпечує поступове просування по ланцюгу обов'язкових кроків згідно з встановленим сценарієм надання електронної послуги. При цьому чутливим відносно довіри тут є засіб ідентифікації (довіра до повного циклу від розроблення до процесу виробництва і постачання), реалізація в ньому визначеного основного та прикладного програмного забезпечення, його захищеність від підробок, надійність механізмів захисту чутливої інформації (зокрема персональних даних), яка зберігається або використовується на конкретних етапах вказаного вище ланцюга, виконання саме встановлених сценаріїв надання послуги і так далі.

У зв'язку з цим, проблематика запровадження електронної ідентифікації набуває актуальності, особливо на тлі імплементації в Україні положень Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС (далі – Регламент-910) [1] в форматі закону України «Про електронні довірчі послуги» (№ 2155-VIII від 5 жовтня 2017 року) [2], розвитку Інтернету речей (IoT) тощо. Цей закон став логічним продовженням розвитку норм прийнятого у 2003 році Закону України «Про електронний цифровий підпис». Основна мета закону – визначити перелік електронних довірчих послуг та встановити організаційні, технологічні та інші вимоги для їх надання таким чином, щоб у одержувача цих послуг була впевненість що інфраструктура забезпечує довіру до них. Ключовим моментом в забезпеченні довіри до будь-якої електронної послуги є електронна ідентифікація суб'єкта (об'єкта) її отримання або звернення на її отримання.

Варто зазначити, що в процесі адаптації Регламенту-910 у відповідний закон належну увагу питанням електронної ідентифікації надано не було, а лише делеговано Державному агентству з питань електронного урядування України, як центральному органу виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства, здійснення розроблення нормативно-правових актів та технічне регулювання у сфері електронної ідентифікації шляхом встановлення вимог до засобів електронної ідентифікації, рівня довіри до засобів електронної ідентифікації та автентифікації для їх використання у сфері електронного урядування.

У зв'язку з неналежним висвітленням у законі питань електронної ідентифікації він і стосується, в переважному ступені, лише питань електронних довірчих послуг. При цьому, в законі уведено основні терміни та окрему статтю 6 щодо характеристик до схем ідентифікації з низьким, середнім та високим рівнем довіри до кожної з них.

Порівнюючи переклад основної термінології щодо ідентифікації, застосованої в Регламенті-910 та закону № 2155-VIII, можна спостерігати певні відмінності (табл. 1)

Таблиця 1

Норма Регламенту-910	Норма ЗУ «Про електронні довірчі послуги»
electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;	9) електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;
'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;	17) засіб електронної ідентифікації – матеріальний та/або нематеріальний об'єкт, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;
'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;	21) ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;
	22) ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на папері та/або в електронній формі, яка однозначно встановлює фізичну, юридичну особу або представника юридичної особи;
'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons	46) схема електронної ідентифікації – система електронної ідентифікації, в якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб

Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них.

Різниця між ними полягає лише в тому що, низький (середній, високий) рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений (суттєвий та найвищий відповідно) ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності.

Запроваджені Законом України «Про електронний цифровий підпис» та системою підзаконних актів механізми використання електронного цифрового підпису забезпечили впровадження та активне використання схем електронної ідентифікації в переважній

більшості з високим ступенем довіри. Водночас, ця схема, забезпечивши можливість надання юридично значущих послуг державою, почала вимагати надання належної уваги і іншим схемам, коли такий високий рівень довіри до електронної ідентифікації може бути економічно не виправданим або стримуватиме можливість розвитку інших способів, у тому числі комбінованих, способів ідентифікації, та, як наслідок, гальмування запровадження нових видів електронних послуг. При цьому забезпечення довіри до електронної ідентифікації може бути забезпечено і комбінацією інших, в тому числі організаційних, договірних тощо, механізмів.

Недостатня донедавна нормативна врегульованість питань електронної ідентифікації на тлі стрімкого розвитку сфери електронних послуг змусила як державні органи, так і розробників рішень з їх надання розробляти і впроваджувати інші схеми ідентифікації з відповідним до отримуваних електронних послуг рівнем довіри до них. Яскравим прикладом запровадження іншої схеми електронної ідентифікації стало запровадження BankID – постанова Правління Національного банку України №378 від 30 серпня 2016 року «Про затвердження Положення про Єдину національну систему електронної дистанційної ідентифікації фізичних і юридичних осіб BankID Національного банку України» [3].

Це Положення встановлює порядок функціонування Єдиної національної системи електронної дистанційної ідентифікації фізичних і юридичних осіб BankID (далі – система BankID), здійснення банками України електронної дистанційної ідентифікації клієнтів (користувачів) з метою отримання ними адміністративних послуг на Єдиному державному порталі адміністративних послуг (далі – портал) або від суб'єктів надання адміністративних послуг та доступу користувачів до інформаційно-телекомунікаційних систем державних органів. Воно є прикладом використання за встановленими правилами та способом персональних даних, які користувачем системи ідентифікації через систему BankID вже колись раніше вносились до банку, клієнтом якого є цей користувач. При цьому, критична інформація, яка містить персональні дані користувачів, перед пересиланням шифрується, а інформаційні повідомлення про результати обробки абонентами запитів на ідентифікацію підписуються електронним цифровим підписом суб'єкта, що здійснює ідентифікацію. В такій схемі більшість питань відповідальності за безпеку даних регулюється договорами між користувачами та абонентами та банками. Вимога, що встановлена Національним банком України – це дотримання вимог Положення, специфікації на підключення та наявність у абонента комплексної системи захисту інформації відповідно до законодавства України.

Іншою новою для України технологією є технологія MobileID. Ця технологія не є тільки технологією електронної ідентифікації за допомогою мобільних терміналів. Правильніше було б її розглядати як технологію, що забезпечує застосування електронного цифрового підпису (ЕЦП) за допомогою мереж мобільних телекомунікацій, у тому числі і для електронної ідентифікації та інших сервісів.

Порівняльний аналіз позначень та термінів в сфері електронної ідентифікації

Слід зазначити, що на сьогодні спостерігаються деякі відмінності у визначенні понять «ідентифікація» та «автентифікація». Якщо перший застосовується в сенсі встановлення об'єкта, то автентифікація є процесом доведення (proofing) належності або тотожності встановленого об'єкта тим рисам та характеристикам, які або раніше, або в конкретний момент часу десь наявні, тобто процес встановлення ідентичності (identity). Нижче наводиться порівняння застосованих визначень для цих понять в нормативних документах Сполучених Штатів Америки, Міжнародної організації зі стандартизації та Міжнародного Союзу Електрозв'язку та України (табл 2).

У NIST Special Publication 800-63-2 Electronic Authentication Guideline[4] визначається, що Електронна автентифікація (електронна перевірка автентичності) – це процес встановлення довіри до ідентифікацій користувачів, електронно представлених до інформаційної системи.

Електронна перевірка автентичності представляє технічну проблему, коли цей процес містить віддалену автентифікацію окремих людей через відкриту мережу з метою електронного уряду та торгівлі. Керівні принципи цього документа передбачають автентифікацію та транзакцію через відкриту мережу, таку як Інтернет.

У випадках, коли автентифікація та транзакція здійснюються через контрольовану мережу, агентства можуть враховувати таке управління безпекою як частину їх оцінки ризику.

Ця настанова надає технічні рекомендації агентствам, які дозволяють індивіду віддалено автентифікувати свою особу в Федеральній IT-системі.

Ця настанова стосується лише традиційних, широко впроваджених методів дистанційної автентифікації, яка базується на основі секретів. За допомогою цих методів індивідуум щоб бути автентифікованим доводить, що він або вона знає або володіє деякою секретною інформацією.

В цій настанові термін «ідентичність» визначено як «набір атрибутів, які однозначно описують людину в певному контексті». А термін «автентифікація» визначається як «процес встановлення довіри до ідентичності користувачів або інформаційних систем».

В міжнародному стандарті ISO/IEC 29115:2013 Information technology – Security techniques — Entity authentication assurance framework (Інформаційні технології – Методи захисту – Схеми забезпечення довіри до автентифікації суб'єктів) [6] термін «ідентичність» визначено як «набір атрибутів, пов'язаних з суб'єктом», а «автентифікація» визначений як «надання впевненості в ідентичності суб'єкта». При цьому термін «доказування ідентичності» (Identity proofing) визначено як процес, за допомогою якого провайдер цифрових послуг та орган реєстрації (ОР) збирають та перевіряють інформацію про особу з метою надання посвідчень цій особі.

В цьому стандарті термін «доказування ідентичності» визначено декілька іншим чином: «процес, за допомогою якого орган реєстрації фіксує та перевіряє достатність інформації для визначення суб'єкта до визначеного або зрозумілого рівня впевненості».

Міжнародний союз електрозв’язку випустив низку рекомендацій серії «x: Мережі даних, відкриті системи зв'язку та безпека», в яких, зокрема, також здійснюється визначення відповідних термінів.

Так, рекомендація ITU-T X.1254 «Структура забезпечення автентичності суб'єктів» [7] визначає чотири рівні підтвердження автентифікації суб'єкта (наприклад, LoA 1 – LoA 4), а також критерії та загрози для кожного з чотирьох рівнів забезпечення автентифікації організації. Крім того, він:

- визначає рамки для управління рівнем забезпечення;
- надає рекомендації щодо технологій управління, які повинні використовуватися для пом'якшення загроз автентифікації, на основі оцінки ризику;
- надає керівництво для відображення чотирьох рівнів забезпечення в інші схеми забезпечення автентичності;
- надає керівництво для обміну результатами автентифікації, які базуються на чотирьох рівнях забезпечення.

Рекомендація ITU-T X.1258 «Безпека в кіберпросторі – Управління ідентифікацією – Посилена автентифікація об'єкта на основі агрегованих (зібраних) атрибутів» [8] представляє концепцію агрегації атрибутів, яка дозволяє суб'єкту об'єднувати атрибути з декількох ідентифікаторів. Агрегація атрибутів – це механізм збору атрибутів суб'єкта, отриманого з декількох ідентифікаторів доступу.

В цій рекомендації термін «ідентичність» визначено як представлення суб'єкта у формі одного або декількох атрибутів, які дозволяють істотно розрізняти суб'єкт або об'єкти в контексті. Для цілей ідентифікації ідентифікатор розуміється як контекстна ідентичність (підмножина атрибутів), тобто різноманітність атрибутів обмежена рамкою з визначеними граничними умовами (контекстом), в яких суб'єкт існує та взаємодіє. А термін

«автентифікація» визначений як процес, який використовується для досягнення достатньої впевненості при пов’язанні між об'єктом і представленою ідентичністю.

Визначення терміну «доказування ідентичності» в цьому стандарті не спостерігається.

У нормативних документах системи технічного захисту інформації України, наприклад у НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах (КС) від несанкціонованого доступу» [9], затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.99 № 22, термін “автентифікація” визначений як процедура перевірки відповідності пред’явленого ідентифікатора об’єкта КС на предмет належності його цьому об’єкту; встановлення або підтвердження автентичності. Термін «ідентичність» та «доказування ідентичності» не визначаються. Водночас визначено термін «ідентифікація» як процедура присвоєння ідентифікатора об’єкту КС або встановлення відповідності між об’єктом і його ідентифікатором; впізнання.

У табл. 2 наводяться зведені визначення термінів з цих документів.

Таблиця 2

	USA NIST Special Publication 800-63-2	**ISO/IEC**	**Рекомендація ITU-T X.1258**	**НД ТЗІ** 1.1-003-99	**НБУ**
Authentication	The process of establishing confidence in the identity of users or information systems Процес встановлення довіри до ідентичності користувачів або інформаційних систем	provision of assurance in the identity of an entity Надання впевненості в ідентичності суб'єкта **(29115:2013)** **автентифікація** (*authentication*) Забезпечення гарантії, що характеристики об'єкта, які було заявлено, є правильними **(ДСТУ ISO/IEC 27000:2015)**	**(entity) authentication** [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity. Процес, який використовується для досягнення достатньої впевненості при пов'язанні між об'єктом і представленою ідентичністю.	процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комунікаційної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності	електронний процес, що дає змогу підтвердити електронну дистанційну ідентифікацію фізичної або юридичної особи чи походження та цілісність даних в електронній формі
Identity	A set of attributes that uniquely describe a person within a given context. Identity Proofing Набір атрибутів, які однозначно описують людину в певному контексті	set of attributes related to an entity Набір атрибутів, пов'язаних з суб'єктом	**identity** [b-ITU-T X.1252]: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts. Представлення суб'єкта у формі одного або декількох атрибутів, які дозволяють істотно розрізняти суб'єкт або об'єкти в контексті. Для цілей ідентифікації ідентифікатор розуміється як контекстна ідентичність (підмножина атрибутів), тобто різноманітність атрибутів обмежена рамкою з визначеними граничними умовами (контекстом), в яких суб'єкт існує та взаємодіє		

Закінчення табл. 2

Identity proofing	The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. Процес, за допомогою якого провайдери сертифікації та орган реєстрації (ОР) збирають та перевіряють інформацію про особу з метою надання посвідчень цій особі	process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance Процес, за допомогою якого орган реєстрації (ОР) фіксує та перевіряє достатність інформації для визначення суб'єкта до визначеного або зрозумілого рівня впевненості			
Identification				Процедура присвоєння ідентифікатора об’єкту КС або встановлення відповідності між об’єктом і його ідентифікатором; впізнання	

Висновки

Порівняльний аналіз визначення термінів дозволяє зробити певні висновки. Існує розбіжність у визначеннях термінів «ідентифікація», «автентифікація» і пов'язаних з ними процесів в нормативних та регулюючих документах. Також неоднозначним є застосування в національних нормативних документах перекладеного терміну «assurance» не як запевнення та його міра, а як рівень гарантій.

Наслідком такої розбіжності може бути складність у застосовності норм міжнародних стандартів в нормативно-експлуатаційних документах з функціонування інформаційно-телекомунікаційних систем (ІТС), де застосовуються механізми ідентифікації та автентифікації. Складним також буде проведення в Україні оцінки відповідності таких механізмів на відповідність міжнародним стандартам або визнання в Україні результатів такої оцінки, які отримані поза межами України.

У зв'язку з цим, упровадження тотожних з міжнародною термінологію цих базових термінів та визначень в українське законодавство спростить надалі, з одного боку, реалізацію відповідних технічних механізмів в ІТС, а з іншого – можливість довіри до безпеки при їх застосуванні.

Список літератури: 1. *Регламент* (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС. 2. *Закон* України «Про електронні довірчі послуги» № 2155-VIII від 5 жовтня 2017 року. 3. *Постанова* Правління Національного банку України №378 від 30 серпня 2016 року «Про затвердження Положення про Єдину національну систему електронної дистанційної ідентифікації фізичних і юридичних осіб BankID Національного банку України» // Офіційний вісник України від 04.10.2016. – 2016. – № 76. – С. 8, ст. 2545, код акту 83254/2016. 4. *NIST* Special Publication 800-63-2. Electronic Authentication Guideline. 5. *William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W, Timothy Polk, Sarbari Gupta, Emad A. Nabb*. – U.S. Department of Commerce, National Institute of Standards and Technology, August 2013. – 112 p. 6. *ISO/IEC 29115*. Information technology. Security Techniques – entity authentication assurance framework. – ISO/IEC JTC 1/SC 27 IT Security techniques. – 2013. – 36p. 7. *Рекомендація* ITU-T X.1254 «Структура забезпечення автентичності суб'єктів» 8. *ITU-T X.1258* «Безпека в кіберпросторі – Управління ідентифікацією – Посилена автентифікація об'єкта на основі агрегованих (зібраних) атрибутів» Rec. ITU-T X.1258 (09/2016). 9. *НД ТЗІ 1.1-003-99* «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.99 № 22.

Державна служба спеціального зв'язку
та захисту інформації України,
Харківський національний
університет імені В.Н.Каразіна,
Акціонерне товариство
«Інститут інформаційних технологій»

Надійшла до редколегії 11.12.2017