doi: https://doi.org/10.15407/visn2017.09.053

МЕЛАЩЕНКО
Андрій Олегович —
кандидат фізико-математичних наук, старший науковий співробітник Інституту кібернетики ім. В.М. Глушкова НАН України
ORCID: 0000-0002-7827-5165

РОЗРОБКА СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

За матеріалами наукового повідомлення на засіданні Президії НАН України 5 липня 2017 року

Побудова інформаційного суспільства спирається насамперед на довіру. Століття паперового діловодства створили інфраструктуру довіри, яка ґрунтується на підписах і печатках. Завдання XXI ст. — побудувати досконалішу інфраструктуру в інформаційному суспільстві, тобто у віртуальному світі. Інформаційне суспільство — суспільство, де всі процеси з технологічної та організаційної точок зору, крім матеріального виробництва, виконуються в електронному (віртуальному) вигляді. Така організація праці має безліч переваг, від економічних до екологічних. Основою довіри в сучасній концепції інформаційного суспільства є інфраструктура відкритих ключів (PKI) та її юридичне вдосконалення у ЄС — кваліфікована інфраструктура відкритих ключів (QPKI). У доповіді розкрито різні аспекти організації QPKI та проаналізовано першочергові дії, необхідні для зведення Національної системи електронних цифрових підписів до Європейської еталонної моделі QPKI.

***Ключові слова*:** QPKI, електронний цифровий підпис, електронний документообіг, стандартизація.

В Україні переважна більшість проектів національного рівня у сфері інформатизації [1—3] спрямована на спрощення взаємодії державних установ, громадян, приватних, колективних підприємств та інших суб'єктів підприємницької діяльності з органами державної влади та органами місцевого самоврядування. Проте, на жаль, впровадження е-послуг у державі розвивається досить повільно. Більшість підходів ґрунтуються на необхідності побудови електронного документообігу (ЕДО), тоді як світова спільнота вже перейшла на наступну сходинку еволюції, а саме: на побудову інфраструктури електронних бізнесів.

Практика застосування електронних документів

Динаміку розвитку інфраструктури електронних бізнесів доцільно продемонструвати на прикладі історії розвитку Націо-

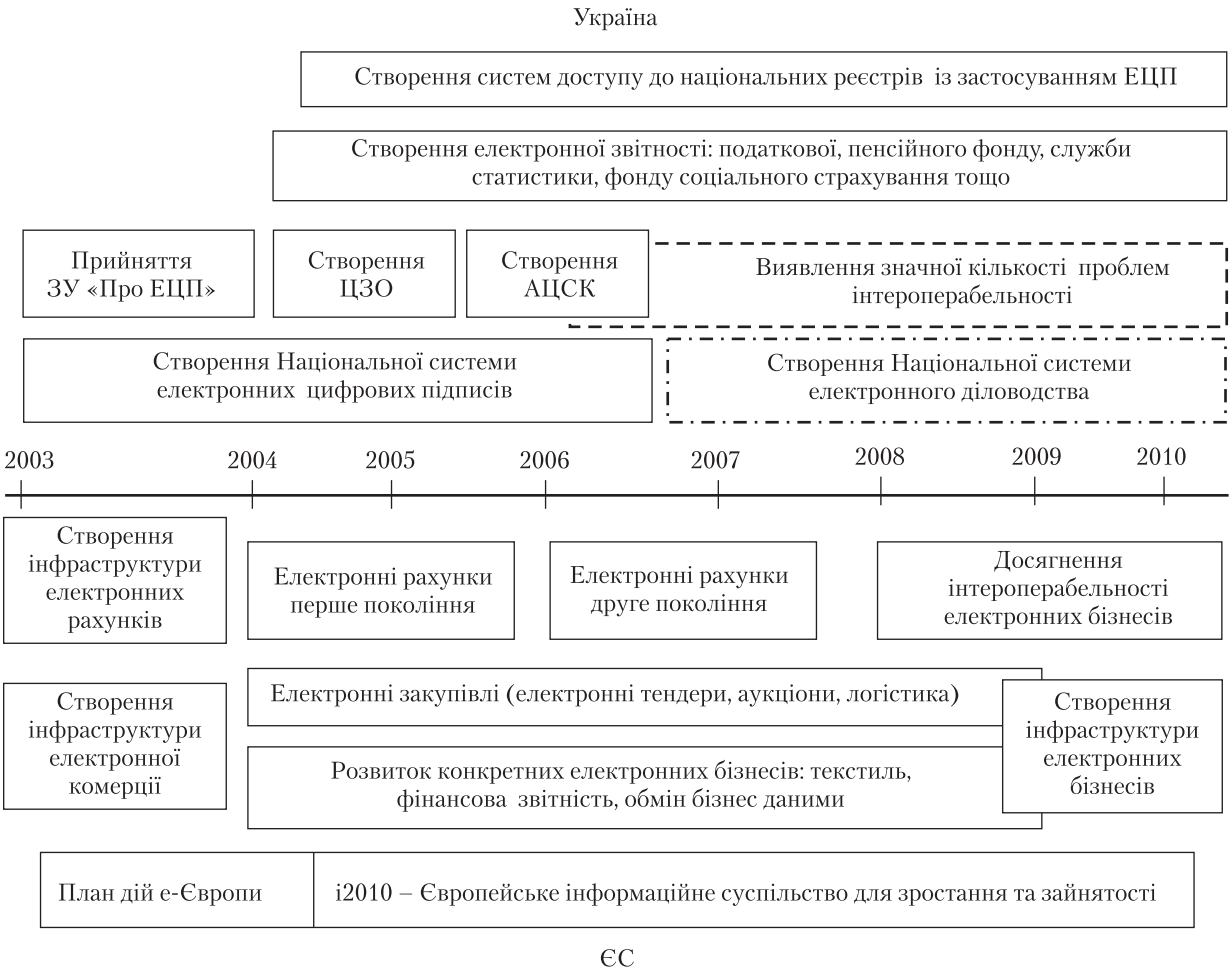

Рис. 1. Порівняльна характеристика розвитку сектору інформаційно-телекомунікаційних технологій в ЄС і Україні. ЦЗО — центральний засвідчувальний орган; АЦСК — акредитований центр сертифікації ключів; ЗУ — Закон України; ЕЦП — електронний цифровий підпис

нальної системи електронних цифрових підписів (НСЕЦП) (рис. 1). Аналіз факторів розвитку сфери інформаційно-телекомунікаційних технологій (ІКТ) в Україні та ЄС за період з 2003 по 2010 р. свідчить про суттєву різницю в застосуванні електронного цифрового підпису (ЕЦП), зумовлену людським фактором та передісторією використання ІКТ бізнесом і державними структурами.

Глибоке проникнення ІКТ у бізнес та державну сферу відбулося на початку 1990-х років, метою чого було спрощення взаємодії бізнесу і державного сектору, а також створення нового ринку. Протягом 90-х років інформаційні технології найактивніше розвивалися у фінансовому секторі, їх досягнення успішно впроваджувалися у виробничі підприємства по всій Європі. Вершиною розвитку ІТ того часу стало створення серії міжнародних стандартів EDIFACT, які формалізували, оптимізували та імплементували взаємодії між державними органами та підприємствами. У цей період з'явилося нове покоління керівників, які зрозуміли великий потенціал ІКТ та оволоділи механізмами їх впровадження.

Рис. 2. Схема взаємодії підприємства та фіскальних органів при поданні електронної звітності в Україні

У 1999 р. опубліковано Директиву 93/1999/ЄС [4], яка започаткувала новий етап розвитку сфери ІКТ, увівши поняття електронних бізнесів та їх інфраструктури. Це було насамперед спрямовано на спрощення взаємодії людини та ІКТ, на якому наголошував ще В.М. Глушков у своїх працях [5]. Крім того, наявність формалізованих і оптимізованих бізнес-процесів взаємодії держави, бізнесу та громадян дає можливість створити якісно нове середовище в соціально-економічному та культурному аспектах.

Історія створення НСЕЦП (рис. 1) свідчить про фактичне застосування ЕЦП тільки для імплементації алгоритмів звітності, навіть у випадку реєстрів. Складну ситуацію з практичним використанням НСЕЦП проілюстровано на рис. 2, де відображено послідовність дій, які необхідно здійснити підприємству для налагодження взаємодії з національними фіскальними органами при поданні фінансової звітності в електронному вигляді. Такий алгоритм передбачає підписання трьох договорів:

1) між фіскальним органом (ФО) та акредитованим центром сертифікації ключів (АЦСК); основною метою цього договору є надання АЦСК технічних засобів та спеціалістів ФО для валідації ЕЦП;

2) між підприємством та АЦСК для отримання послуг з обслуговування як мінімум трьох ЕЦП (підпису директора, бухгалтера та печатки підприємства);

3) між підприємством та ФО, за яким підприємству надається можливість подання електронної звітності.

Після підписання договору підприємство отримує щонайменше два програмних продукти: перший — для створення фіскальної звітності та підписування і другий — для надсилання відповідної звітності. Слід зазначити, що згідно з законодавством України [6, 7] наявність першого та третього договорів є зайвою і значно ускладнює застосування ЕЦП в інших сферах.

Враховуючи чинну практику подання звітності в Україні (рис. 3), кожне підприємство повинне мати не менше трьох ЕЦП, тобто, з огляду на те, що вартість одного ЕЦП стано-

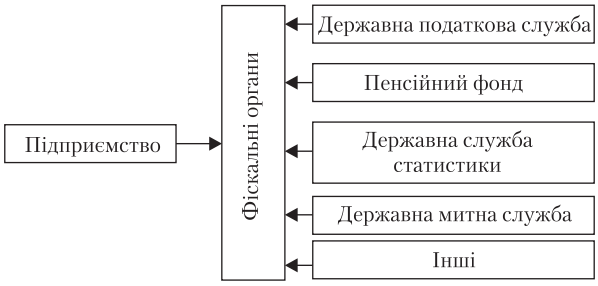

Рис. 3. Схема поточної взаємодії між підприємством і фіскальним органом

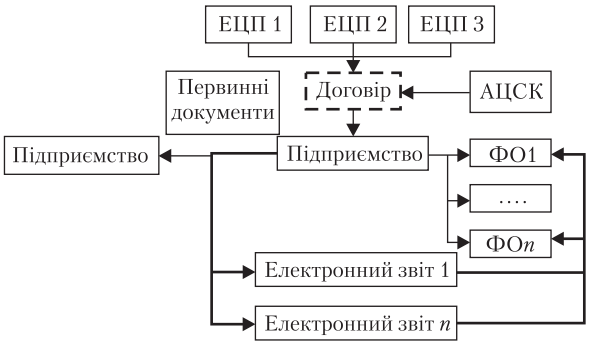

Рис. 4. Схема коректної реалізації механізму подання фіскальної звітності відповідно до законодавства України

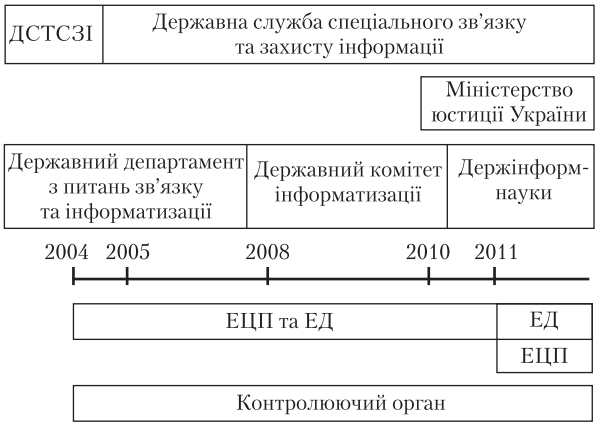

Рис. 5. Органи влади в Україні, відповідальні за ЕЦП та електронний документообіг

вить 127 грн, підприємство щороку витрачає на їх отримання як мінімум 381 грн. Нині в Україні налічується 2 млн платників податків, які подають звітність в електронному вигляді, а отже, обіг коштів у цій сфері становить приблизно 762 млн грн на рік. Цей факт крім іншого також сповільнює розвиток електронних бізнесів в Україні. З 1 червня 2012 р. розпочав свою роботу акредитований центр сертифікації ключів Міністерства доходів і зборів України, який надає суб'єктам підприємництва безкоштовні ЕЦП. Однак ця послуга не передбачає програмного забезпечення для подання звітності в інші фіскальні органи, тому підприємства змушені придбати додаткове програмне забезпечення середньою вартістю порядку 800 грн.

Застосування чинних алгоритмів взаємодії згідно з Законами України «Про електронний цифровий підпис» [6] та «Про електронні документи та електронний документообіг» [7] (рис. 4) здатне зменшити прибутки псевдомонополій мінімум удвічі, тобто знизити їх до 381 млн грн.

Відображені на рис. 1 тренди показують значний розрив між розвитком ІКТ в ЄС та в Україні і засвідчують нинішній стан розвитку ІКТ в Україні на рівні 1990-х років в Європі. Це підтверджується відсутністю конкретних державних програм розвитку ІКТ на кшталт Плану дій е-Європи [8], і2010 — Європейське інформаційне суспільство для зростання та зайнятості [9], Цифровий порядок денний Європи [10]. Наявна в Україні структура Національної програми інформатизації (НПІ) [11] є де-юре механізмом координації дій, а де-факто — лише механізмом контролю за витратою коштів на ІКТ. За останні п'ять років у рамках НПІ не розроблено жодного конкретного плану заходів, спрямованих на вирішення нагальних соціально-економічних проблем.

Сучасний стан електронних бізнесів в Україні

Сучасний стан електронних бізнесів в Україні характеризується відсутністю створеного державою сприятливого технологічно-організаційного середовища для розвитку цього сектору.

Як аналог необхідних вимог можна навести приклад застосування єдиної системи допусків і посадок (ЄСДП) згідно з ГОСТ 25346—89 [12]. На сьогодні у більшості країн світу використовують системи допусків і посадок ISO. Системи ISO створено для уніфікації національних систем допусків і посадок з метою полегшення міжнародних технічних зв'язків у металообробній промисловості. Включення міжнародних рекомендацій ISO в національні стандарти створює умови для забезпечення взаємозамінності однотипних деталей, складових частин і виробів, виготовлених у різних країнах. Радянський Союз вступив до

організації ISO в 1977 р., а згодом перейшов на ЄСДП та основні норми взаємозамінності, які ґрунтуються на стандартах і рекомендаціях ISO. Тобто завдяки використанню стандартів стало можливим створювати вироби, як «конструктор», із готових блоків, гарантуючи високу якість.

На відміну від металообробної промисловості, в ІКТ, за винятком комунікаційної складової, в Україні немає єдиного «простору координат», у якому можливо створювати критично необхідні для управління державою і бізнесом інформаційно-аналітичні системи. Згідно з [13], подання даних та довіра до них є базою будь-якого електронного бізнесу. В чинному законодавстві України ці складові реалізуються, відповідно, як електронний документ та ЕЦП. Створення повноцінної національної системи електронного діловодства (НСЕД) є першим кроком у розбудові інфраструктури електронних бізнесів, однак за майже 10 років дії відповідних Законів України [6, 7] комплексної програми стандартизації НСЕЦП та НСЕД так і не було розроблено та реалізовано. Ситуацію ускладнює неузгодженість функцій у державній політиці у сферах НСЕЦП та НСЕД між двома центральними органами виконавчої влади (рис. 5).

Інфраструктура електронних бізнесів

Інфраструктура електронних бізнесів складається з п'яти взаємно пов'язаних технічних настанов. Метою інфраструктури є створення стабільного ІТ-базису розбудови електронних бізнесів із забезпеченням належної якості послуг. До інфраструктури електронних бізнесів входять такі технічні настанови (рис. 6 і 7):

1. Національна система електронних цифрових підписів (НСЕЦП) — настанова напряму — через посилання на національні стандарти України вказує на обов'язкові для виконання вимоги до АЦСК, які надають послуги ЕЦП та обслуговують виключно посилені сертифікати ключів. Регламент встановлює також вимоги до програмних продуктів, які генерують визнані в ЄС кваліфіковані підписи.

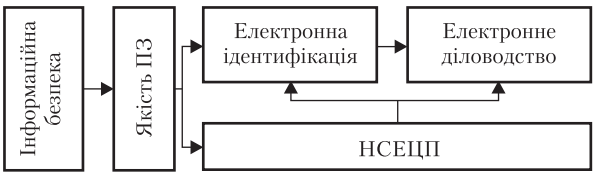

Рис. 6. Взаємозв'язок технічних настанов

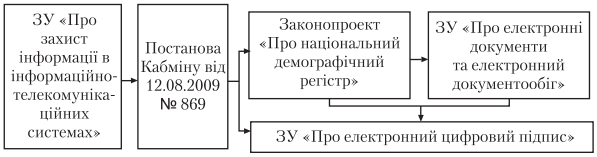

Рис. 7. Взаємозв'язок законодавчих актів

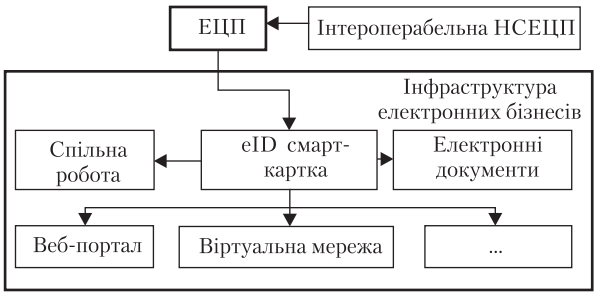

Рис. 8. Схема впровадження послуг ЕЦП

2. Національна система електронного діловодства (НСЕД) — формулює вимоги до форматів та функцій роботи з електронними документами з акцентом на можливість довічного зберігання юридично правочинних електронних документів.

3. Національна система електронної ідентифікації — необхідність застосування систем електронної ідентифікації (eID) зумовлена досконалим поєднанням інформаційної безпеки і зручності для користувачів, які мають взаємодіяти зі значною кількістю застосувань (ідентифікація, автентифікація), підписувати електронні документи (ЕЦП), ініціювати надійні екстранет-з'єднання з узгодженням ключів тощо (рис. 8).

4. Якість програмних продуктів — нині в Україні діє радянська модель Єдиної системи програмної документації, яка не гарантує дотри-

мання повного життєвого циклу розробки програмного забезпечення. Створення регламенту дасть можливість викласти обов'язкові вимоги до розробників програмного забезпечення, що значно підвищить якість та здешевить розробку.

5. Комплексна система захисту інформації — діючу нормативно-правову базу комплексної системи захисту інформації створено ще наприкінці 1990-х років і вона не відповідає вимогам сьогодення, а саме — мережній природі більшості застосувань. Настанова підносить сучасний стан нормативно-правової бази до світового рівня і, як наслідок, підвищує рівень інформаційної безпеки систем, що експлуатуються державними органами та приватними підприємствами.

Застосування технічних настанов згідно з Законом України «Про стандартизацію» є доцільним через високу складність та наявні вимоги до швидкодії і стабільності роботи всіх компонентів інфраструктури електронних бізнесів.

Висновки

Існуючий вектор розвитку електронних бізнесів в Україні характеризується відсутністю системного підходу і вирішенням лише локальних завдань державних органів та бізнесу. Інфраструктура електронних бізнесів охоплює всі верстви населення України. Вона інтегрує більшість систем державних органів, що характеризує її як систему з найвищим рівнем складності, який неможливо подолати без тотальної стандартизації всіх її складових. Оскільки національні стандарти мають переважно добровільний характер виконання, необхідно розробити комплекс технічних настанов, які б гарантували якість послуг в інфраструктурі електронних бізнесів.

Розроблення та імплементація норм технічних настанов інфраструктури електронних бізнесів має стати складовою розвитку сфери ІКТ в Україні у найближчі п'ять років.

REFERENCES
[СПИСОК ЛІТЕРАТУРИ]

1. Order of the Cabinet of Ministers of Ukraine No. 2250 of 13.12.2010. http://zakon3.rada.gov.ua/laws/show/2250-2010-%D1%80
   [Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні» № 2250 від 13.12.2010. http://document.ua/pro-shvalennja-koncepciyi-rozvitku-elektronnogo-urjaduvannja-doc40786.html]
2. Decree of the President of Ukraine No. 187/2012 of 12.03.2012. http://www.president.gov.ua/documents/14581.html
   [Указ Президента України «Про Національний план дій на 2012 рік щодо впровадження Програми економічних реформ на 2010—2014 роки» № 187/2012 від 12.03.2012. http://www.president.gov.ua/documents/14581.html]
3. Order of the Cabinet of Ministers of Ukraine No. 1236 of 17.09.2008. http://zakon1.rada.gov.ua/laws/show/1236-2008-%D1%80
   [Розпорядження Кабінету Міністрів України «Про схвалення Концепції створення багатофункціональної комплексної системи "Електронна митниця"» № 1236 від 17.09.2008. http://zakon1.rada.gov.ua/laws/show/1236-2008-%D1%80]
4. EU Directive 1999/93/EC of the European Parliament and the Council on a Community framework for electronic signatures of 13.12.1999. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT
5. Glushkov V.M. Some problems in the synthesis of digital automata. *USSR Computational Mathematics and Mathematical Physics*. 1962. **1**(3): 399.
   [Глушков В.М. Некоторые проблемы использования вычислительных машин для управления социальными процессами. *Журнал вычислительной математики и математической физики*. 1961. Т. 1, № 3. С. 371—411.]
6. The Law of Ukraine. No. 852-15 of 22.05.2003. http://zakon3.rada.gov.ua/laws/show/852-15
   [Закон України «Про електронний цифровий підпис» № 852-15 від 22.05.2003. http://zakon3.rada.gov.ua/laws/show/852-15]
7. The Law of Ukraine. No. 851-15 of 22.05.2003. http://zakon1.rada.gov.ua/laws/show/851-15

[Закон України «Про електронні документи та електронний документообіг» № 851-15 від 22.05.2003. http://zakon1.rada.gov.ua/laws/show/851-15]
8. eEurope Action Plan. http://ec.europa.eu/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf
9. i2010 — European Information Society for growth and employment. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:en:PDF
10. A Digital Agenda for Europe. http://ec.europa.eu/information_society/newsroom/cf/item-detail-dae.cfm?item_id=8285&language=default
11. The Law of Ukraine. No. 74/98-вр of 04.02.1998. http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80
[Закон України «Про Національну програму інформатизації» № 74/98-вр від 04.02.1998. http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80]
12. State Standard GOST 25346-89. http://gostexpert.ru/gost/gost-25346-89
[Основные нормы взаимозаменяемости. Единая система допусков и посадок. Общие положення, ряды допусков и основных отклонений: ГОСТ 25346-89. http://gostexpert.ru/gost/gost-25346-89]
13. Melaschenko A.O., Pervezchikova O.L. The organization of a qualified infrastructure of public keys. (Kyiv: Naukova Dumka, 2010).
[Мелащенко А.О., Перевозчикова О.Л. Організація кваліфікованої інфраструктури відкритих ключів. К.: Наукова думка, 2010].
14. eID Interoperability for PEGS: Analysis and Assessment of similarities and differences — Impact on eID interoperability, November 2007. http://ec.europa.eu/idabc/en/document/6484
15. CWA 15264-1: Architecture for a European interoperable eID system within a smart card infrastructure, April 2005. ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eAuth/cwa15264-01-2005-Apr.pdf

A.O. Melashchenko

Glushkov Institute of Cybernetics
of the National Academy of Sciences of Ukraine (Kyiv)
http://orcid.org/0000-0002-7827-5165

DEVELOPMENT OF SPECIALIZED COMPUTER
TECHNOLOGIES OF ELECTRONIC TRUST SERVICES

According to the materials of scientific report
at the meeting of the Presidium of NAS of Ukraine, July 5, 2017

Building an information society is based primarily on trust. Centuries of paperwork have created a trust infrastructure based on signatures and seals; the task of the XXI century is to build a better infrastructure in an information society. The information society is a society where all processes from the technological and organizational point of view, except the material production, are executed in an electronic (virtual) form. Such an organization of labor has many advantages, from economic to environmental. The key to trust in the modern information society concept is the Public Key Infrastructure (PKI) and its legal enhancement in the EU — Qualified Public Key Infrastructure (QPKI). The purpose of the work is to cover various aspects of QPKI organization and to analyze the necessary actions in Ukraine to build the National Digital Signature System consistent with the European Standard Model QPKI.

Keywords: QPKI, digital signature, electronic document management, standardization.