

**НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ**

Кваліфікаційна наукова
праця на правах рукопису

КОСТЕНКО ОЛЕКСІЙ ВОЛОДИМИРОВИЧ

УДК: 342.9(004.9)

**ДИСЕРТАЦІЯ
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ТРАНСКОРДОННОГО НАДАННЯ
ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ**

081 - Право

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ /Костенко О.В./

Науковий керівник:
БАРАНОВ Олександр Андрійович,
доктор юридичних наук,
старший науковий співробітник

Київ – 2020

АНОТАЦІЯ

Костенко О.В. Правове забезпечення транскордонного надання електронних довірчих послуг. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – Право. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ, 2020.

Дисертація є першою в Україні комплексною науковою працею, в якій вирішується важливе наукове завдання з формування теоретико-методологічних та практичних положень щодо правового забезпечення транскордонного надання електронних довірчих послуг шляхом удосконалення національного законодавства, що сприятиме ефективній реалізації стратегії цифрової трансформації України.

У дисертації розглядаються основні проблеми правового забезпечення транскордонного надання електронних довірчих послуг.

Досвід законодавчого регулювання транскордонного надання електронних довірчих послуг практично не вивчався, не узагальнювалися процедури їх транскордонного визнання, оскільки ці питання так чи інакше комплексно пов'язані із міжнародним правом, національними юридичними та технічними нормативними актами, стандартами, порядками застосування різних математичних алгоритмів тощо. Для забезпечення застосування транскордонного надання електронних довірчих послуг необхідно вдосконалення правового регулювання, а в умовах активізації міжнародної співпраці розробка та внесення відповідних змін до законодавства України, що є суспільно необхідним завданням.

На основі сформульованих в роботі висновків автором обґрунтовано науковий погляд щодо необхідності проведення досліджень щодо визначення теоретико-методологічних положень правового регулювання та вдосконалення національного законодавства для створення умов щодо

транскордонного надання електронних довірчих послуг з метою забезпечення довіри до широкого використання інформаційно-комунікаційних технологій і в суспільному житті України, і в міжнародній співпраці, що сприятиме ефективній реалізації стратегії цифрової трансформації держави.

Автором проаналізовано та удосконалено доктринальні підходи в міжнародному законодавстві щодо вирішення проблеми визнання іноземних електронних підписів. У результаті аналізу концептуальних підходів до принципів визнання іноземних електронних довірчих послуг, узагальнення законодавчого досвіду найбільш відомих міжнародних центрів розробки, впровадження транскордонного надання електронних довірчих послуг, зокрема Комісії ООН з міжнародного торговельного права, Міжнародної торгової палати і Європейської економічної комісії (UNCITRAL), Європейського Союзу, Міжпарламентської Асамблеї держав-учасниць СНД та Асоціації держав Південно-Східної Азії (ASEAN), встановлено, що міжнародні нормативні акти використовують значну кількість термінів щодо транскордонності, зміст яких не конкретизовано, однак ці терміни мають суттєве значення для створення в подальшому нормативно-правових актів національних законодавств у галузі електронних довірчих послуг.

Значну увагу приділено вивченню законотворчого досвіду міждержавних утворень Європейського Союзу та Співдружності Незалежних Держав, країн-учасниць Асоціації держав Південно-Східної Азії (ASEAN), Сполучених Штатів Америки, окремих країн Азії, країн пострадянського простору в напрямі транскордонного надання електронних довірчих послуг.

Здійснено порівняльний аналіз міжнародного законодавства та законодавства окремих країн у галузі електронних підписів. Визначено подібності та відмінності, колізії і спорідненість правових норм з урахуванням практик їхнього застосування.

Предметом окремої уваги в дисертаційній роботі стали особливості фактичного стану українського законодавства, що здійснює регуляцію у сфері електронних довірчих послуг.

Розглянуто суспільні відносини, що виникають під час створення, використання, розповсюдження і споживання електронних довірчих послуг в Україні.

Звернено увагу на характерну спрямованість законотворців виключно в напрямі інтеграції українського законодавства в законодавче поле Європейського Союзу та недостатню інтеграцію в загальносвітові інформаційно-комунікаційні структури.

Визначено, що розвиток нормативної бази в одному напрямі створює юридичні та технічні проблеми у вітчизняній галузі електронних довірчих послуг. Також констатовано, що на сьогодні так і не створено дієвих правових механізмів визнання іноземних електронних довірчих послуг.

Вказано на необхідність удосконалення правової моделі суспільних відносин та необхідності правового регулювання вітчизняної інфраструктури відкритого ключа, яка забезпечить швидку транскордонну інтеграцію національних та іноземних електронних довірчих послуг.

Доведено, що відсутність універсальних понять «транскордонність» та «транскордонні довірчі послуги» створює проблеми взаємного визнання вказаних послуг у транскордонному режимі між країнами світу. Виокремлено ключові проблеми, що перешкоджають взаємному транскордонному визнанню електронних довірчих послуг: використання різноманітних технологій, різних технічних і правових критеріїв; відсутність можливості стандартизувати правові механізми їх транскордонного застосування.

Визначено, що існує достатньо національних та регіональних концепцій і ініціатив у сфері електронних довірчих послуг, які вже досить добре опрацьовані й можуть бути базою при розробці належних правових рішень на міжнародному рівні, які можливо перенести у правові системи, що вже існують.

Аргументовано необхідність створення та прийняття єдиного міжнародного базового словника понять і термінів зі зв'язками між ними у

сфері електронних довірчих послуг, який необхідно реалізувати на рівні міжнародного нормативно-правового.

Встановлено об'єкти та суб'єкти права у сфері електронних довірчих послуг. Визначено перелік наявних проблем предметної сфери та наголошено на тому, що ключовою соціальною проблемою предметної сфери є відсутність довіри у громадян до електронних довірчих послуг, зокрема через наявну правову невизначеність термінів та положень законодавства, що призводить до уразливості споживачів, бізнесу й органів державної влади в частині надійності застосування інформаційно-комунікаційних технологій під час суспільних відносин.

Зауважено, що кореляція між національними й міжнародними нормами, які визначають основні положення та дефініції у цій сфері, ускладнена, а в рамках науки інформаційного права існує потреба глибокого порівняльного аналізу міжнародного, світового та законодавства окремих країн у галузі електронних довірчих послуг для визначення подібностей і відмінностей, колізій та спорідненості правових норм з урахуванням практик їхнього застосування.

Визначено низку проблем, які чинна модель суспільних відносин не вирішує:

відсутність єдиного правового регулювання порядків та процедур транскордонного надання іноземних електронних довірчих послуг, єдиного переліку правових норм та дефініцій у даній галузі різних юрисдикцій; неможливість практичного застосування доктринального тлумачення міжнародного права стосовно визнання електронних довірчих послуг тільки за умови участі третьої сторони, яка надає електронні довірчі послуги або здійснює їх верифікацію;

спрямованість інтеграції законодавства України в законодавче поле Європейського Союзу та відсутність регуляторного наближення до законодавств інших країн світу;

невизначеність юридичної відповідальності за порушення прав і обов'язків суб'єктів, визначених Законом України «Про електронні довірчі послуги».

Обґрунтовано необхідність встановлення відповідальності суб'єктів за порушення у сфері електронних довірчих послуг. Констатовано, що нинішній стан національного законодавства в частині класифікації злочинів у сфері використання інформаційно-комунікаційних технологій, зокрема у сфері електронних довірчих послуг, не відповідає вимогам сьогодення.

Запропоновано удосконалити модель суспільних відносин у сфері електронних довірчих послуг. Наголошено на можливості забезпечення надійної взаємодії суб'єктів електронних довірчих послуг не тільки в національному правовому полі, а й з суб'єктами іноземних юрисдикцій, тобто шляхом створення третьої довірчої сторони, яка гарантує надійність та достовірність правових механізмів визнання іноземних електронних довірчих послуг.

Описано функціонування сучасної моделі суспільних відносин у сфері електронних довірчих послуг та визначено очікувані позитивні досягнення.

Констатовано необхідність створення третьої довірчої сторони у взаємовідносинах між Україною та іноземними країнами та союзами країн у сфері електронних довірчих послуг.

Вказано на необхідність забезпечення надійних процедур визнання іноземних електронних довірчих послуг, визнання або підтвердження достовірності процедур ідентифікації підписувачів/надавачів електронних довірчих послуг шляхом створення правового й технічного шлюзу між юрисдикціями й технологіями різних країн та українським законодавством.

Звернено увагу на необхідність забезпечення додаткової правової регуляції діяльності органів державної влади у сфері електронних довірчих послуг шляхом введення для державних службовців кваліфікованого електронного підпису загальнодержавного зразка.

Сформульовано авторські визначення понять «компрометація особистого ключа цифрового підпису», «державний електронний довірчий центр» та вдосконалено визначення «транскордонні електронні довірчі послуги».

Уперше на концептуальному рівні з урахуванням досвіду розвинених країн світу та міжнародних організацій, а також тенденцій розвитку інформаційно-комп'ютерних технологій розроблено й запропоновано удосконалити соціально-правову модель суспільних відносин під час транскордонного надання електронних довірчих послуг.

Удосконалено перелік та характеристики суб'єктів сфери електронних довірчих послуг, правові механізми запровадження загальнообов'язкової форми юридичної відповідальності підписувачів, користувачів, надавачів кваліфікованих електронних довірчих послуг, а також органів державної влади та місцевого самоврядування під час надання електронних довірчих послуг.

Доведено, що система правового регулювання суспільних відносин, пов'язаних з інформаційною взаємодією, потребує формування власних термінів, які б відображали правову специфіку в цій сфері. Запропоновано та вдосконалено низку дефініцій, зокрема: «електронна довірча послуга», «електронна послуга», «електронний підпис», «компрометація особистого ключа електронного підпису», «державний цифровий довірчий центр (третя довірча сторона)», «транскордонність», «транскордонне визнання електронного підпису або електронної довірчої послуги», «транскордонна електронна послуга», що створило умови для формування гармонізованої системи термінів, які пов'язані з правовим регулюванням визнання іноземних електронних підписів.

Результати дисертаційного дослідження використовуються в освітньо-науковому процесі – при викладанні навчального циклу дисциплін з інформаційного права, програм підвищення кваліфікації державних

службовців за тематикою «Цифрова грамотність публічних службовців. Smart-технології.», «Електронне декларування публічних службовців», «Електронне урядування в сучасній системі державного управління», «Доступ до публічної інформації» (акт впровадження Інституту підвищення кваліфікації керівних кадрів Національної академії державного управління при Президентові України» від 29.10.2019 р. № 23-11/496);

Крім того, викладені в дисертації висновки та практичні рекомендації були використані в науковій діяльності Науково-дослідного інституту інформатики і права Національної академії правових наук України (Акт впровадження результатів дисертаційного дослідження від 20.02.2020 року).

Сформульовані за наслідками наукового дослідження положення наукової новизни та всі результати роботи отримані на підставі особистого вивчення та аналізу теоретичних і законодавчих положень, практики правозастосування.

Окремі висновки містять конкретні пропозиції з удосконалення чинного в Україні адміністративного законодавства, зокрема: нову редакцію ст. 1, 5, 7, 7-1, 10-12, 16, 22, 23, 25, 37, 38 Закону України «Про електронні довірчі послуги».

На основі розроблених рекомендацій розроблено проект Закону України «Про внесення змін до Закону України «Про електронні довірчі послуги».

Ключові слова: інформаційне право, електронний підпис, електронні довірчі послуги, правовідносини у сфері електронного підпису та електронних довірчих послуг, транскордонне визнання електронних довірчих послуг.

SUMMARY

Kostenko O.V. Legal enforcement of the transboundary provision of electronic trust services. – The manuscript.

Thesis for a doctor of philosophy degree, specialty 081 – Law; 12.00.07 – administrative law and process; financial law; informational law. The Research Institute for Informatics and Law of National Academy of Law Sciences of Ukraine, Kyiv, 2020.

The thesis is the first scientific work that undertakes the important scientific task to form the theoretical, methodological, and practical regulations on the legal enforcement of the transboundary provision of electronic trust services through the improvement of national legislation, which will promote the effective realization of digital transformation strategy in Ukraine.

The thesis addresses the main problems of legal enforcement of the transboundary provision of electronic trust services.

Practically, the experience of legislative regulation of transboundary provision of electronic trust services of a signature has not been studied. Besides, procedures of their transboundary recognition have not been generalized. It is explained by the comprehensive connection of questions stated above with the international law, national legal and technical regulations, standards, the use of various mathematical algorithms, etc. To provide the implementation of electronic trust services in the transboundary regime, it is necessary to improve legal regulation. Under activation of international cooperation, development and introduction of amendments in Ukrainian legislation is an essential task.

Based on the conclusions made in the work, the author has justified the scientific approach on the necessity to conduct a research on the identification process of theoretical and methodological rules of legal regulations and improving national legislation to create terms for the transboundary provision of electronic trust services in order to ensure trust for the extensive use of information and communication technologies both in Ukrainian social life and while international

cooperation. It will promote the effective realization of the state's digital transformation strategy.

The author has analyzed and improved doctrinal approaches in the international legislation related to the problem of recognition of foreign electronic signatures. When analyzing conceptual approaches to principles of foreign electronic trust services recognition and generalization of legislative experience of the most famous international centers for development, implementation, and regulation of legal issues of transboundary provision of electronic trust services, namely: International Chamber of Commerce and Economic Commission for Europe (UNCITRAL), the European Union, The Interparliamentary Assembly of Member Nations of the Commonwealth of the Independent States and the Association of South-East Asian Nations, it has been determined that international regulations implement a great number of terms related to "transboundary," the content of which is not specified. However, these terms are essential for creating regulatory legal acts of national legislation in the sphere of electronic signatures in the future.

The considerable attention has been paid to the study of legislative experience of interstate creations of the European Union and the Commonwealth of Independent States, countries-members of the Association of South-East Asian Nations (ASEAN), the United States of America, and certain Asian countries in Post-Soviet countries in the direction of transboundary introduction of electronic signatures.

The comparative analysis of international legislation and that of certain countries in the sphere of electronic signatures has also been conducted. The similarities and differences, collisions, and similarity of legal rules have been identified taking into account the practice of their implementation.

The subject of the special attention of the thesis is peculiarities of the actual state of Ukrainian legislation, which regulates the sphere of electronic trust services.

The modern world is determined by processes of globalization, development of world economy, economic, scientific, business, trade, and informational social relations, which influence not only the international system of interactions but any processes in certain countries. In addition, they have an impact on ensuring the rights and addressing the interests and needs of their citizens and state institutions.

One of the main components of modern social relations is a rapid information exchange and securing its topicality, reliability, integrity, responsiveness, identity, credibility, and completeness.

Powerful informational and computer technologies allowed building new social relations between subjects of legal relations during the process of information exchange in the form of electronic (digital) documents or electronic services. The implementation of electronic signature technology by using algorithms of digital cryptographic protection provides the reliability of information exchange.

Solving a set task can be reached based on the research of theoretical regulations on improving legal mechanisms for ensuring procedures of transboundary provision of electronic signatures using the comparative analysis of international law regulations, the legislation of foreign states, and national legislation. The reason is that there has been no research on the problem.

The social relations appearing while creation, implementation, distribution, and consumption of electronic signatures in Ukraine have been studied.

The attention has been paid to a distinctive orientation of lawmakers exclusively on the integration of Ukrainian legislation into the legislative space of the European Union and their ignoring of integration into global information and communication structures.

It has been determined that the development of the regulatory framework in one direction creates legal and technical problems in the domestic field of electronic trust services, namely the lack of legal mechanisms for ensuring the recognition of foreign electronic trust services.

Both the necessity to improve legal model of social relations and the need to provide legal regulation of domestic infrastructure of the open key, which will ensure the prompt transboundary integration of national and foreign electronic trust services, have been outlined.

It has been proved that the lack of universal concepts of “transboundary” and “transboundary trust services” creates problems of mutual recognition of these services between world countries in the transboundary regime. The research has identified key problems hampering a mutual transboundary recognition of electronic trust services: the implementation of various technologies, different technical and legal criteria, and a lack of the possibility to standardize legal mechanisms of transboundary usage of electronic trust services.

The sufficient number of national and regional concepts and initiatives in the sphere of electronic trust services, which are already well-developed and can be regarded as the basis while developing appropriate legal solutions at the international level, has been identified. Probably, they can be transferred to the current legal systems.

The necessity to create and adopt a single international thesaurus in the sphere of electronic signatures, which is to be realized at the level of a regulatory legal act in the form of a basic dictionary of concepts and terms with their inter-conceptual relations, has been argued.

The scientific work has identified legal objects and subjects in the sphere of electronic signatures. The list of existing problems of a subject area has been provided. Moreover, the research has emphasized the key social problem of a subject area. It is a lack of trust in electronic signatures among citizens, in particular, due to a current legal ambiguity of legislative terms and provisions, which results in the vulnerability of consumers, businesses, and public authorities in the field of the reliability of information and communication technologies implementation in social relations.

It has been marked that correlation between national and international rules, which determine basic provisions and definitions in this sphere, is hampered.

Within the information law, there is a need for a thorough analysis of international and world legislation as well as legislation of certain countries in the sphere of electronic signatures to identify similarities and differences, collisions and similarity of legal rules taking into account practices of their implementation.

A number of problems, which a current model of social relations do not solve, has also been identified:

- a lack of a unified legal regulation of orders and procedures of transboundary provision of foreign electronic trust services; a lack of a unified list of legal rules and definitions in the sphere of various jurisdictions; impossibilities to implement practically doctrinal interpretation of international law in relation to electronic signatures recognition provided that the third party delivering electronic trust services or conducting its verification will take part in the process;

- a focus of Ukrainian legislation on integration into a legislation field of the European Union alone and ignoring regulatory approaching to the legislation of other world countries;

- the ambiguity of legal responsibility for subjects' rights and duties breaking stipulated in the Law of Ukraine "On electronic trust services."

The need to identify the subjects' responsibility for violations in the sphere of electronic trust services has been explained. It has been observed that the current state of national legislation in the area of classification of crimes in the sphere of information and communication technologies implementation, including the sphere of electronic signatures, does not meet today's requirements.

The research has suggested upgrading a legal model of social relations in the sphere of electronic trust services. The work has also emphasized the possibility to provide reliable cooperation between subjects of electronic signature services both in the national legal area and with subjects of foreign jurisdictions by the creation of the third trusted party, which guarantees reliability and credibility of legal mechanisms for the recognition of foreign electronic trust services.

The functioning of a modern model for social relations in the sphere of electronic signature has been described. Moreover, positive achievements that can be obtained in the future are identified.

The necessity to create the third trusted party in the relationship between Ukraine and foreign countries as well as countries unions in the sphere of electronic signature has been stated.

The need to provide reliable procedures of foreign trust services recognition as well as recognition and confirmation of procedures to identify signers/providers of an electronic signature by forming legal and technical gateway between jurisdictions and technologies of different countries and Ukrainian legislation has been outlined.

The attention is drawn to the need to provide additional legal regulation of public authorities operating in the sphere of electronic trust services by introducing a qualified electronic signature of a national sample to public officials.

The author's definition of notions "discredit of a personal key of an electronic signature" and "state electronic trust center" has been introduced in the work. Such definitions as "transboundary electronic trust services" and "transboundary electronic services" have been improved.

For the first time, at the conceptual level, taking into account the experience of developed countries and international organizations, as well as tendencies in the development of information technologies, a new social and legal model of social relations while the transboundary provision of an electronic trust services has been developed and suggested.

The list and characteristics of subjects in the sphere of electronic trust services, legal mechanisms providing generally binding forms of legal responsibility of signers, users, and providers of qualified electronic trust services, public authorities, and local self-government during electronic trust services delivery have been improved.

It has been proved that the system of legal regulation of social relations related to information cooperation needs the creation of own terms that would

reflect the legal specificity in the sphere. The work has suggested and improved a number of definitions, in particular: “electronic trust service,” “electronic service,” “electronic signature,” “discredit of a personal key of an electronic signature,” “state electronic trust center (the third trust party),” “transboundary,” and “transboundary electronic service.” It has created conditions for the formation of the harmonized system of terms related to the legal regulation of foreign electronic signatures recognition.

The results of the dissertation research are used in the educational and scientific process while teaching the educational cycle of disciplines in information law, training programs for civil servants on the topic "Digital literacy of public servants. Smart-technologies," "Electronic declaration of public servants," "E-government in the modern system of public administration," "Access to public information"(the act of implementation of the Institute for Advanced Training of Management of the National Academy of Public Administration under the President of Ukraine" dated 29.10.2019 . № 23-11 / 496).

Besides, the conclusions and practical recommendations set out in the thesis were used in the scientific activities of the Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine (The Act of results implementation of the dissertation research dated 20.02.2020).

The provisions of scientific novelty have been formulated as a result of the scientific research and all the results of the work have been obtained on the basis of personal study and the analysis of theoretical and legislative provisions as well as law enforcement practice.

Some conclusions contain specific proposals to improve the current administrative legislation in Ukraine, in particular, a new version of Art. 1, 5,7,7-1, 10-12, 16, 22, 23, 25, 37, 38 of the Law of Ukraine “On electronic trust services.”

Based on the developed recommendations, the draft law of Ukraine “On amendments to the Law of Ukraine “On electronic trust services” has been developed.

Key words: information law, electronic signature, electronic trust services, legal relationship in the sphere of electronic signatures and electronic trust services, transboundary recognition of electronic trust services.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

У наукових фахових виданнях України:

1. Костенко О.В. Міністерство юстиції України - вікно держави у світовий простір електронного цифрового підпису. *Бюлетень Міністерства юстиції України* №3. 2014. С.142–149.
2. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в законодавстві пострадянських країн. *Фаховий науковий журнал «Право і суспільство»*. № 5. Частина 2. 2018. С. 110–116.
3. Костенко О.В. Проблеми правового регулювання визнання іноземних електронних довірчих послуг в Україні. *Фаховий науковий журнал «Науковий вісник Ужгородського національного університету. Серія «Право»*. № 51. Т. 1. 2018. С. 192–197.
4. Костенко О.В. Електронний підпис та електронні довірчі послуги в законодавстві Сполучених Штатів Америки. *Науковий фаховий журнал «Інформація і право»*. № 3 (26) 2018. С. 76–84.
5. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в міжнародному законодавстві. *Фаховий збірник наукових праць «Науковий вісник публічного та приватного права»*. № 4 2018. С. 13–19.
6. Костенко О.В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі. *Науковий фаховий журнал «Інформація і право»*. № 3 (30) 2019. С. 96–105.
7. Горбенко Ю.И., Потий А.В., Костенко А.В., Исирова Е.В., Горбенко И.Д. Состояние и сущность процессов нормализации европейской

нормативной базы в области электронных подписей. *Прикладная радиоэлектроника*, № 3. Т. 13. 2014. С. 261–267. (1,0/0,2 ум. друк. арк.)

8. Костенко О.В. Костенко В.В. Транскордонна ідентифікація фізичних та юридичних осіб, як елемент правового регулювання електронних довірчих послуг в Європейському союзі. *Фаховий науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки»*. № 29 (68) 2018. С. 90–93.

9. Костенко О.В. Костенко В.В. Шляхи запровадження електронних довірчих послуг в нотаріальному процесі. *Фаховий науковий журнал «Південноукраїнський правничий часопис»* № 4 2018. С.118–123. (0,6/0,3 ум. друк. арк.);

10. Костенко О.В., Костенко В.В. Особливості правового регулювання сфери електронних підписів в законодавстві країн Латинської Америки. *Науковий фаховий журнал «Право і суспільство»*. № 2. 2019. С.102–110. (0,6/0,3 ум. друк. арк.);

11. Костенко О.В., Костенко В.В. Електронні підписи та порядок визнання іноземних сертифікатів електронних підписів в законодавстві окремих країни Азії. *Науковий фаховий журнал «Науковий вісник публічного та приватного права»* №1 2019. С.10–106. (0,6/0,3 ум. друк. арк.);

***У зарубіжних виданнях та наукових фахових виданнях України,
які зареєстрованих у міжнародних наукометричних базах:***

12. Костенко О.В. Компрометація особистого ключа електронного підпису (правовий аспект). *Міжнародний науковий журнал «International journal of innovative technologies in economy»* № 3(15) 2018 С. 15–22.

13. Костенко А.В. Проблемы правового регулирования признания иностранных электронных доверительных услуг в Укроне. *Международный научно-практический правовой журнал «Legea si Viata»*. № 10/2(322). 2018. С. 54–58.

14. Костенко О.В. Сучасна правова модель суспільних відносин сфери електронних довірчих послуг в Україні. *Міжнародний науковий журнал «Recht der Osteuropäischen Staaten»* №4. 2018. С. 139–142.

15. Mykhailo Loshytskyi, Oleksii Kostenko, Ihor Koropatnik, Galyna Tereshchuk, Vladyslav Karelin. Organization competence of NATO information security policy journal of security and sustainability issues. Volume 9, Number 3. 2020. p. 735 -746 (1,0/0,2 ум. друк. арк.)

Публікації в інших виданнях, тези наукових доповідей:

16. Костенко О.В. Проблеми правового регулювання транскордонного визнання іноземних електронних послуг та іноземного сертифікату електронного підпису в Україні. *Стан та перспективи розвитку юридичної науки: матеріали міжнародної науково-практичної конференції, 31 серпня – 1 вересня 2018 р., Дніпро* /упорядн.: Громадська організація «Правовий світ», 2018. С. 65–69.

17. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в законодавстві пострадянських країн. *Пріоритетні напрямки розвитку сучасної юридичної науки: матеріали Міжнародної науково-практичної конференції, 14-15 вересня 2018 р., м. Харків*./упорядн.: Громадська організація «Асоціація аспірантів-юристів». 2018. С. 45–49.

18. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в міжнародному законодавстві. *Інтеграція юридичної науки і практики в сучасних умовах: матеріали Міжнародної науково-практичної конференції, 24-25 серпня 2018 р., м. Запоріжжя*./ упорядн.: Класичний приватний університет. 2018. С. 66–69.

19. Костенко О.В. Шляхи правого регулювання електронних довірчих послуг в Європейському Союзі. *Інформаційне право: сучасні виклики і напрями розвитку: матеріали Першої науково-практичної*

конференції 18 жовтня 2018р., Київ/упорядн.: Національна академія правових наук України, Науково-дослідний інститут інформатики і права, Національний технічний університету України «Київський політехнічний інститут імені Ігоря Сікорського» факультет соціології і права, Навчально-науковий центр інформаційного права та правових питань інформаційних технологій. 2018. С. 190–193.

20. Костенко О.В. Правові питання регулювання довірчих послуг в міжнародних актах UNCITRAL. *Інтернет речей: Проблеми правового регулювання та впровадження: матеріали Другої науково-практичної конференції*, 29 листопада 2018 м. Київ/ упорядн.: Комітет Верховної Ради України з питань інформатизації та зв'язку, Національна академія правових наук України Науково-дослідний інститут інформатики і права НАПрН України, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» факультет соціології і права. 2018. –С. 160–164.

21. Костенко О.В. Правова адаптація суспільних відносин в сфері цифрового підпису та електронних довірчих послуг в Україні до законодавства ЄС. *Особенности адаптации законодательства Молдовы и Украины к законодательству Европейского Союза: матеріали Міжнародної науково-практичної конференції*, 23-24 марта 2019 р., Кишинів, Республика Молдова/упорядн.: Institutul decercetari, politice si sociologice universitate de stat «Alecu Russo» din balti institutul din balti institutul destinte penale criminologie aplicata, 2019. С. 136–139.

22. Костенко О.В. Компрометація особистого ключа електронного підпису (правовий аспект). *Актуальні питання розвитку та взаємодії публічного та приватного права: матеріали Міжнародної науково-практичної конференції*, 16-17 березня 2019 р., Львів./ упорядн.: Західноукраїнська організація «Центр правничих ініціатив». 2018. – С. 102–104.

23. Костенко О.В., Капшук О.О. Проблема інтероперабельності Національної системи електронного цифрового підпису в Україні та шляхи їх вирішення. *6-th International conference SAIT 2014 «System Analysis and Information Technologies»*, 26-30 травня 2014 р. Київ/упорядн. Natalia D.Pankratova, Institute for Applied System Analysis of National Technical University of Ukraine Kyiv Polytechnic Institute, 2014. С. 297–298. (0,6/0,3 ум. друк. арк.);

24. Костенко О.В., Костенко В.В. Імплементація національного законодавства в сфері електронних довірчих послуг до регламенту ЄС. *Чотирнадцяті читання. Проблеми імплементації національного законодавства до угоди про асоціацію між Україною та ЄС.: матеріали міжнародної наукової конференції 17-18 квітня 2019 р.*, Київ. упорядн.: Науково-дослідний інститут інформатики і права НАПрН України, Національний педагогічний університет імені М.П. Драгоманова, Інститут держави і права ім. В.М. Корецького НАН України, Центр правової освіти і науки, Громадська організація «Феміда». 2019. С. 16–19. (0,6/0,3 ум. друк. арк.);

25. Костенко О.В., Костенко В.В. Вирішення проблем правового регулювання сфери цифрового підпису та електронних довірчих послуг в Україні. *Сутність та значення законодавства на розвиток суспільних відносин: матеріали Міжнародної науково-практичної конференції, 8-9 березня 2019 р.*, Одеса./ упорядн.: Причорноморська фундація права. 2019. С. 55–58. (0,6/0,3 ум. друк. арк.);

26. Костенко О.В., Костенко В.В. Вирішення проблем законодавства щодо застосування електронного підпису та електронних довірчих послуг в транскордонному режимі. *Право як ефективний суспільний регулятор: матеріали Міжнародної науково-практичної конференції 15–16 лютого 2019 р.*, Львів/ упорядн.: Західноукраїнська організація «Центр правничих ініціатив». 2019. С. 79–81. (0,6/0,3 ум. друк. арк.);

27. Костенко О.В., Костенко В.В. Модернізація суспільних та правових відносин сфери цифрового підпису відповідно до угоди про асоціацію між Україною та ЄС. *Інтелектуальна власність і право на шляху до сталого розвитку України, матеріали II Міжнародної науково-практичної конференції*, 19 квітня 2019 р., Київ / упорядн.: Міністерство освіти і науки України Національний університет «Одеська юридична академія» Київський інститут інтелектуальної власності та права. 2019. С. 11. (0,6/0,3 ум. друк. арк.);

28. Костенко О.В., Костенко В.В. Проблеми компрометації цифрового підпису, як елемента фіксації авторського права. *Інтелектуальна власність і право на шляху до сталого розвитку України, матеріали II Міжнародної науково-практичної конференції*, 19 квітня 2019 р., Київ/ упорядн.: Міністерство освіти і науки України Національний університет «Одеська юридична академія» Київський інститут інтелектуальної власності та права. 2019. С. 6. (0,6/0,3 ум. друк. арк.);

ЗМІСТ

ВСТУП.....	24
РОЗДІЛ 1. АНАЛІЗ АКТІВ МІЖНАРОДНОГО ЗАКОНОДАВСТВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ НАДАННЯ ТРАНСКОРДОННИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ	36
1.1. Основні теоретичні проблеми міжнародного та внутрішньодержавного права у сфері електронних довірчих послуг та електронних підписів.....	36
1.2. Визнання іноземних електронних довірчих послуг та електронних підписів у міжнародному законодавстві, актах регіональних міжнародних організацій та законах окремих країн Європи.....	45
1.3 Законодавство США та країн Латинської Америки у сфері регулювання транскордонного надання електронних підписів	63
1.4. Законодавство пострадянських країн та окремих країн Азії у сфері регулювання транскордонного надання електронних підписів	77
Висновки до розділу 1	101
РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ СФЕРИ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ В УКРАЇНІ	107
2.1 Загальний стан сфери електронних довірчих послуг та електронного підпису в Україні	107
2.2. Електронні довірчі послуги в Україні.....	114
2.3 Розвиток законодавства України у сфері електронних довірчих послуг та електронного підпису	125
2.4. Порівняльний аналіз понятійно-категоріального апарату сфери електронних довірчих послуг та електронного підпису	130
Висновки до розділу 2	145

РОЗДІЛ 3. ШЛЯХИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РЕГУЛЮВАННЯ ТРАНСКОРДОННОГО НАДАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ	147
3.1. Удосконалення правової моделі регулювання суспільних відносин у сфері електронних довірчих послуг в Україні	147
3.2. Загальні правові підходи до вдосконалення національного законодавства щодо визнання іноземних електронних довірчих послуг	158
Висновки до розділу 3	177
ВИСНОВКИ	180
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	185
ДОДАТКИ	204

ВСТУП

Обґрунтування вибору теми дослідження. Сучасний світ позначений процесами глобалізації, розвитку світової економіки, політичних, економічних, наукових, бізнесових, торговельних, інформаційних суспільних відносин, які безпосередньо впливають не тільки на міжнародну систему взаємовідносин, а й на відповідні процеси в конкретних країнах, а також на забезпечення прав, задоволення інтересів і потреб їхніх громадян та державних інституцій.

Потужні інформаційні комп'ютерні технології дозволили започаткувати нові суспільні відносини між суб'єктами правовідносин під час: електронного обміну інформацією (Electronic Data Interchange); електронного руху капіталу (Electronic Funds Transfer); електронної торгівлі (e-Trade); використання електронних грошей (e-cash); електронного маркетингу (e-market); електронного банкінгу (e-banking); електронної системи здоров'я (e-health) та в інших сферах.

Обмін інформацією здійснюється в процесі електронних транзакцій у формі електронних (цифрових) документів або електронних послуг, а надійність інформації забезпечується застосуванням технології електронного підпису із використанням алгоритмів цифрового криптографічного захисту.

Незважаючи на високу надійність використання криптоалгоритмів, електронні підписи не мають широкого застосування через низьку довіру до цих сервісів. Недовіра до електронних підписів є бар'єром для впровадження в повсякденне життя багатьох сучасних інформаційних технологій через можливість технічного втручання в цифрові транзакції та транскордонні електронні послуги та неоднозначність трактування різних правових систем, норм міжнародного й національних законодавств, які забезпечують юридичні гарантії у сфері електронних довірчих послуг.

Проблема юридичної незахищеності електронного підпису свідчить про необхідність відокремлення правового регулювання суспільних відносин,

пов'язаних із технологіями електронного підпису, від правового регулювання суспільних відносин, пов'язаних із застосуванням електронних довірчих послуг.

Слід зауважити, що досвід законодавчого регулювання використання електронних довірчих послуг під час транскордонного надання практично не вивчався, не узагальнювалися процедури їх транскордонного визнання, оскільки ці питання так чи інакше комплексно пов'язані із міжнародним та національним правом, юридичними та технічними нормативними актами, стандартами, порядками застосування різних математичних алгоритмів тощо.

Нині в національних правових системах різних держав існують різні підходи та відмінності в термінології і механізмах регулювання застосування електронних довірчих послуг, що породжує неврегульованість процедур транскордонного визнання електронних довірчих послуг, які надають та/або використовують суб'єкти різних юрисдикцій.

Враховуючи викладене, актуальним та суспільно необхідним завданням сьогодення є вдосконалення законодавства України, що стосується правового регулювання транскордонного надання електронних довірчих послуг.

Вирішення поставленого завдання можливо на основі дослідження теоретичних положень правових механізмів забезпечення процедур транскордонного визнання електронних довірчих послуг на основі порівняльного аналізу положень міжнародного права й законодавства іноземних держав.

Аналіз міжнародних актів у зазначеній сфері свідчить про нагальну потребу проведення їхньої своєрідної умовної кодифікації з метою імплементації положень «кодифікованого» документа в національне законодавство. Умовна кодифікація означає створення своєрідного «кодифікованого акту» міжнародного права, який би об'єднав правові положення всіх наявних декларацій, резолюцій та інших міжнародних документів за принципами звичайної кодифікації. Такий підхід надав би

можливість суттєво підвищити ефективність імплементації положень міжнародного права до національного законодавства України.

Теоретичним підґрунтям дисертаційної роботи в частині правового регулювання інформаційної сфери стали праці вчених: І.В. Арістової, О.А. Баранова, К.І. Белякова, В.М. Брижка, Р.А. Калюжного, Л.П. Коваленко, С.П. Кудрявцевої, А.І. Марущака, А.М. Новицького, О.В. Олійника, В.Г. Пилипчука, І.М. Сопілко, М.Я. Швеця, В.С. Цимбалюка та ін.

За останні роки питання використання цифрового підпису досліджувалися в наукових працях: І.Л. Бачило, І.В. Гавловського, І.Д. Горбенка, Ю.І. Горбенка, О.В. Корнейка, Ю.М. Куракіної, О.В. Потія, Б.О. Погорелова, А.О. Мелашенка, О.Л. Перевозчикова.

Окремі питання застосування електронних підписів досліджено такими зарубіжними авторами, як: Дон Джонсо, Скот Ванстоун, Ванебо Мао, Алан Турі, Стефан Масон, Кароліна Лаборде, Стефе Блайс, Тромер Пеллігріні, Майк Джаст, Паул ван Ооршот.

Незважаючи на зазначені роботи вчених, проблема правового регулювання транскордонного визнання електронних довірчих послуг досліджувалась недостатньо, окремі її аспекти висвітлено фрагментарно.

Таким чином, актуальним є проведення досліджень щодо визначення теоретико-методологічних положень правового регулювання та вдосконалення національного законодавства для створення умов щодо надання електронних довірчих послуг у транскордонному режимі з метою забезпечення довіри до широкого використання інформаційно-комунікаційних технологій і в суспільному житті України, і в міжнародній співпраці, що сприятиме ефективній реалізації стратегії цифрової трансформації держави.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано з урахуванням «Стратегії розвитку наукових досліджень Національної академії правових наук України на 2016 – 2020 роки», затвердженої Загальними зборами НАПрН України 03.03.2016 року.

Дослідження проведено в рамках науково-дослідних робіт Науково-дослідного інституту інформатики і права НАПрН України «Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері» (січень 2018 р. – грудень 2022 р., номер державної реєстрації 0117U007745) та «Теоретико-методологічні засади правового регулювання суспільних відносин в умовах використання технологій Інтернет речей» (січень 2017 р. – грудень 2019 р., номер державної реєстрації 0116U007744).

Мета і завдання дослідження

Метою дисертаційної роботи є теоретичне обґрунтування та наукова розробка пропозицій щодо удосконалення правового регулювання транскордонного надання електронних довірчих послуг, що сприятиме ефективній реалізації стратегії цифрової трансформації України.

Відповідно до мети дослідження визначено такі основні *завдання*:

- надати характеристику трансформації суспільних відносин в суспільні інформаційні відносини, що стосується транскордонного надання електронних довірчих послуг;
- розкрити основні теоретичні проблеми міжнародного та внутрішньодержавного права у сфері електронних довірчих послуг та електронних підписів;
- дослідити міжнародне законодавство та нормативно-правові акти регіональних міжнародних організацій, окремих країн Європи, що стосується сфери електронних довірчих послуг та електронних підписів;
- проаналізувати досвід законодавчого регулювання правовідносин у сфері електронного підпису та електронних довірчих послуг у Сполучених Штатах Америки та країнах Латинської Америки;
- охарактеризувати існуючі підходи до вирішення проблеми визнання іноземних електронних довірчих послуг та електронних підписів у міжнародних нормативно-правових актах та актах регіональних міжнародних організацій та законах окремих країн Європи;

- здійснити аналіз законодавства пострадянських країн та окремих країн Азії у сфері регулювання транскордонного надання електронних довірчих послуг та електронного підпису;

- проаналізувати існуючу правову модель суспільних відносин у сфері електронних довірчих послуг в Україні, та з урахуванням сучасних світових тенденцій надати пропозиції щодо її удосконалення;

- здійснити порівняльний аналіз міжнародного законодавства та нормативно-правових актів окремих країн щодо понятійно-категоріального апарату сфери застосування електронних довірчих послуг та електронного цифрового підпису;

- окреслити загальний стан розвитку законодавства України у сфері транскордонного надання електронних довірчих послуг та виявити існуючі проблеми у цій сфері;

- розробити пропозиції щодо удосконалення складу суб'єктів правовідносин, пов'язаних з транскордонним наданням електронних довірчих послуг та електронного підпису, а також правових механізмів запровадження загальнообов'язкової форми їх юридичної відповідальності під час застосування електронних підписів;

- напрацювати конкретні пропозиції щодо удосконалення національного законодавства шляхом внесення змін до нормативно-правових актів України у сфері правового забезпечення транскордонного надання електронних довірчих послуг;

Об'єктом дослідження є суспільні відносини у сфері електронних довірчих послуг.

Предметом дослідження є правове забезпечення транскордонного надання електронних довірчих послуг.

Методи дослідження. Для досягнення поставленої мети та завдань у роботі використано загальнонаукові методи, зокрема:

- діалектичний – для узагальнення наукових підходів, розробок, пропозицій учених, виявлення основних напрямів дослідження за темою дисертації;
- історико-правовий – з метою вивчення стану наукової розробки теми дослідження та її джерельної бази;
- порівняльно-правовий – для дослідження регулятивного законодавства в Україні та інших країнах;
- формально-логічний – використано як універсальний спосіб аргументування положень і висновків автора;
- формально-юридичний – для дослідження норм чинного законодавства у сфері електронного підпису;
- соціологічний – для обробки офіційної та власноруч сформованої статистичної інформації як одного з джерел відомостей про предмет дослідження;
- догматичний – для тлумачення юридичних категорій, за його допомогою поглиблено й уточнено понятійний апарат.

Методологічною основою роботи є система методів, яка була дібрана з урахуванням мети та особливостей дослідження для найбільш повного розкриття його предмета. Обґрунтованість та достовірність дослідження забезпечили загальнонаукові, спеціально-наукові та конкретно-наукові методи пізнання, зокрема діалектичний метод пізнання, історичний, формально-логічний, порівняльно-правовий, системно-структурний, метод синтезу, моделювання, логіко-семантичний метод, герменевтичний та інші.

Завдяки *формально-логічному та порівняльно-правовому* методам було досліджено зарубіжні та українські нормативно-правові акти на предмет закріплення в них норм та процедур визнання іноземних електронних підписів на міжнародному та місцевому рівнях (підрозділ 1.1, 1.2, 1.3, 1.4, 2.3), ці методи допомогли виявити шляхи вдосконалення українського законодавства та його гармонізації з нормами міжнародного права в частині визнання іноземних електронних підписів, а також внесення змін до

законодавства, яке регулює предметну сферу (підрозділ 2.1, 2.2, 2.3, 3.1, 3.2). *Формально-логічний метод* також надав можливість виявити прогалини, які існують у правовій регламентації змісту правовідносин під час застосування електронних підписів (підрозділ 2.3).

Використання *системно-структурного методу* забезпечило формулювання системи специфічних правових принципів інформаційної взаємодії (підрозділ 2.2). Об'єднання методів *синтезу моделювання та системно-структурного аналізу* дозволило запропонувати прогресивну сучасну правову модель суспільних відносин сфери електронних підписів в Україні (підрозділи 3.1, 3.2). За допомогою *діалектичного та історичного* методів було визначено витоки проблеми неналежного правового регулювання галузі (підрозділи 1.3, 3.1). *Статистичний* було використано при обробці результатів діяльності суб'єктів сфери цифрового підпису в Україні (підрозділ 2.1).

Нормативно-правову базу дисертації становлять: Конституція України, закони України, укази та розпорядження Президента України, постанови та розпорядження Кабінету Міністрів України, нормативно-правові акти центральних органів виконавчої влади та органів місцевого самоврядування, акти міжнародного права, Комісії ООН з міжнародного торговельного права (ЮНСІТРАЛ), документи Ради Європи, Європейського Союзу, нормативно-правові акти окремих країн світу, що регулюють інформаційні відносини у сферах надання електронних довірчих послуг, електронних підписів та електронної ідентифікації.

Науково-теоретичну основу дисертації становлять теоретико-методологічні розробки та монографічні дослідження вітчизняних та зарубіжних фахівців у галузі інформаційного та інших галузей права, а також напрацювання науковців у цьому напрямі.

Емпіричну основу роботи становлять результати статистичних досліджень та зведених даних органів державної влади й суб'єктів сфери електронних довірчих послуг за період 2014 – 2019 рр.

Наукова новизна одержаних результатів полягає у тому, що дисертація є першою комплексною науковою працею, у якій вирішується важливе наукове завдання з формування теоретико-методологічних та практичних положень щодо правового забезпечення транскордонного надання електронних довірчих послуг шляхом удосконалення національного законодавства, що сприятиме ефективній реалізації стратегії цифрової трансформації України.

У рамках проведеного дослідження одержано такі найбільш значущі результати, що мають наукову новизну й виносяться на захист, зокрема:

уперше:

- запропоновано визначення понять «компрометація особистого ключа цифрового підпису», «державний цифровий довірчий центр», що сприятиме системному правовому використанню електронних довірчих послуг, підвищенню рівня довіри до електронних сервісів;

- запропоновано шляхи удосконалення нормативно-правового регулювання сфери електронних довірчих послуг та електронного підпису;

- розроблено пропозиції щодо внесення змін до національного законодавства з метою забезпечення транскордонного надання електронних довірчих послуг, зокрема, запропоновано: створення Державного цифрового довірчого центру; внесення додаткових суб'єктів до Закону України «Про електронні довірчі послуги», таких як Національне агентство України з питань державної служби та Державного цифрового довірчого центру;

удосконалено:

- визначення понять «транскордонні електронні довірчі послуги», «транскордонні електронні послуги», що сприятиме чіткому правовому регулюванню суспільних відносин, пов'язаних із транскордонним наданням електронних довірчих послуг та електронного цифрового підпису;

- сучасну правову модель суспільних відносин у сфері транскордонного надання електронних довірчих послуг;

- склад та характеристики суб'єктів правовідносин, пов'язаних із наданням електронних довірчих послуг;

- правові механізми запровадження загальнообов'язкової форми юридичної відповідальності підписувачів, користувачів, надавачів кваліфікованих електронних довірчих послуг, а також органів державної влади та місцевого самоврядування під час застосування електронних підписів;

дістали подальшого розвитку:

- підходи до обґрунтування та розуміння трансформації суспільних відносин у сфері електронного підпису, які відбуваються одночасно із перетворенням законодавства не тільки в напрямі адаптації до законодавства Європейського Союзу, але й гармонізації із законодавством інших країн світу;

- науково-теоретичні та практичні рекомендації щодо вдосконалення правових механізмів державного управління у сфері електронних підписів;

- систематизація міжнародного та зарубіжного досвіду у сфері електронних підписів;

- пропозиції щодо вдосконалення національного законодавства в частині регулювання визнання іноземних електронних підписів;

- напрями правового упорядкування проблем застосування електронних підписів;

- напрями розвитку державних електронних сервісів в рамках стратегії «Держава в смартфоні» та перспективи транскордонного надання електронних довірчих послуг.

Практичне значення одержаних результатів проведеного дослідження полягає у тому, що сформульовані та методологічно обґрунтовані висновки можуть бути використані у:

науково-дослідній сфері – положення та висновки дисертації було використано в процесі розробки пропозицій щодо актуальних проблем правового регулювання та першочергових заходів у сфері забезпечення

кібернетичної безпеки України, а також можуть бути використані в процесі подальшої розробки актуальних проблем інформаційного права, правових проблем регулювання інформаційної взаємодії в інших сферах життєдіяльності суспільства, як на місцевому так і на державному рівні (акт впровадження Науково-дослідного інституту інформатики і права Національної академії правових наук України від 20.02.2000 р.);

освітньому процесі – при викладанні навчального циклу дисциплін з інформаційного права, програм підвищення кваліфікації державних службовців за тематикою «Цифрова грамотність публічних службовців. Smart-технології», «Електронне декларування публічних службовців», «Електронне урядування в сучасній системі державного управління», «Доступ до публічної інформації» (акт впровадження Інституту підвищення кваліфікації керівних кадрів Національної академії державного управління при Президентові України» від 29.10.2019 р. № 23-11/496).

Особистий внесок здобувача. Дисертаційна робота є самостійною науковою працею. Наукова новизна, висновки та рекомендації сформульовані автором самостійно, обґрунтовані на підставі особистих досліджень та міркувань. Із наукової праці, опублікованої у співавторстві, використано лише ті ідеї та положення, які одержано особисто здобувачем (90% змісту). При використанні наукових праць інших учених, нормативно-правових актів, джерел емпіричної інформації на них зроблено відповідні покликання.

Апробація результатів дослідження. Результати роботи були оприлюднені автором на міжнародних та науково-практичних конференціях, круглих столах, семінарах, форумах: 16-th International conference SAIT 2014 «System Analysis and Information Technologies» (Київ, 26 – 30 травня 2014 р.); Міжнародна науково-практична конференція «Пріоритетні напрямки розвитку сучасної юридичної науки» (Харків, 14 – 15 вересня 2018 р.); Міжнародна IX Всеукраїнська науково-практична конференція «Актуальні

питання розвитку та взаємодії публічного та приватного права» (Львів, 16 – 17 березня 2018 р.); IV International Scientific and Practical Conference «Methodology of Modern Research» (Dubai, UAE, 31 march 2018); Міжнародна науково-практична конференція «Інтеграція юридичної науки і практики в сучасних умовах», (Запоріжжя, 24 – 25 серпня 2018 р.); Міжнародна науково-практична конференція «Стан та перспективи розвитку юридичної науки» (Дніпро, 1 вересня 2018 р.); Міжнародна науково-практична конференція «Право як ефективний суспільний регулятор» (Львів, 15 – 16 лютого 2019 р.); Міжнародна науково-практична конференція «Сутність та значення впливу законодавства на розвиток суспільних відносин» (Одеса, 8 – 9 березня 2019 р.); Перша науково-практична конференція «Інформаційне право: сучасні виклики і напрями розвитку» (Київ, 18 жовтня 2018 р.); Друга науково-практична конференція «Інтернет речей: проблеми правового регулювання та впровадження» (Київ, 29 листопада 2018 р.); Міжнародна науково-практична конференція «Особенности адаптации законодательства Молдовы и Украины к законодательству Европейского Союза» (Кишинев, Республіка Молдова, 23 – 24 березня 2018 р.); Міжнародна наукова конференція «Чотирнадцяті юридичні читання. Проблеми імплементації національного законодавства до угоди про асоціацію між Україною та ЄС» (Київ, 17 – 18 квітня 2019 р.); II міжнародна науково-практична конференція «Інтелектуальна власність і право на шляху до сталого розвитку України» (Київ, 19 квітня 2019 р.); Міжнародна науково-практична конференція «Право як ефективний суспільний регулятор» (Львів, 15 – 16 лютого 2019 р.); Міжнародний форум «PKI Forum UA-2018» (Київ, 3 – 4 жовтня 2018 р.).

Публікації. Основні положення дисертаційної роботи опубліковано у 15 статтях, 12 з них опубліковано у фахових виданнях у галузі юридичних наук, перелік яких затверджено МОН, 4 у зарубіжних наукових виданнях, які включені до міжнародних науково-метричних баз, у тому числі 1 у Scopus, а також у 13 тезах доповідей на міжнародних та всеукраїнських науково-практичних конференціях, круглих столах, семінарах.

Структура та обсяг дисертаційної роботи. Дисертація складається зі вступу, трьох розділів, висновків до кожного розділу та загальних висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 269 сторінок, з них основного тексту 157 сторінок. Список використаних джерел нараховує 157 найменувань.

РОЗДІЛ 1.

АНАЛІЗ АКТІВ МІЖНАРОДНОГО ЗАКОНОДАВСТВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ НАДАННЯ ТРАНСКОРДОННИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

1.1. Основні теоретичні проблеми міжнародного та внутрішньодержавного права у сфері електронних довірчих послуг та електронних підписів

Кінець минулого століття характеризується початком глобального застосування комп'ютерів та розвитком мереж передачі даних та інформаційних технологій, що майже одразу створили нові суспільні відносини в галузі електронної комерції, електронного документообігу та електронного підпису. Одночасно постала проблема юридичного статусу даних, що передаються, причому вирішити цю проблему необхідно було і на національному, і на міжнародному, транскордонному, рівні.

Одними з основних складників новітніх суспільних відносин є швидкий обмін цифровою інформацією та забезпечення її актуальності, надійності, цілісності, оперативності, ідентичності, достовірності й повноти, що є фактичним підтвердженням того, що сучасне суспільство можна розглядати як інформаційне суспільство, тобто суспільство нового перспективного стану розвитку. Згідно з висновком В.Г. Пилипчука, за цих умов також актуалізується потреба розвитку інформаційного права та його виокремлення в окрему наукову спеціальність як таку, що досліджує суспільні відносини та розв'язує правові проблеми у сфері обігу інформації, створення, формування, зберігання, поширення, використання, охорони й захисту інформаційних ресурсів, розробки й застосування інформаційних технологій та продуктів, забезпечення інформаційної безпеки, надання

послуг і виконання робіт за напрямками діяльності людини, суспільства, держави та міжнародної спільноти в інформаційній сфері [1].

Вивчаючи процеси трансформації суспільних відносин у суспільні інформаційні відносини, І.В. Арістова та В.Д. Чередначук пропонують об'єднати їх одним поняттям «інтегративна інформаційна сфера», яка за інформаційним критерієм (тобто за циркуляцією інформації) об'єднує всі сфери суспільного життя, зокрема й інформаційну. Інформаційну сферу суспільних відносин доцільно визначити як сферу, у якій здійснюється виключно інформаційна діяльність [2].

І.В. Бачилло вважає, що інформаційна сфера може бути структурована за різними критеріями, мати ієрархічну побудову та припускає, що правове чи інше регулювання в галузі обігу інформації більш адекватно визначати як інформаційне середовище. Зважаючи на це, сферу електронного підпису можна розглядати як підсистему загальної інформаційної сфери держави, яка може бути структурована за різними критеріями та мати ієрархічну побудову [3].

На сьогодні в українському законодавстві немає дефініції понять «сфера електронного підпису», «сфера електронних довірчих послуг». Однак ми можемо визначити сферу електронного підпису як просторово-тимчасову область суспільних взаємовідносин, пов'язаних зі створенням, отриманням, використанням, застосуванням, зберіганням (захистом) та знищенням електронних підписів, а сферу електронних довірчих послуг – як сферу суспільних відносин, пов'язаних із забезпеченням створення, перевірки та підтвердження електронних довірчих послуг.

Поряд з тим, така сфера за своєю внутрішньою природою є комплексним різнобічним явищем, і далеко не останню роль у ньому відіграє такий його елемент, як інформаційна сфера. Остання являє собою багатовекторне активне утворення, яке включає всі види інформаційної діяльності фізичних і юридичних осіб, державних органів та інших суб'єктів цієї діяльності, а також самих суб'єктів інформаційної діяльності; сукупність

інформації у будь-якій матеріальній і нематеріальній формі, інформаційних ресурсів, інформаційних технологій та інших інформаційних розробок; чинну інформаційну інфраструктуру з наявними в ній інформаційними послугами, інформаційною продукцією, інформаційними макро- і мікрокліматом; множинність внутрішньої природи інформаційної сфери, яка включає інформацію та інформаційні відносини (первинні/базисні конструкції інформаційної сфери), інформаційну діяльність та інформаційну інфраструктуру, інформаційну культуру, суб'єктів інформаційної діяльності. Надбудовним рівнем названих елементів є державне управління інформаційною сферою, інформаційне право та інформаційне законодавство.

О.А. Баранов констатує, що людство перебуває в процесі широкого впровадження технологій Інтернету на основі використання штучного інтелекту, робототехніки, різноманітних сенсорів, технологій блокчейн, «хмарних» технологій, «великих даних», технологій передачі даних мережі Інтернет, що обумовлює зменшення різноманітних бар'єрів (валютних, транспортних, фінансових, адміністративних, митних тощо), завдяки чому мінімізуються транзакційні витрати [4].

Процеси впровадження комп'ютерних технологій та конвергенції технічних засобів, технологій і послуг набули масштабного поширення, що вимагає термінових змін правової парадигми регулювання відповідних суспільних відносин в інформаційній сфері [5].

Глобалізація торкнулась не лише процесів міжнародного поділу праці, міграції в масштабах усієї планети капіталу, людських та виробничих ресурсів, але й стандартизації законодавства, економічних та технічних процесів, а також зближення культур різних країн [1].

На думку В.В. Ткаченка, глобалізація є каталізатором дослідження концептуальних засад адаптації інформаційного законодавства України до міжнародних правових стандартів в умовах розвитку інформаційного суспільства. Науковці на міжнародному рівні акцентують увагу на дослідженні понятійних апаратів відповідних сфер суспільних

правовідносин, що дозволить з'ясувати сутність процесу адаптації, його зміст та особливості [6].

Крім того, В.В. Ткаченко вважає, що українським законотворцям при розробці та створенні національних нормативно-правових актів, слід враховувати те, що:

- міжнародне та внутрішньодержавне право – це різні правові конструкції, перше не може бути безпосереднім регулятором суспільних відносин у сфері дії другого;
- для надання міжнародно-правовим нормам юридичної сили у сфері дії внутрішньодержавного права вони повинні бути «трансформовані» в норми національного права;
- проведення процедури «трансформації» забезпечується виданням відповідного національно-правового акту [6].

Аналізуючи міжнародне законодавство, Stephen E. Blythe відзначає, що є неоднорідність та специфічність нормативно-правових актів у сфері електронного підпису. Так, Stephen E. Blythe пропонує законодавство в цій сфері поділяти на три категорії. До першої належать країни, які зобов'язали використовувати технологію PKI (PKI – інфраструктура відкритого ключа). До другої категорії науковець відносить міжнародні організації та окремі країни, які застосовують гібридну модель сфери електронного підпису та «обмежений технологічний нейтралітет». Гібридні моделі більш гнучкі та пристосовані до нових технологічних розробок, але одночасно вони більш ефективно формують довіру населення до цифрових підписів. До третьої категорії Stephen E. Blythe відносить країни з «мінімалістськими законами» у сфері електронного підпису. До таких країн належать Великобританія, США, Австралія та Нова Зеландія, законодавство яких надзвичайно орієнтовано на спрощення бізнес-процесів. Однак розвиток суспільних відносин у сфері електронної торгівлі та електронного підпису акцентує питання модернізації «лоскуткової ковдри» законів про електронний підпис на єдине прийнятне для всіх країн законодавство [7].

Питання достовірності дій підпису та довіри до електронних підписів порушує Alan L. Tyree. Проблема виникає, коли важко визначити, хто насправді підписав електронний договір електронним підписом, чи передбачував підписувач наслідки підписання, чи це було дійсно його волевиявлення. Фактично весь процес застосування електронних підписів для посвідчення електронних угод базується на тому, що кожна сторона погоджується на таку форму правовідносин. Наразі все більше правочинів здійснюються із застосуванням електронного підпису, створеного в системі PKI, що підвищує надійність електронних угод [8].

Коментуючи національне законодавство, І.Л. Бачило стверджує, що особливості федерального закону, який регулює сферу електронних підписів, не дозволяють навіть у достатньо далекій перспективі визнати іноземні електронні підписи переважної більшості іноземних країн у Російській Федерації, оскільки передбачають визнання за міжнародним договором або добровільне виконання іноземною державою загального порядку визнання іноземних електронних підписів згідно з законодавством [9].

Вивчаючи роль електронного підпису в умовах ведення електронної комерції в Російській Федерації, В.І. Квашнін зауважує, що російським законодавством процедура юридичного визнання іноземного електронного підпису на сьогодні не має чітких правил. Так, в окремих випадках пропонується застосовувати паперовий носій, на якому друкується інформація щодо іноземного сертифіката електронного підпису, які на території Росії легалізуються із допомогою процедури консульської легалізації. Однак цей підхід є архаїчним. Сучасна схема визнання іноземних електронних підписів базується на міжнародних угодах, що створюють умови уніфікованого та більш чіткого регулювання суспільних відносин у цій сфері. Водночас міждержавні угоди мають тривалі терміни узгодження, потребу юридичних компромісів та узгодження через відмінності політичних позицій різних держав, складність забезпечення рівнів технічної деталізації

та тривалу в часі корекцію угод. В.І. Квашнін вважає за доцільне створити міжнародну систему взаємного визнання електронних підписів [10].

Вивчаючи проблему міжнародного застосування електронних підписів та електронних документів, Ю.М. Куракіна відзначає, що нормотворчість у цій сфері не вирішує проблеми транскордонного визнання електронних підписів. Натомість законодавства різних країн, незважаючи на загалом типові підходи до створення нормативно-правових актів, на сьогодні не мають однозначного тлумачення основних понять у системі електронного підпису [11]. Серед українських науковців проблеми технологічного характеру транскордонного визнання електронних підписів та визначення механізмів крос-сертифікації були предметом наукових досліджень О.Л. Перевозчикової та А.О. Мелашенка.

Аналізуючи шляхи розвитку в Україні Національної системи електронних цифрових підписів (або інфраструктури відкритих ключів (PKI) та її юридичного вдосконалення, О.Л. Перевозчикова та А.О. Мелашенко зазначають, що відсутність довіри призвела до негативного іміджу всієї системи. Міжнародна електронна комерція в Україні ускладнена неможливістю крос-сертифікації, тобто трансграничного визнання електронних підписів, виданих у різних країнах через невпорядкованість на юридичному, організаційному та технологічному рівнях, неможливості перевірки сертифіката відкритого ключа, виданого в іншій країні. У своїх роботах О.Л. Перевозчикова та А.О. Мелашенко приділяють увагу саме аспектам побудови технічних механізмів, які повинні забезпечити функціонування електронних підписів у транскордонному режимі. Застосування правових механізмів транскордонного визнання електронних підписів розглядається як дотичний до технічних заходів процес.

За ствердженнями О.В. Потія, успішне впровадження сучасних технологій електронного урядування, різноманітних електронних сервісів та електронних довірчих послуг неможливо без створення відповідної інфраструктури. Сьогодні такою технологічною інфраструктурою виступає

PKI – інфраструктура відкритих ключів. Використання цифрового підпису базується на довірі між суб'єктами взаємодії, інфраструктурі відкритих ключів та спрямовано на реалізацію моделі довіри. На думку О.В. Потія, на сучасному етапі розвитку інформаційних технологій довіру до електронних підписів можна підвищити шляхом застосування технології blockchain до децентралізованого поширення та управління відкритими ключами. Фактично О.В. Потій пропонує застосувати криптосервер як третю довірчу сторону, обмежившись лише функцією більш надійної аутентифікації. Юридично така схема не знайшла відображення [12]. Як стверджує Р.А. Калюжний, електронний підпис стає дійсно ключовим елементом інформаційного забезпечення державної управлінської діяльності в умовах стрімкої цифровізації [13].

Значну увагу науковці приділяли й дотепер приділяють технічним аспектам застосування електронних підписів. Так, одним із засновників вітчизняної криптографії І.Д. Горбенком було створено цілу сучасну наукову школу, яка розробляє методологічні основи сучасної криптології: криптографії та криптоаналізу. Створюються новітні методи, механізми, системи, державні стандарти, протоколи та засоби криптографічних перетворень, що застосовуються для надання електронних довірчих послуг. Формуються вимоги до криптографічних засобів, криптографічних протоколів, систем і засобів криптографічного захисту інформації, подаються висновки та рекомендації [14]. Аналогічні фундаментальні дослідження в галузі криптографії проводилися й іноземними вченими, такими як, наприклад, Wenbo Mao [15]. Однак, водночас юридичним аспектам застосування електронних підписів приділяється досить мало уваги.

Проблему складності здійснення широкомасштабних транскордонних електронних послуг та забезпечення надійної електронної ідентифікації, автентифікації та електронних підписів вивчав Ю.І. Горбенко. У своїх дослідженнях він спирається на нормативно-правові акти Європейського союзу у сфері електронних підписів, які не поширюються на добровільні

угоди суб'єктів у рамках приватного права, а також договірні відносини або інші правові зобов'язання. Ю.І. Горбенко констатує, що для впровадження надійних процедур взаємного визнання електронних підписів необхідно забезпечити високий рівень інформаційної безпеки, усунути технологічні та юридичні несумісності і зменшити рівень кіберзлочинності. Це можливо досягти, створивши відповідно до Директиви 2006/123/ЕС Європейського парламенту та Ради від 12 грудня 2006 року «Про послуги на внутрішньому ринку» [16] «точки єдиного контакту – спеціалізовані центри» (PSC). Так, точки єдиного контакту, застосовуючи взаємно визнані й прийняті електронні засоби ідентифікації, повинні полегшити транскордонне надання електронних підписів на внутрішньому ринку ЄС і дозволити підприємствам вийти за кордон, не стикаючись із перешкодами при взаємодії з органами державної влади. Однак на сьогодні не визначено перелік компонентів електронного підпису, які мають бути опрацьовані правовою системою іншої держави для визнання іноземного електронного підпису, а самі точки не створено.

Ю.І. Горбенко зауважує, що для України важливою проблемою є гарантія безпеки довірчих електронних послуг, особливо електронних підписів, а також необхідність створення інфраструктури довірчих послуг, які рекомендуються для держав Європейського Союзу [17].

Україна теж є активним учасником глобальних процесів, і це вимагає від держави активного процесу інтеграції у світове законодавче поле. Так, 16 вересня 2014 р. Верховна Рада України та Європейський парламент синхронно ратифікували Угоду про асоціацію між Україною та ЄС.

Угода про асоціацію за своїм обсягом і тематичним охопленням є найбільшим міжнародно-правовим документом за всю історію України та найбільшим міжнародним договором із третьою країною, коли-небудь укладеним Європейським Союзом. Вона визначає якісно новий формат відносин між Україною та ЄС на принципах «політичної асоціації та економічної інтеграції» і слугує стратегічним орієнтиром системних

соціально-економічних реформ в Україні. Положення Угоди також прямо стосуються сфери електронного підпису та електронних довірчих послуг, а саме: статтею 140 задекларовано, що сторони підтримують діалог з питань регулювання електронної торгівлі, що включає, *inter alia*, такі питання:

- визнання сертифікатів електронних підписів, виданих населенню, та сприяння розвитку послуг транскордонної сертифікації;
- відповідальність постачальників посередницьких послуг у зв'язку з переданням або зберіганням інформації;
- поводження з небажаними електронними комерційними повідомленнями;
- захист споживачів у сфері електронної торгівлі;
- будь-які інші питання, які стосуються розвитку електронної торгівлі.

Таке співробітництво може існувати у формі обміну інформацією про відповідне законодавство Сторін стосовно цих питань, а також про впровадження такого законодавства [18].

Як стверджує В.М. Фурашев, сучасна національна нормативно-правова база регулювання суспільних відносин в інформаційній сфері не відповідає вимогам сучасності, цілям та завданням розвитку інформаційного суспільства в Україні [19]. Незважаючи на достатню насиченість нормативно-правовими актами, сфера електронного підпису також потребує суттєвого упорядкування, починаючи з термінологічного апарату.

1.2. Визнання іноземних електронних довірчих послуг та електронних підписів у міжнародному законодавстві, актах регіональних міжнародних організацій та законах окремих країн Європи

Питання правової стандартизації в останнє десятиліття активізувало нормотворчі процеси регуляції суспільних відносин у багатьох галузях. Характерно, що ініціатива одночасно виходить від правознавців та науковців окремих країн та міжнародних організацій.

На міжнародному рівні роботу із правової стандартизації в галузі електронного обміну даними, торгівлі та електронного підпису очолила Комісія ООН з міжнародного торговельного права, Міжнародної торгової палати і Європейської економічної комісії (UNCITRAL) [20]. У 1984 році на 17-й сесії UNCITRAL було заслухано доповідь Генерального секретаря «Правові аспекти автоматичної обробки даних» [21] та доповідь Секретаріату «Правова цінність комп'ютерних записів» [22], у яких порушено питання необхідності внесення змін у правові норми країн, маючи за мету створення законних умов використання електронного повідомлення або даних як доказу в суді, а також законодавчого забезпечення однакової юридичної сили за паперовими та електронними документами. У червні 1996 року затверджено закон, який отримав назву «Про електронну комерцію» («UNCITRAL, Model Law on Electronic Commerce») [23] і який став першим базовим нормативно-правовим актом у галузі електронного обміну даними, електронної пошти, електронних сертифікатів та інших форм електронного обміну даними. Таким чином, на міжнародному законодавчому рівні встановлювалися визначення та правила, що стали фундаментом для побудови законодавства в новій галузі. Типовим законом запроваджено поняття: «повідомлення даних» («data message»), «електронний обмін даними» та інші, що фактично створило умови поглинання наявних на той час недоліків спеціальних правових і технічних термінологій. Однак найважливішим досягненням Типового закону ЮНСІТРАЛ «Про електронну комерцію» є загальний

порядок застосування юридичних вимог відносно «повідомлення даних», встановлений статтями 5, 5 біс та 7 другої глави, якими запроваджено три базові принципи: визнання юридичної сили повідомлення даних; типовий алгоритм роботи з електронними документами; загальні умови визнання іноземних електронних підписів. Слід зазначити, що Типовий закон ЮНСІТРАЛ «Про електронну комерцію» не надає єдиного узагальненого визначення електронного підпису у зв'язку із залежністю його критеріїв від певного етапу технічного розвитку та конкретних умов або режиму його транскордонного використання [24].

Цю проблему повинен був вирішити наступний нормативно-правовий акт – Типовий закон ЮНСІТРАЛ «Про електронні підписи» 2001 року («UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 [25]» (далі – Типовий закон), ратифікований Верховною Радою України в 2007 році.

Типовий закон представив дефініції понять «електронний підпис», «сертифікат», «підписант», «постачальник сертифікаційних послуг» та ін., які стали класичною основою для створення нормативно-правових актів практично для всіх країн. Також Типовий закон заклав правові основи визнання іноземних електронних підписів. Так, статтею 12 цього акту встановлено, що:

сертифікат електронного підпису, виданий за межами держави, що приймає, має таку саму юридичну силу в державі, яка приймає, як і сертифікат, виданий у державі, яка приймає, якщо він забезпечує по суті еквівалентний рівень надійності;

електронний підпис, створений або використовуваний за межами держави, яка приймає, має таку саму юридичну силу в державі, яка приймає, як і електронний підпис, створений або використовуваний в державі, яка приймає, якщо він забезпечує по суті еквівалентний рівень надійності;

при визначенні того, чи забезпечує сертифікат або електронний підпис по суті еквівалентний рівень надійності, слід враховувати визнані міжнародні стандарти та будь-які інші відповідні чинники.

Окремо слід звернути увагу на пункт 5 цієї статті, у якому вперше застосовується термін «транскордонність» у контексті визнання використання певних видів електронних підписів або сертифікатів за умови досягнення взаємних домовленостей, достатніх для їх транскордонного визнання. Водночас закон не надає визначення транскордонних електронних підписів, транскордонних електронних послуг, перелік та порядок їх регулювання.

Зважаючи на певну декларативність виданих ЮНСІТРАЛ нормативно-правових актів, до вирішення правової проблеми застосування електронних підписів у транскордонному режимі долучились міжнародні організації та окремі країни світу.

З метою здійснення електронних угод і розвитку електронної комерції Європейським Союзом 13 грудня 1999 року прийнято Директиву 1999/93/Європейського парламенту та Ради «Про систему електронних підписів, що застосовується в межах Співтовариства» [26] (Directive: 1999/93/EC Community framework for electronic signatures) (далі – Директива). Директива встановлювала юридичний статус і загальні правила використання електронних підписів на території країн Європейського Союзу, а також зобов'язувала всі держави-члени Європейського Союзу у визначений термін прийняти відповідні національні закони, керуючись положеннями Директиви. Директива вдосконалила поняття «електронний підпис» (electronic signature), запровадила дефініції «вдосконалений електронний підпис» (advanced electronic signature), «сертифікат», «чинний сертифікат», «постачальник послуг сертифікації», «продукція для електронного підпису», які позитивно вплинули на формування правничих та впорядкування суспільних відносин під час надання електронних послуг із застосуванням електронних підписів та низки технічних норм, необхідних для формування

інфраструктури відкритих ключів (Public key infrastructure, PKI). Окрему увагу Директива приділяла проблемі транскордонного визнання електронних підписів [26]. Статтею 7 цього акту було встановлено загальні вимоги та порядок транскордонного надання послуг із сертифікації із третіми державами та правове визнання вдосконалених електронних підписів, виданих у третій державі. Так, якщо електронний підпис був створений в державі, яка не є членом ЄС, але при цьому він відповідає вимогам Директиви, то його визнання вважалося можливим. Передбачалося визнання іноземних електронних підписів через двосторонні й багатосторонні угоди між державами.

Слід зазначити, що Директива [26] використовує терміни «транскордонна діяльність», «транскордонні угоди», «надання транскордонних послуг громадянам», «транскордонне надання послуг із сертифікації». Аналіз вказаних термінів та положень Директиви свідчить про відсутність узагальнювальної норми-дефініції щодо понять «транскордонність» та «транскордонні послуги», які вживаються без визначення змісту, а в контексті надання електронних довірчих послуг не розроблено єдиного критерію розуміння цих термінів.

Директива Європейського Союзу «Про електронні підписи» (Directive: 1999/93 / EC Community Framework for electronic signatures) імплементована Верховною Радою України 19 січня 2000 року і стала фундаментальним актом, на основі якого протягом багатьох років створювалась нормативно-правова база України у сфері електронного підпису.

Після запровадження Директиви, Європейський союз активно продовжив вивчати проблематику законодавчого забезпечення транскордонних електронних онлайн-послуг. За результатами досліджень визнано, що Директива охоплює та рекомендує країнам-членам Союзу розвивати нормативну регуляцію виключно у сфері застосування електронних підписів і не надає всебічних транскордонних та міжрегіональних основ для безпечних, надійних і простих електронних

операцій. Водночас аналіз чинного законодавства Європейського союзу засвідчив, що відмінності національних законодавств ЄС часто призводять до правової невизначеності та додаткового навантаження на організацію та забезпечення електронних сервісів. Крім того, фактично відсутні загальноприйнятні транскордонні та міжрегіональні нормативно-правові та системно-технічні основи правового забезпечення застосування населенням та організаціями електронних сервісів та електронних підписів. Також визначено необхідність покращення чинного законодавства і його розширення для забезпечення взаємного визнання і прийняття на рівні ЄС заявлених електронних механізмів ідентифікації, автентифікації, електронних підписів та інших необхідних електронних довірчих послуг ЄС.

Європейський парламент і Рада 12 грудня 2006 року прийняли Директиву 2006/123/ЄС про послуги на внутрішньому ринку [27], згідно з якою держави-члени ЄС зобов'язані вжити заходів зі створення «точок єдиного контакту» (PSC), щоб гарантувати надійність процедур і формальностей, які надаються електронним шляхом та пов'язані з доступом до електронних послуг.

Наступним кроком у розвитку законодавства у сфері надання електронних довірчих послуг у транскордонному режимі став Соціальний звіт 2010 року Комісії Європейського Союзу, яким наголошено на необхідності вирішення проблем, які перешкоджають громадянам Євросоюзу користуватися перевагами єдиного цифрового ринку і транскордонними цифровими послугами [28].

Європейська Рада закликала Комісію, зважаючи на наявні розбіжності в національних правових системах, вжити нормотворчих заходів щодо створення правових умов для взаємного визнання та сумісності ключових компонентів цифрового ринку, таких як електронна ідентифікація, електронні документи, електронні підписи та сертифікати, електронні послуги доставки, а також послуги електронного Уряду на території Європейського Союзу.

Вирішення цієї проблеми покладено на проєкт STORK (Secure identity across borders linked) [29], метою якого є створення і впровадження єдиної загальноєвропейської системи електронної ідентифікації. Перша частина проєкту STORK 1.0 складалась із 6 пілотних завдань:

- 1) використання транскордонних електронних послуг (демонстраційний режим) через національні портали Австрії, Естонії, Німеччини, Португалії та частково Бельгії;
- 2) безпечний «е-чат» між студентами та викладачами навчальних закладів через національні портали Австрії та Ісландії;
- 3) е-мобільність студентів, забезпечена завдяки доступу до баз знань через портали закладів вищої освіти Австрії, Естонії, Іспанії, Італії, Португалії;
- 4) е-доставка – для розвитку транскордонних механізмів безпечної «он-лайн» доставки документів в Австрії, Естонії та Словенії;
- 5) е-реєстрація місця проживання з метою спрощення внутрішньої міграції громадян країн-членів ЄС для фіксації нової адреси адміністраціями нової та базової країни;
- 6) співпраця із Європейською комісією щодо систематизації послуг аутентифікації (European Commission Authentication Service) [30].

Наступний проєкт STORK 2.0 [31] було спрямовано на реалізацію чотирьох пілотних напрямів надання електронних послуг, а саме:

- 1) е-Banking мав на меті надати можливість фізичним і юридичним особам країн-членів ЄС вільно користуватися послугами іноземних банків через їхні вебсервіси (відкривати банківські рахунки, робити фінансові операції);
- 2) сервіс е-Health призначений для швидкого доступу до інформації, що зберігається в закладах охорони здоров'я в країні пацієнта, що сприятиме зменшенню вартості й підвищенню якості лікувальних послуг шляхом залучення інформаційних технологій у разі направлення пацієнта на лікування в іншу країну;

3) e-Learning спрямований на вивчення можливості побудови та запровадження системи міждержавної електронної освіти, а також створення Європейської зони вищої освіти (ЕНАЕ: European Higher Education Area);

4) e-Government for Business має на меті організацію міждержавного доступу до державної або муніципальної інформації про видачу дозвільних документів, переоформлення, видачу дублікатів, анулювання документів дозвільного характеру для підприємств та організацій, що мають наміри працювати в конкретних економічних секторах або галузях шляхом «зарахування в публічні реєстри» або за процедурою «One-stop shop» [32].

У рамках проєктів проаналізовано основні юридичні ризики в питаннях вирішення спорів, захисту даних, відповідальності, гарантій рівня обслуговування електронних послуг тощо. Учасниками проєктів здійснено аналіз суспільних інфраструктур електронної ідентифікації для довірчих послуг у кожній країні-члені ЄС, проаналізовано правові норми, ключові поняття, а також процедури покладання на фізичних та юридичних осіб правових повноважень з використанням електронних засобів, зокрема електронного підпису.

Аналіз використання електронних підписів у різних сферах суспільних відносин країн-членів ЄС поряд із позитивним досвідом зафіксував і достатньо протиріч та недоліків. Це стосується передусім недовіри громадян до електронних операцій на внутрішньому ринку ЄС, електронних підписів, процедур взаємного визнання електронної ідентифікації та електронної аутентифікації, а також неприпустимо високого рівня кіберзлочинності.

За результатами проєктів STORK планується здійснити порівняльний аналіз та систематизацію нормативних розбіжностей між чинними національними законодавствами країн-членів ЄС та Регламентом, проблеми будуть вирішуватися шляхом пошуку та внесення відповідних правових норм у національні законодавства законотворчим органом кожної з країн-учасниць у кожному конкретному випадку.

Проект STORK – це елемент модернізації правової та технічної нормативної бази, що сприятиме регулюванню використання країнами-членами ЄС електронних підписів [33]. Загалом проєкт мав за мету підвищити ефективність співпраці державного та приватного секторів на національному та загальноєвропейському рівнях, спростити адміністративні формальності, забезпечити спрощений онлайн-доступ до публічних транскордонних електронних довірчих послуг через кордони Європейського Союзу в захищеному та безпечному інформаційно-технологічному просторі. Вважалося, що реалізація проєкту збільшить інтероперабельність електронної ідентифікації та електронних довірчих послуг у рамках кордонів європейських держав, а також забезпечить електронну аутентифікацію фізичних осіб із повноваженнями, що дозволяють представляти юридичних осіб [34].

Водночас «Регламент (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку, що скасовує Директиву 1999/93/ЄС» на сьогодні застосовується лише Францією та Німеччиною, а інші країни використовують національне законодавство.

Історично робота над законодавством у сфері цифрового підпису в країнах Європи розпочалася з середини 90-х років XX століття.

Протягом 1996 – 1997 років Італія та Федеративна Республіка Німеччина прийняли відповідні законодавчі акти. Вони, на відміну від чинних тоді законів ЮНСІТРАЛ та окремих штатів США, використовували інший підхід, який розширив сферу застосування закону за межі електронної комерції.

Законотворці Італії у зв'язку із адміністративною реформою спочатку запровадили Закон від 15 березня 1997 року № 59 Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa [35], а згодом, 10 листопада 1997 року, в Італії було прийнято спеціальний законодавчий акт

Президента Республіки, що встановлює правила створення, зберігання та передачі документів за допомогою інформаційних засобів. Одна із частин декрету присвячена електронному цифровому підпису, який визначався як «firma digitale – результат застосування асиметричного криптоалгоритму, коли закритий ключ використовується для створення, а відкритий ключ – для перевірки справжності цифрового підпису».

У лютому 1999 року з'явився ще один правовий акт – «Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3.1 del Decreto del Presidente della Repubblica 10 novembre 1997, № 513», яким вводилося доповнення в чинні законодавчі акти стосовно регуляції національної системи електронного підпису.

Слід зазначити, що італійське законодавство достатньо ефективно реагувало на розвиток сфери електронного підпису та запровадило додатково низку відповідних регуляторних актів (Таблиця 1).

Наступним вдалим досвідом у розробці законодавства став закон Німеччини «Про цифровий підпис». Цей закон розроблено як частину федерального закону «Про регулювання загальних умов надання інформаційних та комунікаційних послуг», прийнятого 22 липня 1997 року. Він складався з 11 частин, кожна з яких являла собою самостійний законодавчий акт, присвячений певному колу питань. Частина третя федерального закону стосувалась електронного підпису. Також на додаток до цього закону в жовтні 1997 року було прийнято постанову «Про цифровий підпис». Таке законодавство встановлювало загальні вимоги використання електронного підпису. У законодавстві застосовується термін «цифровий підпис», який визначається як «печатка, що завіряє цифрові дані, яка створена за допомогою закритого ключа і дозволяє, використовуючи відповідний відкритий ключ, визначити власника ключа і підтвердити цілісність і автентичність даних». При цьому відкритий ключ обов'язково повинен мати сертифікат, виданий відповідним сертифікаційним центром або

іншою державною установою із встановленими законом повноваженнями. Сертифікатом відкритого ключа підпису вважається свідоцтво, скріплене цифровим підписом, яке містить відомості про належність відкритого ключа підпису конкретній фізичній особі. Також запроваджувалося поняття атрибутивного сертифікату як окремого свідоцтва у цифровій формі, що містить додаткові дані про власника відкритого ключа з покликанням на сертифікат ключа підпису.

Законодавство сприяло створенню системи засвідчувальних центрів, на які покладалися основні завдання щодо функціонування технології цифрових підписів: створення ключів, посвідчення власників, сертифікація, ведення реєстрів користувачів, посвідчення документів за допомогою відміток часу. Законом передбачалася сувора процедура ліцензування діяльності засвідчувальних центрів, що проводиться урядовими службами.

Нині дія цього закону скасована, і основними законодавчими актами в цій сфері є закон «Про рамкові умови для електронних підписів і змін інших правових актів» від 16 травня 2001 року та «Регламент (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС».

Слід звернути увагу на той факт, що значний інтерес у свій час викликав також документ під назвою «Офіційна позиція німецького Уряду щодо міжнародного визнання електронних цифрових підписів» [36]. Цей документ не вважається офіційним нормативно-правовим актом, однак дозволяє «підсумувати» дії німецького Уряду й визначити його загальну позицію у сфері регулювання використання електронних документів з електронним підписом в органах влади.

По-перше, для Німеччини у сфері регулювання використання електронних документів з електронним підписом в органах влади мають перевагу такі поняття, як надійність та безпека електронних підписів. Це простежується в Акті про електронний підпис: «...спочатку потрібно

створити систему сертифікації підписів, а потім вже вести роботу з порівняння електронних цифрових підписів із власноручними».

По-друге, пріоритетом є не «bona fide» сторін, а державний контроль за використанням підписів. Відповідно, і визнання електронних підписів можливе лише в умовах жорсткої бюрократичної системи їх сертифікації.

По-третє, у цьому випадку німецький Уряд не може допустити визнання іноземних підписів, що не відповідають внутрішнім стандартам: велика «дірка на кордоні» зробила би безглуздою сувору внутрішню сертифікацію. Власне кажучи, це і зазначено в п.1 параграфа 15 «Акту про електронний цифровий підпис», вірогідність якого може бути перевірена за допомогою відкритого ключа, сертифікованого в «іншій державі, може бути визнана еквівалентною електронному цифровому підпису за дійсним Актом, якщо він має такий самий рівень безпеки».

У липні 1999 року Австрією прийнято федеральний закон «Про електронний підпис», який базується на положеннях Директиви 1999/93/ЄС, а в лютому 2000 року на додаток до закону були прийняті однойменні «Правила електронного підпису», якими встановлені вимоги до технічної безпеки захищених електронних підписів, а також технічні, організаційні та інші вимоги до постачальників сертифікаційних послуг, що видає сертифікати.

Уперше в європейському законодавстві збуло застосовано поняття захищеного електронного підпису (secure electronic signature) як електронного підпису, що задовольняє такі критерії:

- дозволяє ідентифікувати свого підписувача;
- створений із використанням засобів, що перебувають під особистим контролем особи підписувача;
- пов'язаний з підписувачем даних таким чином, що надає можливість відстежити всі подальші зміни;

– створений на підставі якісного сертифіката, з використанням технічних складників і процедур відповідно до вимог забезпечення безпеки цього закону та Правил, створених на його основі.

Закон «Про електронний підпис» встановив, що саме захищений електронний підпис має рівну юридичну силу з власноручним підписом, за виключенням окремих випадків необхідності документів виключно на паперовому носії.

Також окремою статтею запроваджувався новий термін «якісний сертифікат» (qualified certificate), який повинен містити певний набір реквізитів: назву сертифіката; назву або власне ім'я постачальника сертифікаційних послуг; власне ім'я або псевдонім особи підписувача; дані для підтвердження дійсності електронного підпису; дати початку й закінчення дії сертифіката; унікальний ідентифікаційний номер сертифіката; сферу дії сертифіката (за потреби).

Як і в Директиві Європейського Союзу «Про електронні підписи», у законі Австрії детально регулювалися питання створення та діяльності інфраструктури відкритих ключів. Законом Австрії «Про електронний підпис» уперше було встановлено визнання іноземних електронних підписів за умов реєстрації їхніх постачальників у правовому полі Європейського Союзу, достовірність яких може бути підтверджена в Австрії [37].

З метою покращення якості послуг, які надаються державними установами, підвищення безпеки під час передачі електронних документів та даних у січні 2000 року Фінляндія прийняла закон «Про використання електронних технологій в державних установах», тобто закон має обмежену сферу застосування – у державних установах [38].

Законотворчий досвід Великобританії у сфері електронного підпису характеризується прийняттям у 2000 році Закону «Про електронні повідомлення». Цей законодавчий акт став відповідати Директиві Європейського Союзу «Про електронний підпис», «Модельному закону про електронну комерцію» та проєкту «Єдиних правил використання

електронного підпису та організації діяльності засвідчувальних центрів», розроблених Комісією ООН з міжнародного торговельного законодавства.

Законом запроваджено нове поняття «постачальник криптографічних послуг» та встановлено їхній перелік: реєстрація, сертифікація, проставляння відмітки часу й дати на сертифікатах і інших документах, створення і зберігання ключів для процедури електронного підписання документів, організація бази даних сертифікатів тощо, тобто основні функції системи електронних підписів. Закон надає визначення поняття «електронний підпис» і закріплює його юридичну та доказову силу. Так, електронним підписом слід вважати «щось в електронній формі, вбудоване або логічно пов'язане з електронним повідомленням або даними з метою підтвердження їхньої цілісності та автентичності». Такий підхід встановлює лише загальні принципи використання електронного підпису. У зв'язку з цим 8 березня 2002 року набрало чинності нове Положення «Про електронний підпис», у якому увагу більш детально приділено питанням впровадження електронного підпису: створення системи засвідчувальних центрів – постачальників сертифікаційних послуг, визначення їхніх повноважень і відповідальності, організація їхньої діяльності та контролю. Оновлено й дефініцію поняття «електронний підпис»: це «дані в електронній формі, приєднані або логічно пов'язані з іншими даними в електронній формі, які використовуються для підтвердження автентичності». Також до закону включено й поняття «удосконалений електронний підпис»: «електронний підпис, що задовольняє таким умовам: він унікальним чином пов'язаний з підписувачем; надає можливість ідентифікації підписувача; створений із використанням програмних засобів, що перебувають під особистим контролем підписувача; пов'язаний з даними, які підписуються, таким чином, що будь-яку зміну даних після процедури підписання можливо виявити».

У цьому акті електронний підпис визначено як «послідовність даних, які підтверджуються цілісністю та справжністю даних електронного повідомлення загальноприйнятним способом».

Також законом передбачено заходи зі створення національної інфраструктури відкритого ключа, вимоги щодо необхідності використання певної технології створення електронного підпису, деталізовано процедури, пов'язані із використанням сертифіката електронного підпису.

Уперше запроваджено вимоги зі створення центрами сертифікації реєстрів виданих сертифікатів та дійсних відкритих ключів, які мають регулярно оновлюватися.

Для сучасних правознавців закон цікавий тим, що в ньому вперше окремою главою закріплено обов'язки державних органів щодо надання електронних послуг. Згідно із законом, «...за наявності необхідного технічного, фінансового та іншого забезпечення державні органи можуть запропонувати громадянам можливість посилати запити та отримувати відповіді за певними електронними адресами. Більше того, державні органи можуть надати громадянам послуги з електронної доставки законодавчих і нормативних матеріалів, рахунків та інших документів. При наданні подібних послуг державні органи повинні використовувати технічно надійні засоби з дружнім інтерфейсом, а також забезпечувати необхідний рівень безпеки даних при обміні даними всередині й поза організацією».

Цікаво відзначити, що закон Фінляндії дозволив використання іноземних сертифікатів, якщо вони створені за певними правилами, викладеними в законі. Закон Фінляндії «Про використання електронних технологій у державних установах» створив можливості для налагодження обміну достовірною інформацією, що міститься в електронних документах, між установами і громадянами не тільки всередині держави, але й на міжнародному рівні.

Законодавство Франції розпочало роботу зі створення нормативної бази в галузі електронного підпису з ухвалення закону від 13 березня 2000 року. Уряд Франції ухвалив за № 2000-230 «Закон про адаптацію закону про докази в інформаційних технологіях та електронному підписі», яким

вноситься низка змін до Цивільного кодексу, які стосуються передусім форми та доказової сили договорів.

Зазначеним нормативним актом запроваджено визначення електронного підпису як «надійного засобу ідентифікації, що гарантує особистий зв'язок з породжуваною дією».

У березні 2001 року Францією введено в дію Декрет «Про електронний підпис», у якому електронний підпис визначено як «дані, отримані в результаті проходження процедури, що задовольняє умовам, викладеним у першому реченні другого абзацу статті 1316-4 Цивільного Кодексу». Також запроваджено поняття «захищений електронний підпис – електронний підпис, що задовольняє таким умовам:

- є власністю особи підписувача;
- створюється за допомогою засобів, що перебувають під особистим контролем особи підписувача;
- надає можливість відстежити всі зміни, зроблені після підписання».

Що ж стосується самої процедури створення електронного підпису, то і Закон «Про електронні повідомлення», і Положення «Про електронний підпис» не встановлюють будь-якої певної технології, а пропонують лише загальні визначення, за якими можливо застосовувати будь-які сучасні методи криптографії.

Україна цілком орієнтується на Європейський ринок. Так, 5 жовтня 2017 року Верховною Радою України прийнято Закон України «Про електронні довірчі послуги», який розроблено на основі Регламенту (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС», а набрання чинності цього закону відбулося 7 листопада 2018 року. Майже рік законодавці надали профільним органам держави на оновлення та запровадження нової нормативної бази, що регламентуватиме сферу електронних довірчих послуг. Однак, на сьогодні лише частина нормативних

актів перебуває у стадії проектування. Це створює певні юридичні ризики, які можуть стати перешкодою широкому запровадженню електронних довірчих сервісів, зокрема транскордонних.

Для України важливим є вивчення та аналіз можливостей використання європейського досвіду з метою створення необхідного правового забезпечення надання безпечних електронних послуг, таких як: електронна ідентифікація та аутентифікація, електронний підпис, електронні печатки та мітки часу, електронні документи, послуги електронної доставки та перевірки справжності вебсайту в транскордонному режимі.

Не тільки Європейське співтовариство вживає заходи щодо уніфікації електронного підпису під час використання в транскордонних відносинах. Співдружність Незалежних Держав (далі – СНД) також працює в напрямі забезпечення правових умов для використання електронних підписів та електронних сервісів під час міждержавного обміну даними.

Звертає на себе увагу Модельний закон «Про електронний цифровий підпис», прийнятий на 16-му пленарному засіданні Міжпарламентської Асамблеї держав-учасниць СНД (постанова № 16-10 від 09.12.2000) [39], та прийнятий на сорок п'ятому пленарному засіданні Міжпарламентської Асамблеї держав-учасниць СНД Модельний закон «Про транскордонний інформаційний обмін електронними документами» (постанова № 45-12 від 25 листопада 2016 року) [40].

Модельний закон «Про електронний цифровий підпис» СНД створено з метою забезпечення правових умов для використання електронних підписів, при дотриманні яких підпис визнається достовірним, а також обов'язки й відповідальність суб'єктів права, що надають послуги електронних підписів. Разом з тим Модельний закон закладав основи використання електронного підпису при міжнародному інформаційному обміні, включаючи здійснення транскордонних операцій, шляхом створення системи взаємного визнання сертифікатів електронного підпису, випущених однією з держав Співдружності або державою, з якою є договір про визнання таких свідоцтв.

Міжпарламентською Асамблеєю держав-учасниць Співдружності Незалежних Держав розроблено та 25 листопада 2016 року ратифіковано Модельний закон «Про транскордонний інформаційний обмін електронними документами». Мета цього акту – нормативно-правове забезпечення транскордонного обміну електронними документами між країнами-учасниками Співдружності Незалежних Держав. Проблематика надання електронних підписів у транскордонному режимі цим Модельним законом не висвітлюється й не регулюється.

Водночас Модельний закон цікавий правознавцям тим, що характеризується достатньо новою базою правових визначень, які раніше ні в міжнародному, ні в локальних законодавствах не використовувалися, а саме: «транскордонний простір довіри», «транскордонний інформаційний обмін», «юридична значимість електронного документа» тощо. Запропоновано визначення «транскордонний простір довіри – сукупність правових, організаційних і технічних умов, узгоджених державами-учасниками СНД з метою забезпечення довіри при міждержавному обміні даними й електронними документами між державними органами, органами місцевого самоврядування, організаціями та громадянами».

Формування й забезпечення функціонування трансграничного простору довіри покладається на Міждержавний координувальний орган, який створюється державами – учасниками СНД на основі міждержавної угоди про формування трансграничного простору довіри. Своєю чергою, на країни-учасники СНД, які формують транскордонний простір довіри, покладається створення відповідної інфраструктури, функціонування якої має бути гармонізованим на правовому, організаційному та техніко-технологічному рівнях.

Однак Модельний закон оминає визначення поняття «транскордонна послуга» та не містить переліку транскордонних послуг. Проблематика визнання іноземних електронних підписів та транскордонних електронних

довірчих послуг Модельним законом не висвітлюється і не регулюється. Поняття «транскордонність» ототожнюється з поняттям «міжнародний».

Слід зазначити, що в цьому дослідженні термін «транскордонність» («cross-border») розглядається в нових суспільних відносинах, які виникають між суб'єктами правовідносин під час створення та обміну «data message» як характерна ознака певних електронних сервісів «digital service», що здійснюються із використанням механізмів довіри третьої сторони, електронних підписів та їхніх сертифікатів, – транскордонна електронна довірча послуга «cross-border digital trusted service».

Цікавим є досвід країн-учасниць Асоціації держав Південно-Східної Азії (ASEAN) та Японії в напрямі взаємовизнання електронних підписів та довірчих послуг. Широке застосування електронних довірчих послуг та електронних підписів у країнах ASEAN спонукало Таїланд, Сінгапур та Японію до експерименту з транскордонного узгодженого використання та взаємного визнання операцій з електронним підписом. У 2007 році ці країни запровадили пілотну схему обміну електронними довірчими послугами та взаємного визнання електронних підписів у державній та банківській сферах, маючи на меті детальне вивчення можливостей використання електронних підписів як елемента підготовки угоди про взаємне визнання електронних підписів та пов'язаних із ними електронних довірчих послуг країнами-членами ASEAN [41].

За результатами зазначеного робимо висновок, що нормативно-правова база міжнародних організацій збагачувалася нормами, які поступово змінювали форму і зміст від узагальнених визначень до чітких і конкретних формулювань. Водночас проблеми, такі як визнання за електронними документами юридичної сили, визнання іноземних електронних підписів, залишаються такими, що припускають їх різне тлумачення в різних юрисдикціях.

1.3 Законодавство США та країн Латинської Америки у сфері регулювання транскордонного надання електронних підписів

На міжнародному рівні роботу із формування нових правових норм та нормативно-правових актів у галузі електронного обміну даними, електронної торгівлі та електронного підпису першою розпочала Комісія ООН з міжнародного торговельного права, порушивши у 1984 році на 17-й сесії Міжнародної торгової палати і Європейської економічної комісії (UNCITRAL) питання правових аспектів застосування електронних документів та їхньої юридичної сили. Це спонукало до роботи із правової стандартизації в галузі електронної торгівлі та електронного підпису не тільки міжнародні організації та об'єднання (союзи), але й низку країн.

Сполучені Штати Америки активно розпочали законотворчу діяльність у сфері електронного підпису й стали першою країною, яка запровадила електронний підпис як аналог власноручного підпису.

1 травня 1995 року штатом Юта вперше у Сполучених Штатах Америки запроваджено Закон «Про цифровий підпис» (Utah Digital Signature Act) [42], який став основою законодавства в галузі електронного підпису та електронних послуг. Звичайно, США вже використовували електронні підписи в комерційній та банківській діяльності, однак їхнє правове регулювання розпочалося саме із законодавства штату Юта. За своїм первинним задумом Закон «Про цифровий підпис» мав на меті мінімізувати випадки підробки електронного підпису, надати можливості для доказу автентичності інформації в електронній формі, а вже потім сприяти використанню електронного підпису для засвідчення електронних документів та спрощення процедури здійснення комерційних угод в електронному вигляді.

Закон штату Юта «Про цифровий підпис» запровадив визначення не електронного, а саме «цифрового підпису» (digital signature), який визначається як «послідовність бітів, що отримана підписувачем у результаті

проходження повідомлення (message), яке підписується через однобічну функцію, а потім процедуру шифрування за допомогою асиметричного криптографічного алгоритму й закритого ключа». Закон також дає визначення понять «закритий ключ», «відкритий ключ», «підписувач» та «сертифікат підписувача», а також запроваджує правові підстави функціонування засвідчувального центру Міністерства комерції штату Юта та регламентує створення інфраструктури, яка забезпечить надійне та ефективне використання цифрового підпису [43].

Уперше в законодавстві США нормативно-правовим актом встановлюється норма, згідно з якою документ, підписаний за допомогою електронного підпису, набуває однакової юридичної сили з паперовим документом, підписаним власноруч особою. Водночас закон не надає безпосередньо визначень електронних або цифрових послуг, а також не регламентує процедур визнання іноземних електронних підписів, покладаючи ці функції, а рівно як і докази їхньої юридичної надійності на сторони комерційної або іншої правової угоди.

У жовтні 1995 року штат Каліфорнія прийняв Закон «Про цифровий підпис» (California Digital Signature Act) [44]. Зазначений нормативно-правовий акт, на відміну від закону штату Юта, був створений для регулювання правовідносин, які виникають під час застосування електронних підписів у державному секторі між громадянами й державними органами. Закон штату Каліфорнія має суттєві розбіжності з базовими визначеннями закону штату Юта, тобто пропонує власні редакції дефініцій понять «цифровий підпис», «повідомлення», «особа», «підписувач» та ін. Також уперше вводиться поняття «ключова пара», що означає приватний ключ та відповідний йому відкритий ключ в асиметричній криптосистемі. Як і попередній закон штату Юта, закон штату Каліфорнія не надає визначень електронних або цифрових послуг, а процедури визнання електронних підписів, зокрема й іноземних, ґрунтується на вимозі створення електронного підпису за технологією, прийнятною для використання штатом Каліфорнія.

У березні 1996 року штатом Нью-Мексико прийнято Закон «Про електронну аутентифікацію документів» (Electronic Authentication of Documents Act). Мета закону: створення централізованого, загальнодоступного електронного реєстру для аутентифікації електронних документів за допомогою системи відкритого та закритого ключів, спрощення процесу обміну електронними документами та іншою інформацією при укладанні комерційних угод. На відміну від поняття «електронний» або «цифровий підпис», законотворцями запропоновано визначення «електронна аутентифікація» (electronic authentication), яке трактується як «електронне підписання документа, що встановлює гарантований зв'язок між автором документа й самим документом за допомогою системи відкритого та закритого ключів».

Нововведенням можна вважати включення окремого розділу «Повноваження і обов'язки Центру електронної документації». Уперше в законодавстві запроваджується Реєстр відкритих ключів для перевірки автентичності електронних підписів, створених відповідно до стандартів, а також відкритих ключів державних установ, фізичних осіб, які мають ділові відносини з державними структурами, та інших осіб, реєстрація яких може бути здійснена за законом.

Розглядаючи Закон штату Вашингтон «Про електронне посвідчення документів» (Washington Electronic Authentication Act) [45], прийнятий 29 березня 1996 року, констатуємо таку само мету, що і в законі штату Юта. Однак законом штату Вашингтон закріплюється одночасно вся група основоположних понять, використана раніше законодавцями штатів Нью-Мексико, Каліфорнія та Юта, до яких належать: «повідомлення», «цифровий підпис», «відкритий і закритий ключі», «сертифікат», «засвідчувальний центр». Закон штату Вашингтон прирівнює електронний підпис до власноручного підпису за умови, що його справжність підтверджена за допомогою відкритого ключа, відображеного в сертифікаті. Цікавим нововведенням є положення про те, що копія електронного документа,

завірена підписом, має однакову юридичну силу з оригіналом, за винятком випадків, коли автор документа наділяє оригінал унікальною юридичною силою.

У травні 1996 року прийнято Закон штату Флорида «Про електронний підпис» («Florida Electronic Signature Act») [46]. Як і в законі штату Нью-Мексико, закон має загальну сферу застосування. Крім того, законодавці штату Флорида пропонують використовувати термін «writing» (написання) не тільки в значенні написати що-небудь на папері, а й для позначення «процесу створення електронного документа на будь-якому носії з можливістю подання його в загальноприйнятій формі», що законодавчо закріплює єдиний загальний термін для позначення і електронного, і традиційного паперового документа. У законі штату Флорида вперше були запропоновані одразу обидва визначення: «електронний підпис» і «цифровий підпис». «Електронний підпис» (electronic signature) трактується як більш широке поняття: це «будь-які літери або символи, створені електронними засобами, що дозволяють підтвердити авторство і справжність документа або спростувати їх». «Цифровий підпис» (digital signature) розуміється як «різновид електронного підпису, який перетворює повідомлення, використовуючи асиметричний криптографічний алгоритм таким чином, що одержувач повідомлення, маючи відкритий ключ, може визначити: чи було повідомлення спочатку зашифровано з використанням відповідного закритого ключа, чи було повідомлення змінено з моменту перетворення (шифрування)». Ключовим моментом закону штату Флорида є положення, відповідно до якого електронний підпис наділено рівнозначною юридичною силою з власноручним підписом і дозволено його використання для підписання документів.

17 березня 1997 року штатом Міссісіпі прийнято закон «Про цифровий підпис» (Digital Signature Act of 1997), який дозволив використання електронних підписів для підписання електронних документів у комерційній діяльності й законодавчо закріпив весь перелік основних понять попередніх

законів. Крім визначення терміна «цифровий підпис», закон пропонує і загальне визначення терміна «підпис», який розуміється як «будь-яка послідовність слів, букв, символів, імен, назв, включаючи торгові марки, створена від руки, за допомогою спеціальних пристроїв, електронних або інших засобів з наміром підтвердити справжність документа». Питання надання цифровому підпису юридичної сили вирішено традиційно: цифровий підпис, справжність якого засвідчена, може використовуватися для підписання електронного документа й буде мати однакову юридичну силу з власноручним підписом.

Практично одночасно, у квітні 1997 року, прийнято Закон штату Джорджія «Про електронний документ і електронний підпис» (Georgia Electronic Records and Signatures Act, Senate Bill № 103) [46]. Основною метою закону вважалося законодавче закріплення використання електронних документів та електронних підписів у різних галузях діяльності суспільства. Тому можна зробити висновок про те, що творці закону не обмежили сферу його застосування, а загальні визначення, зокрема й електронного підпису, не закріплюють певну технологію створення електронних документів та електронних підписів.

Цікавим рішенням є закріплення на законодавчому рівні основних напрямів політики штату для розвитку електронної комерції і заохочення ведення бізнесу за допомогою електронних засобів зв'язку. Так, усі державні установи спільно з приватними організаціями зобов'язані створювати бізнес-проекти (startup) для вивчення можливостей застосування нових інформаційних технологій (зокрема й технологій електронного підпису). Такий підхід сприяв легалізації використання електронних документів та електронних підписів, але не зобов'язував використовувати будь-яку одну технологію.

Штат Міннесота у травні 1997 року запроваджує Закон «Про електронну аутентифікацію документів» (Minnesota Electronic Authentication Act) [47]. Новизна цього нормативного акту полягає в тому, що разом із

традиційною метою спрощення процедури укладення комерційних угод за допомогою використання електронних документів декларується потреба створення спільно з іншими штатами США універсальних правил, що регулюють питання використання електронних документів. Закон штату Міннесота цікавий тим, що фактично запроваджує основи створення інфраструктури відкритих ключів (Public Key Infrastructure – PKI). Закон закладає правові основи роботи центрів, що надають послуги електронних підписів, такі як: процедура отримання ліцензії; функційні обов'язки засвідчувального центру; процедури призупинення дії, відновлення або відкликання ліцензії; відповідальність, яку несуть ліцензовані засвідчувальні центри за невиконання положень цього закону. Закон штату Міннесота більш суворо підходить до питання юридичної сили електронного підпису.

Практично одночасно із штатом Міннесота в червні 1997 року штатом Індіана прийнято Закон «Про електронний цифровий підпис» – Electronic Digital Signature Act) [47], який закріпив право державних установ використовувати цифровий підпис для укладення угод в електронній формі, за винятком Казначейства, Верховного Суду та юридичних, законодавчих і аудиторських організацій. Сфера застосування електронного підпису була обмежена державними установами. Такий підхід уже згадувався в законі штату Каліфорнія, але без позначення обмежень. Так, як і в законі штату Флорида, у ньому використовувалось одночасно два терміни: «електронний підпис» і «цифровий підпис». Однак законом штату Індіана перевагу все-таки надано саме цифровому підпису. Необхідною умовою володіння юридичною силою для цифрового підпису, приєднаного до вихідних і вхідних електронних документів державних установ, є його відповідність конкретним критеріям за законом штату Індіана.

Водночас у червні 1997 року штатом Техас прийнято Закон «Про електронний підпис» (Texas House Bill 984). Сфера застосування положень закону обмежена діяльністю державних організацій, що отримали право використання електронних документів, які вважалися підписаними й

володіли відповідною юридичною силою, за наявності як реквізиту цифрового, а не електронного підпису. Цифровий підпис використовувався для посвідчення електронних документів, які надсилаються в державні організації. Юридична ж сила цифрового підпису визначалася його відповідністю набору критеріїв, як і в законі штату Індіана.

У кінці липня 1997 року штатом Орегон прийнято Закон «Про електронний підпис» (Electronic Signature Act, 1997 Oregon House Bill) [48]. Сфера дії цього закону така, як і у розглянутого раніше закону штату Техас, вона була обмежена діяльністю державних установ при обміні електронними документами. Нововведенням можна вважати запровадження нового терміна – «key pair» (ключова пара), який складається із закритого ключа і відкритого ключа. Законом також було встановлено необхідність створення системи центрів, що засвідчують та видають сертифікати, визначено уповноважену особу, яка відповідає за реєстрацію та сертифікацію засвідчувальних центрів.

У квітні 1998 року штатом Небраска прийнято Закон «Про цифровий підпис» (Digital Signature Act, Nebraska Revised Statutes), який дозволив використання електронного підпису для засвідчення документів у різних галузях суспільної діяльності. Центральним поняттям закону є саме цифровий підпис, визначення якого достатньо уніфіковане: «цифровий підпис – це електронний ідентифікатор, який створений комп'ютером і використовується підписувачем як власноручний підпис» [49]. Таке визначення спрощує технологічний підхід до побудови інфраструктури відкритих ключів.

28 вересня 1999 року прийнято Закон штату Нью-Йорк «Про електронні документи та електронний підпис» (Electronic Signatures and Records Act, Chapter 57-A of the Consolidated Laws, State Technology Law Sections) [50].

Серед усієї сукупності розглянутих законів окремих штатів закон штату Нью-Йорк насамперед цікавий тим, що він містить визначення поняття «електронний», яке включає «цифровий, магнітний, бездротовий, оптичний,

електромагнітний і інший», а також визначення електронного підпису: «електронний ідентифікатор, що включає в себе і поняття цифрового підпису, який є унікальним для його підписувача, справжність якого може бути підтверджена і який перебуває під особистим контролем підписувача та який приєднаний до підписаних даних таким чином, що можна відстежити зміни документа, зроблені після підписання, а також передбачається, що підписувач наділяє його однаковою силою з власноручним підписом».

Закон штату Нью-Йорк уперше гарантував громадянам можливість використовувати електронні документи та електронний підпис як доказ у суді (за винятком окремих випадків) нарівні з паперовими документами.

Протягом п'яти років у Сполучених Штатах Америки активізовано законотворчу діяльність з метою впорядкування суспільних відносин, які виникали разом із розвитком інформаційних технологій, електронної комерції, структури відкритих ключів РКІ. Наслідком цієї діяльності стали численні нормативні акти у сфері електронного підпису, електронного документа та електронної комерції, що поставило проблему уніфікації правової бази та врегулювання питань термінології та окремих норм права, зокрема порядку визнання іноземних сертифікатів електронних підписів (Додаток Д). Проблема була вирішена за допомогою федеральних законодавчих актів: Модельного закону «Про електронні угоди» («Uniform Electronic Transactions Act» – UETA) [51] та Федерального закону США «Про електронні підписи в міжнародних і внутрішньодержавних торгових відносинах» («Electronic signature global and national act.» Public law 106-229-2000) [52].

Одне із принципових положень модельного закону «Про електронні угоди» є норма, згідно з якою визнання дійсності електронних угод, електронних документів, електронних підписів та їхніх сертифікатів можливі за згодою сторін, що беруть участь в обміні електронними документами. Фактично держава уникає процедур регулювання визнання електронних послуг, електронних підписів та сертифікатів і покладає це на суб'єктів-

учасників правовідносин. Слід зазначити, що цей закон дотепер не підтримали штати Вашингтон, Іллінойс та Нью-Йорк.

Відзначимо, що Федеральний закон США «Про електронні підписи в міжнародних і внутрішньодержавних торгових відносинах», прийнятий Конгресом США 24 січня 2000 року, був публічно підписаний Президентом саме за допомогою електронного підпису.

Після прийняття федерального закону електронний підпис став широко використовуватися сторонами угод. Визначення електронного підпису в законі є технологічно нейтральним і містить лише основну ідею та поняття, надаючи можливість у подальшому виборі оптимальної технології для розвитку інфраструктури електронного підпису. Федеральний закон США встановив на державному рівні рівнозначність електронного документа та електронного підпису нарівні з паперовими документами та власноручним підписом. Виняток склали лише деякі види документів: заповіти, свідоцтва про шлюб, розлучення, усиновлення та інші акти цивільного стану; документи, що містять рішення суду, протоколи; документи про нерухомість, комунальні послуги; медичні документи, наприклад, страховка й деякі інші. Питання визнання сертифікатів вирішується однаково для внутрішньодержавних і для міжнародних торгових операцій – за попередньою згодою сторін угоди та за умови, що електронні підписи відповідають вимогам законодавства.

Проведений аналіз законодавства штатів США засвідчив, що існують численні розбіжності в законодавстві, що призводять до виникнення складнощів адаптації стандартів електронних підписів та документів окремих штатів. З метою запровадження уніфікації в галузі електронного підпису в США законодавство рекомендує використовувати стандарт X.509 з мінімальними змінами та максимально використовувати механізми розширень сертифіката федерального профілю, який розроблено Національним інститутом стандартів і технологій США (The National Institute of Standards and Technology, NIST) Міністерства торгівлі США у

співпраці з Американським Національним інститутом стандартів (ANSI). Також цими установами розроблено федеральний міст сертифікації (Federal Bridge Certification Authority, FBCA), який має на меті об'єднати відомчі інфраструктури відкритих ключів (PKI) США, а також формувати сертифікати, що є дійсними для PKI одного відомства та будуть прийнятими в PKI іншого відомства за умови, що відомства укладають угоду про те, що їхні відомчі PKI зв'язуються через FBCA. Фактично FBCA забезпечує інтероперабельність електронних підписів усередині США шляхом трансляції інформації із відомчих сертифікатів у загальний сертифікат, який буде прийнятним для інших учасників сертифікації. Однак цим технічним рішенням жодним чином не вирішуються проблеми визнання в США іноземних електронних підписів та електронних довірчих послуг.

Як стверджують Don Johnson та Scott Vanstone, американські технічні стандарти в галузі електронного підпису відрізняються від європейських, однак вони цілком задовольняють вимоги для ведення електронної комерції в Сполучених Штатах Америки [53].

На прикладі зазначених законів маємо змогу простежити за досвідом США у сфері правового регулювання електронних документів та електронного цифрового підпису [54]. Американськими нормотворцями було проведено велику роботу, оскільки практично в кожному штаті були прийняті основні закони з цієї проблеми, а також різні доповнення та поправки у вигляді Правил, Інструкцій або нових версій чинних законів.

Протягом досить короткого часу переважна більшість країн світу розробила та запровадила законодавчі акти, які регулюють правовідносини під час використання електронних підписів. Однак відмінність юрисдикцій [55], технологічних підходів, технічних стандартів, а в окремих випадках і технологій взагалі створили проблему юридичного визнання іноземного електронного підпису, створеного відповідно до права іншої країни [56].

Цілком очевидно, що без порівняльного аналізу законодавства, що регулює правовідносини у сфері електронного підпису, досить складно дати

відповідь на питання, яку процедуру слід вводити для визнання іноземних електронних підписів.

На прикладі країн Латинської Америки та Мексики з урахуванням досвіду запровадження національних законів про електронний підпис та розробки інфраструктури відкритого ключа (РКІ) розглянемо, як вирішується в різних юрисдикціях проблема транскордонного визнання іноземних електронних підписів.

Слід визнати, що географічна відокремленість та національний чинник завжди впливав на формування суспільних відносин з огляду на специфіку певного регіону. Законодавство у сфері електронного підпису також не стало виключенням і має характерні особливості [57].

Так, Конгресом Колумбії у 1999 році прийнято Закон № 527 [58] про повідомлення даних, електронну комерцію та електронний підпис, яким визначається і регулюється доступ, використання і обмін електронними даними, електронна комерція, застосування електронних підписів, а також встановлюється порядок діяльності органів сертифікації. Закон вводить поняття «цифровий підпис», яке визначається як «числове значення, що додається до повідомлення математичною процедурою і пов'язане із особистим ключем підписувача, що дає можливість визначити особу підписувача та встановити відсутність змін у даних підписаного документа». Визнання іноземних сертифікатів електронного підпису, виданих іноземними органами сертифікації, здійснюються на підставах і згідно з процедурами, які застосовуються до національних органів сертифікації.

Аргентинська Республіка у 2001 році прийняла «Закон цифрового співробітництва» [58], що запроваджує одночасно поняття цифрового та електронного підпису. Цифровий підпис є результатом: застосування математичної процедури до цифрового документа за наявності інформації про особу підписувача, забезпечення абсолютного контролю з боку підписувача, процедури перевірки третіми сторонами. Електронний підпис визначається як набір інтегрованих або логічно пов'язаних із ними

електронних даних, що використовуються як підпис для їхньої ідентифікації, які не мають будь-яких юридичних вимог, аналогічних цифровому підпису. Тобто, електронний підпис може не містити даних підписувача.

Визнання іноземних електронних підписів, виданих закордонними сертифікаційними центрами, здійснюється за двома схемами. Перша: іноземні електронні підписи відповідають умовам, встановленим законом Аргентини та відповідними положеннями щодо електронних підписів, виданих національними сертифікаційними центрами в межах угоди про взаємовизнання між Аргентинською Республікою та країною походження іноземного електронного підпису. Друга: іноземні електронні підписи можуть видаватися іноземним сертифікаційним центром на підставі ліцензії, виданої уповноваженим органом державної влади Аргентинської Республіки – секретаріатом Кабінету Міністрів Республіки [60; 61].

Федеративна Республіка Бразилія також у 2001 році прийняла відповідний закон про електронні підписи під назвою «Тимчасовий захід 2.200-2, 24 серпня 2001» [62]. Закон цікавий тим, що вводить поняття «інфраструктура відкритих ключів» і одночасно оминає деталізацію визначення електронного підпису. Натомість досить деталізовано регламентує структуру, права й повноваження РКІ.

Особливість законодавства Бразилії полягає в тому, що дозволяє використовувати лише такі електронні підписи, які створені бразильською інфраструктурою відкритого ключа. Водночас законодавство залишає можливість визнання іноземних сертифікатів електронного підпису в межах двосторонньої міждержавної угоди між Бразилією та іншою країною.

Національний конгрес Республіки Чилі у 2002 році прийняв Закон «Про електронні документи, електронний підпис та послуги сертифікації» [63]. Цей законодавчий акт визначає електронний підпис як «будь-який звук, символ або електронний процес, який дозволяє одержувачу електронного документа визначити принаймні формально його автора». Закон переважно стосується взаємодії державних органів, процедури сертифікації надавачів

послуг електронного підпису, а також уперше законом затверджуються права й обов'язки підписувачів електронного підпису. Однак Закон «Про електронні документи, електронний підпис та послуги сертифікації» не порушує питання визнання іноземних електронних підписів або електронних довірчих послуг.

У 2002 році національним Конгресом Республіки Перу прийнято Закон «Про електронний підпис та сертифікати» № 27269. Закон визнає лише правовий статус електронних або вдосконалених електронних підписів, виданих у країні, та одночасно використовує поняття «електронний підпис» та «цифровий підпис». Так, під електронним підписом визначаються будь-які електронні дані, що пов'язані із документом або автентифікують автора й відповідають характеристикам власноручного підпису. Водночас у визначенні цифрового підпису вперше законодавчо закріплюється конкретна технологія криптосистем із відкритим ключем. Цифровий підпис – це підпис, що використовує техніку асиметричної криптографії на основі застосування унікальної пари ключів: приватного ключа і, відповідно, відкритого ключа, які пов'язані між собою таким чином, що користувачі, які знають відкритий, не можуть вивести з нього приватний ключ. Законодавство Перу визнає дійсність цифрових сертифікатів, виданих в інших країнах, лише якщо вони відповідають перуанським стандартам.

У 2009 році Республіка Уругвай (Уругвай) прийняла Закон «Про електронні документи та електронний підпис» [64]. Для правознавців цей закон цікавий тим, що вперше в законодавстві запроваджується поняття «Національна електронна інфраструктура сертифікації». Також уперше в законодавстві країн Латинської Америки застосовуються одночасно терміни «електронний підпис» та «удосконалений електронний підпис». Так, «електронний підпис» означає дані в електронній формі, додані до електронного документа або логічно пов'язані з ним та використовувані підписувачем як засіб ідентифікації. «Удосконалений електронний підпис» означає електронний підпис, який відповідає таким вимогам:

- а) має інформацію про дані підписувача, що дозволяє однозначно ідентифікувати;
- б) зберігається й використовується виключно під контролем підписувача;
- в) доступний для перевірки третіми сторонами;
- г) пов'язаний з електронним документом таким чином, що будь-які подальші зміни в ньому були неможливі;
- д) створений з використанням технічно безпечного та надійного пристрою для створення електронного підпису й базується на визнаному сертифікаті, дійсному під час підписування.

Визнання іноземних електронних підписів цим законом не регулюється й відбувається за принципом «за згодою сторін», що укладають угоди або контракти.

У 2012 році Мексиканськими Сполученими Штатами прийнято ряд змін до Торгового кодексу, Федерального цивільного кодексу, Федерального кодексу про Цивільні процедури одночасно із прийняттям Закону «Про електронний підпис» [65]. Законом, як і відповідним законом Уругваю, запроваджується поняття вдосконаленого електронного підпису. Удосконалений електронний підпис – це електронний підпис, який повинен відповідати принципам функційної еквівалентності, автентифікації та цілісності, які викладаються достатньо деталізовано. Також законодавчо закріплено порядок визнання іноземних електронних підписів шляхом застосування процедур укладання базових угод про співпрацю або координацію у сфері електронного підпису. Вказані процедури можуть здійснювати Секретаріат Конгресу, Міністерство економіки та Служба податкової адміністрації та інші сертифікаційні органи за умови взаємного сповіщення про укладені угоди.

1.4. Законодавство пострадянських країн та окремих країн Азії у сфері регулювання транскордонного надання електронних підписів

У Радянському Союзі перші електронні машини з'явилися на початку 50-х років минулого століття. Поступово вони розвивалися від примітивних лампових і напівпровідникових до побудованих на інтегральних мікропроцесорах. Ці апарати були призначені переважно для здійснення математичних розрахунків та опрацювання інформації, створеної за допомогою архаїчних мов програмування, а сама інформація зберігалася на паперових перфокартах, магнітних стрічках або гнучких дискетах малої ємності. Одночасно виникла потреба і юридичного оформлення електронної інформації. Поняття «електронний документ» у юридичній науці СРСР з'явилося у 1970 році як термін «машиночитаемый документ», а у 1984 році ГОСТ 6.10.4-84 затвердив визначення «машиночитаемый документ – это документ, пригодный для автоматического считывания содержащейся в нем информации».

Юридична значимість перших електронних документів закріплювалась постановою Пленуму Верховного Суду СРСР від 1 грудня 1983 року № 10 «Про застосування процесуального законодавства при розгляді цивільних справ у суді першої інстанції», яка прирівнювала доказові властивості документів, отриманих за допомогою електронно-обчислювальної техніки, до паперових. Як такого електронного цифрового підпису на той час не існувало, хоча до перших електронних документів вже застосовувались вимоги обов'язкової наявності покликань на авторів/підписантів документа та пристроїв (комп'ютерів), на яких створювалися файли. Уся юридична відповідальність за достовірність та цілісність інформації покладалася на експертні можливості науково-обчислювальних центрів, яких в СРСР була обмежена кількість. Питання міжнародного, транскордонного обміну електронними документами або електронними підписами в СРСР офіційно не порушувалось.

Із розпадом у 1991 році СРСР у новостворених незалежних державах виникла ситуація, коли у всіх сферах життєдіяльності суспільства різко збільшилась кількість персонально-обчислювальних машин (комп'ютерів) і, відповідно, зросла потреба в обміні електронними даними. Широке використання електронних документів та технологій швидкого обміну електронними даними надало поштовх розвитку нових суспільних відносин у сфері електронної комерції, електронного документообігу та електронного підпису.

На той час міжнародні інституції вже заклали фундамент правового використання електронного підпису. Протягом досить короткого часу переважна більшість країн світу розробила та запровадила законодавчі акти, які регулюють правовідносини під час використання електронних підписів та сервісів.

На нашу думку, слід звернути увагу на досить цікавий досвід розвитку правових відносин та створення норм права у сфері електронного підпису та електронних довірчих послуг з погляду формування сучасних юрисдикцій низки країн, що утворилися після розпаду СРСР. Юрисдикції пострадянських країн формувались в умовах одночасної дії законодавства СРСР та нових законів, що запроваджувалися новоствореними законодавчими органами [66].

Розглянемо законодавство Російської Федерації. У 2002 році набрав чинність Федеральний закон № 1-ФЗ «Про електронний цифровий підпис» [67]. Законом визначено дефініцію поняття «електронний цифровий підпис» як реквізит електронного документа, призначений для захисту цього ж електронного документа від підробки, отриманий у результаті криптографічного перетворення інформації із використанням закритого ключа електронного цифрового підпису з можливістю ідентифікації власника сертифіката ключа підпису, а також встановлення відсутності змін інформації в електронному документі. Тобто, електронний цифровий підпис не визнавався самотійним, а визначався як один із реквізитів електронного

документа. Отже, формально декларувався принцип визнання іноземного електронного підпису за умови, якщо він був засвідчений відповідно до законодавства іноземної держави, визнавався на території Російської Федерації в разі виконання встановлених законодавством Російської Федерації процедур визнання юридичного значення іноземних документів. Цей законодавчий акт втратив силу на підставі нового Федерального закону від 06.04.2011 р. № 63-ФЗ «Про електронний підпис» [68]. Новий закон запроваджує і нове визначення електронного підпису як інформацію в електронній формі, яка приєднується до іншої інформації в електронній формі (інформація, що підписується) або іншим чином пов'язана із такою інформацією та використовується для встановлення особи, яка підписала інформацію. Також нормативна база поповнилась термінами «простий електронний підпис», «посилений електронний підпис», «посилений некваліфікований та посилений кваліфікований електронний підпис». Стосовно іноземних електронних підписів застосовується правило, згідно з яким електронні підписи, створені відповідно до норм права іноземної країни й міжнародних стандартів, у Російській Федерації визнаються електронними підписами того виду, ознакам якого вони відповідають згідно з чинним Федеральним законом. Однак, на сьогодні офіційної процедури або ознак визнання іноземних сертифікатів у Російській Федерації не існує, а правовідносини, що виникають під час, наприклад, транскордонної електронної торгівлі, регулюються вузькопрофільними підзаконними актами окремих органів влади.

Закон Республіки Білорусь (Білорусь) «Про електронний документ і електронний цифровий підпис» від 28 грудня 2009 р № 113-З [69] є одним із надмірно зрегульованих законодавчих актів на пострадянському просторі. Закон одночасно поєднує в собі порядок регулювання електронного документообігу та порядок регулювання електронного підпису, а основні поняття мають достатньо широке трактування. Також закон закріплює багатостороннє державне регулювання сфери електронного документообігу

та електронного цифрового підпису, яке здійснюється Президентом Республіки Білорусь, Радою Міністрів Республіки, Національним банком, Оперативно-аналітичним центром при Президентові Республіки Білорусь, органами архівної справи і діловодства, державними архівними установами, іншими державними органами та організаціями. Тобто, регулювання суспільних відносин у сфері обігу електронних документів та електронного підпису забезпечується виключно імперативним методом.

Водночас порядок визнання іноземних сертифікатів електронного підпису передбачає, що іноземний сертифікат відкритого ключа, що відповідає вимогам законодавства іноземної держави, у якій цей сертифікат виданий, визнається на території Республіки Білорусь у випадках і порядку, визначених міжнародним договором Республіки Білорусь, які передбачають взаємне визнання сертифікатів відкритих ключів або інший спосіб надання юридичної сили іноземним електронним документам. Сертифікат відкритого ключа, виданий постачальником послуг іноземної держави, акредитованим у Державній системі управління відкритими ключами, визнається на території Республіки Білорусь.

На відміну від Білорусі, Закон Республіки Казахстан (Казахстан) «Про електронний документ і електронний цифровий підпис» від 7 січня 2003 року № 370-ІІ) [70] достатньо спрощений і не перевантажений регулятивними нормами. Ключові визначення сфери електронного підпису та електронного документообігу загалом за змістом тотожні Типовому закону ЮНСІТРАЛ «Про електронні підписи». Натомість у законі Казахстану приділено більше уваги проблемі визнання іноземних електронних підписів, зокрема введено статті, що окремо регулюють визнання іноземного реєстраційного свідоцтва (сертифіката) та іноземного електронного підпису шляхом запровадження третьої довірчої сторони.

Також законодавчо визначено, що при регулюванні правовідносин, які виникають між засвідчувальним центром і власником іноземного реєстраційного свідоцтва, застосовується право держави, у якому було

видано реєстраційне свідоцтво, якщо інше не встановлено угодою сторін. Крім того, встановлюється, що електронний підпис, рівнозначний власноручному підпису підписувача, має однакові юридичні права, якщо електронний підпис створений і реєстраційне свідоцтво видано акредитованим центром, що засвідчує Республіка Казахстан, або іноземним засвідчувальним центром, який зареєстрований довіреною третьою стороною Республіки Казахстан, де довірена третя сторона Республіки Казахстан – інформаційна система, що здійснює в рамках транскордонної взаємодії підтвердження справжності іноземного електронного підпису та електронного підпису, виданих на території Республіки Казахстан.

Закон визначає, що іноземний електронний підпис, який має іноземне реєстраційне свідоцтво, визнається електронним підписом на території Республіки Казахстан:

- відповідно до ратифікованих Республікою Казахстан міжнародних договорів;
- після реєстрації іноземних засвідчувальних центрів довіреною третьою стороною Республіки Казахстан;
- після реєстрації довірених третіх сторін іноземних держав довіреною третьою стороною Республіки Казахстан.

Іноземне реєстраційне свідоцтво визнається нарівні з реєстраційним свідоцтвом, виданим документом центром, що діє на території Республіки Казахстан відповідно до ратифікованих Республікою Казахстан міжнародних договорів, а також після реєстрації іноземних засвідчувальних центрів довіреною третьою стороною Республіки Казахстан та довірених третіх сторін іноземних держав довіреною третьою стороною Республіки Казахстан.

У березні 2008 року Грузією прийнято Закон № 5927-Іс «Про електронний підпис та електронний документ» [71]. Закон визначає правові основи системи електронного документообігу та використання електронного підпису. Цим актом встановлюються терміни, які за змістом практично дублюють аналогічні поняття, що вже застосовувалися законодавством країн-

членів Європейського Союзу. За цим же принципом визначено й умови визнання рівнозначності юридичної сили власноручного підпису й електронного підпису, а також умови визнання електронного підпису, виданого за кордоном.

Однак слід зазначити, що законотворчі ініціативи все ж знайшли відмінний від інших аналогічних законів спосіб визнання іноземних електронних підписів. Цей спосіб полягає в тому, що сертифікат, виданий в іноземній країні, також буде дійсним у Грузії, у разі якщо технічні регламенти цієї країни визнані постановою Уряду Грузії як національні й застосовуються в Грузії паралельно з чинними технічними регламентами. Починаючи з 2016 року, у Грузії запроваджена програма заміни паперових паспортів на електронну ID-карту із електронним підписом та біометричними даними власника. Так, ID-карта та електронний підпис передусім будуть використані під час отримання електронних послуг органів державної влади, у сфері фінансів, страхування та медицини.

У Республіці Молдова у травні 2014 року вийшов Закон «Про електронний підпис та електронні документи» [72]. Він встановлює правовий режим електронного підпису й електронного документа, включаючи окремо основні вимоги щодо їх дійсності й окремо основні вимоги до сертифікаційних послуг. Також запроваджуються три види електронних підписів: «простий електронний підпис», «посилений некваліфікований електронний підпис», «посилений кваліфікований електронний підпис», а також принципи й механізми їх використання.

За загальним правилом визнання електронного підпису й електронного документа за межами Республіки Молдова регламентується міжнародними договорами. Якщо міжнародним договором, однією зі сторін якого є Республіка Молдова, встановлюються інші норми, ніж ті, які передбачені в цьому законі, застосовуються норми міжнародного права.

Крім того, запроваджується порядок визнання іноземних електронних підписів. Так, сертифікат відкритого ключа, виданий постачальником

сертифікаційних послуг, який проживає або перебуває в іншій державі, визнається рівнозначним з погляду правових наслідків, сертифікату відкритого ключа, виданого постачальником сертифікаційних послуг, який проживає або перебуває в Республіці Молдова, якщо дотримано одну з умов:

- постачальник сертифікаційних послуг, який проживає або перебуває в іншій державі, акредитований згідно зі схемою акредитації відповідно до цього Закону;
- акредитований постачальник сертифікаційних послуг, який проживає або перебуває в республіці Молдова, гарантує визнання сертифіката;
- сертифікат або постачальник сертифікаційних послуг, що видав його, визнаються на основі взаємності відповідно до двосторонньої або багатосторонньої угоди між Республікою Молдова та іншими державами або міжнародними організаціями.

Новизна цього порядку визнання полягає в тому, що на іноземного постачальника сертифікатів електронного підпису, акредитованого в Молдові, покладається зобов'язання гарантійного характеру щодо підтвердження юридичної значимості виданого сертифіката.

Закон «Про електронні документи та електронний підпис» [73], прийнятий Республікою Вірменія (Вірменія) у квітні 2004 року, досить лаконічний. Визначення поняття «електронний підпис» аналогічне застосованому в українському законодавстві. Визнання іноземних електронних підписів здійснюється виключно в межах міждержавних угод.

Естонська, Латвійська та Литовська республіки протягом 2000 – 2002 років прийняли закони «Про цифровий підпис» [74], «Про електронні документи» [75] та «Електронний підпис» [76] відповідно. Однак, починаючи з 2004 року, зазначені країни у сфері електронного підпису та електронних довірчих послуг використовували положення Директиви 1999/93/ЄС Європейського парламенту та Ради «Про систему електронних підписів, що застосовується в межах Співтовариства». Починаючи з 2014 року, основним документом для регуляції відносин у сфері електронного підпису для

вказаних країн став Регламент (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС.

Окремо слід звернути увагу на прогрес у використанні електронного підпису Республіки Естонія. У республіці запроваджено ID-карту та digi-ID (електронний паспорт), які містять електронний підпис та використовуються як посвідчення громадянина Естонії. Електронні карти ID-карта та digi-ID дозволяють громадянину здійснювати електронне спілкування із державними органами, отримувати 12 державних електронних послуг та послуги 10 банків, подорожувати в країни-члени ЄС та Європейської економічної зони. Також через Інтернет проводити електронні вибори до органів місцевого самоврядування та парламенту шляхом електронного голосування ID-картою або електронним паспортом digi-ID. Тобто Естонія не тільки інтегрувала Регламент 910/2014, але й запровадила низку ефективних електронних довірчих послуг.

Президентом Республіки Азербайджан (Азербайджан) у травні 2004 року затверджено Закон «Про електронний підпис та електронні документи» [77]. Законом запроваджуються визначення електронного підпису та посиленого електронного підпису. Так, електронним підписом вважаються дані, додані до інших даних або логічно пов'язані з ними, що дозволяють ідентифікувати підписувача. Посиленим електронним підписом є електронний підпис, створений електронними засобами підпису, які контрольовані й належать тільки підписувачу для його ідентифікації, а також для забезпечення цілісності, стабільності, дійсності повідомлення. Відповідно до закону посилені сертифікати електронного підпису застосовуються виключно і в обов'язковому порядку державними органами та органами місцевого управління республіки. Використання електронних підписів в інших сферах регламентується локальними або корпоративними умовами за згодою підписувачів. Законом встановлюються умови, за якими

визначаються дійсними в Азербайджанській Республіці іноземні сертифікати. Так, дійсним буде сертифікат, виданий іноземним центром сертифікації, що акредитований в Азербайджанській Республіці та відповідає вимогам безпеки, встановленим законом та іншими правовими актами Азербайджанської Республіки. Окремо встановлюється вимога гарантій дійсності іноземного сертифіката, які надаються акредитованим центром в Азербайджанській Республіці або відповідним виконавчим органом державної влади. Також дійсними будуть вважатися іноземні електронні підписи, надані іноземними центрами, зазначеними в міждержавних договорах, що підтримуються Республікою Азербайджан.

Законодавство у сфері електронного підпису Республіки Туркменістан [77], Республіки Узбекистан та Республіки Таджикистан, мають єдиний підхід до ролі та місця електронного підпису. Електронний підпис розглядається виключно як складник електронного документа, чим, власне, і обмежуються можливості його використання.

Закон «Про електронний документ», прийнятий Республікою Туркменістан (Туркменістан) у грудні 2000 року, не регламентує визнання іноземних електронних підписів. Визнання електронних документів, а, відповідно, і їхніх складників, таких як електронні підписи, здійснюється виключно в межах міждержавних угод. Разом з тим Закон «Про електронний підпис», запроваджений Республікою Таджикистан, затверджує норму, згідно з якою підписувач може мати будь-яку кількість сертифікатів електронних підписів, що мають однакове або різне юридичне значення, залежно від правових можливостей власника. Визнання іноземних сертифікатів у Республіці Таджикистан здійснюється за чинним законодавством та міжнародними угодами, які визнані Таджикистаном.

Закон Республіки Узбекистан «Про електронний цифровий підпис» прийнято у грудні 2003 року. Він має типові визначення електронного підпису та декларативно регламентує основні права та обов'язки підписувачів, центрів сертифікації, органу контролю, порядок сертифікації

тощо. Використання сертифікатів ключів цифрових підписів іноземних країн здійснюється у встановленому законодавством порядку, який на сьогодні фактично відсутній.

В Україні у 2003 році Верховною Радою України прийнято Закони України «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг» [78], які стали підґрунтям для низки нормативно-правових актів, що згодом врегулювали правовідносини під час використання електронного цифрового підпису. У 2017 році на заміну Закону України «Про електронний цифровий підпис» Верховною Радою України прийнято Закон України «Про електронні довірчі послуги», який набув чинності в листопаді 2018 року. Вказаний Закон здійснює регулювання суспільних відносин, що виникають між юридичними, фізичними особами, суб'єктами владних повноважень у процесі надання, отримання електронних довірчих послуг, процедури надання цих послуг, нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також основні організаційно-правові засади електронної ідентифікації. Слід зазначити, що, на відміну від Закону України «Про електронний підпис», у Законі України «Про електронні довірчі послуги» питанню міжнародного співробітництва та визнання іноземних електронних довірчих послуг присвячено цілий розділ. Визначено, що Україна бере участь у міжнародному співробітництві у сферах електронних підписів та електронної ідентифікації на основі міжнародних договорів України та в порядку, встановленому законом. Порівняно з попереднім актом, у Законі України «Про електронні довірчі послуги» застосовано більш розширений підхід до визнання іноземних електронних підписів. Так, встановлено, що електронні довірчі послуги, які регулюють правові відносини у сфері електронних довірчих послуг в іноземних державах, визнаються в Україні електронними довірчими послугами того самого виду в разі відповідності визначеним законом умовам.

На наш погляд, досвід розробки країнами Азії законодавчих актів щодо правового функціонування інфраструктур відкритого ключа заслуговує на

окремий детальний розгляд. Країни Азії практично одночасно з країнами Західної Європи та США вжили нормотворчі заходи та створили законодавчу базу, що регулює суспільні відносини у сфері електронних документів та електронних підписів. Відразу доцільно звернути увагу на те, що нормативно-правове середовище Азії достатньо складне й через регіональні особливості значно контрастує із звичайними для нас європейськими правовими актами, що створює певні геополітичні бар'єри [79].

Першою країною цього регіону, яка ухвалила 1 жовтня 1998 року відповідний Закон «Про цифровий підпис» [80], стала Малайзія. Метою закону є законодавче закріплення поняття «цифровий підпис» і встановлення певного порядку використання цифрових підписів шляхом створення відповідної інфраструктури сертифікаційних центрів. Відповідно до закону «цифровий підпис» визначається як перетворення повідомлення з використанням асиметричного криптоалгоритму таким чином, що людина, яка має вихідне повідомлення й відкритий ключ підписувача, може точно визначити, чи було це перетворення створено з використанням відповідного закритого ключа та чи змінювалося повідомлення з моменту перетворення. Для позначення поняття «електронний документ» використано термін «message» – цифрове відтворення інформації. Також запроваджено поняття «сертифікат», що визначає документ в електронній формі, який містить: назву сертифікаційного центру, що видав сертифікат; ідентифікацію підписувача; відкритий ключ підписувача, завірений цифровим підписом сертифікаційного центру, який його видав. Слід зазначити, що частину визначень у Законі «Про цифровий підпис» імпортовано із законів про цифрові підписи деяких штатів США.

Діяльність суб'єктів сфери електронного підпису в Малайзії регулюється спеціально уповноваженою особою – Контролером, який призначається Урядом. До його обов'язків входить створення і ведення бази даних, що містить відомості про ліцензовані сертифікаційні центри, а також здійснення публікації відомостей на спеціальному сайті. Діяльність

ліцензованих сертифікаційних центрів додатково перевіряється незалежними недержавними аудиторами.

Майже одночасно із Малайзією законодавчо закріпив використання електронних документів і електронних підписів Сингапур, прийнявши 10 липня 1998 року Закон «Про електронні угоди» [81]. Цим актом Сингапур створив необхідні умови для розвитку національної електронної комерції та її виходу на міжнародний рівень. Дія закону поширюється не тільки на укладення комерційних угод, але й на використання електронних документів державними установами й органами управління. Закон вводить поняття:

«електронний підпис» – будь-які літери, числа або символи в цифровій формі, приєднані або логічно пов'язані з електронним документом, що використовує підписувач для посвідчення електронного документа;

«цифровий підпис» – електронний підпис, отриманий у результаті перетворення електронного документа з використанням асиметричної криптосистеми й хеш-функції таким чином, що людина, яка має вихідний електронний документ і відкритий ключ, може точно визначити: чи був документ перетворений за допомогою закритого ключа підписувача та чи змінювався вихідний документ з моменту вчинення перетворення.

Таким чином, закон Сингапуру запровадив одночасно два поняття: «електронний підпис» та «цифровий підпис». Електронний підпис – це базове поняття, яке визначає, що підписувач може використовувати будь-який метод створення електронного підпису, а цифровий підпис є одним із видів електронного підпису, для створення якого використовується певна технологія з закритим і відкритим ключами відповідно для створення й перевірки автентичності цифрового підпису.

Як і Малайзія, Сингапур під час розробки національного закону використав досвід створення законів про цифрові підписи деяких штатів США: Флориди, Індіани, Орегону, Вашингтону.

Процедура визнання іноземних цифрових підписів має два рішення, одним з яких є добровільне взаємне визнання цифрових підписів під час

укладання угод контрагентами, а другий полягає у визнанні Контролером закордонних цифрових підписів дійсними в законодавчому полі Сингапуру, якщо вони відповідають національним вимогам.

Закон «Про електронні угоди» привертає увагу тим, що законодавці в одному законодавчому акті поєднали загальні вимоги у сфері електронного підпису, детальні вимоги до суб'єктів електронного підпису, встановили окремі повноваження Контролера, який регулює діяльність цієї сфери та запровадили кримінальну відповідальність за певні види порушень. Так, наприклад, загальні заходи державного примусу полягають у застосуванні до правопорушників штрафів від 10 тис. до 50 тис. доларів та/або обмеження волі строком до 6 місяців.

Закон «Про електронні підписи» [82; 83] Китайської Народної Республіки (далі – КНР) прийнято на 11 засіданні Постійного комітету Десятого Національного з'їзду народних депутатів 28 серпня 2004 року, а чинності він набув 1 квітня 2005 року. Закон є складником низки законодавчих актів, які призначені для регулювання електронної комерції, електронних договорів тощо [84].

За ствердженням Minyan Wang, цим правовим актом визначено, що електронний підпис є даними в електронній формі, які містяться в повідомленні даних і додаються до них для ідентифікації особи, що підписує, чим встановлюється, що підписувач визнає зміст повідомлення. Повідомлення даних, як зазначено в цьому законі, означає інформацію, яка генерується, розсилається, приймається або зберігається електронними, оптичними, магнітними або подібними засобами [83]. Також законом запроваджується поняття надійного електронного підпису. Таким вважається електронний підпис, який відповідає таким умовам:

- дані підписувача використовуються виключно для створення його електронного підпису;
- створення електронного підпису відбувається під контролем підписувача;

- є можливість виявлення будь-яких змін в електронному підписі;
- після застосування підпису може бути виявлена будь-яка зміна змісту та форми повідомлення даних.

Сертифікатом електронного підпису вважається повідомлення даних або інші електронні записи, які можуть довести зв'язок між підписувачем і даними створення електронного підпису.

Слід зазначити, що Законом «Про електронні підписи» в КНР запроваджується процедура (послуга) перевірки/верифікації сертифікатів електронних підписів третьою стороною. Електронна перевірочна послуга повинна відповідати таким умовам:

- наявність кваліфікованого персоналу та доступних точок надання послуги верифікації;
- використання технології та обладнання, що відповідають стандартам безпеки держави;
- наявність сертифікатів (ліцензій) щодо здійснення верифікації.

Процедурою верифікації передбачено видачу сертифіката, у якому зазначаються назва електронної служби верифікації, власник сертифіката, серійний номер сертифіката, термін його дії, дані перевірки електронного підпису власника сертифіката, електронний підпис служби електронної перевірки, інші відомості, необхідні для верифікації. Електронна служба перевірки гарантує, що дані в сертифікаті електронного підпису є повними й точними протягом строку його дії, а також гарантує стороні, яка посилається на електронний підпис, можливість довести або знати дані, зазначені в сертифікаті електронного підпису, та іншу інформацію. Закон вводить відповідальність для служби електронної перевірки за надання недостовірних послуг верифікації. Також передбачається кримінальна відповідальність за підробку, копіювання або привласнення електронного підпису іншої особи.

Визнання іноземних електронних підписів здійснюється електронною службою перевірки – державним верифікаційним центром на підставі відповідних угод або принципу взаємності. Принцип взаємності полягає в

тому, що електронні підписи, видані іноземними верифікаційними центрами за межами КНР, мають однакову юридичну силу з тими, що видаються електронними службами верифікації за умови відповідності законодавству КНР.

Розглядаючи законодавство КНР, слід враховувати відомий історичний факт, пов'язаний із районом КНР Гонконг, який має статус спеціального адміністративного району й на сьогодні є одним із ключових фінансових центрів Азії та світу. Так, у 1842 році Гонконг захопило Сполучене Королівство Великої Британії та утримувало його як колонію згідно з Нанкінським договором. Починаючи з 1997 року, відповідно до спільної китайсько-британської декларації та Основного закону, Гонконгу надано широку автономію до 2047 року за формулою «Одна країна, дві системи», тому на території Гонконгу діє власне законодавство.

На відміну від Закону «Про електронні підписи» КНР, у Гонконзі діє Указ «Про електронні операції» [85], який має більш розширену структуру. Указом визначено такі поняття, як сертифікат, електронний запис (дані), цифровий підпис, електронний підпис, хеш-функція, інформаційна система тощо. Так, сертифікатом є документ, виданий сертифікаційним органом з метою забезпечення легітимності цифрового підпису, який передбачає підтвердження ідентичності або інших значущих характеристик особи, яка має певну пару ключів, а також ідентифікує орган, який видав сертифікат і особу підписувача та містить публічний ключ особи, якій він виданий. Відповідно до зазначеного нормативно-правового акту:

«електронний запис» (дані) означає запис, створений у цифровій формі інформаційною системою, який може передаватися в інформаційній системі від однієї інформаційної системи до іншої та зберігатися в інформаційній системі або в іншому середовищі;

«електронний підпис» означає будь-які літери, символи, цифри або інші символи в цифровій формі, прикріплені до електронного запису або

логічно пов'язані з ним, а також створені чи прийняті з метою автентифікації або затвердження електронного запису;

«цифровим підписом» відносно електронного запису є електронний підпис підписувача, отриманий шляхом перетворення електронного запису з використанням асиметричної криптосистеми та хеш-функції особою, яка має початковий нетрансформований електронний запис і відкритий ключ підписувача та дозволяє визначити, що генеровані перетворення здійснено за допомогою закритого ключа, який відповідає відкритому ключу підписувача та може визначити наявність або відсутність змін початкового електронного запису після генерування.

Політиками у сфері електронного підпису керує урядова уповноважена особа – Головний інформаційний директор Уряду. До його обов'язків входить забезпечення процедури сертифікації фізичних та юридичних осіб, які мають наміри здійснювати діяльність із надання послуг цифрового підпису. Головний інформаційний директор Уряду зобов'язаний здійснювати заходи перевірки, зокрема встановлювати: чи має фізична особа засудження в Гонконзі або в інших місцях за шахрайство та корупцію або не є банкрутом; що юридична особа не перебуває у стані ліквідації або банкрутства.

Указ «Про електронні операції» містить кілька достатньо цікавих рішень. Так, запроваджено норму «межа довіри», якою орган сертифікації, який видає сертифікат, може вказати обмеження довіри в сертифікаті, встановлювати різні обмеження в різних сертифікатах або в різних типах, класах або описі сертифікатів. Встановлюється адміністративна та кримінальна відповідальність за вчинення із застосуванням цифрового підпису дій, пов'язаних із шахрайством.

З приводу визнання іноземних електронних підписів та електронних довірчих послуг слід зазначити, що законодавство Гонконгу віддає перевагу користувачам самостійно обирати різні форми електронних підписів та налаштовувати їх у бізнес-процеси, засновані на формі, яка є найбільш зручною та відповідною для кожного випадку використання. Для цього

користувачі узгоджують між собою порядок ведення бізнесу електронними технологіями.

17 жовтня 2000 року Парламентом Індії прийнято Закон «Про інформаційні технології 2000 року» (також відомий як ІТА-2000 або закон № 21 від 2000 року) [86]. Цей акт є базовим законом в Індії, у сферах електронного підпису, кіберзлочинності та електронної комерції. Закон має вищу юридичну силу на всій території країни та стосується не тільки електронного підпису, але й злочинів, пов'язаних із використанням цифрової інформації, комп'ютерів, мереж та інформаційно-комунікаційних технологій безпосередньо в Індії.

У юридичній літературі вживається цікавий термін – «Long status» («довгий статут»), застосований уперше до закону штату ЮТА США «Про цифровий підпис», який не тільки визначає законний статус електронного підпису, але й комплексно вирішує цілу низку питань та проблем, пов'язаних із використанням електронних документів та електронного підпису.

На нашу думку, таке саме визначення можливо застосувати й до закону Республіки Індія, оскільки він складається із більш ніж 94 розділів, поділених на 13 глав, має 4 додатки із понад 50 правками, які внесені в різні розділи Кримінального кодексу Індії, Законів «Про докази», «Про банківські свідчення» та «Про резервний банк Індії».

Відмінність закону Індії від переважної більшості законодавчих актів інших країн полягає в тому, що він не тільки регулює використання електронних підписів, але й визначає та класифікує кіберзлочини і встановлює відповідні покарання за їх вчинення. Крім того, закон регламентує створення й функціонування «Кібер Апеляційного Суду», на який покладено обов'язки вирішення спорів та розгляд справ про злочини у сфері електронного підпису та інформаційно-комунікаційних технологій. Регулювання сфер діяльності, визначених законом, покладається на державний орган «Контролер», який має повноваження вчиняти дії

примусового характеру, за невиконання яких інші суб'єкти можуть нести кримінальне покарання.

Законом запроваджується низка техніко-юридичних понять:

«дані» – представлення інформації, знань, фактів, документів, які готуються або були підготовлені в формалізованому вигляді і призначені для обробки або обробляються зараз у комп'ютерній системі чи комп'ютерній мережі, і можуть бути збережені в будь-якій формі (включаючи комп'ютерні роздруківки, магнітні або оптичні носії, перфокарти, перфострічки) або зберігаються у внутрішній пам'яті комп'ютера;

«комп'ютер» – будь-який електронний, магнітний, оптичний або інший високошвидкісний пристрій обробки даних або система, що виконує логічні, арифметичні й функції пам'яті, здійснює маніпуляції електронними, магнітними або оптичними імпульсами і включає вхід, вихід, обробку, зберігання, комп'ютерне програмне забезпечення або засоби зв'язку, які пов'язані між собою або пов'язані з комп'ютером у комп'ютерні системи або комп'ютерні мережі;

«комп'ютерна мережа» – це з'єднання одного або більше комп'ютерів через супутникові, радіо, проводові лінії або інші засоби зв'язку, а також термінали або комплекси, що складаються з двох або більше взаємопов'язаних комп'ютерів, взаємозв'язок між якими підтримується постійно;

«інформація» – дані, текст, зображення, звук, голос, коди, комп'ютерні програми, програмне забезпечення та бази даних, або мікрофільм, або згенерований комп'ютером машинний текст.

Законом встановлено низку термінів, які застосовуються для регулювання сфери електронного підпису, а саме :

«цифровий підпис» – автентифікація будь-якого електронного запису абонентом за допомогою електронного методу або процедура за законом;

«сертифікат цифрового підпису» – цифровий сертифікат підпису, виданий відповідно до вимог закону»;

«електронна газета» – офіційна газета, опублікована в електронному вигляді;

«електронний запис» – дані, запис або згенеровані дані, зображення або звук, збережені, отримані або відправлені в електронній формі;

«підписувач» – особа, від імені якої цифровий сертифікат підписується або видається.

Процедура визнання іноземних електронних підписів полягає в тому, що будь-який іноземний сертифікаційний центр повинен пройти державну реєстрацію в Індії, інформація про це публікується в національній електронній газеті. Разом з цим в Індії широкого впровадження у бізнесі набула перехресна сертифікація.

Стосовно питань юридичної відповідальності, на відміну від переважної більшості аналогічних законодавчих актів країн, Закон Індії «Про інформаційні технології» 2000 року встановлює перелік правопорушень та злочинів у сфері інформаційних технологій і запроваджує за їх вчинення адміністративну та кримінальну відповідальність. До кримінальних проступків злочинів законом віднесено:

- підробку комп'ютерних вихідних кодів або документів;
- злом за допомогою комп'ютерної системи;
- отримання та зберігання викраденого комп'ютера або пристрою зв'язку;
- шахрайство з використанням комп'ютерного ресурсу;
- публікація приватних зображень інших людей без їхнього відома;
- акти кібертероризму;
- публікація непристойної інформації в електронному вигляді, публікація зображень, що містять статеві акти або дитячу порнографію.

Також закон класифікує правопорушення та злочини у сфері електронного підпису, такі як:

- отримання обманним шляхом та використання паролів, електронного підпису або іншої унікальної інформації, що ідентифікує іншу особу;

- введення в оману Контролера або засвідчувальний центр шляхом подачі неправдивої інформації з метою отримання ліцензії або сертифіката електронного підпису;
- намагання отримати або отримання несанкціонованого доступу до захищених систем, які визначені шляхом опублікування в офіційному віснику Контролера – електронній газеті;
- відмова в наданні уповноваженому державному органу інформації та в дешифруванні даних, які передавалися або передаються через будь-який комп'ютерний ресурс.

Крім того, у 2008 році до зазначеного закону внесено поправку, яка й досі створює юридичні колізії та суперечки серед індійських правознавців. Так, розділ 66А Закону вводить норму «публікація образливої, помилкової або загрозливої інформації», яку класифікує як відправлення будь-якою особою і будь-яким способом з комп'ютерного ресурсу будь-якої інформації, яка є надзвичайно образливою або має загрозливий характер, або є недостовірною і має за мету викликати образу або наругу.

Законом «Про інформаційні технології 2000 року» встановлено достатньо вагомі покарання за вказані вище злочини. Заходи державного примусу можуть полягати в обмеженні волі від трьох до десяти років та штрафу від 200 тисяч до 1 млн рупій. Злочини, які кваліфікуються як кібертероризм, караються довічним позбавленням волі.

У Японії Закон «Про електронний підпис і сертифікації підприємств» [87] (закон № 102) набув чинності 1 квітня 2001 року. Цей закон включає визначення тільки двох термінів – «електронний підпис» та «засвідчення справжності», а також у ньому вказується, що організації, які підлягають конкретному виду сертифікації, потребують акредитації в компетентних міністерствах – Міністерстві з адміністративних справ і комунікацій, Міністерстві юстиції та Міністерстві економіки, торгівлі і промисловості.

У Японії з квітня 2001 року створено та функціонує Державна інфраструктура відкритих ключів. Визнання іноземних електронних підписів

регулюється окремим розділом Закону «Про електронний підпис і сертифікації підприємств», яким передбачено можливість реєстрації іноземного сертифікаційного центру в Державній інфраструктурі відкритих ключів, а також здійснення процедур визнання в межах міждержавних угод.

Суспільні відносини у сфері електронного підпису в Республіці Корея регулюються Законами: «Актом про цифровий підпис» [88] від 5 лютого 1999 року та «Рамковим Актом на електронні документи та угоди» [89] від 1 червня 2012 року. Зазначені Закони запроваджують такі терміни:

- «електронне повідомлення» – частина інформації, яку згенеровано й відправлено і яка приймається або зберігається в цифровому вигляді системою обробки інформації;

- «цифровий підпис» – частина інформації в цифровій формі, прикріплена або логічно об'єднана з електронним повідомленням, яка може ідентифікувати підписувача й надає можливість перевірки того, що електронне повідомлення було підписано цим підписувачем;

- «сертифікований цифровий підпис» – цифровий підпис, який заснований на авторизованому сертифікаті й відповідає таким вимогам: ключ для створення цифрового підпису повинен зберігатися й бути відомим тільки підписувачу; підписувач повинен особисто контролювати створення цифрового підпису та використовувати ключ на момент підписання; можливість встановлення фактів змін у відповідному цифровому підписі з моменту його прикріплення, а також встановлення змін в електронному повідомленні, підписаному цифровим підписом;

- «сертифікат» – комп'ютерний запис, яким встановлюється й перевіряється те, що створений ключ цифрового підпису зберігається і відомий тільки абоненту;

- «підписувач» – особа, яка має власний цифровий підпис та створює ключ і підпис від свого імені або від імені іншої особи.

Досить рідкісним є поняття «інформація про людину». Інформація про людину означає частину інформації, яка стосується живої людини і яка є

такими знаками, буквами, голосом, звуком, зображенням, фізичними характеристиками і т. п., які можуть служити для встановлення особи, яка асоціюється із документами, що посвідчують особу, реєстраційним номером резидента, страховим полісом тощо.

Регуляцію у сфері електронного підпису та електронного документообігу здійснює уряд Республіки Корея в особі міністра державного управління та безпеки. Серед інших регуляторних функцій на міністра покладено обов'язки забезпечення досягнення внутрішньої інтероперабельності систем і технологій електронного підпису шляхом вивчення та дослідження вітчизняних та зарубіжних стандартів для взаємного визнання та використання різноманітних електронних підписів, а також встановлення та адаптації електронного підпису для взаємного визнання.

Слід наголосити, що, на відміну від зазначених вище нормативних актів, Закон «Акт про цифровий підпис» має спеціальну статтю 27-2 «Взаємне визнання». У законі вказано, що уряд може укласти угоду з урядом іншої країни щодо взаємного визнання електронних підписів. Законом передбачено, що в разі укладання міждержавної угоди уряд може сформувати й видати іноземному сертифікаційному центру ліцензію та уповноважений сертифікат, які юридично легалізують обмін та визнання електронних підписів між державами.

В «Акті про цифровий підпис» також визначено низку правопорушень у сфері електронного підпису, за які встановлено покарання іншими нормативно-правовими актами.

Доцільно звернути увагу на те, що «Рамковим Актом на електронні документи та угоди» Республіки Корея запроваджено систему довірчих органів, на які покладено функції третьої довірчої сторони, що забезпечує і гарантує цілісність та надійність електронних угод та електронних документів, посвідчених електронними підписами, а також їх зберігання та надання для використання в судових спорах.

Дослідження показало, що загалом законодавчі акти країн Азії спрямовані на технології та правові рішення за територіальним принципом. Водночас у цих країнах функціують так звані наддержавні технології, які стимулюють людей використовувати певні інформаційні продукти транснаціональних корпорацій. Так, Китай, Гонконг, Індія, Малайзія та Японія мають центри сертифікації та постачання електронних довірчих послуг у межах програми «Затверджений список довірених сертифікатів Adobe (AATL)», за допомогою якої користувачі продуктами компанії «Adobe Systems» (Adobe Acrobat Reader DC, Acrobat DC або Adobe Sign) можуть додавати електронний підпис до документів в Adobe Document Cloud за допомогою довірених цифрових ідентифікаторів.

Зважаючи на викладене, можна констатувати, що законодавство країн колишнього СРСР у сфері електронного підпису на сьогодні не має однозначного вирішення проблеми визначення такого статусу іноземного електронного підпису та електронної довірчої послуги, який одночасно відповідає вимогам національного законодавства й водночас має юридичну силу в міжнародному, транскордонному режимі. Нормативні акти більшості вказаних країн не використовують терміни «транскордонність» або «електронні довірчі послуги», що створює проблеми взаємного визнання вказаних послуг у транскордонному режимі між країнами світу.

При створенні електронного підпису використовуються різноманітні технології, що вимагає вирішення питання запровадження технічних і правових критеріїв, відповідність яким у подальшому дасть змогу стандартизувати правові механізми транскордонного надання електронного підпису та електронних довірчих послуг.

Узагальнюючи нормотворчу діяльність окремих країн Азії у сфері цифрового підпису та електронних довірчих послуг, можемо зазначити таке.

Практично всі розглянуті нормативно-правові акти країн закріпили поняття «електронний підпис», «цифровий підпис», «сертифікат», «підписувач» та інші. Для їхнього створення використано аналогічні норми

Типового закону ЮНСІТРАЛ «Про електронні підписи» та закони деяких штатів США. Крім того, законодавчі акти країн Азії чітко визначають права, обов'язки й відповідальність усіх суб'єктів правовідносин у цій сфері. На відміну від українського законодавства, права державних органів, які здійснюють регулювання у сфері цифрового підпису, посилені можливостями та правом застосування суворих санкцій та оперативного втручання в діяльність суб'єктів у разі загрози національним інтересам.

Законодавство країн Азії у сфері електронних довірчих послуг має суттєві відмінності від «Регламенту (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС» та Закону України «Про електронні довірчі послуги». Водночас у країнах Азії активно розвиваються електронна комерція, електронні послуги, електронна логістика та електронний документообіг, які використовують електронний підпис, що формується за національними вимогами.

На відміну від переважної більшості законодавчих актів у цій сфері, які розроблені країнами Європи, Латинської Америки, США та України, закони країн Азії мають розділи, що визначають види правопорушень та встановлюють конкретні покарання.

Цікавим із наукового погляду є Закон Індії 2000 року «Про інформаційні технології» в частині розділів, присвячених функціюванню «Апеляційного Суду Кібер», переліку правопорушень та злочинів у сфері інформаційних технологій і запровадженню адміністративної та кримінальної відповідальності. На нашу думку, такий підхід позитивно впливає на правову дисципліну в суспільних відносинах під час застосування електронних підписів, покращує інформаційну гігієну та підвищує довіру до електронної комерції і цифрових сервісів.

Висновки до розділу 1

1. У сучасному світі функціують три найбільш відомі міжнародні центри розробки, впровадження та регулювання правових питань у сфері застосування електронних підписів та електронних довірчих послуг у транскордонному режимі: ЮНСИТРАЛ, Європейський Союз та Міжпарламентська асамблея держав – учасників Союзу Незалежних Держав. Ці організації протягом 1996 – 2016 років підготували та прийняли низку модельних законів, директив та регламентів. Європейський Союз наполегливо й поступово здійснює покращення чинного законодавства з метою впорядкування та приведення національних нормативних документів до єдиного типового формату із урахуванням особливостей національних юрисдикцій. У країнах – членах ЄС формуються тестові переліки національних та транскордонних електронних довірчих послуг та електронних підписів, що генеруються органами державної влади та місцевого самоврядування й користуються попитом, довірою і популярністю у населення.

Модельні закони, директиви, регламенти, нормативно-правові акти використовують значну кількість термінів щодо транскордонності, зміст яких не визначено, однак ці терміни мають суттєве значення для створення в подальшому нормативно-правових актів національних законодавств у галузі електронного підпису та довірчих послуг. Відсутність унормованості понять «транскордонність» та «транскордонні довірчі послуги» сьогодні створює проблеми взаємного визнання вказаних послуг між країнами світу.

2. Аналіз концептуальних підходів до принципів визнання іноземних електронних підписів та електронних довірчих послуг, законодавчого досвіду найбільш відомих міжнародних центрів розробки, впровадження та регулювання правових питань у сфері застосування електронних підписів та їхніх сертифікатів: Комісії ООН з міжнародного торговельного права, Міжнародної торгової палати і Європейської економічної комісії

(UNCITRAL), Європейського Союзу, Міжпарламентської Асамблеї держав – учасниць СНД та Асоціації держав Південно-Східної Азії (ASEAN) свідчить про невирішеність проблем транскордонного режиму електронного підпису та електронних довірчих послуг.

Вивчення законотворчого досвіду міждержавних утворень Європейського Союзу та Співдружності Незалежних Держав, які сформували практичні нормативно-правові акти: «Регламент (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС», Модельний закон «Про електронний цифровий підпис» (№ 16-10 від 09.12.2000) та Модельний закон «Про транскордонний інформаційний обмін електронними документами» (№ 45-12 від 25.11.2016) Міжпарламентської Асамблеї держав – учасниць СНД вказує на розвиток нормативної бази з метою врегулювання проблемних питань транскордонного застосування електронного підпису та електронних довірчих послуг.

Досвід країн – учасниць Асоціації держав Південно-Східної Азії (ASEAN) та Японії в напрямі взаємовизнання електронних підписів та довірчих послуг вказує на широке застосування електронних довірчих послуг та електронних підписів у країнах ASEAN.

3. За результатами аналізу нормативно-правових актів визначено, що міжнародні нормативні акти використовують значну кількість термінів щодо транскордонності, зміст яких не визначено, однак ці терміни мають суттєве значення для створення в подальшому нормативно-правових актів національних законодавств у галузі електронного підпису та довірчих послуг. Відсутність унормованих понять «транскордонність» та «транскордонні довірчі послуги» створює проблеми взаємного визнання вказаних послуг у транскордонному режимі між країнами світу. Також виокремлено ключові проблеми, що перешкоджають взаємному транскордонному визнанню електронних підписів: використання різноманітних технологій, різних

технічних і правових критеріїв; відсутність можливості стандартизувати правові механізми транскордонного використання електронного підпису та електронних довірчих послуг.

Відсутність консолідованого підходу до єдиного тлумачення в міжнародному правому полі ключових термінів «транскордонність», «юридичне визнання», «транскордонне визнання цифрового підпису», «транскордонні електронні довірчі послуги», а також відсутність однозначного визначення електронного підпису та електронної довірчої послуги, які би одночасно могли відповідати вимогам національного законодавства й водночас мати юридичну силу в міжнародному, транскордонному режимі негативно впливає на розв'язання проблеми їхнього транскордонного визнання.

4. Існує достатньо національних та регіональних концепцій та ініціатив у сфері електронних довірчих послуг, які вже досить добре опрацьовані й можуть бути базою при розробці належних правових рішень на міжнародному рівні, які можна перенести в чинні правові системи. Нормативно-правова база міжнародних організацій поступово збагачувалася нормами, які з часом змінювали форму та зміст від узагальнених визначень до чітких і конкретних формулювань. Водночас такі проблеми, як визнання за електронними документами юридичної сили, визнання іноземних електронних підписів, довірчих послуг та їхніх сертифікатів, залишаються такими, що припускають їх різне тлумачення в різних юрисдикціях.

5. Узагальнюючи законодавчий досвід США, який регулює використання електронних підписів, можна констатувати таке. Законодавча база США, яка регулює використання електронного підпису, створювалася поступово із застосуванням підходу «від часткового до загального», тобто, від створення законопроектів і прийняття законів в окремих штатах до створення Федерального закону. Також законодавцями США була зроблена спроба використання протилежного підходу – «від загального до конкретного» – шляхом розробки модельного закону «Про електронні угоди»

(UETA) для подальшого створення в усіх штатах локальних законів його основи. Ця спроба виявилася вдалою, і вже до червня 2002 року в 39 штатах були прийняті закони «Про електронні угоди», що регулюють питання використання електронних документів та електронних підписів у певній сфері діяльності – електронній комерції.

Стосовно визнання іноземних електронних підписів, сертифікатів електронних підписів, електронних довірчих послуг слід зазначити, що ці проблемні питання законодавством США не вирішуються окремо або детально – відсутні визначення транскордонності, електронних довірчих послуг та їхній перелік, а також порядок або процедури визнання іноземних електронних підписів та їхніх сертифікатів під час транскордонних відносин, зокрема електронної комерції. Законодавство США не передбачає інших процедур визнання іноземних сертифікатів, ніж за попередньою згодою сторін – учасників угод та за умови, що електронні підписи створені й відповідають вимогам законодавства. Таким чином, при забезпеченні процедур взаємного визнання електронного підпису та електронних довірчих послуг між США та Україною законотворцям необхідно розробити та стандартизувати правові механізми транскордонного використання електронного підпису та електронних довірчих послуг з урахуванням особливостей різних технічних рішень та відмінностей юрисдикцій.

6. Законодавство країн Латинської Америки та Мексики по-різному формує підходи до унормування суспільних відносин у сфері електронного підпису та вирішення проблеми транскордонного визнання іноземних електронних підписів. Запроваджені законодавчі акти відрізняються базовими дефініціями електронного або цифрового підпису та нормами, за якими можливо визнати іноземний електронний підпис. Переважно застосовується підхід на основі Типового закону ЮНСІТРАЛ «Про електронні підписи» шляхом укладання міждержавних угод. Однак, такі країни, як Бразилія та Перу, застосували практику нормативного геоблокування – визнання іноземних електронних підписів можливе лише за

умови виключного використання іноземними сертифікаційними центрами національних стандартів та вимог РКІ, що обмежує споживацькі можливості отримувати закордонні електронні довірчі послуги в транскордонному режимі.

7. Законодавство пострадянських країн у сфері електронного підпису можна поділити на чотири групи. До першої доцільно віднести законодавство Естонії, Латвії, Литви та частково законодавство України. Прибалтійські країни протягом 2000 – 2003 років розробили власні закони, але після приєднання до Європейського Союзу переорієнтували національне право на використання нормативно-правових актів ЄС. При цьому Естонія досягла суттєвого прогресу у створенні власних електронних довірчих послуг, окремі з яких доступні в транскордонному режимі в межах Європейського Союзу. В Україні в листопаді 2018 року набирає чинності новий Закон «Про електронні довірчі послуги», переважно адаптований до Регламенту 910/2014. Однак, незважаючи на достатньо деталізований технічний підхід до визнання іноземних сертифікатів, Україна на сьогодні не має відповідних чітких правових процедур їхнього визнання.

Другу групу складають Азербайджан, Білорусь та Молдова. Законодавство цих країн передбачає процедуру визнання іноземних сертифікатів електронного підпису шляхом акредитації іноземного центру сертифікації в національному сертифікаційному центрі. Водночас законодавчі акти не передбачають застосування національних та транскордонних електронних довірчих послуг.

До третьої групи увійшли Вірменія, Туркменістан, Таджикистан, Узбекистан, Росія. Зазначені країни використовують єдину законодавчу процедуру визнання іноземних сертифікатів електронного підпису – шляхом укладання відповідних міждержавних угод.

До останньої групи слід віднести законодавство Казахстану та Грузії. Казахстаном законодавчо реалізовано процедуру визнання іноземних сертифікатів електронного підпису через застосування третьої довіреної

сторони, на яку саме і покладено обов'язки запровадження необхідних технічних та юридичних процедур визнання. На відміну від інших країн, Грузія використовує алгоритм, за яким визнає іноземні регламенти як національні у сфері електронного підпису, що дає правові підстави визнавати й іноземні сертифікати електронних підписів та довірчих послуг.

8. На сьогодні існує проблема визначення такого статусу електронного підпису та електронної довірчої послуги, які би одночасно відповідали вимогам національного законодавства й мали юридичну силу в міжнародному, транскордонному режимі. Потребують вирішення питання створення технічних і правових критеріїв, відповідність яким стандартизувала би правові механізми транскордонного використання електронного підпису та електронних довірчих послуг.

РОЗДІЛ 2.

ПРАВОВЕ РЕГУЛЮВАННЯ СФЕРИ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ В УКРАЇНІ

2.1 Загальний стан сфери електронних довірчих послуг та електронного підпису в Україні

Основою прогресу людства є ефективність економічного й соціального розвитку. Сучасні національні й міжнародні суспільні відносини, зокрема в економіці, управлінні державою, освіті, охороні здоров'я, культурі тощо, пов'язані з використанням інформації та базуються на надзвичайно широкому застосуванні інформаційно-комунікаційних технологій, зокрема технологій Інтернету речей, електронної комерції, електронного банкінгу, електронного документообігу та ін.

Зазначені суспільні відносини поділяються на багато сфер, які регулюються правом або підлягають такому регулюванню. Одна з таких сфер – це суспільні відносини, що виникають під час інформаційних процесів створення, використання, розповсюдження і споживання електронних довірчих послуг та електронних підписів.

Об'єктами права у сфері електронних довірчих послуг та електронних підписів можуть виступати матеріальні та духовні блага, послуги виробничого й невиробничого характеру та особисті немайнові блага, а саме: електронні підписи та їхні сертифікати, засоби генерації та носії електронних підписів, автоматизовані інформаційні системи й банки даних, телекомунікаційні мережі та засоби зв'язку, комп'ютерні програми, електронні угоди та електронні довірчі послуги, а також права та свободи людини, які забезпечуються за допомогою інформаційних технологій.

До суб'єктів правовідносин у сфері електронного підпису та електронних довірчих послуг можна винести:

- а) підписувачів – фізичних осіб, які створюють електронний підпис;
- б) користувачів – фізичних або юридичних осіб, які використовують електронні підписи і/та споживають електронні довірчі послуги;
- в) постачальників/надавачів – фізичних або юридичних осіб, які надають електронні довірчі послуги та послуги електронного підпису;
- г) державні органи – держава, центральні або місцеві органи влади, установи публічного права та об'єднання, посадові або приватні особи, уповноважені державою на виконання організаційно-розпорядчих чи адміністративно-господарських обов'язків.

Правовідносини у сфері електронних довірчих послуг та електронного підпису регулюються нормами міжнародного та національних законодавств, що забезпечує загалом широкий спектр юридичних прав та обов'язків суб'єктів правовідносин, однак існує багато напрямів правовідносин, які фактично здійснюються суб'єктами, але неврегульовані або недостатньо врегульовані нормами права. Одним із таких напрямів є неврегульованість процедур та процесів транскордонного визнання електронних підписів та електронних довірчих послуг. Саме суспільні відносини, що виникають під час цих процедур та процесів, підлягають правовому регулюванню в Україні.

На національному рівні регуляція забезпечується законодавством, яке створювалося на основі міжнародних Типових законодавчих актів із урахуванням особливостей національних юрисдикцій. Так, підписувачі створюють електронні підписи й використовують їх для укладання угод, отримання електронних сервісів і електронних довірчих послуг. Електронні сервіси та електронні довірчі послуги розробляють і запроваджують постачальники/надавачі та державні органи й надають їх користувачам. Для забезпечення процедур та процесів транскордонного визнання підписувачі та користувачі іноземних електронних підписів та електронних довірчих послуг застосовують механізми використання іноземних електронних підписів та

електронних довірчих послуг на принципах «за умови згоди сторін» та визнання за міждержавними угодами або міждержавними спеціалізованими актами.

Сфера електронного підпису та електронних довірчих послуг розвивається й функціює одночасно з розвитком інформаційно-комунікаційних технологій (ІКТ). Розвиток останніх здійснюється значно швидше, ніж модернізація чинного законодавства в цій сфері. Багато процесів, спрямованих на запровадження єдиного цифрового ринку, не мають належного правового підґрунтя для взаємного транскордонного визнання ключових компонентів, таких як електронна ідентифікація, електронні документи, електронні підписи та електронні довірчі послуги, а також для врегулювання їхнього технічного сумісництва.

Загалом відсутність загальної основи для безпечної електронної взаємодії між підприємствами, громадянами й державними органами викликає недовіру державних і приватних онлайн-послуг, електронного бізнесу та електронної торгівлі, тим самим суттєво зменшуючи їхню ефективність та попит.

Протягом останніх років здійснюється революційна цифровізація українського суспільства. Саме цифровізація суспільних відносин та економіки визначатиме конкурентні позиції держав у подальші роки, оскільки цифрова революція відбувається швидшими темпами, ніж колись індустріальні революції.

Характерна ознака цифровізації – запровадження для громадян державних органів та органів місцевого самоврядування цифрових послуг. Цифрові петиції, е-судочинство, цифровий документообіг, е-посвідчення особистості, е-послуги сфери комунального господарства, соціального захисту населення, здоров'я, транспорту, фінансів та інших сфер діяльності держави створюються швидкими темпами. Також зростає потреба в цифровій комерції та електронних послугах, які надаються іншими державами в транскордонному режимі. Крім електронного підпису, запроваджуються

сучасні сервіси цифрової ідентифікації, такі як BankID та MobileID. Одночасно зростає необхідність у надійній ідентифікації фізичних та юридичних осіб під час створення, надання, отримання та користування електронними послугами та сервісами всіх видів.

Однак, на сьогодні поряд із обов'язковим виконанням законодавчо встановлених норм ще залишається проблемним питання використання ключів електронного підпису при взаємодії держави з фізичними та юридичними особами. Відсутність єдиних уніфікованих стандартів процесу подання, оброблення, використання та зберігання даних, поданих із застосуванням електронного підпису, за ствердженням О.С. Петрова, є проблематичним при організації електронного документообігу між фізичними та юридичними особами та державними органами [90].

В Україні створена й функціонує автономна, вертикально інтегрована система правовідносин, що регулює суспільні відносини, які виникають між фізичними, юридичними особами та державою під час створення, отримання, використання, зберігання та знищення електронних підписів та електронних довірчих послуг. Суспільні відносини у сфері електронного підпису мають чітку ієрархічну структуру, на вершині якої стоїть Закон України «Про електронні довірчі послуги». Закон визначає державні органи, що мають права регуляції в цій сфері та обов'язки, які закріплюються низкою нормативно-правових актів, від Постанов Кабінету Міністрів України до відомчих наказів та розпоряджень. Своєю чергою, за вимогами нормативно-правових актів створено Центральний засвідчувальний орган та центри сертифікації електронного підпису, які взаємодіють із фізичними та юридичними особами в процесі створення, блокування, скасування та зберігання цифрових підписів та їхніх сертифікатів. Фізичні і юридичні особи використовують електронні підписи у процесі взаємовідносин у системах електронного документообігу, фінансовій, господарській та інших видах діяльності. Забезпечення правового статусу цих взаємовідносин

керуються відповідними кодексами, законами та іншими нормативно-правовими актами [91].

Використання іноземних довірчих послуг та визнання іноземних електронних підписів в Україні реалізується виключно в комерційній сфері за згодою й на умовах сторін, учасників комерційних угод. Правове регулювання відносин, пов'язаних із визнанням в Україні іноземних електронних підписів та електронних довірчих послуг, законодавством регулюється формально.

У 2005 році ЦЗО вручив перше в Україні свідоцтво про акредитацію Центру сертифікації ключів ЕЦП виробничій фірмі «Українські національні інформаційні системи». З цього часу в Україні діє 24 акредитованих та 8 зареєстрованих центри сертифікації ключів, з яких Засвідчувальний та Акредитований центри Національного Банку України, 12 державних, 14 приватних акредитованих та зареєстрованих центрів. Слід зауважити, що тривалий час електронний підпис не мав широкого застосування через монополізацію ринку та відсутність технологічної інтероперабельності. Однак після прийняття нового закону виникли сприятливі умови для технічного розвитку галузі, що надало можливості для розширення категорії користувачів (підписувачів) електронного підпису.

Також суттєво змінилися і категорії користувачів (підписувачів) електронного підпису від виключно нотаріусів, держслужбовців окремих категорій до підприємців, фізичних осіб, суддів, працівників Центрів надання адміністративних послуг, студентів, арбітражних керівників, військовослужбовців та працівників правоохоронних органів, лікарів, адвокатів та інших [92].

Набули розвитку не тільки технології електронного підпису. Сьогодні в межах реалізації Комплексної програми розвитку фінансового сектору України до 2020 року Національний банк затвердив порядок функціонування Єдиної національної системи електронної дистанційної ідентифікації фізичних і юридичних осіб BankID [93]. Цей Порядок спрямований на

розвиток електронного врядування в Україні. За останніми даними, громадянам України видано понад 3 млн ID-Card, зокрема із електронним підписом, що закріплює біометричні та персональні дані.

Також в Україні впроваджено новий електронний сервіс Mobile ID від операторів мобільного зв'язку Kyivstar, Vodafone та Lifecell, який дозволяє здійснювати електронну ідентифікацію користувача для доступу до державних електронних послуг шляхом використання електронного підпису абонента, що записується на SIM-карту.

Застосування ІКТ суттєво розширило спектр електронних послуг. Так, органами державної влади забезпечуються 145 онлайн електронних адміністративних послуг, які надаються за допомогою та з використанням електронного підпису. З них 86% доступно на власних порталах ЦОВВ, а 70% надано через електронні кабінети органів влади виключно за наявності електронного підпису. Більшість проєктів – волонтерські, вони суттєво різняться між собою за багатьма параметрами, починаючи від інтерфейсу й закінчуючи алгоритмами програмування. Крім того, понад 50% не відповідають очікуванням громадян, оскільки є лише фактично цифровою заявкою громадянина на отримання послуги або електронним записом до черги, а всі процеси надання послуги органом державної влади так і залишаються в паперовому вигляді і є бюрократичними.

Ці недоліки й корінні властивості інформаційно-комунікаційних технологій створюють атмосферу недовіри між суб'єктами суспільних відносин. Відсутність довіри, зокрема, через високу вірогідність наявності правової невизначеності робить споживачів, бізнес і органи державної влади уразливими в частині достовірності результатів здійснення суспільних відносин із застосуванням інформаційно-комунікаційних технологій, що є суттєвим бар'єром на шляху підвищення ефективності економічного й соціального розвитку людства.

Тривалий час Україна застосовувала геополітичне блокування відносно відомих алгоритмів шифрування у сфері електронного підпису. Це певним

чином було пов'язано із недостатнім розвитком наукових технологій, відсутністю достатньо міцної наукової бази України в галузі криптозахисту та технологій комплексної системи захисту інформації в Україні. Відображаючи точку зору та позицію державного регулятора у сфері цифрового підпису, О.В. Корнейко зауважує, що відомі алгоритми, які застосовуються в багатьох державних закладах, наприклад, США, включаючи ЦРУ, НАСА, міжнародних корпораціях Boeing, Shell Oil, DuPont, Raytheon, Citicorp, у міжнародній банківській системі інформації та платежів S.W.I.F.T., тривалий час в Україні штучно обмежувались у застосуванні [94]. Саме цей чинник донедавна стримував актуалізацію питання трансграничності електронних підписів та електронних довірчих послуг. Однак, незважаючи на значну лібералізацію іноземних нормативно-правових актів у цьому напрямі, значного прогресу в процедурах визнання іноземних електронних підписів не відбулося.

Також слід зазначити, що українське законодавство достатньо послаблене в напрямі встановлення відповідальності за правопорушення у сфері електронного підпису та електронних довірчих послуг. Цей чинник значно впливає на суспільні відносини й суттєво знижує довіру суспільства до криптотехнологій. На думку І.В. Гавловського, необхідно впорядкувати адміністративно-правові відносини у сфері електронного підпису, що позитивно вплине на правову гігієну в цій галузі [95].

2.2. Електронні довірчі послуги в Україні

Зважаючи на вказані вище проблеми, Європейським Союзом розроблено та прийнято пропозицію, а згодом і «Регламент (ЄС) № /2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС» [96] (далі – Регламент). Наразі він є базовим нормативно-правовим документом, який створено як регуляторний акт, що впорядковує суспільні відносини, які розвиваються паралельно вдосконаленню інфраструктури відкритого ключа ЄС.

Регламент має за мету встановити правила електронної ідентифікації та електронних довірчих послуг для електронних операцій з метою забезпечення належного функціонування внутрішнього ринку ЄС. Він також визначає та встановлює умови, за яких держави – члени ЄС повинні визнавати і приймати засоби електронної ідентифікації фізичних та юридичних осіб, які підпадають під повідомлені схеми електронної ідентифікації іншої держави-члена. Регламент по суті встановлює законодавчу базу щодо електронних довірчих послуг та гарантує, що довірчі послуги та продукти, які відповідають йому, можуть вільно циркулювати виключно на внутрішньому ринку Європейського Союзу [97].

Регламент не поширюється на надання електронних довірчих послуг, які базуються на добровільних угодах у рамках приватного права суб'єктів. Також він не поширюється на аспекти та сутності, які пов'язані з укладанням і дійсністю договорів або інших правових зобов'язань, де є вимоги до форми, встановлені національним або союзним законом. Основним принципом внутрішнього ринку в ЄС є те, що не має бути ніяких обмежень на надання довірчих послуг провайдерами на території держави-члена розташованих в інших державах-членах з причин, які належать до галузей, що охоплені Регламентом. При цьому продукти, які відповідають Регламенту, повинні вільно циркулювати на внутрішньому ринку ЄС.

На відміну від раніше виданих Директив та інших нормативно-правових актів Європейського Союзу, Регламент кардинально насичений новою термінологією, визначеннями та поняттями, вимогами та рекомендаціями відносно надання електронних довірчих послуг.

Уперше в законодавстві запроваджуються терміни для електронної ідентифікації та автентифікації: «електронна ідентифікація», «засіб електронної ідентифікації», «схема електронної ідентифікації», «автентифікація». Фактично процедури юридичного розпізнавання та встановлення особи отримали офіційне визначення, що позитивно вплинуло на формування понять, які формують правову основу електронних довірчих послуг.

У попередніх нормативних актах електронний підпис мав однозначне і стає визначення, натомість Регламент суттєво розширює коло визначень, запроваджуючи нові терміни «підписувач», «вдосконалений електронний підпис», «кваліфікований електронний підпис», «кваліфікований сертифікат електронного підпису» тощо.

Одним із прогресивних аспектів Регламенту стали вперше запроваджені в законодавстві визначення електронних довірчих послуг: «довірча послуга» – це будь-яка електронна послуга, що стосується вироблення, перевірки, підтвердження правильності, обробки та зберігання електронних підписів, електронних печаток, електронних міток часу, електронних документів, послуг електронної доставки, підтвердження справжності сайту та електронних сертифікатів, включаючи сертифікати електронного підпису та електронних печаток». Фактично Регламентом створений сучасний глосарій довірчих послуг: «довірча послуга», «кваліфікована довірча послуга», «провайдер довірчих послуг», «провайдер кваліфікованих довірчих послуг», «кваліфікована електронна печатка», «кваліфікований сертифікат електронної печатки» тощо.

Уперше в міждержавному документі запроваджується обов'язковий механізм «довірчих списків», «нотифікації» та «знаку довіри ЄС для

кваліфікованих довірчих послуг», які повинні забезпечити надійність довірчих послуг у простий та надійний спосіб по всій території Європейського Союзу.

Разом з тим, на нашу думку, окремо слід виділити такий момент. Регламент містить значну кількість термінів, зміст яких не визначено, однак вони мають суттєве значення для створення в подальшому нормативно-правових актів національних законодавств у галузі електронного підпису та довірчих послуг. Так, Регламент уживає такі поняття: «транскордонні цифрові послуги», «транскордонне використання онлайн-послуг», «транскордонне визнання ключових компонентів», «транскордонна сумісність електронних підписів», «транскордонна діяльність», «транскордонна система охорони здоров'я», «транскордонний доступ до електронних даних», «транскордонне використання засобів електронної ідентифікації», «транскордонне взаємне визнання засобів електронної ідентифікації», «загальна система транскордонного використання довірчих послуг», «транскордонне визнання кваліфікованих електронних підписів», «транскордонна сумісність та визнання сертифікатів та електронних підписів», «транскордонне визнання між чинними правовими системами у сфері послуг рекомендованих електронних відправлень», «транскордонні трансакції зобов'язань». Фактично опосередковано мова йде стосовно транскордонного режиму застосування електронних довірчих послуг та електронних підписів. Тобто необхідно надати конкретні визначення термінів «транскордонна електронна довірна послуга» та «транскордонний режим електронної довірчої послуги», які в правовому полі зможуть акумулювати поняття транскордонного режиму застосування довірчих послуг, взаємного визнання засобів електронної ідентифікації, сертифікатів та електронних підписів.

У такому випадку Регламент є прикладом нормативно-правового акту для суміщеної правової системи, що ґрунтується на стандартах Міжнародної організації зі стандартизації (ISO) та національних законодавствах країн –

членів Європейського Союзу. Однією із ключових правових проблем впровадження Регламенту стала складність реалізації електронної ідентифікації як складового елемента електронних довірчих послуг.

В Україні електронні довірчі послуги регламентуються відповідним Законом України «Про електронні довірчі послуги».

У Першому розділі визначено сферу дії Закону, яка полягає в регулюванні відносин, що виникають між юридичними, фізичними особами, суб'єктами владних повноважень у процесі надання, отримання електронних довірчих послуг, процедури надання цих послуг, нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також основні організаційно-правові засади електронної ідентифікації. Запроваджено оновлений понятійно-категорійний апарат, який складається з 44 нових або оновлених термінів, з яких 20 запроваджено вперше, а 11 понять запозичено з Регламенту: «автентифікація», «електронний підпис», «удосконалений електронний підпис», «кваліфікований електронний підпис», «засіб електронного підпису чи печатки», «підписувач», «електронна довірча послуга», «довірчий список», «електронна печатка», «електронна ідентифікація», «надавач електронних довірчих послуг». Одночасно правове поле національного законодавства позбулося термінів «електронний цифровий підпис», «акредитація», «надійний засіб електронного цифрового підпису», «захищений носій особистих ключів».

Відповідно до європейського законодавства зазначений Закон запроваджує поняття «електронна позначка часу», «кваліфікована електронна печатка», «схема електронної ідентифікації», «кваліфікований надавач електронних довірчих послуг», «реєстрована електронна доставка», «удосконалена електронна печатка». На думку законотворців, таке юридичне зближення термінології у сфері електронного підпису позитивно сприятиме формуванню в майбутньому спільних міждержавних регуляторних актів.

Водночас Законом України «Про електронні довірчі послуги» сформована низка нових визначень: «електронні дані», «засвідчення чинності

відкритого ключа», «засіб кваліфікованого електронного підпису чи печатки», «засіб удосконаленого електронного підпису чи печатки», «ідентифікація особи», «кваліфікований сертифікат відкритого ключа», «користувачі електронних довірчих послуг», «надавач електронних довірчих послуг», «пара ключів», «перевірка», «поновлення сертифіката відкритого ключа». За нашими оцінками окремі терміни, зокрема «самопідписаний сертифікат відкритого ключа», «вебсайт», «відокремлений пункт реєстрації», «інтероперабельність», можливо віднести, швидше, до категорії технічних або техніко-юридичних норм, оскільки вони не мають соціального характеру й описують певні специфічні технічні процедури чи умови, а поняття «компрометація особистого ключа», «схема електронної ідентифікації», «перевірка», «ідентифікація особи» мають декларативний характер, позбавлений юридичної визначеності.

Другий розділ Закону України «Про електронні довірчі послуги» визначає суб'єктів відносин у сфері електронних довірчих послуг та органи державної влади, що здійснюють їх державне регулювання: Кабінет Міністрів України; Національний банк України (у банківській системі України); головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації; центральний орган виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування й використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства. Така структура системи органів, які здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації, спрямована на забезпечення гнучкого реагування на ймовірні трансформації органів державної влади, що притаманні національному державному устрою та управлінню, яке має тенденцію до постійної зміни.

Формалізоване визначення головних органів спрямоване убезпечити Закон України «Про довірчі послуги» від ситуативних змін у законодавстві.

До суб'єктів відносин у сфері електронних довірчих послуг віднесено користувачів електронних довірчих послуг, надавачів електронних довірчих послуг, органи з оцінки відповідності, засвідчувальний центр, ЦЗО та орган контролю. Однак статті 10-12 Розділу II Закону України «Про електронні довірчі послуги» визначають права та обов'язки лише одного із суб'єктів відносин – користувачів електронних послуг. Водночас стаття 13 визначає права й обов'язки кваліфікованих надавачів електронних довірчих послуг, які згідно зі статтею 11 не входять до переліку суб'єктів відносин у сфері електронних довірчих послуг, натомість мають права й обов'язки. Крім того, закон оминає права й обов'язки органів щодо оцінки відповідності, засвідчувального центру, ЦЗО та органу контролю. Що стосується останніх, то вказані суб'єкти, згідно із статтею 5, не входять до системи органів, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації, натомість статтями 32 та 33 віднесені до органів нагляду (контролю) у сфері електронних довірчих послуг.

Враховуючи викладене, органами оцінки відповідності вважаються такі органи, які акредитовані відповідно до законодавства у сфері акредитації, а проведення процедури оцінки відповідності у сфері електронних довірчих послуг має здійснюватися в порядку, затвердженому Кабінетом Міністрів України. Однак на сьогодні такий порядок відсутній.

Визначення суб'єкта «орган контролю» у ст. 1 Закону відсутнє, однак за повноваженнями, відповідно до статей 5 та 8, до нього можна віднести «спеціально уповноважений орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації». Однак Законом у цій редакції не передбачено прав та обов'язків органу контролю, натомість зазначено, що він здійснює планові та позапланові, а також заходи нагляду (контролю) та певного реагування. Слід зазначити, що права й обов'язки «органу контролю», а також повноваження посадових осіб цього органу під час

здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, визначених ст. 34, не належать до предмета регулювання закону й мають бути врегульовані підзаконним нормативно-правовим актом.

Позитивним досягненням національного законодавства можна вважати уведення Законом понять: «ідентифікація особи», «ідентифікаційні дані особи», «електронна ідентифікація», «засіб електронної ідентифікації». Відповідно до статті 15 Закону передбачено запровадження схеми електронної ідентифікації та рівні довіри до засобів електронної ідентифікації, що створює позитивні перспективи розвитку сфери електронних довірчих послуг.

На окрему увагу заслуговує Розділ IV «Електронні довірчі послуги». По-перше, статтею 16 Закону визначено перелік електронних довірчих послуг, однак Законом не надається визначень або склад вказаних довірчих послуг, натомість деталізовано послуги, які не ввійшли до визначеного складу довірчих послуг, а саме: кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки; кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту; кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки; кваліфікована електронна довірча послуга реєстрованої електронної доставки; кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу; кваліфікована електронна довірча послуга зберігання кваліфікованих електронних підписів, печаток та сертифікатів, пов'язаних із цими послугами.

Така колізія авторами закону мотивується застосуванням правила законотворення «від загального до часткового», оскільки вважається, що кваліфікований електронний підпис є похідним поняттям від удосконаленого

електронного підпису: «кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису й базується на кваліфікованому сертифікаті відкритого ключа». Така правова конструкція досить непевно ототожнює електронні довірчі послуги і кваліфіковані електронні довірчі послуги, що потребує внесення доповнень та уточнень у зазначений Закон з метою уникнення неоднозначного трактування цих понять.

Також регламентується: діяльність кваліфікованих надавачів електронних довірчих послуг, використання електронних довірчих послуг, порядок ідентифікації особи під час формування та видачі кваліфікованого сертифіката відкритого ключа, алгоритм набуття статусу кваліфікованого надавача електронних довірчих послуг, особливості надання кваліфікованих електронних довірчих послуг центральним засвідчувальним органом тощо.

Слід зазначити, що, на відміну від Закону України «Про електронний підпис», у Законі України «Про електронні довірчі послуги» питанню міжнародного співробітництва та визнанню іноземних електронних довірчих послуг присвячено Розділ VI. Так, статтею 37 визначено, що Україна бере участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації на основі міжнародних договорів України та в порядку, встановленому законом. Порівняно з попереднім Законом України «Про електронний підпис» у Законі України «Про електронні довірчі послуги» застосовано більш розширений підхід до визнання іноземних сертифікатів ключів електронних підписів. Так, статтею 38 встановлено, що електронні довірчі послуги, які надаються відповідно до вимог нормативно-правових актів, що регулюють правові відносини у сфері електронних довірчих послуг в іноземних державах, визнаються в Україні електронними довірчими послугами того самого виду в разі відповідності хоча б одній з таких умов:

– кваліфікований надавач електронних довірчих послуг іноземної держави відповідає вимогам цього Закону, що підтверджується центральним

засвідчувальним органом (або засвідчувальним центром у разі надання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів);

– кваліфікований надавач електронних довірчих послуг внесений до Довірчого списку держави, з якою Україна уклала відповідний двосторонній або багатосторонній міжнародний договір.

Законом України «Про електронні довірчі послуги» встановлюється норма, згідно з якою електронні довірчі послуги не можуть визнаватися недійсними лише через те, що вони надані відповідно до вимог нормативно-правових актів, що регулюють відносини у сфері електронних довірчих послуг в іноземних державах. Крім того, Законом визначено, що використання інформаційно-телекомунікаційної системи центрального засвідчувального органу для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, які використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, встановлюється Постановою Кабінету Міністрів України від 23 січня 2019 р. № 60 «Про затвердження Порядку взаємного визнання українських та іноземних сертифікатів відкритих ключів, електронних підписів, а також використання інформаційно-телекомунікаційної системи центрального засвідчувального органу для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав». Цей Порядок визначає механізм взаємного визнання українських та іноземних сертифікатів відкритих ключів, електронних підписів, а також використання інформаційно-телекомунікаційної системи центрального засвідчувального органу з метою забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами

різних держав. Водночас дія цього Порядку не поширюється на кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, та програмно-технічні комплекси, що використовуються ними під час надання кваліфікованих електронних довірчих послуг у банківській системі та під час здійснення переказу коштів.

Згаданою постановою забезпечується лише процедура визнання в Україні електронних довірчих послуг, іноземних електронних підписів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, шляхом укладення відповідного міжнародного договору України про взаємне визнання сертифікатів відкритих ключів та електронних підписів. Так, за процедурою міжнародним договором мають бути передбачені:

- сфера дії міжнародного договору;
- сторони міжнародного договору та перелік нормативно-правових актів, якими встановлено повноваження сторін міжнародного договору;
- суб'єкти сторін міжнародного договору, на яких поширюється його дія та які здійснюють технічне забезпечення реалізації міжнародного договору;
- відомості про відповідність надавачів транскордонних електронних довірчих послуг вимогам національного законодавства кожної із сторін міжнародного договору та умови підтвердження відповідності зазначеним вимогам;
- умови обміну повідомленнями про відповідність надавачів електронних довірчих послуг кожної зі сторін міжнародного договору вимогам до надавачів транскордонних електронних довірчих послуг;
- умови та порядок засвідчення відкритих ключів надавачів транскордонних електронних довірчих послуг, які походять з однієї країни – сторони міжнародного договору, суб'єктами сторони міжнародного договору іншої країни;

- умови та порядок обміну засобами кваліфікованого електронного підпису між сторонами міжнародного договору та їх публікації;
- вимоги до форматів, протоколів, алгоритмів та об'єктних ідентифікаторів, які використовуються у засобах кваліфікованого електронного підпису та кваліфікованих сертифікатах відкритих ключів під час надання транскордонних електронних довірчих послуг;
- умови взаємного визнання, погодження й публікації політик сертифікації та сертифікаційних практик надавачів транскордонних електронних довірчих послуг;
- умови тимчасового зупинення і припинення взаємного визнання сертифікатів відкритих ключів та електронних довірчих послуг;
- особливості ведення довірчих списків сторонами міжнародного договору;
- порядок здійснення нагляду органами контролю сторін міжнародного договору;
- умови щодо захисту інформації та захисту персональних даних;
- інші умови міжнародного договору.

Отже, для українського законодавства чинним є лише один протокол визнання іноземних електронних довірчих послуг та іноземних електронних підписів – виключно шляхом укладання міждержавних угод у сфері електронного підпису.

2.3 Розвиток законодавства України у сфері електронних довірчих послуг та електронного підпису

Розбудову української інфраструктури відкритого ключа в Україні розпочато у грудні 2002 року з українського стандарту, що описує алгоритми формування та перевірки електронного підпису: «ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» [98], уведений в дію наказом державного комітету України з питань технічного регулювання та споживчої політики 2002 року № 31. У 2003 році Верховною Радою України прийнято Закони України «Про електронний цифровий підпис» [99] та «Про електронні документи та електронний документообіг» [100], які стали підґрунтям для низки нормативно-правових актів, які згодом врегулювали правовідносини під час використання електронного цифрового підпису. 28 жовтня 2004 року Кабінетом Міністрів України затверджено Постанову № 1451 «Положення про центральний засвідчувальний орган» [101]. Перший Центральний засвідчувальний орган (далі – ЦЗО) в Україні створено при Державному департаменті з питань зв'язку та інформатизації, який діяв у складі Міністерства транспорту і зв'язку України. З 26.03.2008 р. до 05.07.2010 р. ЦЗО функціонував у складі Державного комітету інформатизації України, а з 06.07.2010 р. до 27.09.2010 р. – у складі Державного комітету України з питань науки, інновацій та інформатизації. Відповідно до постанови Кабінету Міністрів України від 05.10.2011 р. № 1022 функції ЦЗО виконує Міністерство юстиції України.

Також згідно з Постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856 регуляцію у сфері надання електронних та адміністративних послуг, у сферах електронних довірчих послуг та електронної ідентифікації здійснює Міністерство цифрової трансформації України.

Слід зазначити, що законодавча база України в галузі електронного підпису достатньо насичена нормативно-правовими актами, які видаються Кабінетом Міністрів України, Міністерством юстиції України (регулятор) та Державною Службою спеціального зв'язку та захисту інформації України (орган контролю) згідно з розподілом сфер діяльності органів виконавчої влади [102]. Кабінетом Міністрів України видано низку постанов, які здійснюють регулювання застосування електронного підпису на загальнодержавному рівні.

Так, Постанова КМУ від 28 жовтня 2004 р. № 1451 затверджує Положення про центральний засвідчувальний орган [103], яким і регулює його діяльність. Згідно з цим актом Центральний засвідчувальний орган забезпечує організаційно-методологічні, технічні та технологічні умови для функціонування засвідчувальних центрів органів виконавчої влади або інших державних органів та центрів сертифікації ключів. Порядок акредитації центру сертифікації ключів визначено Постановою КМУ від 13 липня 2004 р. № 903 [104].

Слід визнати, що тривалий час широке застосування електронного підпису в державному секторі штучно обмежувалось вимогами Постанови КМУ від 28 жовтня 2004 р. № 1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» [103]. Обмеження, що мали характер дискримінаційних та корупційних ризиків, були скасовані лише на початку 2017 року.

У період з 2004 до 2017 року адміністрацією Державної служби спеціального зв'язку та захисту інформації України та Міністерством юстиції України загалом видано понад 15 нормативно-правових актів (наказів, вимог, листів-роз'яснень), які регулюють технічні та технологічні умови й порядок розроблення, виробництва та експлуатації засобів криптографічного захисту.

За ініціативи Міністерства юстиції України та з метою гармонізації вимог у сфері розвитку та забезпечення інтероперабельності системи електронного цифрового підпису у грудні 2014 року Мінекономрозвитку України наказом № 1493 [103] було прийнято як національні європейські та міжнародні стандарти 89 нормативних документів, що регламентують найбільш поширені у світі криптографічні алгоритми та протоколи, такі як RSA, DSA, KCDSA, ECDSA, EC KCDSA та EC-GDSA. Також протягом 2014 року прийнято два національних стандарти: ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» та ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція хешування на алгоритм симетричного блокового перетворення та на функції хешування».

Міністерством юстиції України спільно із Адміністрацією державного зв'язку та захисту інформації України видано наказ № 1017/5/206 від 29.03.2017 року [105] щодо застосування в Україні міжнародних алгоритмів криптозахисту RSA та ECDSA з метою надання електронних послуг відповідно до Закону «Про електронні довірчі послуги» та запровадження сучасних механізмів електронної ідентифікації Mobile ID.

Насиченість національного законодавства численними нормативно-правовими актами (наказами, стандартами, вимогами тощо) стосовно інфраструктури відкритого ключа в Україні стимулювало законотворців на розробку і впровадження у 2017 році Закону України «Про електронні довірчі послуги» (далі – Закон) [106]. Мета Закону – реформування законодавства у сфері електронного цифрового підпису, розбудови єдиного простору довіри на основі системи електронного підпису, визнання в Україні електронних підписів, які надаються іноземними постачальниками, що забезпечить активний розвиток транскордонного співробітництва та інтеграцію України у світовий електронний інформаційний простір [107].

На нашу думку, зазначений у Законі України «Про електронні довірчі послуги» загальний принцип визнання іноземних електронних підписів у

транскордонному режимі загалом є недосконалим. Зокрема, у законодавстві відсутні базові правові поняття, не представлено правових дефініцій основних термінів, частково визначено інституційні питання у сфері електронного підпису. Усе це створює певні бар'єри та проблеми на шляху співпраці українських юридичних та фізичних осіб, громадських та державних організацій зі своїми іноземними партнерами у світі шляхом здійснення безпечних, надійних і простих транскордонних електронних операцій та послуг із застосуванням електронних довірчих послуг, електронних підписів та їхніх сертифікатів.

Нині відсутні або потребують корінних змін більшість нормативно-правових актів, які могли б упорядкувати правову базу після набрання чинності в листопаді 2018 року Закону України «Про електронні довірчі послуги».

Зазначене створює низький рівень довіри до електронного підпису, електронних операцій та електронних довірчих послуг, що стримує споживачів до здійснення цілісних електронних операцій між підприємствами, громадянами й державними органами. Відсутність технічної сумісності форматів удосконалених та кваліфікованих електронних підписів для доступу до електронних послуг не сприяє транскордонному використанню засобів електронної ідентифікації та онлайн-послуг і стримує подальший розвиток транскордонних електронних операцій між Україною і зарубіжними країнами.

Слід зазначити, що українська законодавча система, що регулює юридичну й технічну сфери застосування електронних підписів, є досить розвинутою. Тільки в межах однієї роботи їхній перелік та аналіз займає великий обсяг. Нині триває активне формування нової нормативно-правової бази. Характерна його спрямованість – виключно в напрямі інтеграції українського законодавства в законодавче поле Європейського Союзу з ігноруванням інтеграції у світові структури. На наш погляд, розвиток нормативно-правової бази в одному напрямі створює юридичні та технічні

проблеми у вітчизняній галузі електронного підпису та електронних довірчих послуг, зокрема в питанні відсутності правових механізмів забезпечення визнання іноземних сертифікатів електронних підписів.

Отже, існує потреба глибокого порівняльного аналізу міжнародного, світового та законодавства окремих країн у галузі електронних підписів для визначення схожості та відмінності, колізій та спорідненості правових норм, з урахуванням практик їхнього застосування. Україна має унікальну можливість побудови сучасної моделі механізму правового регулювання вітчизняної інфраструктури відкритого ключа, яка зможе забезпечити швидку міжнародну інтеграцію національних та іноземних електронних підписів.

2.4. Порівняльний аналіз понятійно-категоріального апарату сфери електронних довірчих послуг та електронного підпису

Розвиток суспільних відносин та технологій у галузі електронного підпису та електронних довірчих послуг став джерелом нових понять і термінів, які використовуються в нормативно-правових актах, наукових публікаціях, доповідях на конференціях, іншій науковій літературі. У результаті одні й ті самі об'єкти стали позначатися різними термінами, подекуди оригінальними. Останнім часом поширюється значна кількість публікацій та нормативних актів, які по суті є перекладами англomовних документів, у яких досить часто застосовуються довільний переклад понять або транслітерація, припускаються термінологічні неточності тощо.

Як стверджує О.Б. Погорелов, часто виникають ситуації, коли один і той самий об'єкт має багато різних назв: система поділу доступу, система управління доступом, система контролю доступу. Крім того, нерідко терміни в різних джерелах визначаються по-різному, а терміни з подібними назвами несуть різне смислове навантаження. Наприклад, електронний підпис залежно від ситуації може означати цифровий підпис, набір символів та даних, код аутентифікації повідомлення або деяку аутентифікаційну біометричну інформацію. Тому нагальною проблемою на сьогодні є міжнародна уніфікація глосарію термінів у галузі електронного підпису, а також приведення національних нормативно-правових актів у цій сфері до єдиної технічної та правової термінології [108].

Загальноприйнято, що в теорії права нормативні документи та терміни повинні складатися стисло, чіткою мовою із застосуванням юридичної техніки. Юридична техніка являє собою сукупність правил і засобів, які застосовуються для створення або внесення змін у правові акти, з метою забезпечення їхньої досконалості та відповідності суспільним відносинам. При цьому слід зазначити, що найважливішим мовним засобом юридичної

техніки є термінологія. Термінологія і дефініції понять, що використовуються в законодавстві, є техніко-юридичними засобами точного й виваженого вираження погляду нормотворця на розв'язання проблем суспільних відносин у цій сфері. У законодавчому тексті правові терміни повинні адекватно розкривати зміст терміна, визначати його ознаки, містити характеристики, дані в концентрованій і узагальнювальній формі. Незавершеність правового регулювання суспільних відносин свідчить про неефективність нормативно-правового акту.

Свою чергою, ефективність правового регулювання безпосередньо залежить від якості законодавства. Серед іншого ефективність практичного застосування нормативно-правового акта багато в чому залежить від використання абсолютно специфічних систем термінів, які обумовлюють особливий характер мови закону й забезпечують точне й повне вираження законодавчої волі в тексті закону.

Такими мовними засобами є правові дефініції і терміни юридичних понять. Вони необхідні не тільки тому, що допомагають реалізувати принцип нормотворчої економії, але головним чином тому, що в багатьох випадках без них неможливо з необхідною точністю висловити думку законодавця. Застосування спеціальної юридичної термінології та правових дефініцій є показником високої юридичної культури правотворчої та іншої юридичної діяльності. За допомогою такого технічного засобу, як дефініція, формулюються значення термінів, що вживаються в текстах нормативних актів, які є основою змісту документа, базою опису механізму правового регулювання.

У ході створення системи законодавства нормотворці формулюють дефініції за допомогою різних прийомів викладу норм права, використання спеціальних термінів, стандартних мовних зворотів, щоб досягти точності та визначеності формулювань. Термінологія нормативних актів повинна бути єдиною. Формалізація понять сприяє точності й визначеності правового регулювання.

Складні конструкції норм права, перевантаженість багатослівністю, суттєве розходження або інколи протилежність легальних дефініцій, що тлумачать один і той самий термін, дають привід та підстави для різного тлумачення та зашкоджують їхньому уніфікованому застосуванню. Тобто будь-яке юридичне визначення повинно виключати будь-яку двозначність і бути одночасно і зрозумілим, і достовірним тлумаченням норми або групи норм права.

Т.В. Кашаніна сформулювала загальні вимоги до складання дефініцій. За її словами, вони повинні:

- відображати тільки суттєві ознаки узагальнених явищ, що мають правове значення;
- бути повними й відображати всі явища, які узагальнюються;
- бути адекватними, тобто мати обсяг, якій збігається із обсягом поняття, що визначається.

Також дефініції не повинні містити суперечливих суджень, а також термінів, що вживаються у цьому понятті (щоб уникнути тавтології).

Дотримання цих вимог під час створення дефініцій позитивно впливає не тільки на окремий нормативно-правовий акт, але й загалом на систему законодавства, зменшуючи ризики довільного трактування норм права [109].

Для сфери електронного підпису точні та виважені дефініції важливі тим, що вони визначають багато нових для права понять і створюють єдиний понятійний простір, який має діяти не тільки в одній державі.

Особливої актуальності набуває вивчення юридичної техніки та технологій на цьому етапі, коли спостерігається розширення меж європейської міжнародної правотворчої діяльності. Так, розширення закріплюється в установчих документах міжнародних організацій і потребує цілеспрямованої діяльності щодо забезпечення підготовки до впровадження результатів міжнародного правотворення в національне правове поле.

Stephen Mason, вивчаючи судову практику використання даних в електронній формі, як докази елементів злочинів у міжнародному та

національному законодавстві, зокрема у сфері електронного підпису, констатує відмінність багатьох положень та норм цієї сфери, що ускладнює вирішення правових проблем різних юрисдикцій. Так, різні норми та дефініції створюють правові бар'єри для транскордонного застосування електронних підписів у законодавствах різних країн, а також є підґрунтям для скоєння різноманітних правопорушень у цій сфері. Крім того, відсутність єдиного законодавчого інформаційного простору або єдиної бази нормативно-правових актів у цій сфері суттєво ускладнює міждержавну правову регуляцію через те, що нові законодавчі акти або інформацію дуже важко своєчасно та в повному обсязі отримати в деяких юрисдикціях [110].

На думку Caroline M. Laborde, законодавство про електронний підпис, яке було прийняте в останні 10 років у різних юрисдикціях, має різний підхід та регулювання використання електронних підписів, зокрема і в міжнародних контрактах. Проблема транскордонної несумісності потребує свого вирішення одночасно в чотирьох напрямках: технологічна та правова сумісність електронних підписів; типовізація правового регулювання електронних підписів; уніфікація законодавства про електронний підпис у частині його застосування до міжнародних договорів і, нарешті, правові наслідки застосування того чи того закону про електронний підпис [111].

В Україні термінологічна основа нормативно-правових актів в інформаційній сфері не є досконалою, громадянам доводиться користуватися різноманітними довідковими джерелами, але внаслідок варіативності значення дефініцій їх часто тлумачать по-різному. Відсутність чіткого і змістовного визначення термінів ускладнює їхнє тлумачення та дезорганізує використання, а також потребує порівняльного аналізу наявних інформаційних термінів та надання їм однозначного трактування для подальшого застосування у сфері електронного підпису.

Базове поняття нормативно-правових актів у сфері електронного підпису – «електронний підпис». У міжнародному та національному законодавствах (таблиця 4) цей термін описує технологічний процес, за яким

дані в електронній формі, що дозволяють ідентифікувати особу підписувача, додаються до даних в електронній формі, які містять будь-яку інформацію.

Зважаючи на особливості національних правових доктрин, маємо достатню кількість варіантів дефініції поняття «електронний підпис», які хоч і ототожнюються з технологічним процесом, але за формою, конструкцією та викладенням суттєво відрізняються один від одного (Додаток К).

Зважаючи на стрімке зростання незаконного використання електронного підпису особами, які не є його підписувачами, відсутність в Адміністративному та Кримінальному кодексах конкретних видів правопорушень у сфері електронного цифрового підпису, а також покарань за їх скоєння, пропонуємо вдосконалити дефініцію поняття «електронний підпис» та посилити її диспозицію правилом, за яким зобов'язати підписувача особисто контролювати електронний підпис, а також застосувати санкцію, якою буде можливо вжити заходи державного примусу. Наприклад, ст. 14 Закону Болгарії «Про електронний підпис» містить норму, яка встановлює, що «ніхто, крім автора, не має права доступу до даних для створення електронного підпису». Однак, ця норма не встановлює обов'язок особи не розкривати третім особам відповідну інформацію, яка необхідна для легітимації цифрового підпису.

В українському законодавстві, що регулює правовідносини у сфері електронного підпису, не передбачено відповідальності за правопорушення в цій галузі.

Зважаючи на викладене, пропонуємо вдосконалити пункт 12 статті 1 Розділу 1 Закону України «Про електронні довірчі послуги» і викласти в такій редакції:

«Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються й використовуються ним як підпис та перебувають під особистим контролем підписувача.

Забороняється передавати третім особам електронний підпис та ідентифікаційні дані особи підписувача, крім випадків, встановлених законом».

Ситуація неузгодженості правових норм також стосується й інших понять, таких як «цифровий підпис», «удосконалений цифровий підпис», «кваліфікований цифровий підпис», «сертифікат електронного підпису», «електронна послуга».

Так, термін «цифровий підпис» описує технологічний процес, згідно з яким дані в електронній формі (будь-яка інформація в електронній формі) за допомогою математичного алгоритму перетворюються на хеш-файл – унікальний «код», який шифрується за допомогою особистого електронного ключа підписувача та поєднується з його відкритим ключем, у результаті чого утворюється цифровий підпис, накладений на електронний документ. Різні нормативно-правові акти містять поняття «цифровий підпис», які суттєво відрізняються між собою. Одні норми пропонують досить стисле визначення й більш загальний зміст, інші в тих чи тих варіаціях досить детально описують технологію створення цифрового підпису (Додаток Л). Такі визначення, швидше, належать до технічних норм.

Розглянувши визначення термінів «удосконалений електронний підпис» та «кваліфікований електронний підпис», можемо констатувати також різне їхнє змістове наповнення. Зважаючи на достатню складність термінології у сфері електронного підпису, нормотворці намагалися найбільш повно описати технічні процеси створення та застосування різновидів електронних підписів, а також встановлені конкретні умови їхньої юридичної значимості.

Так, ключовими умовами створення та застосування вдосконаленого та кваліфікованого електронних підписів є вимоги, за якими ці електронні підписи повинні обов'язково бути пов'язаними з підписувачем, створюються з використанням відповідних технічних засобів електронного підпису та

забезпечують можливість внесення змін в електронне повідомлення, підписане електронним підписом (Додаток М).

Існує неузгодженість у правових нормах та нормативно-правових актах у межах вітчизняного законодавства. Так, поняття «електронна послуга» із різними правовими конструкціями використовується в нормативних документах Кабінету Міністрів України, Міністерства юстиції України, Пенсійного фонду України та в Законі України «Про електронні довірчі послуги», а саме:

електронна послуга (або е-послуга) – це адміністративна або інша публічна послуга, що надається громадянину або юридичній особі в електронній формі. Завдяки цьому громадянин має змогу отримати послугу від держави (оформлення ліцензії, соціальної допомоги, особистого документа тощо) без особистого відвідування органів влади. Е-послуги надаються через Інтернет, тож доступні з дому чи офісу 24 години на добу та сім днів на тиждень. Таким чином, вони є зручнішими та швидшими за особисті візити та мінімізують ризики корупції» [112];

електронна послуга – послуга, надана громадянам та організаціям в електронному вигляді за допомогою інформаційно-комунікаційних технологій (далі – е-послуга) [113];

електронна послуга – передача до відділів державної реєстрації актів цивільного стану наданих користувачами заяв у сфері державної реєстрації актів цивільного стану з накладенням електронного цифрового підпису користувача або звернень з інформацією, необхідною для формування таких заяв, що підписуються під час особистого звернення фізичної особи до відділу, отримання повідомлень про результати їх розгляду [114];

електронна послуга – надання інформації та/або документів з метою вирішення порушених особою, яка звертається до органів Пенсійного фонду, питань за допомогою засобів вебпорталу [115];

електронна послуга – адміністративна та інша публічна послуга, що надається суб'єкту звернення в електронній формі за допомогою засобів

інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем [116];

електронна послуга – будь-яка послуга, що надається через інформаційно-телекомунікаційну систему [116].

Окремо слід звернути увагу на статтю 50 Договору про Співтовариство [117], у якій під «послугами» розуміються послуги, що звичайно надаються за винагороду, якщо вони не регулюються положеннями щодо вільного руху товарів, капіталів та пересування осіб. Послуги включають, зокрема:

- а) діяльність промислового характеру;
- б) діяльність торгового характеру;
- в) діяльність ремісників;
- г) діяльність осіб вільних професій.

За практикою ЄС зміст поняття «послуги» включає туристичну, медичну, фінансову, освітню, спортивну діяльність, надання телевізійного сигналу, продаж лотерей, надання кредитів на придбання житла, діяльність агенцій з працевлаштування тощо.

Частиною 7 статті 1 розділу I Закону України «Про електронні довірчі послуги» визначено, що електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги.

Разом з тим частиною 16 статті 3 «Регламенту (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС» встановлено, що «довірча послуга» – це електронна послуга, що зазвичай надається за винагороду і яка полягає у:

- а) створенні, перевірці та підтвердженні електронних підписів, електронних печаток або електронних позначок часу, послугах рекомендованих електронних відправлень та використанні сертифікатів, що пов'язані з цими послугами; або

б) створенні, перевірці та підтвердженні сертифікатів для автентифікації вебсайту; або

в) збереженні електронних підписів, електронних печаток або сертифікатів, пов'язаних із цими послугами.

Слід зважати на те, що загальноєвропейський підхід до поняття «послуга» полягає в тому, що цим терміном позначаються взаємовідносини між суб'єктами тільки в разі, коли вони мають економічний характер та надаються за винагороду. До цих послуг належать і державні адміністративні послуги, які є різновидом платних послуг, тому що оплачуються державою з державного або місцевих бюджетів.

Зважаючи на багатогранність підходів до визначення поняття «електронна послуга», доцільно внести зміни до Закону України «Про електронні довірчі послуги» та вдосконалити пункт 7 статті 1 Розділу I, виклавши в такій редакції:

«електронна довірча послуга – електронна послуга, яка надається за винагороду для забезпечення інформаційних взаємовідносин між суб'єктами, що здійснюються за допомогою технологій мережі Інтернет або в електронній формі, і яка полягає у:

а) створенні, перевірці та підтвердженні електронних довірчих послуг, електронних підписів, електронних печаток або електронних позначок часу; послугах, рекомендованих електронних відправлень та використанні сертифікатів та інших, що пов'язані з цими послугами; або

б) створенні, перевірці та підтвердженні сертифікатів для автентифікації вебсайту; або

в) збереженні електронних підписів, електронних печаток або сертифікатів, пов'язаних із цими послугами»,

а також удосконалити пункт 11 статті 1 цього ж розділу й викласти в такій редакції:

«електронна послуга – послуга, яка надається за винагороду для забезпечення інформаційних взаємовідносин між суб'єктами суспільних відносин із використанням інформаційно-комунікаційних технологій».

У межах дослідження також вивчалось застосування електронного підпису в транскордонному режимі. Слід зазначити, що в міжнародному законодавстві використання терміна «транскордонний» досить поширено. Уперше термін «транскордонність» вживається у статті 12 Типового закону «Про електронні підписи» 2001 року UNCITRAL, який застосовується для декларації можливої процедури визнання й використання певних видів іноземних електронних підписів або сертифікатів. У різних міжнародних актах трапляється багато таких термінів: «транскордонна діяльність», «транскордонні угоди», «надання транскордонних послуг громадянам», «транскордонне надання послуг із сертифікації», «транскордонне співробітництво», «транскордонні цифрові послуги», «транскордонне використання онлайн-послуг», «транскордонне визнання ключових компонентів», «транскордонна сумісність електронних підписів», «транскордонна діяльність», «транскордонна система охорони здоров'я», «транскордонний доступ до електронних даних», «транскордонне використання засобів електронної ідентифікації», «транскордонне взаємне визнання засобів електронної ідентифікації», «загальна система транскордонного використання довірчих послуг», «транскордонне визнання кваліфікованих електронних підписів», «транскордонна сумісність та визнання сертифікатів та електронних підписів», «транскордонне визнання між чинними правовими системами у сфері послуг рекомендованих електронних відправлень», «транскордонні трансакції зобов'язань» тощо [118].

Регламентом (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних «транскордонна обробка» означає або:

обробку персональних даних, яка відбувається в контексті діяльності підприємства більш ніж в одній державі-члені контролера або оператора в Союзі, де контролер або оператор встановлений у більш ніж одній державі-члені, або обробку персональних даних, яка відбувається в контексті діяльності однієї установи контролера або оператора в Союзі, але яка істотно впливає або може становити суттєвий вплив на суб'єктів даних у більш ніж одній державі-члені [119].

Однак саме визначення поняття «транскордонність» відсутнє, натомість є численні трактування, які суттєво відрізняються між собою, що створює неоднозначність тлумачення норми або групи норм права у сфері електронного підпису та електронних довірчих послуг.

Враховуючи зазначене, доцільно доповнити частину 1 статті 1 Розділу I Закону України «Про електронні довірчі послуги» після пункту 45 новим пунктом 46 такого змісту:

«Транскордонність – це унормована або взаємоузгоджена діяльність суб'єктів права різних країн та юрисдикцій у сфері електронного обміну даними із застосуванням електронних підписів, спрямована на забезпечення електронними сервісами суспільних відносин цих суб'єктів у міждержавному та міжнародному режимах».

Суспільні відносини на сучасному етапі розвитку людства створили нові, особливі інформаційні відносини, спрямовані на організацію руху інформації в суспільстві, що сприяло виникненню нового виду послуг – електронних.

Узагальнюючи поняття «транскордонність» та «електронна довірча послуга», можемо рекомендувати до застосування нове визначення, для чого необхідно внести зміни до частині 1 статті 1 Розділу I Закону України «Про електронні довірчі послуги» і доповнити пунктом 47 такого змісту:

«Транскордонне визнання електронного підпису або електронної довірчої послуги – це унормована або взаємоузгоджена діяльність суб'єктів права різних країн та юрисдикцій у сфері електронних підписів та

електронних довірчих послуг, спрямована на встановлення юридичної сили електронного підпису, яка надається у транскордонному режимі»,

а також частину 1 статті 1 Розділу I Закону України «Про електронні довірчі послуги» доповнити пунктом 48:

«Транскордонна електронна послуга – електронна послуга, яка надається за винагороду і спрямована на забезпечення електронних взаємовідносин між суб'єктами різних країн із транскордонним використанням електронних підписів».

На нашу думку, необхідність запровадження нового терміна «компрометація особистого ключа» зумовлена наявністю таких причин. По-перше, міжнародні законодавчі норми в галузі електронного підпису не мають чітких загальноприйнятих визначень поняття «компрометації». Термін «компрометація» в контексті «компрометація електронного підпису», застосовано в Типовому законі ЮНСІТРАЛ «Про електронні підписи і Керівництво із прийняття рішень» [120], прийнятого у Відні 5 липня 2001 року на 34-й сесії ЮНСІТРАЛ, статтею 57 якого поняття «ненадійний сертифікат» трактується як такий, особистий ключ якого «скомпрометовано» внаслідок втрати підписувачем контролю над ним. У США поняття «компрометація» визначено Національним інститутом стандартів і технологій (National Institute of Standards and Technology – NIST) як «неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (включаючи криптографічні ключові тексти та інші дані Центру політики безпеки (CSP) [121] або неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (наприклад, ключів, метаданих та іншої інформації, що стосується безпеки)» [122;123].

Вивчаючи ризики транскордонного застосування електронних цифрових підписів та електронних довірчих послуг, Mike Just, Paul C. van Oorschot приділяють окрему увагу проблемі довіри до таких послуг, яка базується на дотриманні підписувачем вимог до користування електронними підписами. Так, науковці визнають проблему компрометації особистого

ключа електронного підпису як одного з ключових елементів довіри в загальній системі правової регуляції цієї сфери [124].

Крім ризиків компрометації особистого ключа, зростають ризики технологічної компрометації, наслідки якої більш масштабні, ніж несанкціонований доступ до одного особистого ключа електронного підпису. Так, за твердженням P.Pellegrini, у Словачії виявлено технічну загрозу компрометації електронного підпису, який розміщується на чіпі електронного посвідчення громадянина, унаслідок чого було заблоковано низку державних електронних сервісів [125]. Ізраїльські науковці D.Shamir та Tromer E. створили технічні пристрої, здатні на відстані до 10 метрів копіювати 4096-біті ключі алгоритму RSA, під час використання електронного підпису на користувацькому комп'ютері [126].

Вітчизняне законодавство також по-різному трактує поняття «компрометація». Так, пунктом 26 статті 1 Закону України «Про електронні довірчі послуги» визначено, що «компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа. Однак, таке саме тлумачення містив і попередній Закон України «Про електронний цифровий підпис». На жаль, таке формулювання, з одного боку, не надає визначення, які саме об'єкти або суб'єкти правових відносин вчиняють вказані вище дії та які саме дії/події призводять до несанкціонованого використання особистого ключа, а з іншого боку, невизначеність дефініції створює підстави довільного трактування вказаної норми закону. Водночас українські технічні спеціалісти в галузі захисту інформації запровадили кілька варіантів визначення поняття «компрометація» як технічного терміна. Так, Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України у 1999 році при створенні НД ТЗІ 1.1.-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» застосовано термін «компрометація» (compromise) у значенні «порушення політики безпеки; несанкціоноване ознайомлення» [127]. Це визначення

компрометації спрямоване на врегулювання деструктивних подій у системі безпеки, пов'язаних із порушенням чітких правил використання цифрових підписів. Проте, таке визначення не поширюється на відносини, що пов'язані з використанням особистого ключа поза межами, визначеними політикою безпеки, а сама політика безпеки може суттєво відрізнятися. Також зазначена дефініція не пояснює термін «несанкціоноване ознайомлення». Крім того, наказом Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 р. № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису» визначено більш розширене тлумачення компрометації – як будь-який випадок (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами криптографічного захисту інформації, який призвів (може призвести) до розголошення (витоку) інформації про них, а також інформації, яка обробляється та передається [128].

В українському законодавстві склалася ситуація, коли відсутність поняття «компрометація особистого ключа» в суспільних відносинах, які регулюють сферу використання електронних ключів, позбавила право ясності та конкретики, ускладнивши процес його застосування, що зменшило довіру до електронних документів та правочинів, які вчиняються за допомогою електронних підписів, про що свідчить судова практика. За останні роки збільшилася кількість правопорушень та злочинів, пов'язаних саме із компрометацією та незаконним використанням особистих ключів електронних підписів.

Отже, «компрометація» в чинному законодавстві – це фактично розпливчастий термін, щодо якого можуть виникати пограничні правові випадки. Тому слід розширити встановлену практику використання поняття «компрометація», щоб зробити термін менш розпливчастим та більш

інформативним, врахувати поняття явної та неявної компрометації, що сприятиме більш якісному застосуванню норм права [129].

Зважаючи на наявну, не врегульовану нормами права проблему, доцільно внести зміни до Закону України «Про електронні довірчі послуги» та вдосконалити пункт 26 частини 1 Розділу I і викласти його в такій редакції:

«Компрометація особистого ключа електронного підпису – будь-яка явна або неявна подія та/або дія (втрата, розголошення, крадіжка, несанкціоноване копіювання) з даними особистого ключа електронного підпису та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого розголошення, зміни, знищення, блокування, перехоплення, копіювання та використання особистого ключа електронного підпису, а також інформації, яка обробляється та передається за його допомогою. Явною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа за участю або без участі підписувача або третіх осіб без застосування технічних засобів. Неявною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа електронного підпису із застосуванням будь-яких технічних засобів без участі підписувача».

Це визначення включає загальну норму компрометації та два деталізованих визначення явної та неявної компрометації. Такий підхід дозволить здійснювати більш якісну кваліфікацію суспільно небезпечних протиправних дій з використанням особистого ключа електронного підпису.

Висновки до розділу 2

1. Дослідження стану сфери електронних послуг та електронних довірчих послуг на основі статистичних даних, наданих Кабінетом Міністрів України, Міністерством юстиції України, Державним агентством з питань електронного урядування України, постачальниками кваліфікованих електронних довірчих послуг (акредитованими центрами сертифікації), а також стану та напрямів розвитку державних електронних сервісів у рамках стратегії Президента України «Держава в смартфоні» та перспектив застосування електронних підписів та електронних довірчих послуг виявило наявність проблем застосування сучасних інформаційно-телекомунікаційних технологій, технологій електронного підпису через низьку довіру громадян до інформаційних сервісів, потребу підвищення громадянської цифрової гігієни, культурного та правового рівня поінформованості населення.

2. Українська законодавча система, що регулює юридичну й технічну сфери застосування електронних підписів, є досить розвинутою та має значну кількість регуляторних актів різних органів державного управління. На сьогодні триває ревізія чинних нормативно-правових актів та розпочато активне формування нової нормативної бази. Детальний аналіз Закону України «Про електронні довірчі послуги» виявив ключові чинники, що створюють у суспільних відносинах правову невизначеність та неврегульованість.

3. Існує спрямованість законотворців виключно в напрямі інтеграції українського законодавства в законодавче поле Європейського Союзу та ігнорування інтеграції в загальносвітові інформаційно-комунікаційні структури. Розвиток нормативної бази в одному напрямі створює юридичні та технічні проблеми у вітчизняній сфері електронного підпису, зокрема в питанні відсутності правових механізмів забезпечення визнання іноземних електронних підписів. На сьогодні не створено дієвих правових механізмів визнання іноземних електронних підписів.

4. Модернізація правової моделі суспільних відносин правового регулювання вітчизняної інфраструктури відкритого ключа забезпечить швидку міжнародну інтеграцію національних та іноземних електронних підписів.

5. У результаті порівняльного аналізу міжнародного та законодавства окремих країн у галузі електронних підписів виявлено їхню схожість та відмінності, колізії і спорідненість правових норм з урахуванням практик їхнього застосування. Доведено необхідність створення та прийняття єдиного міжнародного тезаурусу у сфері електронних підписів, який необхідно реалізувати на рівні міжнародного нормативно-правового акту у вигляді базового словника понять і термінів із зв'язками між ними.

РОЗДІЛ 3.

ШЛЯХИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РЕГУЛЮВАННЯ ТРАНСКОРДОННОГО НАДАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

3.1. Удосконалення правової моделі регулювання суспільних відносин у сфері електронних довірчих послуг в Україні

Сфера цифрового підпису вдосконалюється одночасно із розвитком інформаційно-комунікаційних технологій. Розвиток останніх проходить значно швидше, ніж здійснюється модернізація чинного законодавства в цій галузі. Багато процесів, спрямованих на запровадження єдиного цифрового ринку, не мають належного правового підґрунтя для взаємного транскордонного визнання ключових компонентів, таких як електронна ідентифікація, електронні документи, цифрові підписи та електронні довірчі послуги, а також для врегулювання їхнього технічного сумісництва.

Ці недоліки й корінні властивості інформаційно-комунікаційних технологій створюють атмосферу недовіри між суб'єктами суспільних відносин. Відсутність довіри, зокрема, через високу вірогідність правової невизначеності робить споживачів, бізнес і органи державної влади уразливими в частині достовірності результатів здійснення суспільних відносин із застосуванням інформаційно-комунікаційних технологій, що є фундаментальним бар'єром на шляху підвищення ефективності економічного й соціального розвитку людства.

Таким чином, основна проблема – це забезпечення довіри при застосуванні ІКТ в будь-яких суспільних відносинах. Побудова довіри в онлайн-середовищі є ключовим завданням для економічного та соціального розвитку. Проблема довіри в суспільних відносинах у сфері цифрових підписів загалом полягає в такому.

У більшості випадків громадяни не можуть використати свої цифрові підписи для отримання електронних послуг в іншій державі, оскільки електронні підписи та електронні довірчі послуги, які створені їхніми національними системами цифрового підпису, не визнаються на території інших держав.

Цифрова ідентифікація іноземної фізичної/юридичної особи під час використання іноземного цифрового підпису не має чітких визначених процедур правового визнання в Україні, які закріплені нормативно-правовими актами.

Відсутні правові механізми перевірки цифрової ідентифікації фізичної/юридичної особи, надійності та достовірності національного цифрового підпису, а також іноземних цифрових підписів в Україні, а наявні локальні технічні механізми не легалізовані законодавчо. Визначені в Законі загальні принципи визнання як іноземних цифрових підписів є недосконалими й недієвими.

Електронні послуги в Україні сьогодні розвиваються ситуативно за відсутності чіткого планування та обліку самих державних послуг, що потребують цифровізації. Для запровадження електронних послуг органи державної влади та місцевого самоврядування часто розроблюють власні програми розвитку цифрових послуг, залучають розробників, які використовують різні технології, технічні підходи, візуалізацію сервісів, інтуїтивні інтерфейси користувача, доступність цільової аудиторії тощо.

Так, електронні послуги, зібрані на сайті Міністерства цифрової трансформації України, тільки транслують користувача на електронні ресурси окремих органів влади, які і створюють ці послуги за власним баченням. Фактично розвиток електронних послуг повторює шлях, яким впроваджувалися системи електронного документообігу в органах державної влади, унаслідок чого держава згодом змушена запроваджувати єдину інформаційну шину «Трембіта», яка виступає як транскодер між різними системами електронного документообігу.

Переважна більшість українських електронних послуг не має обов'язкової надійної ідентифікації користувача шляхом залучення технологій цифрового підпису, Mobile ID, BankID та інших. Механізми перевірки цифрової ідентифікації фізичної та юридичної особи, надійності та достовірності національного електронного підпису, а в нашому випадку іноземних електронних підписів в Україні не носять закріплених законом юридичних наслідків (відповідальності та покарання).

Одним із елементів надійності та достовірності електронного підпису є його сертифікат, який містить необхідні ідентифікаційні відомості про підписувача, надавача послуг електронного підпису та необхідні технічні дані. Перевірити дійсність електронного підпису можна, переглянувши зміст електронного сертифіката шляхом:

- а) добровільного обміну сертифікатами між підписувачами;
- б) звернення підписувача до ресурсів відповідного АЦСК (списків чинних, блокованих та скасованих сертифікатів);
- в) використання електронних механізмів, які мають факультативний характер і розміщені на сайтах Центрального засвідчувального органу Міністерства цифрової трансформації України та Національного банку України.

Така перевірка зазвичай стосується або окремо національного електронного підпису, або електронного документа, засвідченого національним електронним підписом, і є неофіційною процедурою.

Статтею 12 Закону визначено права й обов'язки підписувачів, тобто користувачів довірчих послуг, а також зазначено, що захист прав користувачів електронних довірчих послуг, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України «Про захист прав споживачів». Водночас законодавство оминає такий важливий аспект, як юридична відповідальність користувачів довірчих послуг у частині невиконання або порушення зобов'язань, щодо забезпечення конфіденційності та неможливості доступу інших осіб до особистого ключа

(тобто його компрометації), а також надання недостовірної інформації під час отримання та використання електронних довірчих послуг.

Усе це створює недовіру, певні бар'єри та проблеми на шляху співпраці українських юридичних та фізичних осіб, громадських та державних організацій зі своїми зарубіжними партнерами під час здійснення безпечних, надійних і простих транскордонних електронних операцій та послуг із застосуванням електронних підписів. Хоча фізичні та юридичні особи, що здійснюють комерційну діяльність, можуть використовувати будь-які електронні підписи «за згодою сторін», при цьому ризики ненадійної ідентифікації підписувачів та достовірності електронних підписів досить високі.

Положення універсальних конвенцій, міжнародних типових і локальних законів не гармонійні в тій частині, яка стосується вживання термінів. У більшості міжнародно-правових актів так чи інакше застосовують юрисдикційні аспекти, правові норми та терміни, що позбавлені конкретного змісту й розглядаються більше як рекомендації загального порядку, які державам-учасникам слід прийняти і здійснити у сфері електронного підпису для досягнення кінцевої мети національного законодавства.

Мусимо констатувати, що на сьогодні маємо характерну спрямованість українських законотворців у напрямі інтеграції законодавства України у сфері електронного підпису виключно в законодавче поле Європейського Союзу (тобто інтеграція до внутрішнього ринку ЄС) та ігнорування універсальності національного законодавства та регуляторного наближення до законодавства інших країн світу.

Розвиток нормативної бази в одному напрямі створює юридичні та технічні проблеми у вітчизняній сфері електронного підпису, зокрема в питанні відсутності правових механізмів забезпечення визнання іноземних електронних підписів.

Сфера дії Закону України «Про електронні довірчі послуги», визначена в Розділі I, полягає в регулюванні відносин, що виникають між юридичними,

фізичними особами, суб'єктами владних повноважень у процесі надання, отримання електронних довірчих послуг, процедури надання цих послуг, нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також у визначенні основних організаційно-правових засад електронної ідентифікації. Цим Розділом запроваджується оновлений правовий понятійно-категорійний апарат, який частково складається з понять, що визначені в Регламенті (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС (далі – Регламент).

Водночас Законом сформовано низку нових понять, які носять технічний або техніко-юридичний характер та описують певні специфічні технічні процедури чи умови. Деякі правові дефініції мають декларативний характер, тобто позбавлені юридичної визначеності.

Насиченість Закону деталізованими для українського законодавства термінами й широка палітра дефініцій в одній достатньо вузькій правовій сфері створюють проблеми тотожності українського законодавства із міжнародним та національними законами інших країн на предмет взаємовідповідності під час транскордонного надання електронних підписів.

Визнання іноземних електронних підписів та іноземних електронних довірчих послуг зафіксовано формально у ст. 37, 38 Розділу VI Закону України «Про електронні довірчі послуги». Так, статтею 38 Закону встановлено, що електронні довірчі послуги, надані відповідно до вимог нормативно-правових актів, які регулюють правові відносини у сфері електронних довірчих послуг в іноземних державах, визнаються в Україні електронними довірчими послугами того самого виду в разі відповідності кваліфікованого надавача електронних довірчих послуг іноземної держави вимогам Закону, що підтверджується центральним засвідчувальним органом.

Відповідно до ст. 38 Закону України «Про електронні довірчі послуги» іноземний сертифікат цифрового підпису визнається в разі, якщо

кваліфікований надавач електронних довірчих послуг буде внесений до Довірчого списку держави, з якою Україна уклала відповідний двосторонній або багатосторонній міжнародний договір. Відповідно до чинного законодавства укладання міжнародних угод здійснюється згідно з вимогами Закону України від 29 червня 2004 року № 1906-IV «Про міжнародні угоди». Зазначена процедура може застосовуватися від імені України, від імені Уряду України, а також міністерствами та іншими центральними органами виконавчої влади, державними органами – від імені міністерств, інших центральних органів виконавчої влади, державних органів у порядку, встановленому Кабінетом Міністрів України.

Підпунктом 75 Положення про Міністерство юстиції України, затвердженого постановою Кабінету Міністрів України від 2 липня 2014 р. № 228, встановлено, що Міністерство виконує функції центрального засвідчувального органу, зокрема забезпечує взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг. Однак юридичних механізмів забезпечення визнання іноземних сертифікатів на сьогодні не створено. Крім того, не у всіх країнах національні системи цифрового підпису керуються органами юстиції, що ускладнює застосування механізму міжвідомчих угод, а процес укладання міжнародних угод досить тривалий і кропіткий, причому внесення змін у міжнародні акти за необхідності здійснюється вкрай неоперативно.

Статтею 38 Закону визначено використання інформаційно-телекомунікаційної системи центрального засвідчувального органу для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, що встановлюється окремим Порядком, який затверджує Кабінет Міністрів України. Наразі такий порядок не визначений.

Функціонування інформаційно-телекомунікаційної системи центрального засвідчувального органу здійснюється відповідно до Наказу Міністерства юстиції України від 05.11.2018 № 3439/5 «Про затвердження Регламенту центрального засвідчувального органу». Цей нормативно-правовий акт дає визначення інформаційно-телекомунікаційної системі ЦЗО (ІТС ЦЗО) та встановлює, що Адміністратор ІТС ЦЗО – державне підприємство «Дія» Міністерства цифрової трансформації – здійснює технічне та технологічне забезпечення виконання функції використання ІТС ЦЗО для визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав. Однак Регламент ЦЗО не встановлює ні порядку юридичного визнання іноземних довірчих послуг та іноземних електронних підписів, ні технічних процедур, які повинні забезпечувати цей порядок.

Отже, мусимо констатувати, що в Україні використання іноземних довірчих послуг та визнання іноземних електронних підписів реалізується виключно в комерційній сфері за згодою і на умовах сторін, учасників комерційних угод. Правове регулювання відносин, пов'язаних із визнанням в Україні іноземних електронних підписів, наразі законодавством регулюється формально [130].

Загалом відсутність загальної основи для безпечної електронної взаємодії між підприємствами, громадянами й державними органами викликає недовіру державних і приватних онлайн-послуг, електронного бізнесу та електронної торгівлі, тим самим суттєво зменшуючи їхню ефективність та попит.

Враховуючи суттєвий прогрес у цифровізації всіх сфер діяльності держави, прагнення населення та органів державної влади долучитися до інформаційних сервісів, які створені багатьма країнами, розширити можливості електронної комерції, е-банкінгу, е-здоров'я, е-освіти та інших сфер діяльності, доцільно запровадити ідеальну (гіпотетичну) модель

суспільних відносин у сфері електронного підпису та електронних довірчих послуг.

Як приклад гіпотетичної правової моделі пропонуємо використати проєкцію Моделі OSI (EMBBC) (Open Systems Interconnection Basic Reference Mode) – абстрактної мережевої моделі для комунікацій і розробки мережевих протоколів. У ній закладено принцип рівневого підходу, де кожен рівень обслуговує свою частину процесу, що дає системі прозорість, простоту і взаємодію.

Чинна правова модель регулювання суспільних відносин у сфері електронних довірчих послуг (див. рис. 3.1) полягає в такому.

1. Перший рівень правової моделі призначений для взаємодії між підписувачами – фізичними та юридичними особами під час використання електронних довірчих послуг. На цьому рівні встановлюються права й обов'язки суб'єктів.

2. Другий рівень правової моделі призначений для правового регулювання діяльності фізичних, юридичних осіб, органів державної влади, які надають електронні довірчі послуги. На цьому рівні встановлюються права й обов'язки суб'єктів цієї сфери.

3. Третій рівень моделі забезпечує правове регулювання діяльності органів державної влади та Національного банку України у сфері електронних довірчих послуг. Правове регулювання здійснює Міністерство цифрової трансформації України, а функцію контролю – Державна служба спеціального зв'язку та захисту інформації.

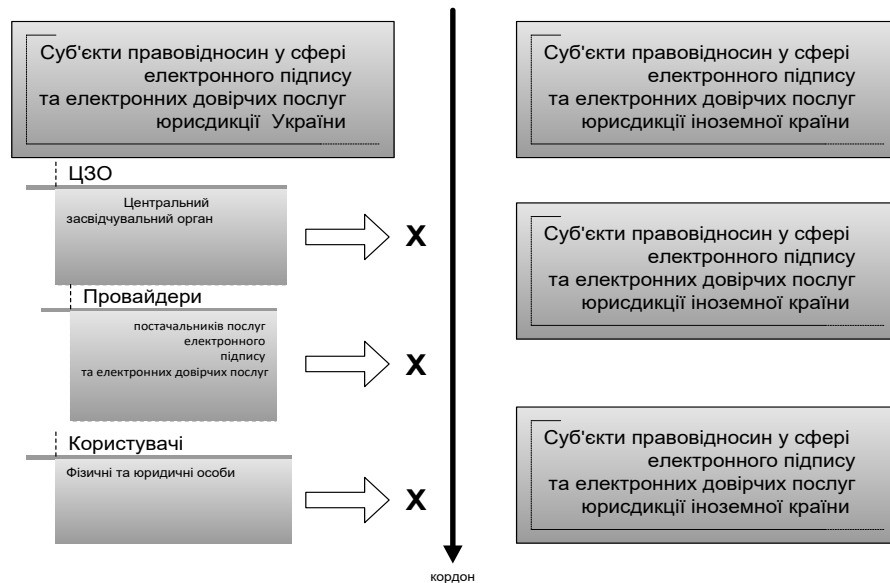


Рис 3.1. Чинна модель регулювання суспільних відносин у сфері електронних довірчих послуг

Основною проблемою такої соціальної моделі є відсутність довіри до інформаційно-комунікаційних технологій взагалі і, зокрема, у частині здійснення суспільних відносин із застосуванням технологій електронного підпису. У більшості випадків громадяни не можуть використати свої електронні підписи для отримання електронних послуг в іншій державі, оскільки національні системи електронного підпису іноземні електронні підписи не визнають. Це призводить до того, що суб'єкти сфери електронних підписів не мають можливості ознайомитися або перевірити інформацію, яка міститься в іноземних сертифікатах електронних підписів. Крім того, відсутність загальної унормованої системи транскордонного надання електронних довірчих послуг та суттєві відмінності різних юрисдикцій ускладнюють використання їх як доказів у ході судового розгляду в інших державах, оскільки саме національне законодавство визначає умови надання юридичної сили електронним довірчим послугам. Також суттєво ускладнена кореляція між національними нормами, які визначають основні положення та дефініції понять у цій сфері [131].

Загалом відсутність загальної основи для безпечної електронної взаємодії між підприємствами, громадянами та державними органами

викликає недовіру до державних і приватних електронних довірчих послуг, електронного бізнесу та електронної торгівлі, чим суттєво зменшує їхню ефективність та попит.

Існує потреба глибокого порівняльного аналізу міжнародного, світового та законодавства окремих країн у галузі електронних підписів для визначення схожості та відмінностей, колізій та спорідненості правових норм, із урахуванням практик їхнього застосування. У цьому сенсі українські правознавці та фахівці інформаційного права повинні забезпечити передумови створення унікальної моделі правового та технічно-юридичного регулювання вітчизняної інфраструктури відкритого ключа, яка забезпечить швидку транскордонну інтеграцію національних та іноземних електронних підписів.

Враховуючи викладене, можемо констатувати, що в Україні чинна модель суспільних відносин у сфері електронного підпису має суттєві недоліки, що ускладнює інтеграцію нашої держави у світ транскордонних електронних послуг і значно обмежує економічний потенціал країни загалом. Розвиток законодавства й запровадження запропонованої нової моделі суспільних відносин надасть можливість застосовувати поліпшені норми права для визнання іноземних електронних підписів.

Це, своєю чергою, сприятиме підвищенню рівня суспільної довіри до інформаційно-комунікаційних технологій, доступності для населення й бізнесу електронних підписів, електронних довірчих послуг, онлайн-послуг та електронних транзакцій, які задіяні на міжнародному ринку. Також значно зросте відповідальність суб'єктів сфери електронних довірчих послуг за шкоду, завдану будь-якій фізичній або юридичній особі в результаті недотримання зобов'язань. Запровадження механізму державної верифікації електронних довірчих послуг дозволить чітко відрізнити кваліфіковані довірчі послуги від інших електронних послуг та сприятиме підвищенню прозорості електронної комерції.

Взаємне визнання сертифікатів електронних підписів спростить доступ до внутрішніх ринків і дозволить вести транскордонну діяльність, не стикаючись із численними перешкодами під час взаємодії з суб'єктами іноземних держав.

3.2. Загальні правові підходи до вдосконалення національного законодавства щодо визнання іноземних електронних довірчих послуг

На сьогодні світова загальна соціальна модель сфери електронного підпису функціонує одночасно на двох рівнях: міжнародному та національному. На міжнародному рівні правове регулювання здійснюється Типовими законами ЮНСІТРАЛ. На національному рівні регулювання забезпечується законодавством, яке створювалося на основі міжнародних Типових законодавчих актів з урахуванням особливостей національних юрисдикцій. Так, суб'єкти суспільних відносин створюють електронні підписи й використовують їх для укладання угод, отримання електронних сервісів та електронних довірчих послуг. Для забезпечення процедур та процесів транскордонного визнання суб'єкти як користувачі сертифікатів іноземних електронних підписів та електронних довірчих послуг застосовують механізми використання іноземних електронних підписів на принципах: «за умови згоди сторін», визнання міждержавними угодами або міждержавними спеціалізованими актами.

Чинна модель суспільних відносин не вирішує важливі проблеми, до яких слід віднести:

- відсутність єдиного правового регулювання порядку та процедур транскордонного визнання іноземних електронних підписів, а також єдиного глосарію правових норм та понять у галузі електронного підпису різних юрисдикцій;
- неможливість практичного застосування доктринального тлумачення міжнародного права в галузі електронного підпису стосовно визнання електронних довірчих послуг тільки за умови участі третьої сторони, яка надає електронні довірчі послуги або здійснює їхню верифікацію;
- застосування одночасно двох рівнів довіри визнання іноземних електронних підписів та електронних довірчих послуг: за принципом «згоди

сторін» та за умови їхньої верифікації третьою стороною як незалежним суб'єктом правовідносин у сфері цифрового підпису;

- спрямованість законодавства України в напрямі інтеграції виключно в законодавче поле Європейського Союзу та ігнорування регуляторного наближення до законодавств інших країн світу;

- невизначеність юридичної відповідальності за порушення прав і обов'язків суб'єктів, визначених Законом України «Про електронні довірчі послуги» [132].

Чинна трирівнева правова модель регулювання суспільних відносин у сфері електронного підпису та електронних довірчих послуг на сьогодні не забезпечує в повному обсязі правовідносини між громадянами, юридичними особами, органами державної влади, іноземними суб'єктами права. Фактично склалися передумови створення нової унікальної моделі правового регулювання вітчизняної інфраструктури відкритого ключа, яка не тільки усуне недоліки, але й забезпечить швидку та надійну процедуру визнання національних та іноземних електронних підписів.

З урахуванням зазначеного вище чинну правову модель доцільно модернізувати та доповнити окремим четвертим рівнем, а також ввести в законодавство нові норми, поняття та суб'єкти, тобто застосувати більш сучасну правову модель [133].

На сьогодні в Україні більшість електронних послуг надається органами державної влади та місцевого самоврядування, тобто за участі держслужбовців. Запроваджується система електронного документообігу державного значення із застосуванням електронних підписів, на важливості якої наголошував К.О. Линьов [134]. У 2019 році Національним агентством України з питань державної служби програмного забезпечення для запуску в Україні за підтримки European Union in Ukraine та World Bank Ukraine розпочато розробку інформаційної системи управління людськими ресурсами на державній службі HRMIS, що дозволить державним органам працювати в єдиній системі, яка об'єднає інформацію про структуру та

штатний розклад, посади державної служби, особові справи державних службовців, нарахування й оплати праці, відпустки, кар'єрні досягнення, професійну компетентність та навчання. Зважаючи на це, доцільно покласти на Національне агентство України з питань державної служби процедуру надання державним службовцям електронних підписів відповідно до займаної посади.

Так, з метою впорядкування правовідносин у сфері управління державною службою та необхідності застосування формалізованих державних електронних підписів та електронних довірчих послуг необхідно внести зміни до Закону України «Про електронні довірчі послуги», виклавши статтю 5 розділу II в такій редакції:

«Стаття 5. Система органів, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації

1. Державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації здійснюють:

Кабінет Міністрів України;

головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг та виконання функцій центрального засвідчувального органу шляхом створення умов для функціонування суб'єктів правових відносин у сфері електронних довірчих послуг;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

центральний орган виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування;

Державний цифровий довірчий центр (третя довірча сторона);

Національний банк України (у банківській системі України)».

Таким чином, впорядковується виконання Постанови Кабінету Міністрів України від 18 вересня 2019 р. № 856 «Питання Міністерства цифрової трансформації», а також вводяться два нових суб'єкти сфери електронного підпису та електронних довірчих послуг: Державний цифровий довірчий центр (третя довірча сторона) та центральний орган виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування. З метою визначення повноважень останнього пропонується статтю 10 Розділу II викласти в такій редакції:

«Стаття 10. Повноваження центрального органу виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування

1. До повноважень центрального органу виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування, належить:

створення та ведення реєстру посад державних службовців в органі державної влади або іншому державному органі та посад служби в органах місцевого самоврядування;

забезпечення державних службовців, органів державної влади, службовців органів місцевого самоврядування та органів місцевого самоврядування кваліфікованими електронними підписами».

Оскільки новою редакцією статті 10 Розділу II Закону вводиться новий суб'єкт правовідносин, який здійснює регуляторну політику у сфері використання електронного підпису та електронних довірчих послуг державними службовцями і працівниками органів державної влади та місцевого самоврядування, доцільно внести такі зміни до Закону:

Статтю 22 Розділу II після частини 6 доповнити частиною 7 такого змісту:

«Ідентифікація особи державного службовця та посадової особи місцевого самоврядування, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа для виконання посадових повноважень, здійснюється за умови її особистої присутності й за паспортом громадянина України та в порядку, встановленому Кабінетом Міністрів України».

Частину 1 статті 23 Розділу II після абзацу 3 доповнити абзацом 4 такого змісту:

«державного службовця та посадової особи місцевого самоврядування: обов'язкові відомості визначаються Кабінетом Міністрів України додатково за вимогами, встановленими органом державної влади та місцевого самоврядування».

Частину 1 статті 25 Розділу II після пункту 1 доповнити пунктом 2 такого змісту:

«подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про скасування виданого йому або державним службовцям органу державної влади або посадової особи органу місцевого самоврядування кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача та особи уповноваженого представника державного органу та органу місцевого самоврядування».

У зв'язку з цим пункт 2 вважати пунктом 3;

Частину 6 статті 25 Розділу II доповнити абзацом 1 такого змісту:

«подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про блокування виданого йому або державним службовцям органу державної влади або посадової особи органу місцевого самоврядування кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача та особи уповноваженого представника державного органу та органу місцевого самоврядування».

У зв'язку з цим абзаци 1, 2, 3 вважати абзацами 2, 3, 4.

Частину 10 статті 25 Розділу II доповнити абзацом 1 такого змісту:

«подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа)».

Зважаючи на реальну проблему низької довіри громадян до електронних підписів та електронних довірчих послуг, численні правопорушення в цій сфері, незаконне створення та використання електронних підписів, шахрайство та зловживання із використанням електронних підписів потребують реагування і вжиття заходів державного примусу. Існує нагальна потреба та вимога дієвого врегулювання суспільних взаємовідносин, що виникають між суб'єктами першого рівня моделі, у частині підвищення відповідальності суб'єктів за вчинені правопорушення із використанням електронних підписів.

Чинним законодавством, що регулює правовідносини в інформаційній сфері, нормами цивільно-правового, трудового, адміністративного та кримінального законодавства встановлено відповідальність за порушення визначених інформаційно-правових норм. Так, Кодекс України про адміністративні правопорушення передбачає адміністративну

відповідальність за порушення права на окремі види інформації, відмову в наданні інформації, надання неповної інформації або недостовірної інформації. До правопорушень в інформаційній сфері можна віднести понад 50 статей, які розміщені в кодексах України, їхніх розділах і стосуються різних видів інформації та інформаційної діяльності, наприклад, стаття 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю» або стаття 362 «Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» [135]. Дисциплінарну відповідальність за проступок в інформаційній сфері несуть працівники підприємств установ і організацій відповідно до положень, статутів, правил та інших нормативних актів [136].

Водночас національне законодавство не містить положень, які б дозволили оперувати визначеннями відповідальності у сфері електронного підпису та електронних довірчих послуг. У законодавстві відсутній склад правопорушень у цій сфері, тобто взагалі законом не встановлено сукупність об'єктивних та суб'єктивних ознак, наявність яких може характеризувати певні діяння як правопорушення, вчинене з електронним підписом та електронними довірчими послугами, відповідно, не встановлено й видів державного примусу за порушення законодавства.

Таким чином, чинний Закон потребує доповнення імперативними нормами матеріального права, які б носили заохочувальний характер, а саме: встановлювали загальнообов'язкові форми юридичної відповідальності за порушення громадянами та юридичними особами зобов'язань, встановлених Законом України «Про електронні довірчі послуги». Взаємовідносини, що виникають між суб'єктами другого рівня моделі, також потребують врегулювання в частині доповнення норм юридичної відповідальності за порушення прав та обов'язків кваліфікованих надавачів електронних довірчих послуг.

Враховуючи зазначене, пропонується передбачити відповідальність підписувачів/користувачів електронних довірчих послуг та викласти статтю 12 Закону України «Про електронні довірчі послуги» в такій редакції:

«Стаття 12. Права, обов'язки та відповідальність користувачів електронних довірчих послуг

1. Користувачі електронних довірчих послуг мають право на:

отримання електронних довірчих послуг;

вільний вибір надавача електронних довірчих послуг;

оскарження в судовому порядку дій чи бездіяльності надавачів електронних довірчих послуг та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг;

відшкодування завданої їм шкоди та захист своїх прав і законних інтересів;

звернення із заявою про скасування, блокування та поновлення свого сертифіката відкритого ключа.

2. Користувачі електронних довірчих послуг зобов'язані:

забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;

невідкладно повідомляти надавача електронних довірчих послуг про підозру або факт компрометації особистого ключа;

надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;

своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між надавачем та користувачем електронних довірчих послуг;

своєчасно надавати надавачу електронних довірчих послуг інформацію про зміну ідентифікаційних даних, які містить сертифікат відкритого ключа;

не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування сертифіката відкритого ключа.

3. Захист прав користувачів електронних довірчих послуг, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України «Про захист прав споживачів».

4. Порушення користувачами електронних довірчих послуг законодавства про електронні довірчі послуги:

порушення правил використання електронних підписів та електронних довірчих послуг,

виготовлення з метою збуту чи збут свідомо незаконно створених електронних підписів,

подання кваліфікованими надавачами електронних довірчих послуг завідомо неправдивої інформації та ідентифікаційних даних особи для створення підроблених електронних підписів,

створення умов для компрометації та компрометація особистого ключа електронного підпису,

використання створених або отриманих у шахрайському або незаконному порядку електронних підписів, кваліфікованих сертифікатів відкритих ключів, кваліфікованих електронних підписів, паролів або будь-яких інших унікальних ідентифікаційних даних особи для доступу або несанкціонованого втручання в роботу систем електронних виборів, а також систем державних адміністративних послуг, електронного суду, державних інформаційних ресурсів та реєстрів, мережі державного управління,

незаконне копіювання, зберігання або розповсюдження персональних чи будь-яких інших унікальних ідентифікаційних даних особи, які використовуються для створення електронних підписів та електронних довірчих послуг,

тягне за собою відповідальність відповідно до закону».

Також пропонується встановити юридичну відповідальність за порушення прав та обов'язків кваліфікованих надавачів електронних довірчих послуг, для чого статтю 13 Закону України «Про електронні довірчі послуги» викласти в такій редакції:

«Стаття 13. Права, обов'язки та відповідальність кваліфікованих надавачів електронних довірчих послуг

1. Кваліфіковані надавачі електронних довірчих послуг мають право: надавати електронні довірчі послуги з дотриманням вимог цього Закону;

отримувати документи, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться в сертифікаті відкритого ключа;

отримувати консультації від центрального засвідчувального органу або засвідчувального центру з питань, пов'язаних із наданням електронних довірчих послуг;

звертатися до органів щодо оцінки відповідності для отримання документів про відповідність;

звертатися із заявою про скасування, блокування або поновлення сформованих у центральному засвідчувальному органі або засвідчувальному центрі кваліфікованих сертифікатів відкритих ключів;

самостійно обирати, які саме стандарти будуть ними застосовуватися при наданні довірчих послуг із переліку стандартів, визначеного Кабінетом Міністрів України, крім сфери спеціального зв'язку.

2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:

захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства;

функціонування програмно-технічного комплексу, що ними використовується, та захист інформації, що в ньому обробляється, відповідно до вимог законодавства;

створення та функціонування свого вебсайту;

впровадження, підтримання в актуальному стані та публікацію на своєму вебсайті реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;

цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів;

скасування, блокування та поновлення сертифікатів відкритих ключів відповідно до вимог цього Закону;

встановлення під час формування сертифіката відкритого ключа належності відкритого ключа та відповідного йому особистого ключа підписувачу чи створювачу електронної печатки;

внесення ідентифікаційних даних підписувача чи створювача електронної печатки до відповідного сертифіката відкритого ключа;

інформування органу контролю про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, не пізніше 24 годин з моменту, коли їм стало відомо про таке порушення;

інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, не пізніше двох годин з моменту, коли їм стало відомо про такі порушення;

унеможливлення використання особистого ключа в разі його компрометації;

постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів;

внесення коштів на поточний рахунок із спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське

обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути заподіяна користувачам таких послуг чи третім особам унаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов'язань, у розмірі, визначеному частиною третьою статті 16 цього Закону;

наймання працівників, які володіють необхідними для надання кваліфікованих електронних довірчих послуг знаннями, досвідом і кваліфікацією, зокрема у сферах інформаційних технологій та захисту інформації;

використання під час надання електронних довірчих послуг виключно кваліфікованих сертифікатів, засвідчених у центральному засвідчувальному органі чи засвідчувальному центрі;

зберігання документів, поданих користувачами для отримання електронних довірчих послуг;

інформування органу контролю та центрального засвідчувального органу або засвідчувального центру про будь-які зміни у процедурі надання електронних довірчих послуг протягом 48 годин з моменту настання таких змін;

передачу центральному засвідчувальному органу або засвідчувальному центру документованої інформації в разі припинення діяльності з надання електронних довірчих послуг.

3. Обов'язкові вимоги до кваліфікованих надавачів електронних довірчих послуг, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

4. Порухення кваліфікованими надавачами електронних довірчих послуг законодавства про електронні довірчі послуги:

порушення правил створення, надання, використання та знищення електронних підписів та електронних довірчих послуг;

виготовлення з метою збуту чи збут свідомо незаконно створених електронних підписів;

створення умов для компрометації та компрометація особистого ключа електронного підпису;

використання створених або отриманих у шахрайському або незаконному порядку електронних підписів, кваліфікованих сертифікатів відкритих ключів, кваліфікованих електронних підписів, паролів або будь-яких інших унікальних ідентифікаційних даних особи для доступу або несанкціонованого втручання в роботу систем електронних виборів, а також систем державних адміністративних послуг, електронного суду, державних інформаційних ресурсів та реєстрів, мережі державного управління,

незаконне копіювання, зберігання або розповсюдження даних, зокрема персональних, чи будь-яких інших унікальних ідентифікаційних даних особи, які використовуються для створення електронних підписів та електронних довірчих послуг, передбачає відповідальність відповідно до закону».

Третій рівень моделі повинен забезпечувати правове регулювання діяльності органів державної влади у сфері електронного підпису та електронних довірчих послуг у частині забезпечення державних службовців та посадових осіб місцевого самоврядування електронними атрибутами повноважень згідно з посадою – кваліфікованими електронними підписами загальнодержавного зразка.

Новий, четвертий, рівень моделі має за мету створити правові умови взаємодії та довіри між суб'єктами сфери електронного підпису та електронних довірчих послуг не тільки в національному правовому полі, але й з відповідними суб'єктами іноземних юрисдикцій. Юридичні механізми четвертого рівня моделі повинні забезпечити надійні процедури визнання іноземних електронних підписів та електронних довірчих послуг, визнання або підтвердження достовірності процедур ідентифікації підписувачів/надавачів електронного підпису, мають стати правовим і

технічним шлюзом у межах України, а також між юрисдикціями та технологіями різних країн та українським законодавством (див. рис. 3.2).

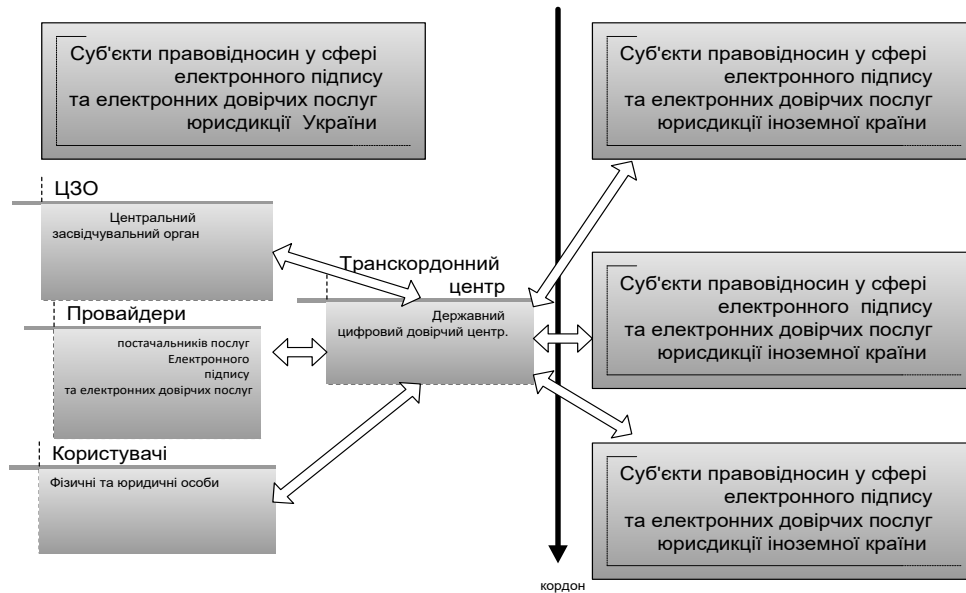


Рис. 3.2. Удосконалена модель регулювання суспільних відносин у сфері електронних довірчих послуг

Забезпечення надійної взаємодії суб'єктів послуг електронного підпису не тільки в національному правовому полі, але й з суб'єктами іноземних юрисдикцій, тобто в транскордонному режимі, доцільно здійснювати шляхом створення Державного довірчого центру (третья довірча сторона) (далі – Державний довірчий центр). Державний довірчий центр має координувати діяльність органів державної влади, надавачів довірчих послуг та користувачів довірчих послуг у напрямі транскордонної взаємодії між закордонними користувачами та надавачами довірчих послуг щодо забезпечення правових механізмів визнання іноземних електронних підписів, забезпечувати надійні процедури верифікації та виступати третьою довірчою стороною у взаємовідносинах між Україною та іноземними країнами та союзами країн у будь-яких взаємовідносинах у сфері електронного підпису [137].

Сучасна модель суспільних відносин може функціювати в такий спосіб. Будь-який суб'єкт відносин під час використання електронного підпису отримає вільний інформаційний доступ до даних будь-якого сертифіката електронного підпису в Україні та іноземного електронного підпису, з яким державний довірчий центр матиме відносини, встановлені законом. Державний довірчий центр від імені держави Україна виступатиме гарантом надійності та довіри будь-яких електронних підписів, створених відповідно до законодавства, та забезпечить надійні юридичні процедури визнання іноземних електронних підписів, визнання або підтвердження достовірності процедур ідентифікації підписувачів/надавачів електронного підпису. Державний довірчий центр виступатиме надійним правовим і технологічним шлюзом між юрисдикціями та технологіями різних країн у сфері електронного підпису й українським законодавством.

Державний довірчий центр має координувати діяльність органів державної влади, надавачів довірчих послуг та користувачів довірчих послуг у напрямі транскордонної взаємодії між зарубіжними користувачами та надавачами довірчих послуг щодо забезпечення правових механізмів визнання іноземних електронних підписів, а також надійної верифікації будь-якого електронного підпису, виданого в Україні або в іноземній країні, за певних правових умов.

Зважаючи на це, доцільно доповнити Закон низкою норм, що регулюватимуть діяльність Державного довірчого центру у сфері електронного підпису та процедур визнання іноземних електронних підписів та електронних довірчих послуг, а саме:

частину 1 статті 1 Розділу 1 після пункту 44 доповнити новим пунктом 45 такого змісту:

«Державний цифровий довірчий центр (третя довірча сторона) – державне підприємство, яке забезпечує інтероперабельність національних технічних, техніко-юридичних та юридичних норм, що використовуються під час надання електронних послуг, механізми визнання іноземних електронних

підписів і електронних довірчих послуг та транскордонну взаємодію надавачів та користувачів довірчих послуг».

1) Частину 1 статті 7 Розділу II після абзацу 17 доповнити абзацом 18 такого змісту:

«управління та контролю Державного цифрового довірчого центру (третьої довірчої сторони), що забезпечує механізми визнання іноземних електронних підписів та електронних довірчих послуг, транскордонну взаємодію надавачів та користувачів довірчих послуг».

2) Статтю 7 Розділу II після частини 3 доповнити частиною 4 такого змісту:

«Технічне, технологічне та правове забезпечення виконання функцій третьої довірчої сторони у сфері електронного підпису та електронних довірчих послуг здійснюється Державним цифровим довірчим центром (третьою довірчою стороною) – державним підприємством, яке належить до сфери управління головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних підписів та електронних довірчих послуг».

3) Розділ II після статті 7 доповнити статтею 7-1 такого змісту:

«Стаття 7-1. Повноваження Державного цифрового довірчого центру (третя довірча сторона)

До повноважень Державного цифрового довірчого центру (третя довірча сторона) належать:

виступати третьою довірчою стороною у взаємовідносинах між Україною та іноземними країнами й союзами країн у будь-яких взаємовідносинах у сфері електронного підпису та електронних довірчих послуг;

узгоджувати порядок визнання та відповідності вимогам законодавства України електронних підписів та електронних довірчих послуг, що надаються іноземними надавачами/постачальниками (окремими суб'єктами іноземної держави) відповідно до вимог нормативно-правових актів, які

регулюють правові відносини у сфері електронних довірчих послуг в іноземних державах та в Україні;

спільно з уповноваженими органами державної влади брати участь у підготовці міжнародних угод у сфері електронного підпису та електронних довірчих послуг, готувати пропозиції щодо відповідності технічних та юридичних норм законодавства сторін міждержавної угоди у сфері електронного підпису, узгоджувати процедури визнання та верифікації, рівні ідентифікації підписувачів/надавачів електронного підпису, а також визначати юрисдикцію, у якій будуть здійснюватися розгляди спірних питань;

забезпечувати інтероперабельність та координувати технологічну діяльність національних суб'єктів сфери електронних довірчих послуг, електронної ідентифікації та державних електронних послуг;

виступати під час судових спорів третьою особою, яка не заявляє самостійних вимог щодо предмета спору для захисту особистих суб'єктивних прав та інтересів у сфері електронного підпису та електронних довірчих послуг, що охороняються законом;

за заявою суб'єктів договірних відносин у разі укладання угод в електронному вигляді здійснювати верифікацію електронних підписів та електронних довірчих послуг підписантів, надавати або долучати до угоди електронну верифікаційну позначку, якою підтверджуються дійсність національних або іноземних електронних підписів, електронних довірчих послуг та даних ідентифікації, які використовують сторони угоди;

за заявою суб'єктів договірних відносин у разі укладання угоди в електронному вигляді здійснювати захист майнових інтересів фізичних осіб та юридичних осіб у разі настання певних подій (страхових випадків), визначених угодою або чинним законодавством, за рахунок грошових фондів, що формуються шляхом сплати суб'єктами договірних відносин страхових платежів (страхових внесків, страхових премій) та доходів від

розміщення коштів цих фондів, відповідно до Закону України «Про страхування».

4) Частину 2 статті 16 Розділу II викласти в такій редакції:

«Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному рахунку із спеціальним режимом використання в банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менш ніж 100 мінімальних розмірів заробітної плати.

Діяльність іноземних кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом Державного цифрового довірчого центру (третя довірча сторона) для страхування цивільно-правової відповідальності або забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам».

5) Статтю 38 Розділу VI доповнити частиною 3 такого змісту:

«Внесення до Довірчого списку України кваліфікованого надавача електронних довірчих послуг, що відповідає умовам п.п. 1 п. 1 ст. 38 цього Закону, за його заявою може здійснюватися Державним цифровим довірчим центром без укладання між іноземною державою та Україною відповідного двостороннього або багатостороннього міжнародного договору за погодженням Центрального засвідчувального органу».

6) Статтю 38 Розділу VI доповнити частиною 4 такого змісту:

«Порядок використання інформаційно-телекомунікаційної системи Державного цифрового довірчого центру (третя довірча сторона) для забезпечення визнання в Україні електронних довірчих послуг, іноземних

сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, встановлюється Кабінетом Міністрів України».

У разі практичної реалізації запропонованої удосконаленої правової моделі регулювання суспільних відносин у сфері електронного підпису, електронних довірчих послуг можливо очікувати такі позитивні досягнення:

поліпшення довіри у суспільних відносинах до сфери електронних довірчих послуг та електронної ідентифікації, особливо під час здійснення транскордонної взаємодії між Україною та країнами світу;

створення державної третьої довірчої сторони суттєво сприятиме поліпшенню бізнесу в Україні, активізує електронну транскордонну торгівлю та інші транскордонні електронні сервіси;

запровадження відповідальності за порушення у сфері електронного підпису та довірчих послуг призведе до поліпшення правової гігієни та зменшення ризиків скоєння правопорушень із використанням електронного підпису серед суб'єктів сфери електронного підпису, що сприятиме росту довіри у населення до інформаційних технологій і цифрових послуг, поширенню використання електронного підпису як надійного засобу електронної ідентифікації особи під час електронної взаємодії з державою;

забезпечення цифровізації державних органів та органів місцевого самоврядування, що стане основою державного електронного документообігу, шляхом надання посадовій особі органу державного управління надійного засобу електронної ідентифікації – державного кваліфікованого електронного підпису з зафіксованими в сертифікаті відповідними повноваженнями, правами та обов'язками.

Висновки до розділу 3

1. Констатовано необхідність створення у сфері електронного підпису третьої довірчої сторони у взаємовідносинах між Україною та іноземними країнами й союзами країн у сфері електронного підпису та електронних довірчих послуг. Доведено необхідність забезпечення надійних процедур визнання іноземних електронних підписів та електронних довірчих послуг, визнання або підтвердження достовірності процедур ідентифікації підписувачів/надавачів електронного підпису шляхом створення правового й технічного шлюзу між юрисдикціями й технологіями різних країн та українським законодавством.

2. Звернено увагу на необхідність забезпечення додаткового правового регулювання діяльності органів державної влади у сфері електронного підпису шляхом введення для державних службовців кваліфікованого електронного підпису загальнодержавного зразка.

3. За результатами аналізу виявлено недоліки у визначенні юридичних прав, обов'язків та відповідальності за їх порушення у суб'єктів сфери електронного підпису. Суспільні взаємовідносини, що виникають між суб'єктами, потребують доповнення імперативними нормами матеріального права, які б носили заохочувальний характер, зокрема встановлювали загальнообов'язкові форми юридичної відповідальності за порушення громадянами та юридичними особами зобов'язань, встановлених законодавством.

4. Запропоновано авторські визначення понять «компрометація особистого ключа цифрового підпису» та «державний цифровий довірчий центр (третя сторона)», а також удосконалено дефініції термінів «транскордонні електронні довірчі послуги», «транскордонні електронні послуги».

5. Констатовано відсутність загальної унормованої системи транскордонного надання електронних підписів та суттєві відмінності різних

юрисдикцій, що ускладнюють використання їх як доказів у ході судового розгляду в інших державах, оскільки саме національне законодавство визначає умови надання юридичної сили електронним довірчим послугам.

6. У результаті аналізу чинної моделі суспільних відносин у сфері електронного підпису та електронних довірчих послуг виявлено ряд недоліків та потреб суттєвого вдосконалення механізму правового регулювання зазначених суспільних відносин.

7. Запропоновано сучасну модель суспільних відносин у сфері електронного підпису та електронних довірчих послуг. Наголошено на необхідності забезпечення надійної взаємодії суб'єктів послуг електронного підпису не тільки в національному правовому полі, але й із суб'єктами іноземних юрисдикцій, тобто шляхом створення третьої довіреної сторони, яка гарантуватиме надійність та достовірність правових механізмів визнання іноземних електронних підписів.

8. Обґрунтовано включення окремого розділу «Державний електронний довірчий центр» до структури Закону України «Про електронні довірчі послуги». Обґрунтовано права, обов'язки нового суб'єкта, зокрема в частині забезпечення порядку визнання та відповідності вимогам законодавства України електронних підписів та електронних довірчих послуг, що надаються іноземними надавачами/постачальниками (окремими суб'єктами іноземної держави), створеними відповідно до вимог нормативно-правових актів у сфері електронних довірчих послуг в іноземних державах.

9. Звернено увагу на необхідність забезпечення додаткового правового регулювання діяльності органів державної влади у сфері електронного підпису та електронних довірчих послуг шляхом введення для державних службовців кваліфікованого електронного підпису загальнодержавного зразка. Надано пропозицію покласти на Національне агентство України з питань державної служби право державної регуляції в напрямі впорядкування використання кваліфікованих електронних підписів

службовцями державних органів та органів місцевого самоврядування, зокрема в міждержавних відносинах.

ВИСНОВКИ

Дисертація є першою в Україні комплексною науковою працею, в якій вирішується важливе наукове завдання з формування теоретико-методологічних та практичних положень щодо правового забезпечення транскордонного надання електронних довірчих послуг шляхом удосконалення національного законодавства, що сприятиме ефективній реалізації стратегії цифрової трансформації України.

На основі проведеного дослідження сформульовано такі головні висновки та пропозиції, що мають важливе теоретичне й практичне значення.

1. Складовими сучасних суспільних інформаційних відносин є швидкий обмін цифровою інформацією та забезпечення її актуальності, надійності, цілісності, оперативності, ідентичності, достовірності і повноти. В результаті дослідження історичних процесів трансформації суспільних відносин в суспільні інформаційні відносини, у частині, що стосується транскордонного надання електронних довірчих послуг доведено, що досвід законодавчого врегулювання застосування транскордонних довірчих послуг практично не вивчався, не узагальнювалися процедури їх транскордонного визнання.

Визначення теоретико-методологічних положень правового регулювання та удосконалення національного законодавства для створення умов для транскордонного надання електронних довірчих послуг з метою забезпечення довіри до широкого використання інформаційно-комунікаційних технологій сприятиме ефективній реалізації стратегії цифрової трансформації України.

2. Застосування загальнонаукових методів дослідження суспільних правовідносин у сфері електронних довірчих послуг надало можливість виявити особливості правовідносин із застосуванням електронних підписів, зокрема в транскордонному режимі. Отримані результати забезпечили ефективний підхід до аналізу нормативно-правових актів у цій сфері щодо

виявлення недоліків системи правового регулювання електронних підписів та електронних довірчих послуг. Результати мають загальнотеоретичне значення для аналізу суспільних відносин та процесів модернізації нормативно-правових актів, що здійснюють їх регулювання.

3. Результати аналізу міжнародних документів UNCITRAL, Ради Європи з питань електронного підпису підтверджують гіпотезу про те, що потреба в негайному юридичному врегулюванні процедур взаємного визнання іноземних електронних підписів є актуальною. Міжнародними актами встановлено загальні принципи визнання іноземних електронних підписів, однак такі процедури застосувати неможливо через їхню неврегульованість нормами права. Неврегульованість, своєю чергою, створює підстави до недовіри користувачів до електронних сервісів, електронних транзакцій, електронних довірчих послуг тощо.

4. Нормативно-правова база України, що регулює відповідальність за правопорушення у сфері цифрових технологій, зокрема у сфері електронного підпису, характеризується відсутністю правових підстав для притягнення до відповідальності суб'єктів суспільних правовідносин, які беруть участь у створенні, одержанні, використанні, зберіганні та знищенні електронних підписів, обмежується лише переліком злочинів у сфері застосування електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Зазначене не сприяє підвищенню рівня довіри громадян до електронних підписів.

5. Порівняльно-правовий аналіз національного законодавства та міжнародно-правових документів свідчить про термінологічну та нормативно-правову невизначеність або/та розбіжність в об'єктно-предметній області понять, що складають базовий термінологічний набір сфери електронного підпису. Встановлено правові розбіжності в законодавчих актах різних юрисдикцій у сфері електронного підпису, виявлено недоліки національної системи правового регулювання в цій сфері.

6. Уперше на концептуальному рівні з урахуванням досвіду розвинених країн світу та міжнародних організацій, а також тенденцій розвитку інформаційно-комп'ютерних технологій розроблено й запропоновано нову правову модель суспільних відносин у сфері електронного підпису, що дозволяє сформувати обґрунтовану сукупність правових інструментів удосконалення законодавства відповідно до потреб сучасного суспільства.

Удосконалена правова модель створює умови для проведення системного аналізу й надання правових характеристик суб'єктам, їхнім юридичним правам, обов'язкам та відповідальності, вдосконалює правові механізми транскордонного надання електронних підписів.

7. Результати аналізу нормативно-правової бази України у сфері електронного підпису довели її неефективність через виявлення факторів, які ускладнюють досягнення високого рівня довіри до даних технологій, зокрема через відсутність норм державного примусу за правопорушення у сфері цифрових технологій, у тому числі у сфері електронного підпису, а також відсутність на державному рівні ефективного підходу до правового регулювання механізмів визнання транскордонних іноземних цифрових підписів. Вивчення цих проблем, зокрема через дослідження конкретних правовідносин, принципів інформаційного права та термінологічного апарату дозволило сформувати напрями правового регулювання визнання транскордонних іноземних електронних підписів.

8. Удосконалено перелік та характеристики суб'єктів сфери електронних підписів, правові механізми запровадження загальнообов'язкової форми юридичної відповідальності підписувачів, користувачів, надавачів кваліфікованих електронних довірчих послуг, а також органів державної влади та місцевого самоврядування під час надання послуг електронних підписів.

9. Розроблено рекомендації щодо вдосконалення національного законодавства у сфері електронного підпису в частині впровадження нових понять, суб'єктів правовідносин, удосконалення процедур взаємного

визнання іноземних електронних підписів, а також запровадження правового регулювання певних інструментів юридичної відповідальності за порушення прав і обов'язків суб'єктів суспільних відносин, які отримані на основі теоретико-методологічного підходу до аналізу нормативно-правових актів щодо регулювання інструментів інформаційної взаємодії на предмет їхньої відповідності положенням теорії інформаційних правовідносин, а також на базі специфічних правових принципів інформаційної взаємодії з використанням сформульованих у роботі термінів і з урахуванням положень міжнародних документів та законодавства європейських країн.

10. Доведено, що система правового регулювання суспільних відносин, пов'язаних з інформаційною взаємодією, потребує формування власних термінів, які б відображали правову специфіку в цій сфері. Запропоновано дефініції низки термінів, зокрема: «електронна довірча послуга», «електронна послуга», «електронний підпис», «компрометація особистого ключа електронного підпису», «державний цифровий довірчий центр (третя довірча сторона)», «транскордонність», «транскордонне визнання електронного підпису або електронної довірчої послуги», «транскордонна електронна послуга», що створило умови для формування гармонізованої системи термінів, які пов'язані з правовим регулюванням визнання іноземних електронних підписів.

11. На основі розроблених рекомендацій розроблено проєкт Закону України «Про внесення змін до Закону України «Про електронні довірчі послуги». Зміст норм законопроєкту спрямований на впорядкування нормативної бази України, яка:

- поліпшить довіру в суспільних відносинах до сфери електронних довірчих послуг та електронної ідентифікації, особливо під час здійснення транскордонної взаємодії між Україною та країнами світу;
- утворить довірчий орган «Державний електронний довірчий центр», що суттєво сприятиме поліпшенню бізнесу в Україні, активізує

електронну транскордонну торгівлю та інші транскордонні електронні сервіси;

- запровадить окремі види відповідальності за порушення у сфері електронного підпису та електронних довірчих послуг, що поліпшить правову гігієну та зменшить ризики вчинення правопорушень;

- сприятиме поширенню використання електронного підпису як надійного засобу електронної ідентифікації особи під час електронної взаємодії з державою;

- покращить репутацію державних електронних сервісів, що поліпшить імідж України як цифрової держави;

- забезпечить цифровізацію органів державної служби та органів місцевого самоврядування;

- спростить процедури транскордонної взаємодії у сфері електронного підпису між Україною та суб'єктами аналогічної сфери різних юрисдикцій, а також доступ до внутрішніх ринків і дозволить вести транскордонну діяльність, оминувши численні перешкоди під час взаємодії з суб'єктами іноземних держав.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пилипчук В. Г. Становлення і розвиток інформаційного суспільства в Україні: Особливості, проблеми, правове регулювання. *Теоретико-правові основи формування та розвитку інформаційного суспільства*: матеріали науково-практичної конференції (м. Київ, 29 листопада 2017 р.) / упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. С. 7-12.
2. Арістова І. В., Чередначук В. Д. Концепція інформаційних правовідносин: сукупність та особливості використання у сфері банківської діяльності. *Інформація і право*. 2012. № 3(6). С.47-56.
3. Бачило И.Л. Информационное право : основы практической информатики : учеб. пособие ; Ин-т государства и права Рос. акад. наук. Москва : Юринформцентр : Тихомиров М. Ю., 2001. 352 с.
4. Баранов О.А. Інтернет речей: теоретико-методологічні основи правового регулювання : монографія. Київ : Видавничий дім «АртЕк». 2018. Т.1. 344 с.
5. Баранов О. А. Напрями перспективних досліджень у галузі інформаційного права. *Інформація і право*. 2016. № 2. С. 15-31.
6. Ткаченко В. В. Концептуальні засади адаптації інформаційного законодавства України до міжнародних правових стандартів в умовах розвитку інформаційного суспільства: понятійний апарат. *Правова інформатика*. 2013. № 3. С. 81-90.
7. Blythe S. E. Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. *Richmond Journal of Law & Technology*. 2005. Vol. 11(2). P. 6-8.

8. Electronic Signatures, How Valid Are They? *This We Know*, 2015. URL: <https://www.thisweknow.org/electronic-signatures-how-valid-are-they> (Last accessed: 17.03.2020)
9. Бачило И.Л., Семилетов С.И. Комментарий к Федеральному закону «Об электронной цифровой подписи» (постатейный). Краснодар: Российский государственный торгово-экономический университет, 2013. 24 с.
10. Квашнин В.И. Об условиях ведения международной электронной коммерции в России с использованием электронной цифровой подписи. *Вестник Санкт-Петербургского университета*. 2009. Вып. 3(14). С. 89-97.
11. Куракина Ю. М. Законодательное регулирование вопросов использования электронных документов и электронной цифровой подписи в Федеративной Республлик Германии. *Секретарское дело*. 2002. № 2. С.43-45.
12. Исирова Е. В., Потий А. В., Семенец В. В. Принципы построения децентрализованной инфраструктуры открытых ключей. *Радиотехника*. 2018. №. 193. С. 82-93.
13. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики / Р.А. Калюжний, М.Я. Швець, В.С. Цимбалюк, В.Д. Гавловський та ін.; за ред. Р.А. Калюжного, В.О. Шамрая; Академія державної податкової служби України. Київ : Видавництво «КВІЦ», 2002. 296 с.
14. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: Терія. Практика. Застосування : монографія. Харків : Вид-во «Форт», 2012. 880 с.
15. Мао Венбо. Современная криптография : теория и практика ; Компания Hewlett-Packard ; пер. с англ. и ред. Д. А. Ключина. Москва [и др.] : Вильямс, 2005. 763 с.
16. Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. *EUR-Lex*, 2006. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0123> they (Last accessed: 17.03.2020)

17. Горбенко Ю. І., Проблеми та вимоги до надання довірчих послуг в Європейському Союзі в період 2015–2030 рр. *Прикладная радиоэлектроника*. 2013. Т. 12, № 2. С. 184-193.

18. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. № 1678-VII. URL: https://zakon3.rada.gov.ua/laws/show/984_011 (дата звернення: 17.03.2020).

19. Фурашев В. М. Інформаційне право в інформаційному суспільстві. *Теоретико-правові основи формування та розвитку інформаційного суспільства*: матеріали науково-практичної конференції (м. Київ, 29 листопада 2017 р.) / упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. С. 19-22.

20. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в міжнародному законодавстві. *Науковий вісник публічного та приватного права*. 2018. № 4. С. 13–19.

21. Правовые аспекты автоматической обработки данных. *Комиссия Организации Объединенных Наций по праву международной торговли*: материалы семнадцатой сессии (г. Нью-Йорк, 25 июня - 11 июля 1984 г.). URL: <https://undocs.org/pdf?symbol=ru/A/CN.9/254> (дата обращения: 17.03.2020).

22. Barlow J. P. A Declaration of the Independence of Cyberspace. *Duke Law & Technology Review*. 2019. Vol. 18. No. 1. P. 5-7.

23. Типовой закон ЮНСИТРАЛ об электронной торговле и Руководство по принятию 1996 год с дополнительной статьей 5 бис, принятой в 1998 году. *Организация Объединенных Наций*. Нью-Йорк, 2006. URL: http://www.uncitral.org/pdf/russian/texts/electcom/05-89452_Ebook.pdf (дата обращения: 17.03.2020).

24. Костенко О.В. Костенко В.В. Шляхи розвитку правового регулювання електронних довірчих послуг в міжнародних актах UNCITRAL. *Приватне та публічне право*. 2019. № 1. С. 78–84.

25. Типовой закон ЮНСИТРАЛ об электронных подписях и Руководство по принятию 2001 год. *Организация Объединенных Наций*. Нью-Йорк, 2002. URL: <http://www.uncitral.org/pdf/russian/texts/electcom/ml-elecsig-r.pdf> (дата обращения: 17.03.2020).

26. Директива 1999/93/ЄС Європейського парламенту та Ради «Про систему електронних підписів, що застосовується в межах Співтовариства» : Міжнародний документ від 13.12.1999 р. № 1999/93/ЄС. URL: http://zakon3.rada.gov.ua/laws/show/994_240 (дата звернення: 17.03.2020).

27. Директива 2006/123/ЄС Європейського Парламенту і Ради «Щодо послуг на внутрішньому ринку»: Міжнародний документ від 12.12.2006 р. № 2006/123/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_906/page?text=%EF%F3%ED%EA%F2#Text (дата звернення: 17.03.2020).

28. Dismantling the obstacles to EU citizens' rights. EU Citizenship Report 2010. Brussels, 27.10.2010. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52010DC0603> (Last accessed: 17.03.2020)

29. STORK. Take your e-identity with you, everywhere in the EU. *European Commission*, 2020. URL: <https://www.eid-stork.eu/> (Last accessed: 17.03.2020)

30. Михалюк Н. Ю. Транскордонне співробітництво ЄС в рамках реалізації проектів STORK та STORK 2.0. *Інформаційне забезпечення транскордонного співробітництва України* : матеріали I Міжнародної науково-практичної Інтернет-конференції (14–15 травня 2013 р., м. Луцьк) : в 2 т. / під заг.ред. Митко А.М. Луцьк : Вежа-Друк, 2013. Т.1. С. 246 - 252.

31. Горбенко І. Д. Проблеми, протиріччя та шляхи інтеграції України в міжнародний та європейський електронний простір транскордонних довірчих послуг. *Безпека інф. в інф.-телеком. Системах* : матеріали XVI

міжнар. наук.-практ. конф. (м. Київ, 26-28 травня 2015 р.). Київ: ДССЗІ, 2015. С.128-129.

32. Honcharova Y., Eryomenko A. Stork-promising project of european transnational electronic identification. *2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*. IEEE, 2014. P. 188-189.

33. Гончарова Ю. В., Ерёмченко А. А. Stork–перспективный проект европейской транснациональной электронной идентификации. *Прикладная радиоэлектроника*. 2014. №. 13(3). С. 275-280.

34. Костенко О.В., Костенко В.В. Транскордонна ідентифікація фізичних та юридичних осіб, як елемент правового регулювання електронних довірчих послуг в Європейському союзі. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. Київ, 2018. № 29 (68). С. 90–93.

35. Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa. *Gazzetta Ufficiale* n. 63 del 17 marzo 1997. URL: <http://www.parlamento.it/parlam/leggi/97059l.htm> (Last accessed: 17.03.2020)

36. German Government Position Paper on the International Recognition of Digital Signatures. Web site of Christopher Kuner, 1998. URL: http://www.kuner.com/data/sig/gov_digsig_recognition.html. (Last accessed: 17.03.2020)

37. Dieses Bundesgesetz tritt mit Ausnahme des 5. Abschnitts mit 1. Juli 2016 in Kraft. Der 5. Abschnitt tritt mit dem der Kundmachung folgenden Tag in Kraft. Das Signaturgesetz, BGBl. I Nr. 190/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 75/2010, tritt mit Ablauf des 30. Juni 2016 außer Kraft. Bundesministerium für Digitalisierung und Wirtschaftsstandort, 2020. URL: <https://www.ris.bka.gv.at/eli/bgbl/i/2016/50/P20/NOR40184749> (Last accessed: 17.03.2020)

38. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, 7.8.2009/617. URL : <https://www.finlex.fi/fi/laki/ajantasa/2009/20090617> (Last accessed: 17.03.2020)

39. Об электронной цифровой подписи: Модельный Закон от 9 декабря 2000 г. № 16-10. *Законодательство СНГ* : база данных / Межпарламентская Ассамблея государств. URL : <http://pravo.levonevsky.org/bazazru/texts16/txt16390.htm> (дата обращения: 17.06.2020).

40. О трансграничном информационном обмене электронными документами : Модельный Закон от 25 ноября 2016 г. *Законодательство СНГ* : база данных / Межпарламентская Ассамблея государств. URL : <http://www.parliament.am/library/modelayin%20orenqner/341.pdf> (дата обращения: 17.06.2020).

41. Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations. United Nations Conference on Trade and Development, 2013. URL : https://unctad.org/en/publicationslibrary/dtlstict2013d1_en.pdf (Last accessed: 17.03.2020)

42. Utah Digital Signature Act. Utah Code §§ 46-3-101 to 46-3-504 Enacted by L. 1995, ch. 61. 1995. URL : <http://www.jus.unitn.it/USERS/PASCUZZI/privcomp97-98/documento/firma/utah/udsa.html>. (Last accessed: 17.03.2020)

43. Костенко О.В. Электронний підпис та електронні довірчі послуги в законодавстві Сполучених Штатів Америки. *Інформація і право*. – 2018. № 3 (26). С. 76–84.

44. Digital Signatures. Alex Padilla California Secretary of State, 1995. URL :

<http://www.sos.ca.gov/administration/regulations/current-regulations/technology/digital-signatures/>. (Last accessed: 17.03.2020)

45. Washington electronic authentication act. 1996. URL : <http://apps.leg.wa.gov/rcw/default.aspx?cite=19.34>. (Last accessed: 17.03.2020)

46. William E. Wyrough Jr. The Electronic Signature Act of 1996: Breaking Down Barriers to Widespread Electronic Commerce in Florida. 24 Florida State University Law Review. 1997. 407. <https://ir.law.fsu.edu/lr/vol24/iss2/5> (Last accessed: 17.03.2020)
47. Electronic authentication. State of Minnesota. Chapter 325K. 1998. URL : <https://www.revisor.leg.state.mn.us/statutes/?id=325K>. (Last accessed: 17.03.2020)
48. Electronic and Digital Signatures. Indiana State Board of Accounts. 1997. URL : <https://www.in.gov/sboa/3232.htm> (Last accessed: 17.03.2020)
49. The electronic Signature Act. Legislative Administration Committee, Policy and Research Office. 1997. URL : <http://library.state.or.us/repository/2010/201010061538333/1997.pdf>. (Last accessed: 17.03.2020)
50. Electronic Signatures and Records Act (ESRA). New York State. 1999. URL : <https://its.ny.gov/electronic-signatures-and-records-act-esra>. (Last accessed: 17.03.2020)
51. Uniform electronic transactions act. National conference of commissioners on uniform state laws. 1999. URL : http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf. (Last accessed: 17.03.2020)
52. Electronic signature in global and national commerce act. Public Law 106–229. 2000. URL : <https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf> (Last accessed: 17.03.2020)
53. Don Johnson Alfred Menezes Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security* August 2001. URL : <https://link.springer.com/article/10.1007/s102070100002> (Last accessed: 17.03.2020)

54. Johnson D., Menezes A., Vanstone S. The elliptic curve digital signature algorithm (ECDSA). *International journal of information security*. 2001. Vol. 1(1). P. 36-63.
55. Mason S. Electronic signatures in law. University of London Press, 2016. P. 476. URL : <http://stephenmason.co.uk/books/electronic-signatures-law> (Last accessed: 17.03.2020)
56. Carolina M. Laborde. Electronic Signatures in International Contracts. URL : https://books.google.com.ua/books?id=Cne-igPOkhgC&printsec=frontcover&hl=uk&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (Last accessed: 17.03.2020)
57. Костенко О.В. Костенко В.В. Особливості правового регулювання сфери електронних підписів в законодавстві країн Латинської Америки. *Право і суспільство*. 2019. № 2. С.102–110.
58. Ley 527 sobre Mensajes de Datos. Comercio Electrynico y Firma Digital de 18 de agosto de 1.999). URL : <https://co.groupseres.com/images/d/rs/Ley-527-1999.pdf> (Last accessed: 17.03.2020)
59. Ley De Firma Digital №25.506. URL : <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm> (дата звернення 12.05.2018).
60. Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias. *Infoleg*, 2001. URL : <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm> (Last accessed: 17.03.2020)
61. Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. O Presidente Da República, 2001. URL : http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-1.htm (Last accessed: 17.03.2020)

62. Digital Certification in Brazil. 2020. URL : <http://www.v-brazil.com/science/internet/digital-id/law.html> (Last accessed: 17.03.2020)
63. Ley Sobre Documentos Electronicos, Firma Electronica y Servicios de Certificaciyn de Dicha Firma No. 19.799, 25 de marzo 2002. URL : <https://www.leychile.cl/Navegar?idNorma=196640> (Last accessed: 17.03.2020)
64. Ley №18.600 de 21.09.009 Documento Y Firma Electrynica. URL : <https://www.dgi.gub.uy/wdgi/page?2,principal,Ampliacion-Normativa,O,es,0,PAG;CONC;1059;7;D;ley-no-18-600-de-21-09-009;3;PAG;> (Last accessed: 17.03.2020)
65. Ley de firma electronica avanzada texto vigente. URL : <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf> (Last accessed: 17.03.2020)
66. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в законодавстві пострадянських країн. *Право і суспільство*. 2018. № 3. С. 110–116.
67. Об электронной цифровой подписи, № 1-ФЗ. 2002. URL : <https://rg.ru/2002/01/10/podpis-dok.htm>. (дата обращения: 17.06.2020)
68. Об электронном документе и электронной цифровой подписи от 28 декабря 2009 г. № 113-З: Закон Республики Беларусь. URL : https://kodeksy-by.com/zakon_rb_ob_elektronnom_dokumente_i_elektronnoj_tsifrovoj_podpisi.htm (дата обращения: 17.06.2020)
69. Law on Electronic Signatures and Electronic Documents. 2008. URL : <https://matsne.gov.ge/ru/document/download/20866/4/en/pdf>. (Last accessed: 17.03.2020)
70. Law of the Republic of Kazakhstan On Electronic Document and Digital Signature, No 307-II. 2007. URL : <http://cis-legislation.com/document.fwx?rgn=3148>. (Last accessed: 17.03.2020)

71. Legea Republicii Moldova, cu privire la documentul electronic si semnatura digitala, Nr. 264-XV. 2004. URL : <http://lex.justice.md/viewdoc.php?id=313061&lang=1>. (Last accessed: 17.03.2020)

72. On Electronic Document and Electronic Signature. 2007. URL : http://www.parliament.am/law_docs/150105HO40eng.pdf. (Last accessed: 17.03.2020)

73. Digitaalalkirja seadus Vastu võetud. 2000. URL : Riigi Teataja. 2007. URL : <https://www.riigiteataja.ee/akt/694375> (Last accessed: 17.03.2020)

74. Elektronisko dokumentu likums. Law on Electronic Documents Act. 2003. URL : <https://likumi.lv/doc.php?id=68521>. (Last accessed: 17.03.2020)

75. Elektroninio parašo istatymas. 2000. URL : <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.105849/PMkVEwEiKo>. (Last accessed: 17.03.2020)

76. Law of the Republic of Azerbaijan on Electronic Signature and Electronic Document. 2004. URL : <http://www.e-imza.az/downloads/qanunlar/E-signature%20law/e-Signature%20Law%20English.pdf>. (Last accessed: 17.03.2020)

77. Об электронной цифровой подписи. 2007. URL : <https://digital.report/zakonodatelstvo-tadzhikistana-v-sfere-elektronnogo-pravitelstva-4/>. (дата звернення 12.07.2018).

78. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. / *Законотворчість* : база даних / Верхов. Рада України. URL : <https://zakon.rada.gov.ua/laws/show/851-15#Text> (дата звернення 29.03.2020).

79. Костенко О.В. Костенко В.В. Електронні підписи та порядок визнання іноземних сертифікатів електронних підписів в законодавстві окремих країни Азії. *Науковий вісник публічного та приватного права*. 2019. №1. С.10–106.

80. Digital Signature Act 1997. Laws of Malaysia Act 562: Reprint. The Commissioner of Law Revision, Malaysia Under The Authority of The Revision of Laws Act 1968 In Collaboration With Percetakan Nasional Malaysia Bhd, 2006
URL : <https://www.wipo.int/edocs/lexdocs/laws/en/my/my058en.pdf>. (дата звернення 10.02.2019).

81. Electronic Transactions Act (Chapter 88), 2010. URL: <https://sso.agc.gov.sg/Act/ETA2010>. (Last accessed: 17.03.2020).

82. Law of the People's Republic of China on Electronic Signatures, 2010.
URL: http://www.china.org.cn/business/2010-01/21/content_19281152.htm.
(Last accessed: 17.03.2020).

83. Wang M., Wang M. Introduction to the Electronic Signatures Law of People's Republic of China. *Digital Evidence & Elec. Signature L. Rev.* 2005. Vol. 2. P. 79-85.

84. Blythe S. E. China's new electronic signature law and certification authority regulations: A catalyst for dramatic future growth of e-commerce. *Chicago-Kent Journal of Intellectual Property*. 2007. Vol. 7. URL: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/jointpro7&div=3&id=&page=> (Last accessed: 17.03.2020).

85. Electronic Transactions Ordinance. 2000. URL: <https://www.elegislation.gov.hk/hk/cap553>. (дата звернення 12.04.2019).

86. Information Technology Act 2000. No. 21. Baker & McKenzie, 2003.
URL : <http://www.bmck.com/ecommerce/india-t.htm> (Last accessed: 17.03.2020).

87. Act on Electronic Signature and Certification Business (Japan). Act No. 102 of May 31, 2000. URL: <http://afyonluoglu.org/PublicWebFiles/e-imza/int-legislation/Japan-Act%20on%20Electronic%20Signature%20and%20Certification%20Business.pdf>.
(Last accessed: 17.03.2020).

88. Republic of Korea Digital Signatures Act, 1999. URL: <http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN042823.pdf>. (Last accessed: 17.03.2020).

89. Framework Act On Electronic Documents And Transactions. *Law Viewer*, 2002. URL: http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=27334&type=part&key=28. (Last accessed: 17.03.2020).

90. Петров О. С. Самоздра М. М., Бородулін А.В. Електронно-цифровий підпис як механізм електронної взаємодії держави з фізичними та юридичними особами. *Інформаційна безпека*. 2013. № 2. С. 117-122.

91. Костенко О. В. Проблеми правового регулювання визнання іноземних електронних довірчих послуг в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Ужгород, 2018. № 51. Т. 1. С. 192–197.

92. Костенко О. В. Костенко В. В. Шляхи запровадження електронних довірчих послуг в нотаріальному процесі. *Південноукраїнський правничий часопис*. Одеса, 2018. № 4. С.118–123.

93. Про затвердження Положення про Систему BankID Національного банку України: Постанова Національного банку України від 30.08.2016 р. № 378 / *Законотворчість* : база даних / Верхов. Рада України. URL : <https://zakon.rada.gov.ua/laws/show/v0378500-16#Text> (дата звернення 29.03.2020).

94. Жилин А. В., Корнейко А. В., Мохор В. В. Использование RSA алгоритма для обеспечения задач криптографической защиты информации в современных информационно-телекоммуникационных системах. *Захист інформації*. 2013. №. 15(3). С. 225-231.

95. Гавловський І. А. Адміністративно-правові відносини у сфері електронно-цифрового підпису. *Прикарпатський юридичний вісник*. Івано-Франківськ : Гельветика, 2015. Вип. 3(9). Т. 3. С.169-172.

96. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *EUR-Lex*. URL : <https://eur-lex.europa.eu/legal->

content/EN/TXT/?qid=1527856717659&uri=CELEX:32014R0910 (Last accessed: 17.03.2020).

97. Горбенко Ю.И., Потий А.В., Костенко А.В., Исирова Е.В., Горбенко И.Д. Состояние и сущность процессов нормализации европейской нормативной базы в области электронных подписей. *Прикладная радиоэлектроника*. Т. 13. № 3. 2014. С. 261–267.

98. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: Державний Стандарт України від 28.12.2002 р. № 31. URL : http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=68769 (дата звернення 19.06.2018).

99. Про електронний цифровий підпис: Закон України від 22 травня 2003 р. № 852-IV / *Законотворчість* : база даних / Верхов. Рада України. URL : <http://zakon0.rada.gov.ua/laws/show/852-15> (дата звернення 29.06.2018).

100. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV/ *Законотворчість* : база даних / Верхов. Рада України. URL : <http://zakon5.rada.gov.ua/laws/show/851-15> (дата звернення 29.06.2018).

101. Про затвердження Положення про центральний засвідчувальний орган: Постанова Кабінету Міністрів України від 28.10.2004 р. № 1451. *Законотворчість* : база даних / Кабінет Міністрів України. URL : <http://zakon5.rada.gov.ua/laws/show/1451-2004-%D0%BF>. (дата звернення 01.07.2018).

102. Про визначення сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання: Постанова Кабінету Міністрів України від 16.12.2015 р. № 1057. *Законотворчість* : база даних / Кабінет Міністрів України. URL : <http://zakon2.rada.gov.ua/laws/show/1057-2015-%D0%BF>. (дата звернення 29.06.2018).

103. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності: Постанова від 28 жовтня 2004 р. № 1452/ Кабінет Міністрів України. Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1452-2004-%D0%BF> (дата звернення 08.06.2018).

104. Про затвердження Порядку акредитації центру сертифікації ключів: Постанова від 13 липня 2004 р. №903 / Кабінет Міністрів України. Режим доступу : <http://zakon1.rada.gov.ua/laws/show/903-2004-%D0%BF> (дата звернення 11.07.2018).

105. Про внесення змін до наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.03.2017 р. № 1017/5/206/. *Законотворчість* : база даних / Міністерство Юстиції України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України. URL : <http://zakon5.rada.gov.ua/laws/show/en/z0422-17>. (дата звернення 18.06.2019).

106. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. *Законотворчість* : база даних / Верхов. Рада України. URL : : <http://zakon3.rada.gov.ua/laws/show/2155-19>. (дата звернення 18.06.2018).

107. Костенко О.В. Правова адаптація суспільних відносин в сфері цифрового підпису та електронних довірчих послуг в Україні до законодавства ЄС. *Особенности адаптации законодательства Молдовы и Украины к законодательству Европейского Союза*: материалы Международной научно-практической конференции (г. Кишинев, Республика Молдова, 3-24 марта 2019 г.). Кишинев: Institutul de Cercetări Juridice, Politice și Sociologice. С. 136–139.

108. Словарь криптографических терминов / Акад. криптографии Российской Федерации ; под ред. Б. А. Погорелова и Б. Н. Сачкова. Москва : МАКС Пресс, 2006. 91 с.

109. Кашанина Т.В. Юридическая техника : учебник / Т. В. Кашанина. 2-е изд., пересмотр. Москва : Норма : ИНФРА-М, 2011. 495 с.
110. Mason S. World electronic signature legislation. *Digital Evidence and Electronic Signature Law Review*. 2013. Vol. 10. URL : https://www.researchgate.net/publication/329107553_World_electronic_signature_legislation (Last accessed: 17.03.2020).
111. Laborde C. M. Electronic signatures in international contracts. Peter Lang, 2010. URL : https://books.google.com.ua/books?id=Cne-igPOkhgC&printsec=frontcover&hl=uk&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (Last accessed: 17.03.2020).
112. Усі питання по е-послугах. Урядовий портал. *Єдиний веб-портал органів виконавчої влади України*. 2019. URL : <https://www.kmu.gov.ua/ua/usi-pitannya-po-e-poslugam/sho-take-elektronna-posluga> (дата звернення 15.08.2019).
113. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. *Законотворчість* : база даних / Верхов. Рада України. URL : <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80/ed20130515/sp:max100#n16> (дата звернення 15.08.2019).
114. Про запровадження пілотного проекту щодо подання заяв у сфері державної реєстрації актів цивільного стану через мережу Інтернет: Наказ Міністерства юстиції України від 09.07.2015 р. № 1187/5 *Законотворчість* : база даних / Верхов. Рада України. URL : <https://zakon.rada.gov.ua/laws/show/z0812-15/ed20181107/sp:max100#n46> (дата звернення 15.08.2019).
115. Про організацію прийому та обслуговування осіб, які звертаються до органів Пенсійного фонду України: Постанова Пенсійного фонду України від 30.07.2015 р. №13-1. *Законотворчість* : база даних / Верхов. Рада України. URL : <https://zakon.rada.gov.ua/laws/show/z0991-15/ed20171208/sp:max100#n24> (дата звернення 15.08.2019).

116. Про схвалення Концепції розвитку системи електронних послуг в Україні: Розпорядження Кабінету Міністрів України від 16.11.2016 р. № 918-р. *Законотворчість* : база даних / Верхов. Рада України. URL : <https://zakon.rada.gov.ua/laws/show/918-2016-%D1%80/ed20161116/sp:max100#n15> (дата звернення 30.08.2019).

117. Договір про заснування Європейської Спільноти (консолідована версія станом на 1 січня 2005 року). Урядовий портал: єдиний веб-портал органів виконавчої влади України. URL : https://zakon.rada.gov.ua/laws/show/994_017 (дата звернення 30.08.2019).

118. Костенко О. В., Костенко В. В. Вирішення проблем правового регулювання сфери цифрового підпису та електронних довірчих послуг в Україні. *Сутність та значення законодавства на розвиток суспільних відносин*: матеріали Міжнародної науково-практичної конференції, (м. Одеса, 8-9 березня 2019 р.). Одеса : Причорноморська фундація права. 2019. С. 55–58.

119. Регламент Європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист. *Законотворчість* : база даних / Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/984_008-16 (дата звернення: 17.03.2020)

120. Типовий закон ЮНСІТРАЛ про електронні підписи: Міжнародний документ від 05.07.2001 р. № 995_937. URL : https://zakon.rada.gov.ua/laws/show/995_937.#Text (дата звернення: 17.03.2020)

121. Federal Information Processing Standards Publication 140-2, U.S. Department of Commerce, 05/2001. Security Requirements for Cryptographic Modules. URL : <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> (Last accessed: 17.03.2020).

122. Recommendation for Key Management, Part 1: General. Withdrawn NIST Technical Series Publication. 2016. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf> (Last accessed: 17.03.2020).

123. A framework for designing cryptographic key management systems / E. Barker et al. *NIST Special Publication*. 2013. Vol. 800(130). P. 1-112. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-130.pdf>

124. Just M., van Oorschot P. C. Addressing the Problem of Undetected Signature Key Compromise. NDSS. 1999. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.26.507&rep=rep1&type=pdf>. (Last accessed: 17.03.2020).

125. Pellegrini P. Pellegrini: If Security in E-signatures Violated, They Must Be Made Invalid. *NewSnow*. 2017. URL: <https://newsnow.tasr.sk/policy/pellegrini-if-security-in-e-signatures-violated-they-must-be-made-invalid/> (Last accessed: 17.03.2020).

126. Genkin D., Shamir A., Tromer E. RSA key extraction via low-bandwidth acoustic cryptanalysis. *Annual Cryptology Conference*. Springer, Berlin, Heidelberg, 2014. P. 444-461.

127. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», 2020. URL: <http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=41640> (дата звернення: 17.03.2020)

128. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації: Наказ від 20.07.2007 р. № 141. Законодавство України : база даних / Верхов. Рада України. URL: <http://zakon2.rada.gov.ua/laws/show/z0862-07>. (дата звернення: 17.03.2017)

129. Костенко О.В. Компрометація особистого ключа електронного підпису (правовий аспект). *International journal of innovative technologies in economy*. 2018. № 3(15). С. 15–22.

130. Костенко О.В. Проблеми правового регулювання транскордонного визнання іноземних послуг та іноземного сертифікату електронного підпису в Україні. *Стан та перспективи розвитку юридичної науки: матеріали міжнародної науково-практичної конференції (Дніпро, 31 серпня – 1 верес. 2018 р.)* / упорядн.: Громадська організація «Правовий світ», 2018. С. 65–69.

131. Костенко А.В. Проблемы правового регулирования признания иностранных электронных доверительных услуг в Украине. *Leges si Viata*. 2018. № 10/2(322). С. 54–58.

132. Костенко О.В., Капшук О.О. Проблема інтероперабельності Національної системи електронного цифрового підпису в Україні та шляхи їх вирішення. *System analysis and information technologies: 16-th International conference SAIT 2014 (Kyiv, Ukraine, May 26–30, 2014)*. Institute for Applied System Analysis of National Technical University of Ukraine Kyiv Polytechnic Institute, 2014. Р. 297–298.

133. Костенко О.В. Сучасна правова модель суспільних відносин сфери електронних довірчих послуг в Україні. *«Recht der Osteuropäischen Staaten»*. 2018. №4. С. 139–142.

134. Електронний документообіг у державному управлінні: навч. посіб. / І. В. Клименко, К. О. Линьов, І. Д. Горбенко, В. В. Онопрієнко ; Нац. акад. держ. упр. при Президентові України. Київ : НАДУ ; Х. : Форт, 2009. 227 с.

135. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131

136. Писаренко Г. М. Підстави юридичної відповідальності в інформаційній сфері. *ДЕРЖАВА ТА РЕГІОНИ : науково-виробничий журнал. Серія: Право / Гуманітарний ун-т «Запорізький ін-т держ. та*

муниципального управління» ; редкол.: В. Г. Лукашевич (голов. ред.) [та ін.].
Запоріжжя : [б. в.], 2017. №2(56). С.14-18.

137. Костенко О. В. Міністерство юстиції України – вікно держави у світовий простір електронного цифрового підпису. *Бюлетень Міністерства юстиції України*. Київ, 2014. №3.С.142–149

ДОДАТКИ

Додаток А

ПРОЄКТ

ЗАКОН УКРАЇНИ

«Про внесення змін до Закону України «Про електронні довірчі послуги»

Верховна Рада України п о с т а н о в л я є:

Внести зміни до Закону України «Про електронні довірчі послуги»:

Пункт 7 частини 1 статті 1 Розділу I викласти в такій редакції:

«електронна довірча послуга – електронна послуга, яка надається за винагороду для забезпечення інформаційних взаємовідносин між суб'єктами, що здійснюються за допомогою технологій мережі Інтернет або в електронній формі, і яка полягає у:

а) створенні, перевірці та підтвердженні електронних довірчих послуг, електронних підписів, електронних печаток або електронних позначок часу, послугах рекомендованих електронних відправлень та використанні сертифікатів, інших, що пов'язані з цими послугами; або

б) створенні, перевірці та підтвердженні сертифікатів для автентифікації вебсайту; або

в) збереженні електронних підписів, електронних печаток або сертифікатів, пов'язаних із цими послугами».

Пункт 11 частини 1 статті 1 Розділу I викласти в такій редакції:

«електронна послуга – послуга, яка надається за винагороду для забезпечення інформаційних взаємовідносин між суб'єктами суспільних відносин із використанням інформаційно-комунікаційних технологій».

Пункт 12 частини 1 статті 1 Розділу I викласти в такій редакції:

«Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються й використовуються ним як підпис та перебувають під особистим контролем підписувача.

Забороняється передавати третім особам електронний підпис та ідентифікаційні дані особи підписувача, крім випадків, встановлених законом».

Пункт 26 частини 1 статті 1 Розділу I викласти в такій редакції:

«Компрометація особистого ключа електронного підпису – будь-яка явна або неявна подія та/або дія (втрата, розголошення, крадіжка, несанкціоноване копіювання) з даними особистого ключа електронного підпису та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого розголошення, зміни, знищення, блокування, перехоплення, копіювання та використання особистого ключа

електронного підпису, а також інформації, яка обробляється та передається за його допомогою.

Явною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа за участю або без участі підписувача або третіх осіб без застосування технічних засобів.

Неявною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа електронного підпису із застосуванням будь-яких технічних засобів без участі підписувача»;

Частину 1 статті 1 Розділу 1 після пункту 44 доповнити новим пунктом 45 такого змісту:

«Державний цифровий довірчий центр (третя довірча сторона) – державне підприємство, яке забезпечує інтероперабельність національних технічних, техніко-юридичних та юридичних норм, що використовуються під час надання електронних послуг, механізми визнання іноземних електронних підписів і електронних довірчих послуг та транскордонну взаємодію надавачів та користувачів довірчих послуг».

Частину 1 статті 1 Розділу 1 після пункту 45 доповнити новим пунктом 46 такого змісту:

«Транскордонність – це унормована або взаємоузгоджена діяльність суб'єктів права різних країн та юрисдикцій у сфері електронного обміну даними із використанням електронних підписів, спрямована на забезпечення електронними сервісами суспільних відносин цих суб'єктів у міждержавному та міжнародному режимах».

Частину 1 статті 1 Розділу 1 після пункту 46 доповнити новим пунктом 47 такого змісту:

«Транскордонне визнання електронного підпису або електронної довірчої послуги – це унормована або взаємоузгоджена діяльність суб'єктів права різних країн та юрисдикцій у сфері електронних підписів та електронних довірчих послуг, спрямована на встановлення юридичної сили електронної довірчої послуги або електронного підпису, які надаються у транскордонному режимі».

Частину 1 статті 1 Розділу I після пункту 47 доповнити новим пунктом 48 такого змісту:

«Транскордонна електронна послуга – електронна послуга, яка надається за винагороду і спрямована на забезпечення електронних взаємовідносин між суб'єктами різних країн із використанням електронних підписів у міждержавному та міжнародному режимах».

Частину 1 Статті 5 Розділу II викласти в такій редакції:

«1. Державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації здійснюють:

Кабінет Міністрів України;

головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг та виконання функцій центрального

засвідчувального органу шляхом створення умов для функціонування суб'єктів правових відносин у сфері електронних довірчих послуг;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

центральний орган виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування;

Державний цифровий довірчий центр (третя довірча сторона);

Національний банк України (у банківській системі України)».

Частину 1 статті 7 Розділу II після абзацу 17 доповнити абзацом 18 такого змісту:

«управління та контролю Державного цифрового довірчого центру (третьої довірчої сторони), що забезпечує механізми визнання іноземних електронних підписів та електронних довірчих послуг, транскордонну взаємодію надавачів та користувачів довірчих послуг».

Статтю 7 Розділу II після частини 3 доповнити частиною 4 такого змісту:

«Технічне, технологічне та правове забезпечення виконання функцій третьої довірчої сторони у сфері електронного підпису та електронних довірчих послуг здійснюється Державним цифровим довірчим центром (третьою довірчою стороною) – державним підприємством, яке належить до сфери управління головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних підписів та електронних довірчих послуг».

Розділ II після статті 7 доповнити статтею 7-1 такого змісту:

«Стаття 7-1. Повноваження Державного цифрового довірчого центру (третя довірча сторона)

До повноважень Державного цифрового довірчого центру (третя довірча сторона) належать:

виступати третьою довірчою стороною у взаємовідносинах між Україною та іноземними країнами й союзами країн у будь-яких взаємовідносинах у сфері цифрового підпису та електронних довірчих послуг;

узгоджувати порядок визнання та відповідності вимогам законодавства України електронних підписів та електронних довірчих послуг, що надаються іноземними надавачами/постачальниками (окремими суб'єктами іноземної держави) відповідно до вимог нормативно-правових актів, які регулюють правові відносини у сфері електронних довірчих послуг в іноземних державах та в Україні;

спільно із уповноваженими органами державної влади брати участь у підготовці міжнародних угод у сфері цифрового підпису та електронних

довірчих послуг, готувати пропозиції щодо відповідності технічних, техніко-юридичних та юридичних норм законодавства сторін міждержавної угоди у сфері електронного підпису, узгоджувати процедури визнання та верифікації, рівні ідентифікації підписувачів/надавачів цифрового підпису, а також визначати юрисдикцію, у якій будуть здійснюватися розгляди спірних питань;

забезпечувати інтероперабельність та координувати технологічну діяльність національних суб'єктів сфери електронних довірчих послуг, електронної ідентифікації та державних електронних послуг;

виступати під час судових спорів як третя особа, яка не заявляє самостійних вимог щодо предмета спору для захисту особистих суб'єктивних прав і охоронюваних законом інтересів у сфері електронного підпису та електронних довірчих послуг;

за заявою суб'єктів договірних відносин у разі укладання угод в електронному вигляді здійснювати верифікацію цифрових підписів та електронних довірчих послуг підписантів, надавати або долучати до угоди електронну верифікаційну позначку, якою підтверджуються дійсність національних або іноземних цифрових підписів, електронних довірчих послуг та даних ідентифікації, які використовують сторони угоди;

за заявою суб'єктів договірних відносин у разі укладання угоди в електронному вигляді здійснювати захист майнових інтересів фізичних осіб та юридичних осіб у разі настання певних подій (страхових випадків), визначених угодою або чинним законодавством, за рахунок грошових фондів, що формуються шляхом сплати суб'єктів договірних відносин страхових платежів (страхових внесків, страхових премій) та доходів від розміщення коштів цих фондів відповідно до Закону України «Про страхування».

Статтю 10 Розділу II викласти в такій редакції:

«Повноваження центрального органу виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування

1. До повноважень центрального органу виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування, належить:

створення та ведення реєстру посад державних службовців в органі державної влади або іншому державному органі та посад служби в органах місцевого самоврядування;

забезпечення державних службовців, органів державної влади, службовців органів місцевого самоврядування та органів місцевого самоврядування кваліфікованими електронними підписами».

Статтю 12 Розділу II викласти в такій редакції:

«Стаття 12. Права, обов'язки та відповідальність користувачів електронних довірчих послуг

1. Користувачі електронних довірчих послуг мають право на:
отримання електронних довірчих послуг;
вільний вибір надавача електронних довірчих послуг;
оскарження в судовому порядку дій чи бездіяльності надавачів електронних довірчих послуг та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг;

відшкодування завданої їм шкоди та захист своїх прав і законних інтересів;

звернення із заявою про скасування, блокування та поновлення свого сертифіката відкритого ключа.

2. Користувачі електронних довірчих послуг зобов'язані:

забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;

невідкладно повідомляти надавача електронних довірчих послуг про підозру або факт компрометації особистого ключа;

надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;

своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між надавачем та користувачем електронних довірчих послуг;

своєчасно надавати надавачу електронних довірчих послуг інформацію про зміну ідентифікаційних даних, які містить сертифікат відкритого ключа;

не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування сертифіката відкритого ключа.

3. Захист прав користувачів електронних довірчих послуг, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України «Про захист прав споживачів».

4. Порушення користувачами електронних довірчих послуг законодавства про електронні довірчі послуги:

порушення правил використання електронних підписів та електронних довірчих послуг;

виготовлення з метою збуту чи збут свідомо незаконно створених електронних підписів;

подання кваліфікованими надавачами електронних довірчих послуг завідомо неправдивої інформації та ідентифікаційних даних особи для створення підроблених електронних підписів;

створення умов для компрометації та компрометація особистого ключа електронного підпису;

використання створених або отриманих у шахрайському або незаконному порядку електронних підписів, кваліфікованих сертифікатів відкритих ключів, кваліфікованих електронних підписів, паролів або будь-яких інших унікальних ідентифікаційних даних особи для доступу або несанкціонованого втручання в роботу систем електронних виборів, а також систем державних адміністративних послуг, електронного суду, державних інформаційних ресурсів та реєстрів, мережі державного управління;

незаконне копіювання, зберігання або розповсюдження персональних чи будь-яких інших унікальних ідентифікаційних даних особи, які використовуються для створення електронних підписів та електронних довірчих послуг

передбачає відповідальність відповідно до закону».

Статтю 13 Розділу II викласти в такій редакції:

«Стаття 13. Права, обов'язки та відповідальність кваліфікованих надавачів електронних довірчих послуг

1. Кваліфіковані надавачі електронних довірчих послуг мають право:

надавати електронні довірчі послуги з дотриманням вимог цього Закону;

отримувати документи, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться у сертифікаті відкритого ключа;

отримувати консультації від центрального засвідчувального органу або засвідчувального центру з питань, пов'язаних із наданням електронних довірчих послуг;

звертатися до органів з оцінки відповідності для отримання документів про відповідність;

звертатися із заявою про скасування, блокування або поновлення сформованих у центральному засвідчувальному органі або засвідчувальному центрі кваліфікованих сертифікатів відкритих ключів;

самостійно обирати, які саме стандарти будуть ними застосовуватися при наданні довірчих послуг із переліку стандартів, визначеного Кабінетом Міністрів України, крім сфери спеціального зв'язку.

2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:

захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства;

функціонування програмно-технічного комплексу, що ними використовується, та захист інформації, що в ньому обробляється, відповідно до вимог законодавства;

створення та функціонування свого вебсайту;

впровадження, підтримання в актуальному стані та публікацію на своєму вебсайті реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус

сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;

цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів;

скасування, блокування та поновлення сертифікатів відкритих ключів відповідно до вимог цього Закону;

встановлення під час формування сертифіката відкритого ключа належності відкритого ключа та відповідного йому особистого ключа підписувачу чи створювачу електронної печатки;

внесення ідентифікаційних даних підписувача чи створювача електронної печатки до відповідного сертифіката відкритого ключа;

інформування органу контролю про порушення конфіденційності та/або цілісності інформації, що впливає на надання електронних довірчих послуг або стосується персональних даних користувачів електронних довірчих послуг, не пізніше 24 годин з моменту, коли їм стало відомо про таке порушення;

інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливає на надання їм електронних довірчих послуг або стосується їхніх персональних даних, не пізніше двох годин з моменту, коли їм стало відомо про таке порушення;

унеможливлення використання особистого ключа в разі його компрометації;

постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів;

внесення коштів на поточний рахунок зі спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути заподіяна користувачам таких послуг чи третім особам унаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов'язань, у розмірі, визначеному частиною третьою статті 16 цього Закону;

наймання працівників, які володіють необхідними для надання кваліфікованих електронних довірчих послуг знаннями, досвідом і кваліфікацією, зокрема у сферах інформаційних технологій та захисту інформації;

використання під час надання електронних довірчих послуг виключно кваліфікованих сертифікатів, засвідчених у центральному засвідчувальному органі чи засвідчувальному центрі;

зберігання документів, поданих користувачами для отримання електронних довірчих послуг;

інформування органу контролю та центрального засвідчувального органу або засвідчувального центру про будь-які зміни у процедурі надання електронних довірчих послуг протягом 48 годин з моменту настання таких змін;

передачу центральному засвідчувальному органу або засвідчувальному центру документованої інформації в разі припинення діяльності з надання електронних довірчих послуг.

3. Обов'язкові вимоги до кваліфікованих надавачів електронних довірчих послуг, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

4. Порухення кваліфікованими надавачами електронних довірчих послуг законодавства про електронні довірчі послуги:

порушення правил створення, надання, використання та знищення електронних підписів та електронних довірчих послуг;

виготівлення з метою збуту чи збут свідомо незаконно створених електронних підписів;

створення умов для компрометації та компрометація особистого ключа електронного підпису;

використання створених або отриманих у шахрайському або незаконному порядку електронних підписів, кваліфікованих сертифікатів відкритих ключів, кваліфікованих електронних підписів, паролів або будь-яких інших унікальних ідентифікаційних даних особи для доступу або несанкціонованого втручання в роботу систем електронних виборів, а також систем державних адміністративних послуг, електронного суду, державних інформаційних ресурсів та реєстрів, мережі державного управління,

незаконне копіювання, зберігання або розповсюдження даних, зокрема персональних чи будь-яких інших унікальних ідентифікаційних даних особи, які використовуються для створення електронних підписів та електронних довірчих послуг, передбачає відповідальність відповідно до закону».

Частину 2 статті 16 Розділу II викласти в такій редакції:

«Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок зі спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному рахунку зі спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менш як 100 мінімальних розмірів заробітної плати.

Діяльність іноземних кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів поточний рахунок зі спеціальним режимом Державного цифрового довірчого центру (третя довірча сторона) для страхування цивільно-правової відповідальності або

забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам».

Статтю 22 Розділу II після частини 6 доповнити частиною 7 такого змісту:

«Ідентифікація особи державного службовця та посадової особи місцевого самоврядування, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа для виконання посадових повноважень, здійснюється за умови її особистої присутності за паспортом громадянина України та в порядку, встановленому Кабінетом Міністрів України».

Частину 1 статті 23 Розділу II після абзацу 3 доповнити абзацом 4 такого змісту:

«державного службовця та посадової особи місцевого самоврядування: обов'язкові відомості визначаються Кабінетом Міністрів України додатково за вимогами, встановленими органом державної влади та місцевого самоврядування».

Частину 1 статті 25 Розділу II після пункту 1 доповнити пунктом 2 такого змісту:

«подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про скасування виданого йому або державним службовцям органу державної влади або посадової особи органу місцевого самоврядування кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача та особи уповноваженого представника державного органу та органу місцевого самоврядування».

У зв'язку з цим пункт 2 вважати пунктом 3.

Частину 6 статті 25 Розділу II доповнити абзацом 1 такого змісту:

«подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про блокування виданого йому або державним службовцям органу державної влади або посадової особи органу місцевого самоврядування кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача та особи уповноваженого представника державного органу та органу місцевого самоврядування».

У зв'язку з цим абзаци 1, 2, 3 вважати абзацами 2, 3, 4;

Частину 10 статті 25 Розділу II доповнити абзацом 1 такого змісту:

«подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа)».

У зв'язку з цим абзаци 1, 2 вважати абзацами 2, 3;

Статтю 38 Розділу VI доповнити частиною 3 такого змісту:

«Внесення до Довірчого списку України кваліфікованого надавача електронних довірчих послуг, що відповідає умовам п.п. 1 п. 1 ст. 38 цього Закону за його заявою може здійснюватися Державним цифровим довірчим центром без укладання між іноземною державою та Україною відповідного двостороннього або багатостороннього міжнародного договору за погодженням Центрального засвідчувального органу».

Статтю 38 Розділу VI доповнити частиною 4 такого змісту:

«Порядок використання інформаційно-телекомунікаційної системи Державного цифрового довірчого центру (третя довірча сторона) для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, встановлюється Кабінетом Міністрів України».

Голова Верховної Ради України

Додаток Б**ПРОЄКТ****ПОЯСНЮВАЛЬНА ЗАПИСКА****до проєкту Закону України «Про внесення змін до Закону України
„Про електронні довірчі послуги”»****1. Обґрунтування необхідності прийняття законопроєкту**

Закон України «Про електронні довірчі послуги» було розроблено з метою гармонізації українського законодавства із законодавством Європейського Союзу, а саме з Регламентом (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), який набрав чинності 01 липня 2016 року.

Закон України «Про електронні довірчі послуги» прийнятий Верховною Радою України 5 жовтня 2017 року і набрав чинності 07 листопада 2018 року.

У проєкті Закону України «Про внесення змін до Закону України «Про електронні довірчі послуги» (далі – проєкт Закону) пропонується вдосконалити правові та організаційні засади надання електронних довірчих послуг, зокрема у транскордонному режимі. Актуальність такої пропозиції обумовлена потребою модернізувати наявні суспільні відносини у сфері електронного підпису та електронних довірчих послуг і приведення національного законодавства у відповідність до сучасних світових практик у цій галузі.

Запропоновані зміни спрямовані на розбудову єдиного простору довіри на основі системи електронного підпису та електронних довірчих послуг, удосконалення регулювання найбільш важливих на сьогодні відносин у цій сфері суспільного життя, встановлення загальнообов'язкових правил поведінки та відповідальності суб'єктів правовідносин, спрощення та встановлення чітких процедур транскордонного визнання цифрових підписів.

2. Мета і шляхи її досягнення

Проєкт Закону розроблений з метою вдосконалення законодавства у сфері електронного цифрового підпису з урахуванням досвіду міжнародних організацій, Європейського Союзу та окремих країн, напрямів розбудови єдиного простору довіри на основі системи електронних довірчих послуг, визнання в Україні електронних довірчих послуг, які надаються їхніми

іноземними постачальниками, що спростить і забезпечить активний розвиток транскордонного співробітництва та інтеграцію України у світовий електронний інформаційний простір.

Прийняття проекту Закону сприятиме:

підвищенню рівня довіри громадян до електронних довірчих послуг, зокрема транскордонних, згідно з потребами сучасного суспільства й відповідно до концепції Президента України «Держава у смартфоні» щодо цифровізації держави та взаємодії громадян із органами державної влади за допомогою електронних сервісів;

вільному та масовому обігу електронних підписів та електронних довірчих послуг в Україні, підвищенню рівня правової гігієни під час їх використання в процесах державного управління та електронних адміністративних державних послугах;

удосконаленню нормативно-правової бази, що регулює відповідальність за правопорушення у сфері цифрових технологій, цифрового підпису та електронних довірчих послуг;

створенню умов для розвитку та функціонування сфери електронних довірчих послуг у транскордонному режимі, доступу до електронних довірчих послуг постачальниками електронних довірчих послуг, що провадять діяльність в інших державах;

захисту прав і законних інтересів користувачів електронних довірчих послуг;

відкритості для інновацій у сфері електронних довірчих послуг.

3. Правові аспекти

Проектом Закону пропонується внести зміни:

до статті 1 Закону із визначенням нових термінів, які розкривають зміст та суть відносин у цій сфері: «Компрометація особистого ключа електронного підпису», «Державний цифровий довірчий центр (третя довірча сторона) та інші»;

до статті 5, які стосуються вдосконалення системи органів, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації;

до статті 7 щодо повноваження головного органу в системі центральних органів виконавчої влади, який забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг;

до статті 10, яка визначає повноваження центрального органу виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з

питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування;

до стаття 12, що встановлює права, обов'язки та відповідальність користувачів електронних довірчих послуг;

до статті 13, що встановлює права, обов'язки та відповідальність кваліфікованих надавачів електронних довірчих послуг;

до статті 16, що встановлює вимоги до електронних довірчих послуг;

до статті 23, яка визначає умови надання кваліфікованих сертифікатів відкритих ключів;

до статті 25, яка встановлює підстави скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів;

до статті 37, що регулює участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації;

ввести статтю 7-1, у якій визначити повноваження Державного цифрового довірчого центру (третя довірча сторона).

4. Фінансово-економічне обґрунтування

Реалізація положень проєкту Закону не потребує матеріальних чи інших витрат із Державного бюджету України.

5. Регіональний аспект

Проєкт Закону не стосується питань розвитку адміністративно-територіальних одиниць.

6. Запобігання дискримінації

У проєкті Закону відсутні положення, які містять ознаки дискримінації.

Проєкт Закону не потребує проведення громадської антидискримінаційної експертизи.

7. Запобігання корупції

У проєкті Закону відсутні правила і процедури, які можуть містити ризики вчинення корупційних правопорушень.

Проєкт Закону не потребує проведення громадської антикорупційної експертизи.

8. Позиція соціальних партнерів

Проєкт Закону не стосується соціально-трудової сфери.

9. Оцінка регуляторного впливу

Проєкт Закону є регуляторним актом.

10. Вплив реалізації акта на ринок праці

Реалізація проєкту Закону не вплине на ринок праці.

11. Прогноз результатів

Прийняття проекту Закону України «Про внесення змін до Закону України „Про електронні довірчі послуги”» дасть змогу модернізувати в Україні модель та принципи надання електронних довірчих послуг шляхом гармонізації із міжнародним законодавством, законодавством Європейського Союзу та інших країн світу з урахуванням національних особливостей, не руйнуючи систему взаємодії суб’єктів у сфері електронного цифрового підпису, що склалась в Україні.

У разі практичної реалізації проекту Закону України «Про внесення змін до Закону України „Про електронні довірчі послуги”» будуть досягнуті такі позитивні результати:

- поліпшення довіри в суспільних відносинах до електронних підписів та електронних довірчих послуг, особливо під час здійснення транскордонної взаємодії між Україною та країнами світу;

- створення третьої довірчої сторони – Державного цифрового довірчого центру – суттєво сприятиме поліпшенню бізнесу в Україні, активізує електронні послуги, електронну транскордонну торгівлю та інші транскордонні електронні сервіси;

- запровадження відповідальності за порушення у сфері цифрового підпису та довірчих послуг призведе до поліпшення правової гігієни та зменшення ризиків скоєння правопорушень із використанням цифрового підпису, що сприятиме росту довіри у населення до інформаційних технологій і цифрових послуг, поширенню застосування цифрового підпису як надійного засобу електронної ідентифікації особи під час електронної взаємодії;

- покращення репутації державних електронних сервісів, які можуть отримати реальне публічне визнання, що поліпшить імідж Уряду, підвищить соціальну відповідальність постачальників цих послуг;

- залучення державного органу, що здійснює функційне управління державною службою до участі у сфері цифрового підпису, електронних довірчих послуг та електронної ідентифікації прискорить цифровізацію органів державної служби та органів місцевого самоврядування.

Додаток В

ПОРІВНЯЛЬНА ТАБЛИЦЯ до проєкту Закону України «Про внесення змін до Закону України „Про електронні довірчі послуги”»

Зміст положення (норми) чинного акта законодавства	Зміст відповідного положення (норми) проєкту акта
Розділ І ЗАГАЛЬНІ ПОЛОЖЕННЯ	
Стаття 1. Визначення термінів У цьому Законі терміни вживаються в такому значенні: 7) електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб’єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги	Стаття 1. Визначення термінів У цьому Законі терміни вживаються в такому значенні: 7) «електронна довірча послуга – електронна послуга, яка надається за винагороду для забезпечення інформаційних взаємовідносин, що здійснюються за допомогою технологій мережі Інтернет або в електронній формі, між суб’єктами і яка полягає у: а) створенні, перевірці та підтвердженні електронних довірчих послуг, електронних підписів, електронних печаток або електронних позначок часу, послугах рекомендованих електронних відправлень та використанні сертифікатів, інших, що пов’язані з цими послугами; або б) створенні, перевірці та підтвердженні сертифікатів для автентифікації вебсайту; або в) збереженні електронних підписів, електронних печаток або сертифікатів, пов’язаних із цими послугами»

11) електронна послуга – будь-яка послуга, що надається через інформаційно-телекомунікаційну систему	11) електронна послуга – послуга, яка надається за винагороду для забезпечення інформаційних взаємовідносин між суб'єктами суспільних відносин із використанням інформаційно-комунікаційних технологій
12) електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються й використовуються ним як підпис	12) електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис та перебувають під особистим контролем підписувача. Забороняється передавати третім особам електронний підпис та ідентифікаційні дані особи підписувача, крім випадків, встановлених законом»
26) компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа	26) Компрометація особистого ключа електронного підпису – будь-яка явна або неявна подія та/або дія (втрата, розголошення, крадіжка, несанкціоноване копіювання) з даними особистого ключа електронного підпису та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого розголошення, зміни, знищення, блокування, перехоплення, копіювання та використання особистого ключа електронного підпису, а також інформації, яка обробляється та передається за його допомогою. Явною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа за участю або без участі підписувача або третіх осіб без застосування технічних засобів.

	Неявною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа електронного підпису із застосуванням будь-яких технічних засобів без участі підписувача
	45) Державний цифровий довірчий центр (третя довірча сторона) – державне підприємство, яке забезпечує інтероперабельність національних технічних, техніко-юридичних та юридичних норм, що використовуються під час надання електронних послуг, механізми визнання іноземних електронних підписів і електронних довірчих послуг та транскордонну взаємодію надавачів та користувачів довірчих послуг
	46) Транскордонність – це унормована або взаємоузгоджена діяльність суб'єктів права різних країн та юрисдикцій у сфері електронного обміну даними із застосуванням електронних підписів, спрямована на забезпечення електронними сервісами суспільних відносин цих суб'єктів у міждержавному та міжнародному режимах
	47) транскордонне визнання електронного підпису або електронної довірчої послуги – це унормована або взаємоузгоджена діяльність суб'єктів права різних країн та юрисдикцій у сфері електронних підписів та електронних довірчих послуг, спрямована на встановлення юридичної сили електронної довірчої послуги або електронного підпису, які надаються у

транскордонному режимі

Розділ II

СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТА ОРГАНИ, ЩО ЗДІЙСНЮЮТЬ ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРАХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТА ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ

Стаття 5. Система органів, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації

1. Державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації здійснюють:

Кабінет Міністрів України;

головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

центральний орган виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування й використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства;

Національний банк України (у банківській системі України)

Стаття 5. Система органів, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації

1. Державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації здійснюють:

Кабінет Міністрів України;

головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг та виконання функцій центрального засвідчувального органу шляхом створення умов для функціонування суб'єктів правових відносин у сфері електронних довірчих послуг;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

Національний банк України (у банківській системі України);

центральний орган виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у

	державних органах, а також у сфері служби в органах місцевого самоврядування
Стаття 7. Повноваження головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг 1. Головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг щодо юридичних осіб, фізичних осіб-підприємців, які мають намір надавати електронні довірчі послуги, виконує функції центрального засвідчувального органу шляхом внесення відомостей про них до Довірчого списку відповідно до вимог цього Закону. 2. До повноважень головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг, належить забезпечення: - розроблення нормативно-правових актів у сфері електронних довірчих послуг; - розроблення норм, стандартів у сфері електронних довірчих послуг; - надання адміністративної послуги шляхом внесення юридичних осіб та фізичних осіб-підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку; - функціонування програмно-технічного комплексу	Стаття 7. Повноваження головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг 1. Головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг, щодо юридичних осіб, фізичних осіб-підприємців, які мають намір надавати електронні довірчі послуги, виконує функції центрального засвідчувального органу шляхом внесення відомостей про них до Довірчого списку відповідно до вимог цього Закону. 2. До повноважень головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг, належить забезпечення: - розроблення нормативно-правових актів у сфері електронних довірчих послуг; - розроблення норм, стандартів у сфері електронних довірчих послуг; - надання адміністративної послуги шляхом внесення юридичних осіб та фізичних осіб-підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку; - функціонування програмно-технічного комплексу

центрального засвідчувального органу та захисту інформації, що в ньому обробляється, відповідно до вимог законодавства; функціонування вебсайту центрального засвідчувального органу;

ведення Довірчого списку;

ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

генерації пари ключів та створення самопідписаних кваліфікованих сертифікатів електронної печатки центрального засвідчувального органу;

надання кваліфікованих електронних довірчих послуг надавачам електронних довірчих послуг з використанням самопідписаного сертифіката електронної печатки центрального засвідчувального органу, що призначений для надання таких послуг;

надання послуги постачання передачі сигналів точного часу, синхронізованого з Державним еталоном одиниць часу і частоти;

погодження розроблених постачальниками електронних довірчих послуг порядків синхронізації часу із Всесвітнім координованим часом (UTC);

погодження планів припинення діяльності кваліфікованих постачальників електронних довірчих послуг;

приймання та зберігання документованої інформації, сформованих кваліфікованих сертифікатів відкритих ключів, реєстру чинних, блокованих та скасованих кваліфікованих сертифікатів відкритих ключів у разі припинення діяльності

центрального засвідчувального органу та захисту інформації, що в ньому обробляється, відповідно до вимог законодавства; функціонування вебсайту центрального засвідчувального органу;

ведення Довірчого списку;

ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

генерації пари ключів та створення самопідписаних кваліфікованих сертифікатів електронної печатки центрального засвідчувального органу;

надання кваліфікованих електронних довірчих послуг надавачам електронних довірчих послуг із використанням самопідписаного сертифіката електронної печатки центрального засвідчувального органу, що призначений для надання таких послуг;

надання послуги постачання передачі сигналів точного часу, синхронізованого з Державним еталоном одиниць часу і частоти;

погодження розроблених постачальниками електронних довірчих послуг порядків синхронізації часу із Всесвітнім координованим часом (UTC);

погодження планів припинення діяльності кваліфікованих постачальників електронних довірчих послуг;

приймання та зберігання документованої інформації, сформованих кваліфікованих сертифікатів відкритих ключів, реєстру чинних, блокованих та скасованих кваліфікованих сертифікатів відкритих ключів у разі припинення діяльності

кваліфікованого постачальника електронних довірчих послуг;
розгляду пропозицій (зауважень) суб'єктів відносин у сфері електронних довірчих послуг щодо вдосконалення державного регулювання сфери електронних довірчих послуг;

надання суб'єктам відносин у сфері електронних довірчих послуг консультацій з питань, пов'язаних із наданням електронних довірчих послуг;

інформування органу контролю про обставини, які перешкоджають діяльності центрального засвідчувального органу;

взаємного визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг;

цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;

скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів у випадках, передбачених цим Законом;

інтероперабельності та технологічної нейтральності національних технічних рішень, а також недопущення їх дискримінації;

проведення оцінки стану розвитку сфери електронних довірчих послуг за результатами проведення аналізу

кваліфікованого постачальника електронних довірчих послуг;
розгляду пропозицій (зауважень) суб'єктів відносин у сфері електронних довірчих послуг щодо вдосконалення державного регулювання сфери електронних довірчих послуг;

надання суб'єктам відносин у сфері електронних довірчих послуг консультацій з питань, пов'язаних із наданням електронних довірчих послуг;

інформування органу контролю про обставини, які перешкоджають діяльності центрального засвідчувального органу;

взаємного визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг;

управління та контролю Державного цифрового довірчого центру (третьої довірчої сторони), що забезпечує механізми визнання іноземних електронних підписів і електронних довірчих послуг, транскордонну взаємодію надавачів та користувачів довірчих послуг;

цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;

скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів у випадках, передбачених цим Законом;

інтероперабельності та технологічної нейтральності

інформації про діяльність постачальників електронних довірчих послуг та засвідчувального центру, наданої в порядку, встановленому головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг;

державного регулювання з питань електронної ідентифікації з використанням електронних довірчих послуг у межах своєї компетенції відповідно до цього Закону;

здійснення інших повноважень у сферах електронних довірчих послуг та електронної ідентифікації, визначених законом.

3. Технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу – державним підприємством, яке належить до сфери управління головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг

національних технічних рішень, а також недопущення їх дискримінації;

проведення оцінки стану розвитку сфери електронних довірчих послуг за результатами проведення аналізу інформації про діяльність постачальників електронних довірчих послуг та засвідчувального центру, наданої в порядку, встановленому головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг;

державного регулювання з питань електронної ідентифікації з використанням електронних довірчих послуг у межах своєї компетенції відповідно до цього Закону;

здійснення інших повноважень у сферах електронних довірчих послуг та електронної ідентифікації, визначених законом.

3. Технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу – державним підприємством, яке належить до сфери управління головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг.

4. Технічне, технологічне та правове забезпечення виконання функцій третьої довірчої сторони у сфері електронного підпису та електронних довірчих послуг

	здійснюється Державним цифровим довірчим центром (третьою довірчою стороною) – державним підприємством, яке належить до сфери управління головного органу в системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних підписів та електронних довірчих послуг
	Стаття 7-1. Повноваження Державного цифрового довірчого центру (третя довірча сторона) До повноважень Державного цифрового довірчого центру (третя довірча сторона) належать: виступати третьою довірчою стороною у взаємовідносинах між Україною та іноземними країнами та союзами країн у будь-яких взаємовідносинах у сфері цифрового підпису та електронних довірчих послуг; узгоджувати порядок визнання та відповідності вимогам законодавства України електронних підписів та електронних довірчих послуг, що надаються іноземними надавачами/постачальниками (окремими суб'єктами іноземної держави) відповідно до вимог нормативно-правових актів, які регулюють правові відносини у сфері електронних довірчих послуг в іноземних державах та в Україні; спільно із уповноваженими органами державної влади брати участь у підготовці міжнародних угод у сфері цифрового підпису та електронних довірчих послуг, готувати пропозиції щодо відповідності технічних,

техніко-юридичних та юридичних норм законодавства сторін міждержавної угоди у сфері електронного підпису, узгоджувати процедури визнання та верифікації, рівні ідентифікації підписувачів/надавачів цифрового підпису, а також визначати юрисдикцію, у якій будуть здійснюватися розгляди спірних питань;

забезпечувати інтегрованість та координувати технологічну діяльність національних суб'єктів сфери електронних довірчих послуг, електронної ідентифікації та державних електронних послуг;

виступати під час судових спорів третьою особою, яка не заявляє самостійних вимог щодо предмета спору для захисту особистих суб'єктивних прав і охоронюваних законом інтересів у сфері електронного підпису та електронних довірчих послуг;

за заявою суб'єктів договірних відносин у разі укладання угод в електронному вигляді здійснювати верифікацію цифрових підписів та електронних довірчих послуг підписантів, надавати або долучати до угоди електронну верифікаційну позначку, якою підтверджується дійсність національних або іноземних цифрових підписів, електронних довірчих послуг та даних ідентифікації, які використовують сторони угоди;

за заявою суб'єктів договірних відносин у разі укладання угоди в електронному вигляді здійснювати захист майнових інтересів фізичних осіб та юридичних осіб у разі настання певних подій (страхових випадків), визначених

	угодою або чинним законодавством, за рахунок грошових фондів, що формуються шляхом сплати суб'єктів договірних відносин страхових платежів (страхових внесків, страхових премій) та доходів від розміщення коштів цих фондів, відповідно до Закону України «Про страхування»
Стаття 10. Повноваження центрального органу виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування й використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства 1. До повноважень центрального органу виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування й використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства, належить: участь у розробленні норм, стандартів у сфері електронної ідентифікації; встановлення вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їхнього використання у сфері електронного урядування; здійснення інших повноважень у сфері електронної ідентифікації, визначених законом	Стаття 10. Повноваження центрального органу виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування 1. До повноважень центрального органу виконавчої влади, що здійснює функційне управління державною службою в органі державної влади або іншому державному органі й забезпечує формування та реалізацію державної політики у сфері державної служби та з питань управління персоналом у державних органах, а також у сфері служби в органах місцевого самоврядування, належить: створення та ведення реєстру посад державних службовців в органі державної влади або іншому державному органі та посад служби в органах місцевого самоврядування; забезпечення державних службовців, органів державної влади, службовців органів місцевого самоврядування та органів місцевого самоврядування кваліфікованими електронними підписами та електронними довірчими послугами

Стаття 11. Суб'єкти відносин у сфері електронних довірчих послуг 1. Суб'єктами відносин у сфері електронних довірчих послуг є: - користувачі електронних довірчих послуг; - надавачі електронних довірчих послуг; - органи з оцінки відповідності; - засвідчувальний центр; - центральний засвідчувальний орган; - орган контролю	Стаття 11. Суб'єкти відносин у сфері електронних довірчих послуг 1. Суб'єктами відносин у сфері електронних довірчих послуг є: - користувачі електронних довірчих послуг; - надавачі електронних довірчих послуг; - органи з оцінки відповідності; - засвідчувальний центр; - центральний засвідчувальний орган; Державний цифровий довірчий центр (третя довірча сторона); - Орган контролю
Стаття 12. Права та обов'язки користувачів електронних довірчих послуг 1. Користувачі електронних довірчих послуг мають право на: - отримання електронних довірчих послуг; - вільний вибір надавача електронних довірчих послуг; - оскарження в судовому порядку дій чи бездіяльності надавачів електронних довірчих послуг та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг; - відшкодування завданої їм шкоди та захист своїх прав і законних інтересів; - звернення із заявою про скасування, блокування та поновлення свого сертифіката відкритого ключа. 2. Користувачі електронних довірчих послуг зобов'язані:	Стаття 12. Права, обов'язки та відповідальність користувачів електронних довірчих послуг 1. Користувачі електронних довірчих послуг мають право на: - отримання електронних довірчих послуг; - вільний вибір надавача електронних довірчих послуг; - оскарження в судовому порядку дій чи бездіяльності надавачів електронних довірчих послуг та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг; - відшкодування завданої їм шкоди та захист своїх прав і законних інтересів; - звернення із заявою про скасування, блокування та поновлення свого сертифіката відкритого ключа. 2. Користувачі електронних довірчих послуг зобов'язані:

забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;

невідкладно повідомляти надавача електронних довірчих послуг про підозру або факт компрометації особистого ключа;

надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;

своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між надавачем та користувачем електронних довірчих послуг;

своєчасно надавати надавачу електронних довірчих послуг інформацію про зміну ідентифікаційних даних, які містить сертифікат відкритого ключа;

не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування сертифіката відкритого ключа.

3. Захист прав користувачів електронних довірчих послуг, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України «Про захист прав споживачів»

забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;

невідкладно повідомляти надавача електронних довірчих послуг про підозру або факт компрометації особистого ключа;

надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;

своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між надавачем та користувачем електронних довірчих послуг;

своєчасно надавати надавачу електронних довірчих послуг інформацію про зміну ідентифікаційних даних, які містить сертифікат відкритого ключа;

не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування сертифіката відкритого ключа.

3. Захист прав користувачів електронних довірчих послуг, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України «Про захист прав споживачів».

4. Порушення користувачами електронних довірчих послуг законодавства про електронні довірчі послуги:

правил використання електронних підписів та електронних довірчих послуг;

виготворення з метою збуту чи збут свідомо незаконно створених електронних підписів;

подання кваліфікованими надавачами електронних довірчих послуг завідомо неправдивої інформації та

	ідентифікаційних даних особи для створення підробних електронних підписів; створення умов для компрометації та компрометація особистого ключа електронного підпису; використання створених або отриманих у шахрайському або незаконному порядку електронних підписів, кваліфікованих сертифікатів відкритих ключів, кваліфікованих електронних підписів, паролів або будь-яких інших унікальних ідентифікаційних даних особи для доступу або несанкціонованого втручання в роботу систем електронних виборів, а також систем державних адміністративних послуг, електронного суду, державних інформаційних ресурсів та реєстрів, мережі державного управління; незаконне копіювання, зберігання або розповсюдження персональних чи будь-яких інших унікальних ідентифікаційних даних особи, які використовуються для створення електронних підписів та електронних довірчих послуг, передбачає відповідальність відповідно до закону
Стаття 13. Права та обов'язки кваліфікованих надавачів електронних довірчих послуг 1. Кваліфіковані надавачі електронних довірчих послуг мають право: надавати електронні довірчі послуги з дотриманням вимог цього Закону; отримувати документи, необхідні для ідентифікації	Стаття 13. Права, обов'язки та відповідальність кваліфікованих надавачів електронних довірчих послуг 1. Кваліфіковані надавачі електронних довірчих послуг мають право: надавати електронні довірчі послуги з дотриманням вимог цього Закону; отримувати документи, необхідні для ідентифікації

особи, ідентифікаційні дані якої міститимуться в сертифікаті відкритого ключа;

отримувати консультації від центрального засвідчувального органу або засвідчувального центру з питань, пов'язаних із наданням електронних довірчих послуг;

звертатися до органів з оцінки відповідності для отримання документів про відповідність;

звертатися із заявою про скасування, блокування або поновлення сформованих у центральному засвідчувальному органі або засвідчувальному центрі кваліфікованих сертифікатів відкритих ключів;

самостійно обирати, які саме стандарти будуть ними застосовуватися при наданні довірчих послуг із переліку стандартів, визначеного Кабінетом Міністрів України, крім сфери спеціального зв'язку.

2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:

захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства;

функціонування програмно-технічного комплексу, що ними використовується, та захист інформації, що в ньому обробляється, відповідно до вимог законодавства;

створення та функціонування свого вебсайту;

впровадження, підтримання в актуальному стані та публікацію на своєму вебсайті реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних,

особи, ідентифікаційні дані якої міститимуться в сертифікаті відкритого ключа;

отримувати консультації від центрального засвідчувального органу або засвідчувального центру з питань, пов'язаних із наданням електронних довірчих послуг;

звертатися до органів з оцінки відповідності для отримання документів про відповідність;

звертатися із заявою про скасування, блокування або поновлення сформованих у центральному засвідчувальному органі або засвідчувальному центрі кваліфікованих сертифікатів відкритих ключів;

самостійно обирати, які саме стандарти будуть ними застосовуватися при наданні довірчих послуг із переліку стандартів, визначеного Кабінетом Міністрів України, крім сфери спеціального зв'язку.

2. Кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити:

захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства;

функціонування програмно-технічного комплексу, що ними використовується, та захист інформації, що в ньому обробляється, відповідно до вимог законодавства;

створення та функціонування свого вебсайту;

впровадження, підтримання в актуальному стані та публікацію на своєму вебсайті реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних,

блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;

цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів;

скасування, блокування та поновлення сертифікатів відкритих ключів відповідно до вимог цього Закону;

встановлення під час формування сертифіката відкритого ключа належності відкритого ключа та відповідного йому особистого ключа підписувачу чи створювачу електронної печатки;

внесення ідентифікаційних даних підписувача чи створювача електронної печатки до відповідного сертифіката відкритого ключа;

інформування органу контролю про порушення конфіденційності та/або цілісності інформації, що впливає на надання електронних довірчих послуг або стосується персональних даних користувачів електронних довірчих послуг, не пізніше 24 годин з моменту, коли їм стало відомо про таке порушення;

інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливає на надання їм електронних довірчих послуг або стосується їхніх персональних даних, не пізніше двох годин з моменту, коли їм стало відомо про такі

блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування;

цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів;

скасування, блокування та поновлення сертифікатів відкритих ключів відповідно до вимог цього Закону;

встановлення під час формування сертифіката відкритого ключа належності відкритого ключа та відповідного йому особистого ключа підписувачу чи створювачу електронної печатки;

внесення ідентифікаційних даних підписувача чи створювача електронної печатки до відповідного сертифіката відкритого ключа;

інформування органу контролю про порушення конфіденційності та/або цілісності інформації, що впливає на надання електронних довірчих послуг або стосується персональних даних користувачів електронних довірчих послуг, не пізніше 24 годин з моменту, коли їм стало відомо про таке порушення;

інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливає на надання їм електронних довірчих послуг або стосується їхніх персональних даних, не пізніше двох годин з моменту, коли їм стало відомо про такі порушення;

унеможливлення використання особистого ключа в разі

порушення;

унеможливлення використання особистого ключа в разі його компрометації;

постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів;

внесення коштів на поточний рахунок із спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути заподіяна користувачам таких послуг чи третім особам унаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов'язань, у розмірі, визначеному частиною третьою статті 16 цього Закону;

наймання працівників, які володіють необхідними для надання кваліфікованих електронних довірчих послуг знаннями, досвідом і кваліфікацією, зокрема у сферах інформаційних технологій та захисту інформації;

використання під час надання електронних довірчих послуг виключно кваліфікованих сертифікатів, засвідчених у центральному засвідчувальному органі чи засвідчувальному центрі;

зберігання документів, поданих користувачами для отримання електронних довірчих послуг;

інформування органу контролю та центрального засвідчувального органу або засвідчувального центру про будь-які зміни у процедурі надання електронних довірчих

його компрометації;

постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів;

внесення коштів на поточний рахунок із спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути заподіяна користувачам таких послуг чи третім особам унаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов'язань, у розмірі, визначеному частиною третьою статті 16 цього Закону;

наймання працівників, які володіють необхідними для надання кваліфікованих електронних довірчих послуг знаннями, досвідом і кваліфікацією, зокрема у сферах інформаційних технологій та захисту інформації;

використання під час надання електронних довірчих послуг виключно кваліфікованих сертифікатів, засвідчених у центральному засвідчувальному органі чи засвідчувальному центрі;

зберігання документів, поданих користувачами для отримання електронних довірчих послуг;

інформування органу контролю та центрального засвідчувального органу або засвідчувального центру про будь-які зміни у процедурі надання електронних довірчих послуг протягом 48 годин з моменту настання таких змін;

передачу центральному засвідчувальному органу або

послуг протягом 48 годин з моменту настання таких змін;
 передачу центральному засвідчувальному органу або засвідчувальному центру документованої інформації в разі припинення діяльності з надання електронних довірчих послуг.

3. Обов'язкові вимоги до кваліфікованих надавачів електронних довірчих послуг, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України

засвідчувальному центру документованої інформації в разі припинення діяльності з надання електронних довірчих послуг.

3. Обов'язкові вимоги до кваліфікованих надавачів електронних довірчих послуг, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

4. Порухення кваліфікованими надавачами електронних довірчих послуг законодавства про електронні довірчі послуги:

правил створення, надання, використання та знищення електронних підписів та електронних довірчих послуг;

виотовлення з метою збути чи збут свідомо незаконно створених електронних підписів;

створення умов для компрометації та компрометація особистого ключа електронного підпису;

використання створених або отриманих у шахрайському або незаконному порядку електронних підписів, кваліфікованих сертифікатів відкритих ключів, кваліфікованих електронних підписів, паролів або будь-яких інших унікальних ідентифікаційних даних особи для доступу або несанкціонованого втручання в роботу систем електронних виборів, а також систем державних адміністративних послуг, електронного суду, державних інформаційних ресурсів та реєстрів, мережі державного управління;

незаконне копіювання, зберігання або розповсюдження

	даних, зокрема персональних чи будь-яких інших унікальних ідентифікаційних даних особи, які використовуються для створення електронних підписів та електронних довірчих послуг, передбачає відповідальність відповідно до закону
Стаття 16. Вимоги до електронних довірчих послуг 1. Електронні довірчі послуги надаються, як правило, на договірних засадах надавачами електронних довірчих послуг. 2. До складу електронних довірчих послуг входять: створення, перевірка та підтвердження вдосконаленого електронного підпису чи печатки; формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки; формування, перевірка та підтвердження чинності сертифіката автентифікації вебсайту; формування, перевірка та підтвердження електронної позначки часу; реєстрована електронна доставка; зберігання вдосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних із цими послугами. Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися і окремо, і в сукупності. 3. Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське	Стаття 16. Вимоги до електронних довірчих послуг 1. Електронні довірчі послуги надаються, як правило, на договірних засадах надавачами електронних довірчих послуг. 2. До складу електронних довірчих послуг входять: створення, перевірка та підтвердження удосконаленого електронного підпису чи печатки; формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки; формування, перевірка та підтвердження чинності сертифіката автентифікації вебсайту; формування, перевірка та підтвердження електронної позначки часу; реєстрована електронна доставка; зберігання вдосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних із цими послугами. Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися і окремо, і в сукупності. 3. Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське

обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному рахунку із спеціальним режимом використання в банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менше ніж 1000 мінімальних розмірів заробітної плати.

4. Розподіл ризиків збитків, що можуть бути заподіяні користувачам електронних довірчих послуг та третім особам фізичними або юридичними особами, не внесеними центральним засвідчувальним органом до Довірчого списку, визначається суб'єктами правових відносин на договірних засадах

обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному рахунку із спеціальним режимом використання в банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менше ніж 100 мінімальних розмірів заробітної плати.

Діяльність іноземних кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом **Державного цифрового довірчого центру (третя довірча сторона)** для страхування цивільно-правової відповідальності або забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам.

4. Розподіл ризиків збитків, що можуть бути заподіяні користувачам електронних довірчих послуг та третім особам фізичними або юридичними особами, не внесеними центральним засвідчувальним органом до Довірчого списку, визначається суб'єктами правових відносин на договірних засадах

Стаття 22. Ідентифікація особи під час формування та видачі кваліфікованого сертифіката відкритого ключа

1. Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не дозволяються.

Стаття 22. Ідентифікація особи під час формування та видачі кваліфікованого сертифіката відкритого ключа

1. Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не дозволяються.

2. Ідентифікація фізичної особи, яка звернулася за отриманням послуги з формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливають виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

3. Допускається ідентифікація фізичної особи кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа за умови чинності цього сертифіката.

4. Ідентифікація іноземців здійснюється відповідно до законодавства.

5. Під час перевірки цивільної правоздатності та дієздатності юридичної особи кваліфікований надавач електронних довірчих послуг зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

6. Кваліфікований надавач електронних довірчих послуг під час формування та видачі кваліфікованого сертифіката

2. Ідентифікація фізичної особи, яка звернулася за отриманням послуги з формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливають виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

3. Допускається ідентифікація фізичної особи кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа за умови чинності цього сертифіката.

4. Ідентифікація іноземців здійснюється відповідно до законодавства.

5. Під час перевірки цивільної правоздатності та дієздатності юридичної особи кваліфікований надавач електронних довірчих послуг зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

6. Кваліфікований надавач електронних довірчих послуг під час формування та видачі кваліфікованого сертифіката

відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог цього Закону, а також перевіряє обсяг його повноважень за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, кваліфікованому надавачу електронних довірчих послуг подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами

відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог цього Закону, а також перевіряє обсяг його повноважень за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, кваліфікованому надавачу електронних довірчих послуг подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

7. Ідентифікація особи державного службовця та посадової особи місцевого самоврядування, яка звернулася за отриманням послуги з формування кваліфікованого сертифіката відкритого ключа для виконання посадових повноважень, здійснюється за умови її особистої присутності і за паспортом громадянина України та в порядку, встановленому Кабінетом Міністрів України

Стаття 23. Кваліфіковані сертифікати відкритих ключів

1. Під час надання кваліфікованих електронних довірчих послуг використовуються кваліфіковані сертифікати електронного підпису, кваліфіковані сертифікати електронної печатки та кваліфіковані сертифікати автентифікації вебсайту.

2. Кваліфіковані сертифікати відкритих ключів обов'язково повинні містити:

1) позначку, що сертифікат відкритого ключа виданий як

Стаття 23. Кваліфіковані сертифікати відкритих ключів

1. Під час надання кваліфікованих електронних довірчих послуг використовуються кваліфіковані сертифікати електронного підпису, кваліфіковані сертифікати електронної печатки та кваліфіковані сертифікати автентифікації вебсайту.

2. Кваліфіковані сертифікати відкритих ключів обов'язково повинні містити:

1) позначку, що сертифікат відкритого ключа виданий як кваліфікований сертифікат відкритого ключа;

кваліфікований сертифікат відкритого ключа;

2) позначку, що сертифікат відкритого ключа виданий в Україні;

3) ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа (далі – суб'єкти, які видали сертифікат), зокрема обов'язково:

для юридичної особи: найменування та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено її державну реєстрацію;

для фізичної особи-підприємця: прізвище, ім'я, по батькові (за наявності) та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), за якими здійснено її державну реєстрацію;

4) ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг, зокрема обов'язково:

прізвище, ім'я, по батькові (за наявності) підписувача та

2) позначку, що сертифікат відкритого ключа виданий в Україні;

3) ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа (далі – суб'єкти, які видали сертифікат), зокрема обов'язково:

для юридичної особи: найменування та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено її державну реєстрацію;

для фізичної особи-підприємця: прізвище, ім'я, по батькові (за наявності) та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), за якими здійснено її державну реєстрацію паспорті про право здійснювати платежі за серією та номером паспорта), за якими здійснено її державну реєстрацію;

для державного службовця та посадової особи місцевого самоврядування обов'язкові відомості визначаються Кабінетом Міністрів України додатково за вимогами, встановленими органом державної влади та

унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), або;

найменування або прізвище, ім'я, по батькові (за наявності) створювача електронної печатки та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено його державну реєстрацію, або унікальний номер запису в Єдиному державному демографічному реєстрі, або реєстраційний номер облікової картки платника податків, або серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

5) місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;

6) значення відкритого ключа, який відповідає особистому ключу;

7) відомості про початок та закінчення строку дії

місцевого самоврядування;

4) ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг, зокрема обов'язково:

прізвище, ім'я, по батькові (за наявності) підписувача та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), або;

найменування або прізвище, ім'я, по батькові (за наявності) створювача електронної печатки та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено його державну реєстрацію, або унікальний номер запису в Єдиному державному демографічному реєстрі, або реєстраційний номер облікової картки платника податків, або серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган доходів і зборів та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

кваліфікованого сертифіката відкритого ключа;

8) серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;

9) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені суб'єктом, який видав сертифікат;

10) відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;

11) відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;

12) відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

13) відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

14) ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації вебсайту).

3. Кваліфіковані сертифікати відкритих ключів можуть містити інші ідентифікаційні дані фізичних або юридичних

5) місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;

6) значення відкритого ключа, який відповідає особистому ключу;

7) відомості про початок та закінчення строку дії кваліфікованого сертифіката відкритого ключа;

8) серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;

9) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені суб'єктом, який видав сертифікат;

10) відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;

11) відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;

12) відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

13) відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);

осіб, необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

4. Обов'язкові вимоги до кваліфікованих сертифікатів відкритих ключів, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

5. Правочин, вчинений в електронній формі, може бути визнаний судом недійсним у разі, коли під час його вчинення використовувався кваліфікований електронний підпис чи печатка, кваліфікований сертифікат якого/якої не містить відомостей, передбачених частиною другою цієї статті, або містить недостовірні відомості

14) ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації вебсайту).

3. Кваліфіковані сертифікати відкритих ключів можуть містити інші ідентифікаційні дані фізичних або юридичних осіб, необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

4. Обов'язкові вимоги до кваліфікованих сертифікатів відкритих ключів, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

5. Правочин, вчинений в електронній формі, може бути визнаний судом недійсним у разі, коли під час його вчинення використовувався кваліфікований електронний підпис чи печатка, кваліфікований сертифікат якого/якої не містить відомостей, передбачених частиною другою цієї статті, або містить недостовірні відомості.

Стаття 25. Скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів

1. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин скасовується суб'єктом, який видав сертифікат, у разі:

1) подання користувачем електронних довірчих послуг заяви про скасування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що

Стаття 25. Скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів

1. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин скасовується суб'єктом, який видав сертифікат, у разі:

1) подання користувачем електронних довірчих послуг заяви про скасування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що

забезпечує підтвердження особи-користувача;

2) надходження до суб'єкта, який видав сертифікат, документа, що підтверджує:

- смерть фізичної особи-підписувача;
- припинення діяльності створювача електронної печатки;
- зміни ідентифікаційних даних користувача електронних довірчих послуг;

факт державної реєстрації припинення підприємницької діяльності фізичної особи-підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи;

надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката відкритого ключа;

факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або органом контролю під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

набрання законної сили рішення суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

2. Самопідписаний сертифікат електронної печатки центрального засвідчувального органу не пізніше ніж

забезпечує підтвердження особи-користувача;

2) подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про скасування виданого йому або державним службовцям органу державної влади або посадової особи органу місцевого самоврядування кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача та особи уповноваженого представника державного органу та органу місцевого самоврядування;

3) надходження до суб'єкта, який видав сертифікат, документа, що підтверджує:

- смерть фізичної особи-підписувача;
- припинення діяльності створювача електронної печатки;
- зміни ідентифікаційних даних користувача електронних довірчих послуг;

факт державної реєстрації припинення підприємницької діяльності фізичної особи-підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи;

надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката відкритого ключа;

факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або органом контролю під час здійснення

протягом 24 годин скасовується центральним засвідчувальним органом у разі:

підтвердження факту компрометації особистого ключа центрального засвідчувального органу, виявленого ним самостійно або органом контролю під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

набрання законної сили рішення суду про скасування самопідписаного сертифіката електронної печатки центрального засвідчувального органу.

3. У разі подання повідомлення про прийняття кваліфікованим надавачем електронних довірчих послуг рішення про припинення діяльності з надання кваліфікованих електронних довірчих послуг центральний засвідчувальний орган або засвідчувальний центр на основі відповідного рішення скасовує кваліфікований сертифікат відкритого ключа, виданий цьому надавачу відповідно до вимог цього Закону.

4. Кваліфікований сертифікат відкритого ключа вважається скасованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на скасований.

5. Скасований кваліфікований сертифікат відкритого ключа поновленню не підлягає.

6. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин блокується суб'єктом, який видав сертифікат, у разі:

заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

набрання законної сили рішення суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

2. Самопідписаний сертифікат електронної печатки центрального засвідчувального органу не пізніше ніж протягом 24 годин скасовується центральним засвідчувальним органом у разі:

підтвердження факту компрометації особистого ключа центрального засвідчувального органу, виявленого ним самостійно або органом контролю під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

набрання законної сили рішення суду про скасування самопідписаного сертифіката електронної печатки центрального засвідчувального органу.

3. У разі подання повідомлення про прийняття кваліфікованим надавачем електронних довірчих послуг рішення про припинення діяльності з надання кваліфікованих електронних довірчих послуг центральний засвідчувальний орган або засвідчувальний центр на основі відповідного рішення скасовує кваліфікований сертифікат відкритого ключа, виданий цьому надавачу відповідно до вимог цього

подання користувачем електронних довірчих послуг заяви про блокування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача;

повідомлення користувачем електронних довірчих послуг або органом контролю про підозру в компрометації особистого ключа користувача електронних довірчих послуг;

набрання законної сили рішення суду про блокування кваліфікованого сертифіката відкритого ключа;

порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг.

7. Кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також блокується у разі прийняття рішення органом контролю про блокування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача електронних довірчих послуг за результатами здійснення державного нагляду (контролю) відповідно до вимог цього Закону.

8. Кваліфікований сертифікат відкритого ключа вважається заблокованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на заблокований.

9. Кваліфікований сертифікат відкритого ключа, статус якого змінено на заблокований, у період блокування не використовується.

10. Заблокований кваліфікований сертифікат відкритого

Закону.

4. Кваліфікований сертифікат відкритого ключа вважається скасованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на скасований.

5. Скасований кваліфікований сертифікат відкритого ключа поновленню не підлягає.

6. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин блокується суб'єктом, який видав сертифікат, у разі:

подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про блокування виданого йому або державним службовцем органу державної влади або посадової особи органу місцевого самоврядування кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача та особи уповноваженого представника державного органу та органу місцевого самоврядування;

повідомлення користувачем електронних довірчих послуг або органом контролю про підозру в компрометації особистого ключа користувача електронних довірчих послуг;

набрання законної сили рішення суду про блокування кваліфікованого сертифіката відкритого ключа;

порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг.

ключа не пізніше ніж протягом двох годин поновлюється суб'єктом, який видав сертифікат, у разі:

подання користувачем електронних довірчих послуг заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);

повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або органом контролю, який раніше повідомив про цю підозру;

надходження до суб'єкта, який видав сертифікат, повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката відкритого ключа, що набрало законної сили

7. Кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також блокується в разі прийняття рішення органом контролю про блокування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача електронних довірчих послуг за результатами здійснення державного нагляду (контролю) відповідно до вимог цього Закону.

8. Кваліфікований сертифікат відкритого ключа вважається заблокованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на заблокований.

9. Кваліфікований сертифікат відкритого ключа, статус якого змінено на заблокований, у період блокування не використовується.

10. Заблокований кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин поновлюється суб'єктом, який видав сертифікат, у разі:

подання користувачем електронних довірчих послуг або уповноваженим представником державного органу та органу місцевого самоврядування заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);

повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або органом

контролю, який раніше повідомив про цю підозру;
надходження до суб'єкта, який видав сертифікат, повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката відкритого ключа, що набрало законної сили

Розділ VI МІЖНАРОДНЕ СПІВРОБІТНИЦТВО

Стаття 37. Участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації

1. Україна бере участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації, зокрема на основі міжнародних договорів України.

2. Участь України в міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації здійснюється в порядку, встановленому законом.

3. У разі якщо міжнародними договорами України встановлено інші правила, ніж ті, що містяться в цьому Законі, застосовуються правила міжнародних договорів України.

Стаття 38. Визнання іноземних електронних довірчих послуг

1. Електронні довірчі послуги, що надаються відповідно до вимог нормативно-правових актів, що регулюють правові відносини у сфері електронних довірчих послуг в іноземних

Стаття 37. Участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації

1. Україна бере участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації, зокрема на основі міжнародних договорів України.

2. Участь України в міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації здійснюється в порядку, встановленому законом.

3. У разі якщо міжнародними договорами України встановлено інші правила, ніж ті, що містяться в цьому Законі, застосовуються правила міжнародних договорів України.

Стаття 38. Визнання іноземних електронних довірчих послуг

1. Електронні довірчі послуги, що надаються відповідно до вимог нормативно-правових актів, що регулюють правові відносини у сфері електронних довірчих послуг в іноземних

держав, визнаються в Україні електронними довірчими послугами того самого виду в разі відповідності хоча б одній з таких умов:

кваліфікований надавач електронних довірчих послуг іноземної держави відповідає вимогам цього Закону, що підтверджується центральним засвідчувальним органом (або засвідчувальним центром у разі надання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів);

кваліфікований надавач електронних довірчих послуг внесений до Довірчого списку держави, з якою Україна уклала відповідний двосторонній або багатосторонній міжнародний договір.

2. Електронні довірчі послуги не можуть визнаватися недійсними лише через те, що вони надані відповідно до вимог нормативно-правових актів, що регулюють відносини у сфері електронних довірчих послуг в іноземних державах.

3. Порядок використання інформаційно-телекомунікаційної системи центрального засвідчувального органу для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, встановлюється Кабінетом Міністрів України

держав, визнаються в Україні електронними довірчими послугами того самого виду в разі відповідності хоча б одній з таких умов:

кваліфікований надавач електронних довірчих послуг іноземної держави відповідає вимогам цього Закону, що підтверджується центральним засвідчувальним органом (або засвідчувальним центром у разі надання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів);

кваліфікований надавач електронних довірчих послуг внесений до Довірчого списку держави, з якою Україна уклала відповідний двосторонній або багатосторонній міжнародний договір.

2. Електронні довірчі послуги не можуть визнаватися недійсними лише через те, що вони надані відповідно до вимог нормативно-правових актів, що регулюють відносини у сфері електронних довірчих послуг в іноземних державах.

3. Внесення до Довірчого списку України кваліфікованого надавача електронних довірчих послуг, що відповідає умовам п.п. 1 п. 1 ст. 38 цього Закону за його заявою може здійснюватися Державним цифровим довірчим центром (третя довірча сторона) без укладання між іноземною державою та Україною відповідного двостороннього або багатостороннього міжнародного договору за погодженням Центрального засвідчувального органу.

4. Порядок використання інформаційно-

	телекомунікаційної системи Державного цифрового довірчого центру (третья довірча сторона) для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав, встановлюється Кабінетом Міністрів України
--	--

Додаток Г

Основні національні акти у сфері електронного підпису та електронних
довірчих послуг країн Європейського Союзу

Країна	Основні національні акти у сфері електронного підпису та електронних довірчих послуг
Австрія	Signaturgesetz -SigG, BGBl. I Nr. 190/1999
Бельгія	9 Juli 2001 Wet houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatediensten. Koninklijk besluit van 6 december 2002 houdende organisatie van de controle en de accreditatie van de certificatedienstverleners die gekwalificeerde certificaten afleveren (Belgisch Staatsblad, 17 januari 2003)
Болгарія	Закон за Електронния Документ и Електронния Подпис (номер 34 от 2001 г.)
Велика Британія	Electronic Communications Act 2000
Греція	Presidential Decree 150/2001
Данія	Lov om elektroniske signaturer Nr. 417
Естонія	Digitaalallkirja seadus Vastu võetud 8. märtsil 2000. a. (RT I 2000, 26, 150) jõustunud 15. detsembril 2000. Tsiviilseadustiku üldosa seadus Vastu võetud 27. märtsil 2002. a (RT I 2002, 35, 216) jõustunud 1. juulil 2002
Ірландія	Electronic Commerce Act, 2000
Іспанія	Ley 59/2003, de 19 de diciembre, de firma electrónica.
Італія	Legge 25 marzo 1997, n.59 Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa. Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Decreto del Presidente della Repubblica 7 aprile 2003 n. 137 Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio

	2002, n. 10. Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale. Decreto legislativo 4 aprile 2006, n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale 97
Кіпр	Law on the Legal Framework for Electronic Signatures and Associated Matters of 2004, Law No. 188(I)/2004
Латвія	Elektronisko dokumentu likums
Литва	Elektroninio parašo įstatymas 2000 m. liepos 11 d. Nr. VII-182
Люксембург	Loi du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques, la directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE du 20 mai 1997 concernant la vente à distance des biens et des services autres que les services financiers.
Мальта	Electronic Commerce Act 2002
Нідерланди	Wet van 8 mei 2003 tot aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de Economische Delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (Wet elektronische handtekeningen), Staatsblad 2003
Німеччина	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz –SigG) vom 16.5.2001 (BGBl. I S. 876). VwVfG Verwaltungsverfahrensgesetz [I B 25]

	BGB Bürgerliches Gesetzbuch (BGB)76ZPO Zivilprozessordnung 77
Польща	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym
Португалія	Decreto-lei no. 290-D/99, de 2 de Agosto. Decreto-lei no. 375/99, de 18 de Setembro. Decreto-lei no. 146/2000, de 18 de Julho. Decreto-lei no. 234/2000, de 25 de Setembro143Decreto-lei no. 62/2003, de 3 de Abril.
Румунія	Lege nr. 455 din 18 iulie 2001 privind semnătura electronică
Словаччина	Zakon č. 215/2002 Z.z.o elektronickom podpise a o zmene a doplnení niektorých zákonov
Словенія	Zakon o elektronskem poslovanju in elektronskem podpisu (uradno prečiščeno besedilo), Uradni list Republike Slovenije št. 98/200
Угорщина	2001. évi XXXV. Törvény az elektronikus aláírásról
Фінляндія	Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, 7.8.2009/617
Франція	Loi No 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. Décret no 2001-272 du mars 30, 2001 pris pour l'application de l'article 1316-4 du code civil relatif à la signature électronique. Décret no 2002-535 du avril 18, 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. Arrêté ministériel du mai 31, 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation
Хорватія	Zákon o elektronickém podpisu
Чехія	Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
Швеція	Lag (2000:832) om kvalificerade elektroniska signatur

Додаток Д

Нормативні акти у сфері електронного підпису Сполучених Штатів Америки

№ з/п	Юрисдикція	Назва нормативно-правового акту
1	Федеральний рівень	Electronic Signatures in Global and National Commerce Act (E-SIGN).
2	Алабама	Alabama Uniform Electronic Transactions Code, Ala. Rev. Code Ann. §§ 8-1A-1 to 8-1A-20.
3	Аляска	Electronic Records and Signatures Act, Al. Stat. §§ 09.25.510.
4	Аризона	Uniform Electronic Transactions Act, Ariz. Rev. Stat. Ann. §§ 44-7001 to 44-7051.
5	Арканзас	Uniform Electronic Transactions Act, Ark. Code Ann. §§ 25-31-101 to 25-32-121.
6	Каліфорнія	Uniform Electronic Transactions Act, Cal. Civ. Code § 1624.5, §§ 1633.1 to 1633.17.
7	Колорадо	Government Electronic Transactions Act, Colo. Rev. Stat. Ann. §§ 24-71-101 to 71.3-121.
8	Коннектикут	Connecticut Uniform Electronic Transactions Act, Conn. Gen. Stat. Ann. §§ 1-266 to 1-286.
9	Делавер	Uniform Electronic Transactions Act, Del. Cod Ann. Tit. 6, §§ 12A-101 to 12A-117.
10	Округ Колумбія	Uniform Electronic Transactions Act, D.C. Code Ann. §§ 28-4901 to 4918.
11	Флорида	Uniform Electronic Transactions Act, Fla. Stat. Ann. §§ 668.50 to 668.50.
12	Джорджія	Georgia Electronic Records and Signatures Act, Ga. Code Ann. §§ 10-12-1 to 10-12-5.
13	Гаваї	Uniform Electronic Transactions Act, Haw. Rev. Stat. §§ 489E-1 to HRS § 489E-18.
14	Айдахо	Uniform Electronic Transactions Code, Idaho Code ann. §§ 28-50-101 to 28-50-120.
15	Іллінойс	Electronic Commerce Security Act, 5 Ill. Comp. Stat. §§ 175/5-101 to 175/99-1.
16	Індіана	Uniform Electronic Transactions Act, Ind. Code Ann. §§ 26-2-8-101 to 26-2-8.
17	Айова	Uniform Electronic Transactions Act, Iowa Code Ann. §§ 554D.101 to 554D.123.
18	Канзас	Uniform Electronic Transactions Act, Kan. Stat. Ann. §§ 16-1601 to 16-1620.
19	Кентуккі	Uniform Electronic Transactions Act, Ky. Rev. Stat. Ann. §§ 369.101 to 369.120.
20	Луїзіана	Uniform Electronic Transactions Act, La. Rev. Stat. Ann. §§ 9:2601 to 9:2620.
21	Мен	Uniform Electronic Transactions Act, Me. Rev. Stat. Ann. Tit. 10, §§ 9401 to 9507.

22	Меріленд	Uniform Electronic Transactions Act, Md. Code Ann., Com. Law II §§ 21-101 to 21-120.
23	Массачусетс	Uniform Electronic Transactions Act, ALM GL ch. 110G, § 1 to § 18.
24	Мічиган	Uniform Electronic Transactions Act, Mich. Comp. Laws Ann. §§ 450.831 to 450.849.
25	Міннесота	Uniform Electronic Transactions Act, Minn. Stat. Ann. §§ 325L.01 to 325L.19.
26	Міссісіпі	Mississippi Electronic Transactions Act, Miss. Code Ann. §§ 75-12-1 to 75-12-39.
27	Міссурі	Uniform Electronic Transactions Act, Mo. Rev. Stat. Ann. 432.200 to 432.295.
28	Монтана	Uniform Electronic Transactions Act, Mont. Code Ann. §§ 30-18-101 to 30-18-118.
29	Небраска	Uniform Electronic Transactions Act, Neb. Rev. Stat. §§ 86-611 to 86-643.
30	Невада	Uniform Electronic Transactions Act, Nev. Rev. Stat. Ann. §§ 719.010 to 719.350.
31	Нью-Хампшир	Uniform Electronic Transactions Act, N.H. Rev. Stat. Ann. §§ 294-E:1 to 294-E:20.
32	Нью-Джерсі	New Jersey Electronic Transactions Act, N.J. Stat. Ann. §§ 12A:12-1 to 12A:12-26.
33	Нью-Мексико	Electronic Authentication of Documents Act, N.M. Stat. Ann. §§ 14-16-1 to 14-16-19.
34	Нью-Йорк	Electronic Signatures and Records Act, N.Y. State Technology Law §§ 301 to 309.
35	Північна Кароліна	Uniform Electronic Transactions Act, N.C. Gen. Stat. Ann. §§ 66-308 to 66.328.
36	Північна Дакота	Uniform Electronic Transactions Act, N.D. Cent. Code §§ 9-16-01 9-16-18.
37	Огайо	Uniform Electronic Transactions Act, Ohio Rev. Code Ann. §§ 11306.01 to 1306.23.
38	Оклахома	Uniform Electronic Transactions Act, Okla. Stat. Ann. Tit. 12A §§ 15-101 to 15-121.
39	Орегон	Uniform Electronic Transactions Act, Or. Rev. Stat. §§ 84.001 to 84.064.
40	Пенсильванія	Uniform Electronic Transactions Act, Pa. Stat. Ann. Tit. 73, §§ 2260.101 to 2260.903.
41	Род Айленд	Uniform Electronic Transactions Act, R.I. Code R. §§ 42-127.1-1 to 42-127.1-20.
42	Південна Кароліна	Electronic Commerce Act, S.C. Code Ann. §§ 26-5-10 to 26-6-190.
43	Південна Дакота	Uniform Electronic Transactions Act, S.D. Codified Laws §§ 53-12-1 to 53-12-05.
44	Теннессі	Uniform Electronic Transactions Act, Tenn. Code Ann. §§ 47-10-101 to 47-10-123.
45	Техас	Uniform Electronic Transactions Act, Texas Bus. & Com. Code Ann. §§ 43-001 to 43-021.
46	Юта	Uniform Electronic Transactions Act, Utah Code Ann. §§ 46-4-101 to 46-4-503.
47	Вермонт	Vermont Electronic Transactions Act, Vt. Stat. Ann. 9 §§ 270to 290.

48	Віргінські Острови	Uniform Electronic Transactions Act, Virgin Islands Code, §§ 101 to 120.
49	Вашингтон	Electronic Authentication Act, Rev. Code of Wash. Ann. §§ 19.34.010 to 19.34.903.
50	Західна Вірджинія	West Virginia Electronic Transactions Act, W.V. Code §§ 39A-1-1 to 39A-1-17; 39A-2-1 to 39A-2-12.
51	Вісконсин	Wisconsin Electronic Transactions Act, Wis. Stat. Ann. §§ 137.01, 137.04 to 137.06.
52	Вайомінг	Uniform Electronic Transactions Act, Wyo. Stat. Ann. §§ 40-21-101 to 40-21-119.

Додаток Ж

Узагальнені відомості про стан сфери електронного підпису та електронних довірчих послуг

№ з/п	Кваліфіковані надавачі електронних довірчих послуг	Загальна кількість сформованих електронних підписів	Загальна кількість сформованих кваліфікованих електронних підписів	Кількість сформованих кваліфікованих електронних підписів на захищеному носієві	Кількість наданих кваліфікованих електронних довірчих послуг формування перевірки та підтвердження кваліфікованої ЕПЧ
1	АТ КБ «ПРИВАТБАНК»	6242	2313442	0	72600000
2	Військова частина 2428	22639	5520	746	14651979
3	ГШ Збройних Сил України	12811	3832	1783	539865
4	Генеральна прокуратура України	2	9348	9	0
5	Державна казначейська служба України	347295	50397	44719	265908
6	Державне підприємство «Енергоринок»	1976	320	24	333632
7	ДП «Національні інформаційні системи»	747988	47080	28432	98175110
8	ДП «Український інститут інтелектуальної власності»	1316	120	15	120
9	ДП «Українські	388296	52641	26	693684

	спеціальні системи»				
10	Інформаційно-довідковий департамент ДФС	6984848	580042	13186	87567707
11	МВС України	6586	128	128	10820000
12	Національний банк України	2203	4270	90	924799
13	ПАТ «Державний ощадний банк України»	83863	21295	0	431799
14	ПАТ «Національний депозитарій України»	55346	5744	0	0
15	ПАТ «УкрСиббанк»	76399	10654	9728	78839
16	ТОВ «Алтерсайд»	—	—	—	—
17	ТОВ «Арт-майстер»	911647	30901	0	4950000
18	ТОВ «Інтер-Метл»	53101	9743	0	—
19	ТОВ «Ключові системи»	391978	78054	600	—
20	ТОВ «Центр сертифікації ключів «Україна»	5642256	940837	5143	100603229
21	Філія «Головний інформаційно-обчислювальний центр» ПАТ «Українська залізниця»	397280	41580	1044	15075750
Всього *		22370116	4205948	105673	407712421

- дані надані за весь час функціонування суб'єкта сфери цифрового підпису Інформація про діяльність постачальників електронних довірчих послуг, в частині послуг, що надавались танадаються кваліфікованими надавачами електронних довірчих послуг, станом на 31 березня 2019 року. Режим доступу :<https://czo.gov.ua/download/docs/info310319.pdf>

Порівняльна таблиця дефініцій поняття «електронний підпис»

Термін	Дефініція
Електронний підпис	дані в електронній формі, які містяться в повідомленні даних, включені до нього або логічно асоціюються з ним і які можуть бути використані для ідентифікації підписувача у зв'язку з повідомленням даних і вказівки на те, що підписувач згоден з інформацією, яка міститься в повідомленні даних
	дані в електронній формі, які приєднуються або логічно пов'язуються з іншими електронними даними й використовуються підписувачем як підпис
	електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис
	набір інтегрованих електронних даних, пов'язаних або логічно пов'язаних з іншими електронними даними, які використовуються підписувачем як засіб ідентифікації, при цьому відсутні будь-які юридичні вимоги, за якими підпис можна вважати цифровим підписом
	дані, запис або згенеровані дані, зображення або звук, збережені, отримані або відправлені в електронній формі
	будь-які літери, символи, цифри або інші символи в цифровій формі, прикріплені до електронного запису або логічно пов'язані з ним, а також створені чи прийняті з метою автентифікації або затвердження електронного запису
	щось в електронній формі, вбудоване або логічно пов'язане з електронним повідомленням або даними з метою підтвердження їхньої цілісності та автентичності, або дані в електронній формі, приєднані або логічно пов'язані з іншими даними в електронній формі, які використовуються для підтвердження автентичності
	електронний ідентифікатор, що включає в себе і поняття цифрового підпису, який є унікальним для його підписувача, справжність якого може бути підтверджена і який перебуває під особистим

	контролем підписувача та приєднаний до підписаних даних таким чином, що можна відстежити зміни документа, зроблені після підписання, а також передбачається, що підписувач наділяє його однаковою силою з власноручним підписом
	будь-які літери або символи, створені електронними засобами, що дозволяють підтвердити авторство і справжність документа або спростувати їх

*сформовано автором за джерелами: [98;99;100;108;110;111;112;117;119]

Порівняльна таблиця дефініцій поняття «цифровий підпис»

Поняття	Дефініція
Цифровий підпис	є послідовністю бітів, яку особа, яка має намір підписати, створює відносно явно виділеного повідомлення шляхом проведення повідомлення через односпрямовану функцію, шифруючи потім отриманий дайджест з використанням асиметричної криптосистеми й закритого ключа особи
	результат застосування математичної процедури до цифрового документа, яка потребує унікальної інформації стосовно підписувача та перебуває під його особистим контролем Аргентина
	частина інформації в цифровій формі, що прикріплена або логічно об'єднана з електронним повідомленням, яка може ідентифікувати підписувача й надає можливість перевірки того, що електронне повідомлення було підписано цим підписувачем
	автентифікація будь-якого електронного запису абонентом за допомогою електронного методу або процедура за законом
	електронний підпис підписувача, отриманий шляхом перетворення електронного запису з використанням асиметричної криптосистеми та хеш-функції особою, яка має початковий нетрансформований електронний запис і відкритий ключ підписувача, та дозволяє визначити, що генеровані перетворення здійснено за допомогою закритого ключа, який відповідає відкритому ключу підписувача, та може визначити наявність або відсутність змін початкового електронного запису після генерування
	розуміється як різновид електронного підпису, який перетворює повідомлення, використовуючи асиметричний криптографічний алгоритм таким чином, що одержувач повідомлення, маючи відкритий ключ, може визначити: чи було повідомлення спочатку зашифровано з використанням відповідного закритого ключа і чи було повідомлення змінено з моменту перетворення (шифрування)

	визначається як печатка, що завіряє цифрові дані, яка створена за допомогою закритого ключа й дозволяє, використовуючи відповідний відкритий ключ, визначити власника ключа й підтвердити цілісність і автентичність даних
	набір символів, що виробляється засобами електронного цифрового підпису та є невід'ємною частиною електронного документа

*сформовано автором за джерелами: [42;43;44;46;47;53;108;113;114]

Порівняльна таблиця дефініцій поняття «удосконалений електронний підпис»

Поняття	Дефініція
Удосконалений цифровий підпис	електронний підпис, який відповідає вимогам, викладеним у статті 26 Регламенту
	електронний підпис, створений у результаті криптографічного перетворення електронних даних, з якими пов'язаний цей електронний підпис, з використанням засобу вдосконаленого електронного підпису та особистого ключа, однозначно пов'язаного з підписувачем, який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов'язаний цей електронний підпис
	електронний підпис, що задовольняє такі умови: він унікальним чином пов'язаний із підписувачем; надає можливість ідентифікації підписувача; створений із використанням програмних засобів, що перебувають під особистим контролем підписувача; пов'язаний з даними, які підписуються, таким чином, що будь-яку зміну даних після процедури підписання можливо виявити»
кваліфікований цифровий підпис	удосконалений електронний підпис, який створюється засобом для створення кваліфікованого електронного підпису й базується на кваліфікованому сертифікаті для електронних підписів
	удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису й базується на кваліфікованому сертифікаті відкритого ключа
	цифровий підпис, який заснований на авторизованому сертифікаті й відповідає таким вимогам: ключ для створення цифрового підпису повинен зберігатися й бути відомим тільки підписувачу; підписувач повинен особисто контролювати створення цифрового підпису та використовувати ключ на момент підписання; можливість встановлення фактів змін у відповідному цифровому підписі з моменту його прикріплення, а також встановлення змін в електронному повідомленні, підписаному цифровим підписом

*сформовано автором за джерелами: [42;43;44;46;47;53;108;113;114]

**Довідки про впровадження результатів
дисертації**



УКРАЇНА

**НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОГО УПРАВЛІННЯ
ПРИ ПРЕЗИДЕНТОВІ УКРАЇНИ
ІНСТИТУТ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ КЕРІВНИХ КАДРІВ**
04050 Україна, Київ, вул. Академіка Ромоданова, 12/2
тел.: (044) 483-76-02 факс: (044) 483-76-02

29.10.2019 № *23-11/496*

На № _____

**Довідка
про використання результатів кандидатської дисертації
«Правове забезпечення транскордонного надання
електронних довірчих послуг»
Костенка Олексія Володимировича**

Наукові та науково-практичні результати дисертаційного дослідження Костенка Олексія Володимировича щодо правових засад транскордонного надання електронних довірчих послуг.

Наукові результати дисертаційного дослідження може бути використані при висвітленні окремих тем модулів програм підвищення кваліфікації державних службовців 1-5 груп оплати праці центральних і місцевих органів виконавчої влади, органів судової влади, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування I-IV категорій посад, до яких можна віднести:

- результати порівняльно-правового аналізу міжнародних документів UNCITRAL, Ради Європи, а також законів та нормативних правових актів окремих країн світу з питань з питань електронного підпису та електронних довірчих послуг;

- результати аналізу створення, розвитку та сучасного стану нормативно-правової бази України в сфері електронного підпису та електронних довірчих послуг, ефективності використання електронного підпису та електронних довірчих послуг в процесах державного управління та електронних адміністративних державних послуг;

- напрямки вдосконалення нормативно-правової база, що регулює відповідальність за правопорушення в сфері цифрових технологій,

електронного підпису та електронних довірчих послуг, в тому числі визначення правових підстав для притягнення до відповідальності суб'єктів правовідносин, які беруть участь в створенні, одержанні, використанні, зберіганні та знищенні електронних підписів та наданні електронних довірчих послуг.

Теоретичні положення щодо побудови сучасної правової моделі суспільних відносин в сфері електронного підпису та електронних довірчих послуг дозволяють сформулювати обґрунтовану сукупність правових інструментів вдосконалення законодавства відповідно до потреб суспільства за напрямком концепції Президента України «Держава у смартфоні» щодо цифровізації взаємодії громадян із органами державної влади за допомогою електронних сервісів та відповідно Указу Президента України №647/2019 від 4 вересня 2019 року «Про деякі заходи із забезпечення надання якісних публічних послуг».

Перспективним є використання низки результатів дисертаційного дослідження Костенка О. В. на тему: «Правові засади надання електронних підписів та електронних довірчих послуг в транскордонному режимі» при підготовці короткострокових програм підвищення кваліфікації державних службовців: «Цифрова грамотність публічних службовців. Smart-технології»; «Електронне декларування публічних службовців»; «Електронне урядування в сучасній системі державного управління»; «Доступ до публічної інформації» тощо.

В якості додаткової літератури слухачам підвищення кваліфікації можуть бути рекомендовані наступні праці, в яких знайшли своє відображення результати дисертаційного дослідження:

1. Костенко О. В. Міністерство юстиції України – Вікно держави у світовий простір електронного цифрового підпису / О. В. Костенко // Бюлетень Міністерства юстиції України. – № 3. – 2014. – С. 142-149.
2. Костенко О. В. Компрометація особистого ключа електронного підпису (правовий аспект). / О. В. Костенко // International journal of innovative technologies in economy. – № 3(15). – 2018. – С. 15-22.
3. Костенко О. В. Шляхи розвитку правового регулювання електронних довірчих послуг в міжнародних актах UNCITRAL / О. В. Костенко, В. В. Костенко // Приватне та публічне право. – № 1. – 2019. – С. 78-84.
4. Костенко О. В. Проблеми правового регулювання визнання іноземних електронних довірчих послуг в Україні / О. В. Костенко // Науковий вісник Ужгородського національного університету. – Серія «Право». – № 51. – Т. 1. – 2018. – С. 192-197.
5. Костенко О. В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в міжнародному законодавстві. / О. В. Костенко // Науковий вісник публічного та приватного права. – № 4 – 2018. – С. 13-19.
6. Костенко О. В. Транскордонна ідентифікація фізичних та юридичних осіб, як елемент правового регулювання електронних довірчих послуг в

Європейському союзу. / О. В. Костенко, В. В. Костенко // Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. – № 29 (68). – 2018. – С. 90-93.

7. Костенко О. В. Шляхи запровадження електронних довірчих послуг в нотаріальному процесі. / О. В. Костенко, В. В. Костенко // Південноукраїнський правничий часопис. – № 4. – 2018. – С. 118-123.

8. Костенко О. В. Сучасна правова модель суспільних відносин сфери електронних довірчих послуг в Україні/ О. В. Костенко // Recht der Osteuropäischen Staaten. – № 4– 2018 – С. 139-142.

Директор Інституту
підвищення кваліфікації керівних кадрів
Національної академії державного управління
при Президенті України, д.політ.н., професор



В. А. Гошовська

ЗАТВЕРДЖУЮ

Директор Науково-дослідного інституту інформатики і права Національної академії правових наук України
юридичних наук, професор

В.Г.Пилипчук

2020 року



АКТ

**впровадження результатів дисертаційного дослідження
Костенка Олексія Володимировича**

Комісія у складі: першого заступника директора з наукової роботи, доктора юридичних наук, професора Довганя О.Д.; в.о. керівника науково-дослідного центру цифрових трансформацій і права доктора юридичних наук, старшого наукового співробітника Баранова О.А., ученого секретаря Інституту, кандидата юридичних наук Белашок М.В., склала цей акт про те, що результати дисертаційного дослідження на здобуття наукового ступеня доктора філософії зі спеціальності «081 – Право» *Костенка О.В. на тему: «Правове забезпечення транскордонного надання електронних довірчих послуг»*, яке проводилося в рамках планової науково-дослідної теми Науково-дослідного інституту інформатики і права НАІПрН України «Теоретико-методологічні засади правового регулювання суспільних відносин в умовах використання інтернет речей» (№ державної реєстрації 0116U007744), «Стратегії розвитку Науково-дослідного інституту інформатики і права НАІПрН України на 2018-2025 роки», схваленої президією НАІПрН України (постанова від 15.06.2018 № 106/7) у частині, що стосується трансформації суспільної діяльності в умовах розвитку і застосування новітніх інформаційних технологій, а саме: теоретико-методологічних положень правового регулювання суспільних відносин для забезпечення транскордонного режиму електронних підписів та електронних довірчих послуг з метою стрімкого зростання рівня довіри громадян до широкого використання інформаційно-комунікаційних технологій, як в Україні, так і в міжнародній співпраці.

Положення та висновки дисертації були використані при підготовці матеріалів для РНБО України щодо проблем правового регулювання та першочергових заходів у сфері забезпечення кібернетичної безпеки України (вих. № 94 від 09.08.2019 р.).

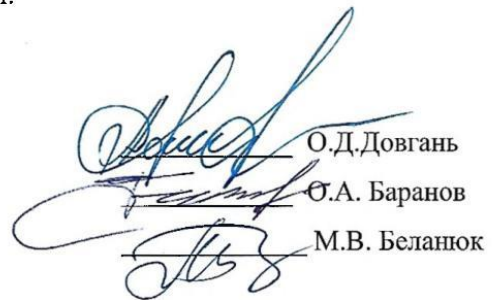
Матеріали дисертації можуть бути використані в процесі подальшої розробки актуальних проблем інформаційного права, правових проблем регулювання інформаційної взаємодії в інших сферах життєдіяльності суспільства, як на місцевому так і на державному рівні.

Члени комісії:

доктор юридичних наук, професор

доктор юридичних наук, с.н.с.

кандидат юридичних наук



О.Д.Довгань
О.А. Баранов
М.В. Беланюк

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

У наукових фахових виданнях України:

1. Костенко О.В. Міністерство юстиції України - вікно держави у світовий простір електронного цифрового підпису. *Бюлетень Міністерства юстиції України* №3. 2014. С.142–149.
2. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в законодавстві пострадянських країн. *Фаховий науковий журнал «Право і суспільство»*. № 5. Частина 2. 2018. С. 110–116.
3. Костенко О.В. Проблеми правового регулювання визнання іноземних електронних довірчих послуг в Україні. *Фаховий науковий журнал «Науковий вісник Ужгородського національного університету. Серія «Право»*. № 51. Т. 1. 2018. С. 192–197.
4. Костенко О.В. Електронний підпис та електронні довірчі послуги в законодавстві Сполучених Штатів Америки. *Науковий фаховий журнал «Інформація і право»*. № 3 (26) 2018. С. 76–84.
5. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в міжнародному законодавстві. *Фаховий збірник наукових праць «Науковий вісник публічного та приватного права»*. № 4 2018. С. 13–19.
6. Костенко О.В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі. *Науковий фаховий журнал «Інформація і право»*. № 3 (30) 2019. С. 96–105.
7. Горбенко Ю.И., Потий А.В., Костенко А.В., Исирова Е.В., Горбенко И.Д. Состояние и сущность процессов нормализации европейской нормативной базы в области электронных подписей. *Прикладная радиоэлектроника*, № 3. Т. 13. 2014. С. 261–267. (1,0/0,2 ум. друк. арк.)

8. Костенко О.В. Костенко В.В. Транскордонна ідентифікація фізичних та юридичних осіб, як елемент правового регулювання електронних довірчих послуг в Європейському союзі. *Фаховий науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки»*. № 29 (68) 2018. С. 90–93. (0,6/0,3 ум. друк. арк.);

9. Костенко О.В. Костенко В.В. Шляхи запровадження електронних довірчих послуг в нотаріальному процесі. *Фаховий науковий журнал «Південноукраїнський правничий часопис»* № 4 2018. С.118–123. (0,6/0,3 ум. друк. арк.);

10. Костенко О.В., Костенко В.В. Особливості правового регулювання сфери електронних підписів в законодавстві країн Латинської Америки. *Науковий фаховий журнал «Право і суспільство»*. № 2. 2019. С.102–110. (0,6/0,3 ум. друк. арк.);

11. Костенко О.В., Костенко В.В. Електронні підписи та порядок визнання іноземних сертифікатів електронних підписів в законодавстві окремих країн Азії. *Науковий фаховий журнал «Науковий вісник публічного та приватного права»* №1 2019. С.10–106. (0,6/0,3 ум. друк. арк.);

***У зарубіжних виданнях та наукових фахових виданнях України,
які зареєстрованих у міжнародних наукометричних базах:***

12. Костенко О.В. Компрометація особистого ключа електронного підпису (правовий аспект). *Міжнародний науковий журнал «International journal of innovative technologies in economy»* № 3(15) 2018 С. 15–22.

13. Костенко А.В. Проблемы правового регулирования признания иностранных электронных доверительных услуг в Украине. *Международный научно-практический правовой журнал «Legea si Viata»*. № 10/2(322). 2018. С. 54–58.

14. Костенко О.В. Сучасна правова модель суспільних відносин сфери електронних довірчих послуг в Україні. *Міжнародний науковий журнал «Recht der Osteuropäischen Staaten»* №4. 2018. С. 139–142.

15. Mykhailo Loshytskyi, Oleksii Kostenko, Ihor Koropatnik, Galyna Tereshchuk, Vladyslav Karelin. Organization competence of NATO information security policy journal of security and sustainability issues. Volume 9, Number 3. 2020. p. 735 -746 (1,0/0,2 ум. друк. арк.)

Публікації в інших виданнях, тези наукових доповідей:

16. Костенко О.В. Проблеми правового регулювання транскордонного визнання іноземних електронних послуг та іноземного сертифікату електронного підпису в Україні. *Стан та перспективи розвитку юридичної науки: матеріали міжнародної науково-практичної конференції*, 31 серпня – 1 вересня 2018 р., Дніпро /упорядн.: Громадська організація «Правовий світ», 2018. С. 65–69.

17. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в законодавстві пострадянських країн. *Пріоритетні напрямки розвитку сучасної юридичної науки: матеріали Міжнародної науково-практичної конференції*, 14-15 вересня 2018 р., м. Харків./упорядн.: Громадська організація «Асоціація аспірантів-юристів». 2018. С. 45–49.

18. Костенко О.В. Правове регулювання транскордонного визнання сертифікатів електронних підписів та електронних довірчих послуг в міжнародному законодавстві. *Інтеграція юридичної науки і практики в сучасних умовах: матеріали Міжнародної науково-практичної конференції*, 24-25 серпня 2018 р., м. Запоріжжя./ упорядн.: Класичний приватний університет. 2018. С. 66–69.

19. Костенко О.В. Шляхи правого регулювання електронних довірчих послуг в Європейському Союзі. *Інформаційне право: сучасні виклики і напрями розвитку: матеріали Першої науково-практичної конференції* 18 жовтня 2018р., Київ/упорядн.: Національна академія правових наук України, Науково-дослідний інститут інформатики і права, Національний технічний університету України «Київський політехнічний

інститут імені Ігоря Сікорського» факультет соціології і права, Навчально-науковий центр інформаційного права та правових питань інформаційних технологій. 2018. С. 190–193.

20. Костенко О.В. Правові питання регулювання довірчих послуг в міжнародних актах UNCITRAL. *Інтернет речей: Проблеми правового регулювання та впровадження: матеріали Другої науково-практичної конференції*, 29 листопада 2018 м. Київ/ упорядн.: Комітет Верховної Ради України з питань інформатизації та зв'язку, Національна академія правових наук України Науково-дослідний інститут інформатики і права НАПрН України, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» факультет соціології і права. 2018. –С. 160–164.

21. Костенко О.В. Правова адаптація суспільних відносин в сфері цифрового підпису та електронних довірчих послуг в Україні до законодавства ЄС. *Особенности адаптации законодательства Молдовы и Украины к законодательству Европейского Союза: матеріали Міжнародної науково-практичної конференції*, 23-24 марта 2019 р., Кишинів, Республика Молдова/упорядн.: Institutul decercetari, politice si sociologice universitate de stat «Alecu Russo» din balti institutul din balti institutul destinte penale criminologie aplicata, 2019. С. 136–139.

22. Костенко О.В. Компрометація особистого ключа електронного підпису (правовий аспект). *Актуальні питання розвитку та взаємодії публічного та приватного права: матеріали Міжнародної науково-практичної конференції*, 16-17 березня 2019 р., Львів./ упорядн.: Західноукраїнська організація «Центр правничих ініціатив». 2018. – С. 102–104.

23. Костенко О.В., Капшук О.О. Проблема інтероперабельності Національної системи електронного цифрового підпису в Україні та шляхи їх вирішення. *6-th International conference SAIT 2014 «System Analysis and Information Technologies»*, 26-30 травня 2014 р. Київ/упорядн. Natalia

D.Pankratova, Institute for Applied System Analysis of National Technical University of Ukraine Kyiv Polytechnic Institute, 2014. С. 297–298.

24. Костенко О.В., Костенко В.В. Імплементція національного законодавства в сфері електронних довірчих послуг до регламенту ЄС. *Чотирнадцяті юридичні читання. Проблеми імплементації національного законодавства до угоди про асоціацію між Україною та ЄС.: матеріали міжнародної наукової конференції 17-18 квітня 2019 р., Київ.* упорядн.: Науково-дослідний інститут інформатики і права НАПрН України, Національний педагогічний університет імені М.П. Драгоманова, Інститут держави і права ім. В.М. Корецького НАН України, Центр правової освіти і науки, Громадська організація «Феміда». 2019. С. 16–19. (0,6/0,3 ум. друк. арк.);

25. Костенко О.В., Костенко В.В. Вирішення проблем правового регулювання сфери цифрового підпису та електронних довірчих послуг в Україні. *Сутність та значення законодавства на розвиток суспільних відносин: матеріали Міжнародної науково-практичної конференції, 8-9 березня 2019 р., Одеса.*/ упорядн.: Причорноморська фундація права. 2019. С. 55–58. (0,6/0,3 ум. друк. арк.);

26. Костенко О.В., Костенко В.В. Вирішення проблем законодавства щодо застосування електронного підпису та електронних довірчих послуг в транскордонному режимі. *Право як ефективний суспільний регулятор: матеріали Міжнародної науково-практичної конференції 15–16 лютого 2019 р., Львів.*/ упорядн.: Західноукраїнська організація «Центр правничих ініціатив». 2019. С. 79–81.

27. Костенко О.В., Костенко В.В. Модернізація суспільних та правових відносин сфери цифрового підпису відповідно до угоди про асоціацію між Україною та ЄС. *Інтелектуальна власність і право на шляху до сталого розвитку України, матеріали II Міжнародної науково-практичної конференції, 19 квітня 2019 р., Київ* / упорядн.: Міністерство освіти і науки України Національний університет «Одеська юридична

академія» Київський інститут інтелектуальної власності та права. 2019. С. 11. (0,6/0,3 ум. друк. арк.);

28. Костенко О.В., Костенко В.В. Проблеми компрометації цифрового підпису, як елемента фіксації авторського права. *Інтелектуальна власність і право на шляху до сталого розвитку України, матеріали II Міжнародної науково-практичної конференції*, 19 квітня 2019 р., Київ/ упорядн.: Міністерство освіти і науки України Національний університет «Одеська юридична академія» Київський інститут інтелектуальної власності та права. 2019. С. 6. (0,6/0,3 ум. друк. арк.);

