НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

ГАВЛОВСЬКИЙ ІГОР АНАТОЛІЙОВИЧ

УДК 342.76:35

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВІ ВІДНОСИНИ З ВИКОРИСТАННЯМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В УКРАЇНІ

12.00.07 «Адміністративне право і процес;
фінансове право; інформаційне право»

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____І. А. Гавловський

(підпис, ініціали та прізвище здобувача)

Науковий керівник – **Чижмарь Катерина Іванівна**,
доктор юридичних наук, доцент

Київ – 2018

АНОТАЦІЯ

Гавловський І. А. Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут публічного права, Київ, 2018.

У дисертації на основі теорії адміністративного права, вітчизняного та зарубіжного законодавства, досягнень публічної адміністрації наведено нове розв'язання наукового завдання стосовно розвитку засад та адміністративного інструментарію у сфері адміністративно-правових відносин із використанням електронного цифрового підпису в Україні.

Доведено, що у вузькому розумінні адміністративно-правові відносини з використанням електронного цифрового підпису – це суспільні відносини, які виникають, змінюються і припиняються завдяки електронному цифровому підпису, отриманому за результатом криптографічного перетворення набору електронних даних, що дає змогу підтвердити його цілісність та ідентифікувати підписувача, і врегульовуються нормами адміністративного права.

З'ясовано, що адміністративно-правова природа електронного цифрового підпису в Україні полягає в тому, що він, базуючись на науковій природі математичних категорій криптографії та криптоперетворення, коли завдяки об'єктивній юридичній регламентації через норми адміністративного права забезпечує адміністративно-правовий та організаційно-правовий захист особистих ключів підписувачів від несанкціонованого використання (через використання закритого ключа), підвищує ефективність управлінської діяльності органів публічної влади та зручність користування приватними особами, дорівнюється до

власноручного підпису (печатки) і не може заперечуватися виключно на підставі того, що має електронну форму.

Виявлено адміністративно-правові відносини, що виникають щодо електронного цифрового підпису, віддзеркалюють вплив адміністративно-правових норм на поведінку суб'єктів, які використовують електронний цифровий підпис, та об'єктів публічного управління, через що між ними виникають сталі правові зв'язки публічновладного характеру. Іншими словами, адміністративно-правова норма містить абстрактну конструкцію адміністративно-правового відношення. Сутність такої конструкції полягає в тому, що адміністративно-правова норма від імені держави визначає належну поведінку кожного зі своїх адресатів. Вона встановлює обов'язкові правила, за якими відбувається «спілкування». Ці правила формуються у вигляді взаємних адміністративних прав і обов'язків.

З'ясовано адміністративно-правовий статус суб'єктів адміністративно-правових відносини у сфері електронного цифрового підпису в Україні, які за своєю юридичною природою є публічними або приватними особами, наділені нормами адміністративного права різними за формулою правового регулювання суб'єктивними адміністративними обов'язками і правами, коли суб'єкти публічної адміністрації (центральний засвідчувальний орган і акредитовані центри сертифікації ключів) надають адміністративні послуги та здійснюють виконавчо-розпорядчу діяльність, а приватні особи (споживачі та підписувачі) отримують адміністративні послуги, користуються всіма можливостями електронного цифрового підпису та можуть піддаватися адміністративній відповідальності за порушення режиму використання і зберігання електронних ключів.

Розкрито, що об'єкт адміністративно-правових відносин у сфері електронного цифрового підпису в Україні є об'єктивно чинним явищем матеріального інтелектуального права, похідним від суб'єктів адміністративного права – як складова формального змісту адміністративно-правових відноси, існує з метою задоволення прав,

свобод, інтересів і потреб споживачів і підписувачів, визначається межами юридичних норм, регулюється в ході адміністративної діяльності суб'єктів публічної адміністрації та захищатися від порушення засобами адміністративного примусу.

Здобувач доводить, що суб'єкти адміністративно-правових відносин із використанням електронного цифрового підпису вступають у них з метою задоволення своїх прав, свобод, інтересів і потреб, які опосередковують об'єкти адміністративно-правових відносин. Визначено, що такою метою є однозначна юридична ідентифікація клієнтів фізичної чи юридичної особи, що надає їй можливість дистанційно за допомогою інформаційних систем і глобальної системи Інтернет здійснювати різноманітні юридичні дії як публічного, так і приватного характеру в різних місцях країни чи за її межами. Сфера застосування електронного цифрового підпису суб'єктами адміністративного права є надзвичайно широкою (від отримання офіційної електронної довідки до дистанційного управління компанією) і постійно розширюється.

Визначено, що адміністративними діями суб'єктів публічної адміністрації у сфері електронного цифрового підпису в Україні є такі:

1) надання приватним особам (споживачам і підписувачам електронного цифрового підпису) відповідних адміністративних послуг, щоб вони могли комфортно і безпечно отримувати, продовжувати термін і відмовлятися від електронних ключів, користуватися ними в усіх сферах публічного і приватного життя. Дії споживачів та підписувачів електронного цифрового підпису можуть мати як публічноправову (наприклад, у разі подання податкової звітності), так і приватноправову природу;

2) здійснення публічного адміністрування цифровим електронним підписом. У цьому разі спеціальні суб'єкти публічної адміністрації здійснюють увесь перелік передбачених адміністративним законодавством заходів, пов'язаних зі здійсненням організаційно-правових, технічних,

організаційно-технічних, техніко-безпекових і організаційно-безпекових заходів, для того щоб система електронного цифрового підпису надійно працювала і задовольняла споживачів і підписувачів.

Визначено, що зміст у системі адміністративно-правових відносин у сфері електронного цифрового підпису полягає в тому, що кожному суб'єктивному адміністративному праву одного суб'єкта адміністративного права встановлюється нормами адміністративного права юридичний обов'язок іншого, і навпаки. Тут вагому увагу було приділено сутнісній різниці змісту адміністративно-правових відносини суб'єктів владних повноважень і приватних осіб. Для перших домінантом є адміністративні обов'язки, а їх адміністративні права мають додатковий забезпечувальний характер і надаються адміністративним законодавством виключно тією мірою, яка їм мінімально потрібна для ефективного виконання поставлених перед ними завдань. Виділяються адміністративні обов'язки суб'єктів публічної адміністрації: надавати адміністративні послуги щодо електронного цифрового підпису; забезпечувати однозначну ідентифікацію сертифіката ключа та відповідного особистого ключа підписувачу, захист інформації та персональних даних, цілодобовий доступ користувачів до сертифікатів ключів; своєчасно скасовувати, блокувати та поновлювати сертифікатів ключів. По виконанні зазначеного спеціальні суб'єкти публічної адміністрації мають адміністративні права щодо отримання та перевірки інформації, що потрібна для реєстрації підписувача і формування посиленого сертифіката ключа; перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів.

Здійснено компаративістичну характеристику ефективного зарубіжного досвіду використання електронного цифрового підпису, у результаті чого виявлено, що переважна більшість демократичних правових держав функціонують у вимірі інформаційного суспільства, в якому цифрові технології ефективно використовуються в економіці,

публічному управління та торгівлі, і їх невід'ємним елементом є електронні цифрові підписи, що використовуються в усіх публічних і приватних сферах суспільного життя. Здійснено класифікацію електронного цифрового підпису за рівнем легалізації (безпеки і контролю) на три основні групи держав, у яких: 1) статус електронного підпису дорівнений до статусу власноручного; 2) електронний підпис широко використовується, але не має повної тотожності власноручному; 3) електронний підпис використовується в окремих сферах. З'ясовано, що діє директива, яка проголошує рівність правового статусу паперового й електронного документів.

Удосконалено законодавство у сфері використання електронного цифрового підпису в Україні шляхом формування концептуальних положень і конкретних змін і доповнення до чинного законодавства щодо підвищення ефективності використання цифрового підпису в Україні через розширення сфери його застосування, посилення захищеності, покращення зручності користування, захист санкціями через установлення відповідної адміністративної відповідальності. Це має реалізуватися в концепції впровадження електронного цифрового підпису в усі сфери суспільного життя, поєднання ID-картки громадянина України та можливостей технологій NFC у смартфонах користувачів і встановлення адміністративної відповідальності за відмову надавати адміністративні послуги за електронним цифровим підписом та неналежне його зберігання.

Ключові слова: адміністративна послуга, адміністративно-правові відносини, адміністративно-правовий статус, адміністративно-правовий захист, публічна адміністрація, аналог власноручного підпису, електронна форма правочину, електронний підпис, електронний цифровий підпис, електронний підпис одноразовим ідентифікатором.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Гавловський І. А. Адміністративно-правові відносини у сфері електронно-цифрового підпису. *Прикарпатський юридичний вісник.* 2015. № 3. Том 4. С. 167-171.

2. Гавловський І. А. Об'єкти адміністративно-правових відносин у сфері електронно-цифрового підпису. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2015. Випуск 33. Ч. 2. С. 84-89.

3. Гавловський І. А. Адміністративно-правова природа електронного цифрового підпису. *Науковий вісник публічного та приватного права.* 2016. Випуск 2. Том 4. С. 134-138.

4. Гавловский И. А. Зарубежный опыт электронной цифровой подписи. *Право и Политика.* 2017. № 1. С. 55-58 (Кыргызская Республика).

5. Гавловський І. А. Поняття та зміст адміністративно-правових відносин з використанням електронного цифрового підпису. *Науковий вісник Херсонського державного університету.* Серія «Юридичні науки». 2017. Випуск 2. Т. 4. С. 112-117.

6. Гавловский И. А. Содержание административно-правовых отношений в сфере электронно-цифровой подписи. *Право и Закон.* 2017. № 4. С. 67-70 (Кыргызская Республика).

7. Гавловський І. А. Суб'єкти адміністративно-правових відносини у сфері електронно-цифровий підпису. *Науковий вісник публічного та приватного права.* 2018. Випуск 1. Том 1. С. 122-127.

які засвідчують апробацію матеріалів дисертації:

8. Гавловський І. А. Генеза виникнення електронного документообігу та цифрового підпису. *Сучасне державотворення та правотворення: питання теорії та практики:* матер. Міжнар. наук.-практ.

конф. (м. Одеса, Україна, 11-12 груд. 2015 р.). Одеса: ГО «Причорноморська фундація права», 2015. С. 86-90.

9. Гавловський І. А. Програмні інформаційні комплекси, які використовуються в України. *Особливості розвитку публічного та приватного права в Україні:* матер. Міжнар. наук.-практ. конф. (м. Харків, 15-16 лип. 2016 року). Харків: ГО «Асоціація аспірантів-юристів», 2016. С. 23-26.

10. Гавловський І. А. Правове регулювання електронних документів та цифрового підпису. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи:* матер. Міжнар. наук.-практ. конф. (м. Київ, 10-11 берез. 2017 р.). К.: Центр правових наукових досліджень, 2017. С. 57-60.

SUMMARY

Havlovskyi I. A. Administrative-legal relations with the use of electronic digital signature in Ukraine - *Qualifying scientific work (manuscript).*

Thesis for a Candidate Degree in Law, specialty 12.00.07 "Administrative Law and Process; finance law; information law" - Research Institute of Public Law, Kyiv, 2018.

The dissertation is based on the theory of administrative law, domestic and foreign legislation, achievements of public administration presented a new solution to the scientific problem with regard to the development of ambushes and administrative tools in the field of administrative-legal relations using an electronic digital signature in Ukraine.

It is proved that administrative-legal relations in the narrow sense using electronic digital signature are social relations that arise, change and cease due to electronic digital signature. What is obtained as a result of cryptographic transformation of the set of electronic data. This allows it to confirm its integrity and identify the signatories that are regulated by the rules of administrative law.

The administrative-legal nature of electronic digital signature in Ukraine is determined. He is based on the scientific nature of the mathematical categories of cryptography and cryptography. This is done through objective legal regulation through the rules of administrative law. It provides administrative and legal and organizational-legal protection of personal keys of signers from unauthorized use (through the use of a private key). This increases the efficiency of management activities of public authorities and the convenience of using private individuals, equates to a handwritten signature (stamp). No one can deny an electronic digital signature for the reason that he has an electronic form.

It was revealed that the administrative-legal relations arising in relation to the electronic digital signature reflect the influence of administrative and legal

norms on the behaviour of subjects who use electronic digital signature and objects of public administration, because of which there are established legal ties of public authority character . In other words, the administrative law contains an abstract construction of an administrative-legal relationship. The essence of such a design is that the administrative law on the state's behalf determines the proper conduct of each of its recipients. It establishes mandatory rules for "communicating". These rules are formed in the form of mutual administrative rights and responsibilities.

The administrative-right status is determined subjects of administrative-legal relations in the sphere of electronic digital signature in Ukraine which by their legal nature are public or private persons endowed with the norms of administrative law are different by the formula of legal regulation subjective administrative duties and rights when public administration actors (central certifying authority and accredited key certification centres as the key certification centre) provide administrative services and execute executive and regulatory activities, and private individuals (consumers and signers) receive administrative services, use all possibilities of electronic digital signature and can be subject to administrative responsibility for violation of the mode of use and storage of electric on keys.

It is exposed, that object of administrative-legal relations in the field of an electronic digital signature in Ukraine are the objectively existent phenomenon material intellectual right, to the derivatives from administrative legal subjects from the point of view, as a constituent of formal maintenance of administrative-legal relationship, it exists with the aim of satisfaction of rights, freedoms, interests and necessities of consumers and signers, determined by the limits of legal norms regulated during administrative activity of subjects of public administration and to ward off violation facilities administrative compulsion.

It is proved that the subjects of administrative-legal relations using an electronic digital signature join them in order to meet their rights, freedoms, interests and needs which mediate the objects of administrative-legal relations. It

is determined that such a goal is unambiguous legal identification of clients physical or legal entity which provides its opportunity remotely with the help of information systems and the global Internet system to carry out various legal actions both public and private in different places of the country and one outside it. Scope of electronic digital signature by subjects administrative law is extremely broad (from receiving official electronic help to remote management company) and it is constantly expanding.

It is determined that the administrative actions of the subjects of public administration in the field of electronic digital signature in Ukraine are: First, providing private individuals (consumers and signers of electronic digital signature) administrative services in this area so that they can get comfortable and safe, extend the term and refuse the electronic keys, enjoy them in all spheres of public and private life. The actions of consumers and signers of electronic digital signature can be worn as public-law (for example, in the case of tax returns) and private law nature. Secondly, the implementation of public administration by digital electronic signature. In this case, special subjects of public administration carry out the entire list provided by administrative law measures related to the implementation of organizational, legal, technical, organizational-technical, technical-security and organizational-security measures to ensure that the electronic digital signature system works reliably and satisfies consumers and subscribers.

Determined that the content in the system of administrative-legal relations in the field of electronic digital signature is that, that each subjective administrative law of one subject administrative law is established by the norms of administrative law, the legal obligation of another and vice versa. In this, considerable attention was paid to the essential difference between the content of administrative and legal relations between the subjects of power and private individuals. For the first dominant there are administrative responsibilities, their administrative rights are additional nature and are provided by administrative law only to the extent that which is minimal for them to effectively perform

their tasks. The administrative duties of the subjects of public administration are allocated: provide administrative services for electronic digital signature; provide unambiguous identification of the key certificate and corresponding personal key the signer, the protection of information and personal data, round-the-clock user access to key certificates; cancel, block and renew key certificates in a timely manner. According to the specified subjects of public administration have administrative rights regarding the receipt and verification of information, within the limits of which it is necessary for registration of the signatory and formation enhanced certificate key; check the legality of requests for cancellation, blocking and renewal of key certificates.

Made comparative characteristics of effective foreign experience with the use of electronic digital signature. As a result, it was found that the overwhelming majority of democratic legal states function in the dimension of the information society in which digital technology effectively used in the economy, public administration and trade, an integral element of which is electronic digital signatures, which is used in all public and private spheres of public life. Classification of electronic digital signature according to the level of legalization (security and control) into three main groups, states where: 1) the status of the electronic signature is equal to status of the person's manual; 2) the electronic signature is widely used, but does not have a complete identity of its own; 3) electronic signature is used in separate areas. It is clarified that the EU has a directive that proclaims the equality of legal status of paper and electronic documents.

Enhanced legislation on the use of electronic digital signature in Ukraine, through the formation of conceptual provisions and specific changes and additions to the current legislation on increasing the efficiency of use digital signature in Ukraine by expanding its scope of application, digital signature in Ukraine by expanding its scope of application, enhancing security, improved ease of use, protection of sanctions through the establishment of appropriate administrative liability. What should be realized in the concept of

implementation of electronic digital signature in all spheres of public life, the combination of an ID-card of a citizen of Ukraine and the capabilities of NFC technology in smartphone users establishment of administrative responsibility for refusal to provide administrative service by electronic digital signature and improper storage of it.

Key words: administrative service, administrative-legal relations, administrative-legal status, administrative-legal protection, public administration, analogue of a personal signature, notion, electronic form of transaction, electronic signature, electronic digital signature, electronic signature with one-time identifier.

LIST OF PUBLISHED WORKS ON THE TOPIC OF THE THESIS

in which the main scientific results of the thesis are highlighted:

1. Havlovskyi I. A. Administrative-legal relations in the field of electronic-digital signature. *Precarpathian Legal Bulletin.* 2015. No. 3. Volume 4. P. 167-171.

2. Havlovskyi I. A. Objects of administrative-legal relations in the field of electronic-digital signature. *Scientific herald of Uzhgorod National University.* The series "Right". 2015. Issue 33. Part 2. P. 84-89.

3. Havlovskyi I. A. The administrative nature of the electronic digital signature. *Scientific Bulletin of Public and Private Law.* 2016. Issue 2. Volume 4. P. 134-138.

4. Havlovskyi I. A. Foreign experience of electronic digital signature. *Law and Politics.* 2017. No. 1. P. 55-58 (Kyrgyz Republic).

5. Havlovskyi I. A. The concept and content of administrative-legal relations with the use of electronic digital signature. *Scientific Herald of Kherson State University. Series "Legal Sciences".* 2017. Issue 2. T. 4. P. 112-117.

6. Havlovskyi I. A. Contents of administrative-legal relations in the field of digital signature. *Law and Law.* 2017. No. 4. P. 67-70 (Kyrgyz Republic).

7. Havlovskyi I. A. Subjects of administrative-legal relations in the field of electronic-digital signature. *Scientific Bulletin of Public and Private Law.* 2018. Issue 1. P. 122-127.

which certify the approbation of the thesis materials:

8. Havlovskyi I. A. Genesis of the emergence of electronic document circulation and digital signature. *Modern state-building and law-making: questions of theory and practice:* Materials of the International science-practice conf. (Odessa, Ukraine, December 11-12, 2015). Odessa: NGO "Black Sea Fund of Law", 2015. P. 86-90.

9. Havlovskyi I. A. Software information systems used in Ukraine. *Features of the development of public and private law in Ukraine:* Materials of the International science-practice conf. (Kharkiv, July 15-16, 2016). Kharkiv: NGO "Association of Postgraduate Lawyers", 2016. P. 23-26.

10. Havlovskyi I. A. Legal regulation of electronic documents and digital signature. *Modern legal systems of the world in the conditions of globalization: realities and prospects:* Materials of the International science-practice conf. (Kyiv, 10-11 March 2017). K .: Center for Legal Research, 2017. P. 57-60.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Людське суспільство розвивається за законами соціального прогресу з одночасним ускладненням суспільних відносин. Одним із найбільш наглядних прикладів цього є утвердження в житті людства різних новітніх інститутів, що пов’язані із комп’ютеризацією суспільства та глобальним розповсюдженням мережі Інтернет. Зокрема, це призвело до розквіту різноманітних криптологічних технологій, серед яких найбільшого практичного застосування отримав електронний цифровий підпис, що зумовлює нові вимоги до безпеки особистих даних і зручності їх використання. Адже електронний цифровий підпис в рази збільшує ефективність діяльності публічних органів та бізнесу, спрощує доступ громадян до адміністративних послуг, є вагомим чинником протидії корупції.

Незважаючи на зазначені позитивні чинники, використання електронного цифрового підпису таїть в собі низку небезпечних викликів. В першу чергу, виходячи із презумпції єдності фізичної і юридичної особи з легальним електронним цифровим підписом, внаслідок протиправних діянь цей взаємопов’язаний ланцюг може розриватися внаслідок хакерських зламів комп’ютерних систем чи халатності користувачів, коли ключі від нього потрапляють до сторонніх осіб. Заволодіння чужим ключем призводить до того, що зловмисники можуть від імені справжнього власника здійснювати неправомірні дії – проводити певні грошові транзакції, змінювати записи в базах даних тощо.

Тобто кіберзлочинність і публічна інформаційна безпека осіб на сьогоднішній день поширилась на всі країни. З розвитком комп’ютерних технологій, штучного інтелекту ця проблема поглиблюється. В таких випадках актуальним є виявлення та опис внутрішніх засад та правового інструментарію захисту цього феномену, який практично вже

використовується фізичними і юридичними особами, що підвищують ефективність своєї управлінської праці за допомогою захищених криптологічними засобами захисту і такими, що постійно модернізуються технологіями. Вагоме місце у цій системі належить нормам адміністративного права. Саме на основі них визначаються засади, підстави, форми, методи та адміністративні процедури отримання і використання електронного цифрового підпису.

Однак в Україні проблема полягає не тільки в ефективному адміністративно-правовому захисті електронного цифрового підпису, але й в стимулюванні громадян до його отримання і використання, адже ним користується лише 6 % українців, що не йде в ніяке порівняння із країнами-учасницями ЄС (наприклад в Естонії 95 % населення використовують електронний цифровий підпис)[1]. Іншими словами мова йде про необхідність широкого реформування адміністративно-правових відносин у цій сфері, які в умовах сьогодення перебувають на початкових етапах як теоретичного, так і практичного розвитку. Зазначений висновок корелюється із результатами власного соціологічного опитування, яке показало, що 86 % громадян позитивно оцінюють інститут електронного цифрового підпису, разом з тим 53 % із них в силу різних причин не збираються його отримувати у короткостроковій перспективі (Додаток Б до дисертації).

Таким чином, необхідність дієвого механізму надання фізичним і юридичним особам різноманітних адміністративних послуг, необхідність забезпечення прав і законних інтересів користувачів електронного цифрового підпису, нерозробленість теорії й практики використання

---

[1] Офіс реформи адмінпослуг. 2017. URL. https://biz.nv.ua/ukr/experts/ryabchinska_l/de-vihid-z-kvest-kimnati-tsifrovogo-pidpisu-1644303.html

електронного цифрового підпису і зумовлюють актуальність аналізованого дослідження.

Зв'язок теми дисертації із сучасними дослідженнями. У більш широкому форматі схожу з нашою проблематику аналізувала у своїх працях О. Харитонова, яка сформувала юридичну концепцію правовідносин в адміністративному праві України [2], М. Савюк, що з'ясувала деякі аспекти місця і ролі цифрового підпису в інформаційному суспільстві [3]. Більш спеціальній тематиці присвятила свої праці І. Стаценко-Сургучова, яка розкрила процес адміністрування податків шляхом безпаперової технології за допомогою засобів комунікаційного зв'язку із використанням електронного цифрового підпису[4].

Крім них окремі питання адміністративно-правових відносин з використанням електронного цифрового підпису в Україні досліджували: В. Авер'янов, Ю. Атаманова, Н. Армаш, Н. Бааджи, В. Басс, В. Бевзенко, І. Бородін, А. Бойков, І. Верес, В. Галунько, Ю. Гаруст, А. Гетьман, В. Ковальська, А. Ковальчук, Т. Коломоєць, В. Колпаков, А. Комзюк, А. Манжула, В. Мілаш, Л. Миськів, Р. Мельник, А. Новицький, О. Світличний, В. Оксінь, С. Пєтков, К. Чижмарь, А. Чубенко, В. Шкарупа ін. Проте вищезазначені вчені розкривали лише загальні чи спеціальні аспекти адміністративно-правових відносин з використанням електронного цифрового підпису, не звертаючись до глибинних засад теорії цього інституту адміністративного права та інструментарію його втілення у правотворчість і правозастосування.

---

[2] Харитонова О. Адміністративно-правові відносини: концептуальні засади та правова природа: автореф. дис... д-ра юрид. наук: 12.00.07. Одеса, 2004. 36 с.

[3] Савюк М. Адміністративно-правові засади інформаційного суспільства: автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2016. 17 с.

[4] Стаценко-Сургучова І. Організаційно-правові засади інформаційно-аналітичної роботи в органах державної податкової служби України: автореф. дис... канд. юрид. наук: 12.00.07. Ірпінь, 2008. 20 с.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до Угоди про асоціацію між Україною та Європейським Союзом, ратифікованої Законом України від 16 вересня 2014 р. № 1678-VII, Стратегії сталого розвитку «Україна-2020», затвердженої Указом Президента України від 12 січня 2015 р. № 5, Концепції реформування державної системи правової охорони інтелектуальної власності в Україні, схваленої розпорядженням Кабінету Міністрів України від 1 червня 2016 р. № 402-р., Концепції розвитку системи електронних послуг в Україні, схваленої розпорядженням Кабінету Міністрів України від 16 листопада 2016 р. № 918-р. та плану науково-дослідницької роботи Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0115U005495).

Мета і завдання дослідження. *Мета* роботи полягає в тому, щоб на основі комплексного аналізу теоретико-методологічних засад, нормативних основ і практичної реалізації вирішити наукове завдання стосовно адміністративно-правових відносин з використанням електронного цифрового підпису в Україні.

Відповідно до поставленої мети в роботі заплановано вирішити такі *завдання*:

– сформувати поняття адміністративно-правових відносин з використанням електронного цифрового підпису;

– з'ясувати адміністративно-правову природу електронного цифрового підпису;

– виявити фактичний зміст адміністративно-правових відносини у сфері електронного цифрового підпису;

– з'ясувати адміністративно-правовий статус суб'єктів адміністративно-правових відносин у сфері електронного цифрового підпису в Україні;

– розкрити об’єкти адміністративно-правових відносини у сфері електронного цифрового підпису в Україні;

– з’ясувати зміст адміністративно-правових відносин у сфері електронного цифрового підпису в Україні;

– здійснити компаративістичну характеристику ефективного зарубіжного досвіду стосовно використання електронного цифрового підпису;

– удосконалити законодавство у сфері використання електронного цифрового підпису в Україні.

Об’єкт дослідження – суспільні відносини, що виникають у сфері адміністративно-правових відносин з використанням електронного цифрового підпису в Україні.

Предмет дослідження – адміністративно-правові відносини з використанням електронного цифрового підпису в Україні.

Методи дослідження. У ході дослідження було використано сукупність філософських, загальнонаукових, загально-логічних та спеціально-юридичних методів наукового пізнання. *Діалектичний* метод дав змогу виділити наукову новизну «уперше», а саме сформулювати поняття адміністративно-правових відносин у сфері використання електронного цифрового підпису в широкому розумінні, з’ясувати адміністративно-правову природу електронного цифрового підпису (підрозділи 1.1, 1.2).

Системний підхід використовувався для розкриття елементів формального змісту адміністративно-правових відносин в аналізованій сфері (підрозділи 2.1, 2.2, 2.3). Практично в усіх підрозділах дисертації використовувалися такі методи наукового пізнання як логічні методи *аналізу* й *синтезу*, *логіко-семантичний* та спеціально-юридичний *формально-догматичний* методи (підрозділи 1.1, 1.2, 1.3, 2.1, 2.2, 2.3, 3.1). Метод *дедукції* дав змогу здійснити аналіз правових явищ та їх узагальнення від загального до окремого (підрозділи 1.1, 1.2, 1.3).

Використання методу *індукції* шляхом узагальнення одиничних юридичних фактів дало можливість сформулювати нові кількісні і якісні положення дослідження (підрозділи 2.1, 2.2, 2.3). Метод *порівняльного законодавства* дозволив здійснити аналіз зарубіжного досвіду щодо використання електронного цифрового підпису (підрозділ 3.1). Метод *правового прогнозування* став незамінним при удосконаленні законодавства у сфері використання електронного цифрового підпису в Україні (підрозділ 3.2). *Соціологічний* метод допоміг здійснити власне соціологічне опитування (Додаток Б до дисертації).

Наукова новизна отриманих результатів аргументується тим, що дисертація є першим теоретичним монографічним дослідженням, присвяченим аналізу адміністративно-правових відносин з використанням електронного цифрового підпису в Україні. У результаті проведеного аналізу сформовано низку висновків, рекомендацій і пропозицій щодо вдосконалення чинного законодавства України в зазначеній сфері, зокрема:

уперше:

– сформовано поняття «адміністративно-правові відносини у сфері використання електронного цифрового підпису» в широкому розумінні як форма соціального прогресу щодо взаємодії спеціальної публічної адміністрації, яка легалізує електронний цифровий підпис та підписувачів і споживачів електронного цифрового підпису на підставі адміністративно-правових норм з метою більш ефективного забезпечення прав, свобод і законних інтересів фізичних і юридичних осіб, нормального функціонування громадянського суспільства і держави, учасники якої несуть адміністративні обов’язки та мають суб’єктивні права;

– з’ясовано адміністративно-правову природу електронного цифрового підпису, яка, базуючись на математичній моделі криптографії, через норми адміністративного права набуває нової соціальної значимості та забезпечує публічне адміністрування фізичних і юридичних осіб щодо

зручності у задоволенні своїх прав, свобод та законних інтересів шляхом легалізації юридичного статусу стосовно тотожності електронного цифрового підпису і власноручного підпису (печатки);

удосконалено:

– фактичний зміст адміністративно-правових відносин з використанням електронного цифрового підпису як суспільних відносини, які виникають (можуть виникати), змінюються і припиняються завдяки електронному цифровому підпису, отриманому в результаті криптографічного перетворення набору електронних даних, що дає змогу підтвердити його цілісність та ідентифікувати підписувача та об'єктивно потребують врегулювання нормами адміністративного права;

– наукове розуміння об'єкту адміністративно-правових відносин у сфері використання електронного цифрового підпису як об'єктивно існуючого та законодавчо закріпленого права на отримання послуг (електронний цифровий підпис), а також дій, які здійснюють з ним підписувачі і споживачі, а також суб'єкти публічної адміністрації на основі реалізації норм адміністративного права;

– законодавство у сфері використання електронного цифрового підпису в Україні щодо розширення сфери його застосування, посилення захищеності, покращення зручності користування, захисту санкціями через встановлення адміністративної відповідальності за відмову його визнання і неналежне зберігання;

отримали подальшого розвитку:

– наукові положення стосовно суб'єктів адміністративно-правових відносин у сфері електронного цифрового підпису як учасників адміністративно-правових відносин, які мають суб'єктивні адміністративні обов'язки та юридичні права, наділені специфічними юридичними властивостями надання повної юридичної легитимності електронному цифровому підпису та можливостей використання його підписувачем і користувачем як аналогу письмового підпису;

– зміст адміністративно-правових відносин у сфері електронного цифрового підпису як сукупності адміністративних обов'язків і прав суб'єктів публічної адміністрації, підписувачів і споживачів електронного цифрового підпису, коли чисельним адміністративним обов'язкам суб'єктів публічної адміністрації відповідає встановлене адміністративним законодавством право отримання від них якісних і своєчасних адміністративних послуг стосовно електронного цифрового підпису;

– наукові положення щодо ефективного зарубіжного досвіду використання електронного цифрового підпису, коли демократичні правові держави функціонують у вимірі інформаційного суспільства, невід'ємним елементом якого є електронні цифрові підписи, що використовуються в усіх публічних і приватних сферах суспільного життя.

Практичне значення отриманих результатів полягає в тому, що вони можуть бути використані у:

– *науково-дослідній сфері* – для подальшого теоретичного розроблення питань адміністративно-правових відносин з використанням електронного цифрового підпису в Україні (акт впровадження Науково-дослідного інституту публічного права);

– *правозастосовній діяльності* – щодо вдосконалення адміністративно-правових відносин з використанням електронного цифрового підпису в Україні (акт впровадження Інституту права та післядипломної освіти Міністерства юстиції України);

– *навчальному процесі* – під час розроблення та викладання навчальної дисципліни «Проблеми теорії адміністративного права», при підготовці відповідних підручників, навчальних посібників, конспектів лекцій (акт впровадження Відкритого міжнародного Університету розвитку людини «Україна»).

Апробація матеріалів дисертації. Основні положення дисертаційного дослідження обговорювалися під час роботи трьох науково-практичних конференцій: «Сучасне державотворення та

правотворення: питання теорії та практики (м. Одеса, 11-12 грудня 2015 р.); «Особливості розвитку публічного та приватного права в Україні» (м. Харків, 15-16 липня 2016 року); «Сучасні правові системи світу в умовах глобалізації: реалії та перспективи» (м. Київ, 10-11 березня 2017 р.).

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації складає 212 сторінок. Робота містить список використаних джерел із 184 найменувань на 19 сторінках.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВИХ ВІДНОСИН З ВИКОРИСТАННЯМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

1.1 Поняття адміністративно-правових відносин з використанням електронного цифрового підпису

Конституція України проголошує, що Україна є суверенною і незалежною, демократичною, соціальною, правовою державою. Статтею 3 закріплено, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю, а права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Стаття 6 закріплює, що державна влада в Україні здійснюється на засадах її поділу на законодавчу, виконавчу та судову, а органи законодавчої, виконавчої та судової влади здійснюють свої повноваження у встановлених цією Конституцією межах і відповідно до законів України [78]. Статтею 19 визначено, що органи державної влади та місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі та в межах повноважень та у спосіб, що передбачені Конституцією та законами України [78].

Здійснюючи владні повноваження, держава не може обійтись без інформаційних технологій. О. Маруховський вважає, що інформаційне суспільство в широкому розумінні – це суспільство, в якому інформація, знання й інформаційно-комунікаційні технології перетворюються на основну продуктивну силу та джерело епохальних зрушень в усіх сферах суспільного життя, зокрема в політичній, що виявляється в метаморфозах політичної влади, трансформації політичних режимів («е-демократія», електронна демократія), владних інститутів («е-уряд» та «е-само-

врядування»), партійних («е-партія») і виборчих систем («е-вибори» та «е-референдум»), у прискоренні переходу від представницької демократії до демократії участі, у зміцненні громадянського суспільства та посиленні інших демократичних перетворень на користь людини, суспільства й людства в цілому.

Інформаційне суспільство у вузькому розумінні – це суспільство, в якому інформація, знання й інформаційно-комунікаційні технології перетворюються на основну продуктивну силу та джерело епохальних зрушень в усіх сферах суспільного життя [92]. Зміна наявного документообігу та застосування «електронних» документів, створення ресурсу документів у цифровому форматі в органах державної влади, установах, організаціях та на підприємствах України набуває дедалі більшого розвитку в Україні. З цією метою Кабінет Міністрів України та інші органи виконавчої влади в межах повноважень, визначених законом, реалізують державну політику «електронного» документообігу, яка спрямована на реалізацію єдиної державної політики «електронного» документообігу; забезпечення прав і законних інтересів суб'єктів «електронного» документообігу; нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення «електронних» документів [125].

На думку І. Арістової, потреба здійснення належного документообігу та його вдосконалення зумовлені такими чинниками:

– ускладнення функцій державного управління підвищує вимоги до складання документів, їх оформлення та обробки;

– раціоналізація роботи з документами – важливий напрямок підвищення ефективності управлінської праці, що дозволяє уникати невиправданих часових витрат, зосередити зусилля управлінців на оперативному і якісному вирішенні конкретних управлінських питань;

– забезпечення прав та інтересів громадян, які вступають у правовідносини з державними органами [10].

Низка вчених говорять, що електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості й прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [28]. Громадяни завдяки інформаційно-комунікаційним технологіям можуть отримати адміністративну послугу або необхідну інформацію від органів державної влади чи місцевого самоврядування в будь-який час і незалежно від місцеперебування.

Електронне урядування є своєрідною адаптацією державного управління до вимог інформаційного суспільства. Його сутність полягає в інтерактивній взаємодії держави з громадянами завдяки системі зворотного зв'язку (громадянин – уряд – громадянин і навпаки) із залученням інформаційно-комунікаційних технологій. Електронна демократія – це форма демократії, що характеризується залученням громадян до процесу вироблення та ухвалення управлінських рішень за допомогою використання сучасних інформаційних комунікаційних технологій як основного засобу [48].

З цією метою кабінетом Міністрів схвалено Концепцію розвитку електронного урядування в Україні. Документом визначено напрямки, механізми і строки формування ефективної системи електронного урядування в Україні для задоволення інтересів та потреб фізичних і юридичних осіб, удосконалення системи державного управління, підвищення конкурентоспроможності та стимулювання соціально-економічного розвитку держави. Реалізація Концепції дасть змогу підвищити ефективність роботи органів державної влади й органів місцевого самоврядування та досягти якісно нового рівня управління державою, що базується на принципах результативності, ефективності,

прозорості, відкритості, доступності, довіри та підзвітності; покращити якість надання публічних послуг фізичним та юридичним особам відповідно до європейських вимог, а також забезпечити необхідну мобільність і конкурентоспроможність громадян та суб'єктів господарювання в сучасних економічних умовах; мінімізувати корупційні ризики при виконанні владних повноважень; покращити інвестиційну привабливість, діловий клімат і конкурентоспроможність країни; стимулювати соціально-економічний розвиток в Україні. Реалізація Концепції передбачена на період до 2020 року.

Відповідно до Указу Президента України від 12 січня 2015 р. №5 «Про Стратегію сталого розвитку «Україна-2020», розпорядження Кабінету Міністрів України від 3 квітня 2017 р. № 275 «Про затвердження середньострокового плану пріоритетних дій Уряду до 2020 року та плану пріоритетних дій Уряду на 2017 рік» розвиток електронного урядування визначено одним і першочергових пріоритетів реформування системи державного управління. Також у рамках реалізації Угоди про асоціацію між Україною, з одного боку, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами – з іншого – Україна має забезпечити комплексний розвиток електронного урядування відповідно до європейських вимог. Цим документом визначено, що електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади й органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [161].

О. Тодчук наголошує, що перехід до «електронного» документообігу є найбільш прогресивним шляхом до підвищення ефективності роботи органів державної влади та суб'єктів господарювання, оскільки за умови його впровадження зникає необхідність вручну заповнювати паперову

звітність, відслідковувати переміщення документів всередині організації, контролювати порядок передання конфіденційних відомостей. Однак упровадження «електронного» документообігу є дуже складним процесом, який вимагає наявності обчислювальної техніки, адекватної програмному забезпеченню, оснащеності робочих місць установи персональними комп'ютерами на 100 %, психологічної готовності керівників до використання «електронних» аналогів підпису на документі, технічних можливостей переведення вихідних паперових документів в електронну форму, перепідготовки службовців і, звісно, правової основи цього процесу [159].

З цього приводу І. Поліщук вказує, що для успішного втілення електронного урядування як ідеї та забезпечення повної реалізації всіх його переваг нашій державі, безперечно, необхідно пройти складний шлях наближення системи державного управління до європейських стандартів. Для цього Україні необхідний певний час, оскільки остаточний перехід до електронного врядування потребує багато проміжних етапів: від декларування на найвищому державному рівні цього напрямку як пріоритетного – до вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації державних службовців, які будуть безпосередньо здійснювати відповідні функціональні обов'язки. При цьому перехід від традиційного управління до електронного урядування має відбуватися поступово та супроводжуватися відповідними змінами в розвитку суспільства, що сприятиме його стабілізації [108].

Електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості й прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян. Саме поняття «електронного уряду» з'явилося на початку 90-х років минулого століття. Ідею цього проекту започаткував Сінгапур, який

став першою країною, де 1999 року було створено масштабний урядовий портал eCitizen Centre, який не тільки почав надавати інформаційні послуги, але й дозволив отримати деякі державні послуги [28].

В. Авер'янов наголошує, що розроблені міжнародними та європейськими регіональними організаціями принципи і стандарти належного урядування досі не знайшли комплексного впровадження в актах адміністративного законодавства України, що зумовлено насамперед відсутністю концепції запровадження принципів і стандартів належного урядування у вітчизняній правовій системі [2].

Статтею 4. Закону України «Про електронні довірчі послуги» державне регулювання та управління у сферах електронних довірчих послуг та електронної ідентифікації» здійснюється на засадах:

– забезпечення принципу верховенства права у процесі надання і отримання електронних довірчих послуг та електронної ідентифікації;

– створення сприятливих та конкурентних умов для розвитку та функціонування сфер електронних довірчих послуг та електронної ідентифікації;

– вільного обігу електронних довірчих послуг в Україні, а також можливості вільного надання електронних довірчих послуг надавачами електронних довірчих послуг, розташованими в інших державах, діяльність яких відповідає вимогам Закону;

– забезпечення захисту прав і законних інтересів користувачів електронних довірчих послуг;

– гарантування доступності та можливостей використання електронних довірчих послуг для людей з обмеженими фізичними можливостями;

– відповідності вимог до надання електронних довірчих послуг та електронної ідентифікації європейським та міжнародним стандартам;

– забезпечення функціональної сумісності та технологічної нейтральності національних технічних рішень, а також недопущення їх дискримінації;

– забезпечення захисту персональних даних, що обробляються під час надання електронних довірчих послуг та електронної ідентифікації [124].

Законом України від 1 червня 2010 р. «Про захист персональних даних» регулюються правові відносини, пов’язані із захистом і обробкою персональних даних, які спрямовані на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних, і поширюються на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться в картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [135].

В умовах постійного ускладнення суспільних відносин поступово виникає нова якісна ситуація, коли накопичення постійно повторюваного одиничного суспільного досвіду призводить до виникнення нової якості, яка є більш складною від існуючих раніше, одночасно більш простою для користувачів. Останнім часом вагомим кроком у розвитку світового суспільства є практичне використанні різноманітних «крипто»-технологій, які в силу того що стають найбільш важливими для великої кількості осіб, починають регулюватися нормами права, зокрема адміністративного, іншими словами – можемо говорити про надання адміністративних послуг.

Адміністративну послугу визначають як діяльність адміністративного органу, спрямовану на юридичне оформлення умов, визначених законодавством як необхідні для забезпечення належної реалізації суб’єктивних прав, охоронюваних законом інтересів і виконання обов’язків фізичних або юридичних осіб, що здійснюється за зверненням

цих осіб і офіційним результатом якої є адміністративний (індивідуальний) акт відповідного органу [1].

Серед криптологічних технологій найбільшого практичного застосування отримав електронний цифровий підпис, що зумовлює нові вимоги до безпеки особистих даних і зручності їх використання.

Основний Закон, який регулює правову поведінку використання цифрового – електронного – підпису, є Закон України «Про електронний цифровий підпис». Документи, які були підписані електронним цифровим підписом, мають таку ж юридичну силу, як і звичайний письмовий підпис. Якщо паперовий документ може бути підписаний звичайною шариковою ручко, то в цифровому світі, зокрема в Інтернеті все набагато складніше. Для того щоб забезпечити можливість підписання електронних документів, було розроблено спеціальні технології, названі за аналогією електронним підписом. Специфічність електронного – цифрового – підпису, його відмінність від власноручно написаного зумовили необхідність розроблення й ухвалення спеціального законодавства, що регулює порядок використання новітніх програмних засобів ідентифікації електронних документів [123].

Одним із напрямів правового забезпечення створення та оброблення «електронних» документів є затвердження Кабінетом Міністрів України Постанови «Про затвердження Типової інструкції з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади» [134], де встановлено загальні вимоги щодо функціонування служб діловодства, документування управлінської інформації та організації роботи з документами в міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади.

Положення означеної вище Інструкції поширюються на організацію роботи з документами незалежно від способу фіксації та відтворення

інформації, включаючи їх підготовку, реєстрацію, облік і контроль за виконанням, що здійснюються за допомогою програмово-технічних комплексів. До сфери регулювання в новій Інструкції віднесено всю документацію, що створюється та використовується в управлінській діяльності. Але вимоги до підготовки документів (склад реквізитів, порядок їх оформлення і розташування), що закріплені в Інструкції, поширюються лише на організаційно-розпорядчу документацію.

В Інструкції розмежовано два поняття – «електронний документ» та «документ в електронній формі». Це зумовлено тим, що відповідно до Закону України від 22 травня 2003 року № 851-IV «Про електронні документи та електронний документообіг» «електронним» документом визнається документ, засвідчений «електронним» цифровим підписом, а документ в електронній формі – це документ, інформація в якому зафіксована у вигляді «електронних» даних без «електронного» цифрового підпису (в сканованій формі) [125].

Відповідно до вимог статті 6 Закону України «Про електронні документи та електронний документообіг» накладання «електронного» цифрового підпису, який є обов'язковим реквізитом «електронного» документа, використовується для ідентифікації автора та/або підписувача «електронного» документа іншими суб'єктами «електронного» документообігу. Пунктом 2 Інструкції зазначено, що порядок організації «електронного» документообігу із застосуванням «електронного» цифрового підпису, роботи з «електронними» документами в діловодстві установи, здійснення діловодства стосовно документів, що містять інформацію з обмеженим доступом, здійснення діловодства за зверненнями громадян, запитами на інформацію визначаються окремими нормативно-правовими актами. Так, у країнах Європейського Союзу діє Конвенція «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [76].

Говорячи про електронні документи, відповідно до ДСТУ «Діловодство й архівна справа» «документ – це інформація, зафіксована на матеріальному носії, основною функцією якого є зберігати та передавати її в часі та просторі». «Електронний» документ – це документ, який створюють та використовують тільки в межах комп'ютерної системи» [46].

І. Клименко визначає «електронний» документообіг як цілеспрямовану організовану сукупність інформаційних процесів, яка забезпечує високу швидкість обробки даних, швидкий пошук інформації, доступ до джерел інформації незалежно від місця їх розташування, автоматизацію документообігу засобами комп'ютерної техніки і зв'язку [67].

О. Косовець зазначає, що це набір даних, записаних у комп'ютерозчитуваному вигляді, для яких виконана така умова: існує визнана учасниками електронного документообігу або затверджена компетентним органом процедура, що дозволяє однозначно перетворювати ці дані на документ традиційного режиму [80].

М. Женченко визначає, що електронні» ресурси – це інформаційні ресурси, якими управляє комп'ютер, зокрема ті, що потребують використання периферійного пристрою, підключеного до комп'ютера». За видом інформації, призначеної для сприйняття, електронні ресурси вчена поділяє на: «електронні» дані (інформація у вигляді чисел, букв, символів, зображень, включаючи графічну інформацію, відеоінформацію тощо або їхні комбінації); «електронні» програми (набори операторів чи підпрограм, які забезпечують виконання певних завдань, включаючи опрацювання даних); комбінацію (об'єднання) «електронних» даних і програм в одному ресурсі (мультимедіа, відеоігри) [56; 99].

У Законі України «Про інформацію» визначено, що документ – це матеріальний носій, який містить інформацію, основними функціями якого є її збереження та передавання в часі та просторі. Відповідно до статті 20 Закону України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим

доступом. У статті 21 до інформації з обмеженим доступом законодавець відносить: конфіденційну; таємну; службову інформацію [136].

На нашу думку, законодавство України не розкриває сутності поняття «електронного» документа, оскільки не містить певних категорій, таких як, наприклад, «реквізит». Так, К. Архіпова під електронним цифровим підписом розуміє реквізит електронного документа, призначений для захисту певного електронного документа від підробки, одержаний у результаті криптологічного перетворення інформації з використанням закритого ключа електронного цифрового підпису, що дозволяє ідентифікувати власника сертифікату ключа підпису, а також установити відсутність несанкціонованих змін або підміни інформації в електронному документі [12].

Отже, правове регулювання електронного цифрового підпису здійснюється з урахуванням широкої нормативної бази, яка чинна на території України.

Проте, незважаючи на захищеність використання такого підпису, на сьогодні існує велика небезпека з боку хакерів, тобто кіберзлочинність, яка нині існує майже в усіх країнах, розвивається зі своїм розвитком і методами; також розвиваються і шляхи подолання цих проблем, що зроблено для запобігання володіння чужим ключем: якщо зловмисник заволодіє чужим ключем, він може потенційно від імені справжнього власника здійснювати неправомірні дії – наприклад, проводити певні грошові транзакції, змінювати записи в базах даних тощо.

У таких випадках актуальним є виявлення та опис внутрішніх засад цього феномену, який практично вже використовується фізичними і юридичними особами, що підвищують ефективність своєї управлінської праці за допомогою захищених криптологічними засобами захисту і такими, що постійно модернізуються, новими технологіями.

До проблеми адміністративно-правових відносин з використанням електронного цифрового підпису зверталися вчені-юристи І. Арістова,

К.Архіпова, Ю. Атаманова, Н. Бааджи, І. Верес, В. Галунько, А. Гетьман, А. Дегтярьов, М. Дутов, Р. Еннан, О. Кирилюк, С. Короєд, В. Курило, В. Мілаш, С. Лур'є, M. Dawn та ін. Проте безпосередньо до аналізованої нами проблематики вони зверталися, лише аналізуючи інші більш загальні, спеціальні чи суміжні проблеми.

Правові відносини наповнюють усю правову матерію суспільства. Зокрема вони мають важливе значення у використанні криптотехнологій для потреб фізичних і юридичних осіб. Адже саме завдяки цьому їх використання стає можливим і безпечним. У цій площині вагоме місце займають норми адміністративного права. Наприклад, урегулювання потреб суспільства при використанні електронно-цифрового підпису здійснюють насамперед завдяки адміністративно-правовим нормам. Зовнішнім виразом цих норм є нормативно-правові акти, які визначають роль кожного суб'єкта – як фізичної, так і юридичної особи, які вступають у правовідносини з приводу об'єкта електронно-цифрового підпису. Серед таких актів доцільно виділити міжнародні правові джерела (Конвенція ООН про використання електронних повідомлень у міжнародних договорах (2005); Регламент ЄС від 23.07.2014 «Про електронну ідентифікацію та довірчі служби для електронних операцій на внутрішньому ринку», вітчизняні джерела – закони («Про електронний цифровий підпис» (спеціальний); «Про електронні документи та електронний документообіг»; «Про електронний цифровий підпис»; «Про обов'язковий примірник документів»; «Про Національну програму інформатизації»; «Про телекомунікації»; «Про Національну систему конфіденційного зв'язку»; «Про захист інформації в інформаційно-телекомунікаційних системах»); підзаконні нормативно-правові акти (Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації»), інші нормативно-правові акти. Ці

нормативно-правові акти зосереджують свою юридичну силу і на правових відносинах, які виникають з приводу електронно-цифрового підпису.

У теорії права під правовими відносинами розуміють суспільні відносини, урегульовані правом. Вони є наслідком дії останнього. Але правові відносини з'являються не лише тому, що діють правові норми, а й тому, що певні суспільні відносини об'єктивно потребують правової регламентації, не можуть нормально розвиватися без неї [29; 171]. Професор В. Авер'янов уважав, що адміністративно-правові відносини – це врегульовані нормами права суспільні відносини, в яких їх сторони (суб'єкти) взаємопов'язані та взаємодіють шляхом здійснення суб'єктивних прав і обов'язків, установлених і гарантованих відповідними адміністративно-правовими нормами [1].

Професор В. Галунько визначив, що адміністративно-правові норми врегульовують відносини між публічною адміністрацією та фізичними особами (громадянами, іноземцями, особами без громадянства); публічною адміністрацією та юридичними особами, які не мають владного статусу, та фізичними особами зі спеціальним невладним статусом (наприклад, фізичних осіб-підприємців); між вищими та нижчими органами й посадовими особами публічної адміністрації. Тим самим загальним для всіх видів адміністративно-правових відносин є те, що як мінімум однією зі сторін є суб'єкт публічної адміністрації, наділений народом України владною компетенцією [39].

З цього приводу професор В. Курило, аналізуючи адміністративно-правові відносини в аграрному секторі, визначає їх як урегульовані нормами адміністративного права суспільні відносини у вигляді стійких правових зв'язків між їх сторонами (суб'єктами), що виникають у процесі реалізації ними суб'єктивних прав та обов'язків на підставі приписів адміністративно-правових норм, якими вони встановлені й гарантовані [87].

На думку В. Шуби, адміністративно-правові відносини в діяльності органів прокуратури України визначено як урегульовані адміністративно-правовими нормами суспільні відносини, які складаються як під час зовнішньої, так і внутрішньої організаційної діяльності органів прокуратури, одним з обов'язкових учасників яких є прокуратура або її посадова особа [171].

С. Лопатін дав визначення адміністративно-правових відносин у сфері забезпечення права громадян на інформацію як урегульованих нормами адміністративного права суспільних відносин, які виникають в інформаційній сфері у процесі здійснення державної влади у зв'язку з реалізацією інформаційних прав і свобод та забезпеченням інформаційних процесів [89].

Адміністративно-правові відносини у сфері фінансової безпеки – це врегульовані нормами права суспільні відносини у сфері фінансової безпеки, у яких їх сторони (суб'єкти) взаємопов'язані та взаємодіють через здійснення суб'єктивних прав та обов'язків, установлених і гарантованих відповідними адміністративно-правовими нормами й державою.

Адміністративно-правові відносини у сфері фінансової безпеки є різновидом адміністративно-правових відносин, і тому мають певні характерні риси [90; 146]. На думку професора Т. Коломоєць, вони подаються як суспільні відносини, урегульовані нормами адміністративного права, суб'єкти яких наділені правами й обов'язками у сфері забезпечення прав, свобод і законних інтересів фізичних і юридичних осіб, а також у процесі публічного (державного і самоврядного) управління у сферах соціально-економічного й адміністративно політичного розвитку та охорони громадського порядку [72].

Структура адміністративно-правових відносин, що виникають в діяльності органів прокуратури, складається з таких елементів: суб'єктів адміністративно-правових відносин, яких визначено як індивідуальних чи

колективних осіб, фізичних чи юридичних, одні з яких, як правило, наділені владними повноваженнями (правами та обов'язками), що реалізуються ними у сфері владної управлінської діяльності стосовно інших суб'єктів, які визначено як поведінку учасників цих відносин, тобто суб'єктів (дії, утримання віддій), що можуть мати як зовнішній, так і внутрішній організаційний характер; змісту адміністративно-правових відносин, які визначено як вид і міра можливої (дозволеної) та належної (необхідної) поведінки, що передбачені адміністративно-правовими нормами, перебувають у тісному взаємозв'язку, тобто є взаємозалежними і забезпечуються державою [171].

Здійснене за методами аналізу й синтезу дослідження дає можливість дійти таких узагальнень: усі вчені вважають, що адміністративно-правові відносини – це суспільні відносини, урегульовані нормами адміністративного права. Учені-адміністративісти В. Галунько, В. Курило, В. Шуба вважають, що одним із суб'єктів таких відносин обов'язково є публічна адміністрація. Крім того В. Шуба зазначає, що адміністративно-правові відносини реалізуються через зовнішню і внутрішню діяльність публічної адміністрації. Професори В. Авер'янов, В. Кирило, Т. Коломоєць уважають, що кожен з учасників адміністративно-правових відносин має права та обов'язки.

Об'єктом адміністративно-правових відносин є те матеріальне або нематеріальне благо, на використання чи охорону якого спрямовано суб'єктивні права та юридичні обов'язки учасників адміністративно-правових відносин, а також певні дії, заради яких суб'єкти вступають в адміністративно-правові відносини. Об'єктом адміністративно-правових відносин може бути все, що здатне слугувати здійсненню публічних інтересів. Об'єкти адміністративного права поділяються на нематеріальні особисті блага людини (життя і здоров'я, честь і гідність, недоторканність, безпеку, свободу пересування та ін.) та матеріальні – предмети матеріального світу, створені природою чи людиною.

У теорії адміністративного права визначено, що об'єктом адміністративно-правових відносин є те матеріальне або нематеріальне благо, на використання чи охорону якого спрямовано суб'єктивні права та юридичні обов'язки учасників адміністративно-правових відносин. Це блага матеріальні або нематеріальні, а також певні дії, заради яких суб'єкти вступають в адміністративно-правові відносини. Об'єктом адміністративно-правових відносин може бути все, що здатне служити здійсненню публічних інтересів. У цій ролі можуть бути права людини і громадянина, право власності й послуги інших осіб. Права людини і громадянина стають об'єктом адміністративного права, оскільки є природними; законодавець через Конституцію України та інші закони їх установлює та визначає межі, в яких ними можна беззаперечно користуватися. У такий спосіб об'єктами адміністративного права стає вся палітра прав, визначених у розділі першому та другому Конституції України [39].

У свою чергу Е. Шевченко вважає, що адміністративно-правові відносини – це врегульовані адміністративно-правовими нормами на засадах «влада – підпорядкування» взаємовідносини (взаємозв'язки), що виникають у сфері публічного (державного і самоврядного) управління між органами державного управління та іншими суб'єктами адміністративного права з реалізації їхніх суб'єктивних прав і юридичних обов'язків, що здійснюються в особливому правовому режимі забезпечення їх законності з боку держави [170].

З цього приводу В. Курило, аналізуючи адміністративно-правові відносини в аграрному секторі, вважає їх урегульованими нормами адміністративного права суспільними відносинами у вигляді стійких правових зв'язків між їх сторонами (суб'єктами), що виникають у процесі реалізації ними суб'єктивних прав та обов'язків на підставі приписів адміністративно-правових норм, якими вони встановлені й гарантовані [87].

Професор В. Колпаков вважає, що поняття адміністративно-правових відносин стає все ширшим і виходить за межі державного управління. Про це насамперед свідчить їх висвітлення у навчальній літературі [74]. Так, В. Авер'янов уважав, що адміністративно-правові відносини – це врегульовані нормами права суспільні відносини, в яких їх сторони (суб'єкти) взаємопов'язані і взаємодіють шляхом здійснення суб'єктивних прав і обов'язків, установлених і гарантованих відповідними адміністративно-правовими нормами [1].

Професор Т. Коломоєць адміністративно-правові відносини розглядає як суспільні відносини, врегульовані нормами адміністративного права, суб'єкти яких наділені правами і обов'язками у сфері забезпечення органами виконавчої влади й органами місцевого самоврядування реалізації та захисту прав, свобод і законних інтересів фізичних і юридичних осіб [72].

Виходячи з таких позицій вважаємо, що адміністративно-правові відносини, що виникають з приводу електронно-цифрового підпису діяльності певних структур України, визначено як урегульовані адміністративно-правовими нормами суспільні відносини, які складаються як під час зовнішньої, так і внутрішньої організаційної діяльності органів, одним з обов'язкових учасників яких є посадова особа.

З урахуванням думки В. Шуби вважаємо, що особливостями адміністративно-правових відносин у сфері електронно-цифрового підпису є такі:

– вони регулюються адміністративно-правовими нормами, які визначають межі належної, допустимої та рекомендованої поведінки їх учасників;

– наявність як зовнішніх, так і внутрішніх адміністративно-правових відносин (повноважень їх працівників; адміністративно-правові відносини під час використання електронного підпису);

– особливий суб’єктний склад, оскільки однією стороною цих відносин є посадова особа, наділена владними повноваженнями у зовнішніх адміністративних відносинах;

– вольовий характер адміністративно-правових відносин, який полягає в тому, що в них через норми права відображається загальна державна владна воля, яка у свою чергу є підставою для можливого вираження (конкретизації) державної волі під час діяльності посадових осіб;

– адміністративно-правові відносини посадових осіб України пов’язані з практичною реалізацією завдань, функцій і владних повноважень їх працівників;

– як зовнішні, так і внутрішні адміністративно-правові відносини, що виникають з приводу електронного цифрового підпису, можуть виникати з приводу як матеріальних, так і нематеріальних благ, проте є обов’язковою умовою;

– суб’єкти адміністративно-правових відносин у діяльності органів прокуратури України є носіями адміністративних прав та обов’язків, які охороняються і захищаються нормами адміністративного права (у деяких випадках – нормами інших галузей права – наприклад, кримінального, цивільного тощо);

– захист прав суб’єктів адміністративно-правових відносин і спонукання до виконання адміністративних обов’язків здійснюється за допомогою як специфічних адміністративних заходів впливу, так і в порядку адміністративного судочинства [171].

У цілому адміністративно-правові відносини, що виникають з приводу електронного цифрового підпису, характеризуються такими особливостями:

1) вони нерозривно пов’язані з адміністративно-правовими нормами, виникають і здійснюються на їх основі;

2) основною їх метою є забезпечення прав та свобод людини і громадянина, нормальне функціонування громадянського суспільства та держави;

3) вони регулюють широке коло суспільних відносин між публічною адміністрацією та об'єктами публічного управління;

4) провідною рисою адміністративно-правових відносин є їх публічна природа, вони виникають з ініціативи будь-якої сторони, при цьому згода іншої сторони, як правило, не є обов'язковою;

5) адміністративно-правові відносини є переважно виконавчо-розпорядчими: у вузькому розумінні суб'єкти публічного управління наділені владною компетенцією, а об'єкти зобов'язані виконувати їх законні вимоги; поряд із цим за широкого підходу сторони адміністративно-правових відносин завжди мають суб'єктивні права та юридичні обов'язки, які взаємопов'язані між собою: кожному суб'єктивному праву однієї сторони відповідає юридичний обов'язок іншої, і навпаки;

6) вони мають свідомо вольовий характер, адже держава через видання відповідних адміністративно-правових норм виражає свою волю народу України, учасники цих відносин здійснюють своє волевиявлення, усвідомлюють значення своїх дій та можуть нести за них відповідальність;

7) адміністративно-правові відносини охороняються державою, яка сприяє здійсненню суб'єктивних публічних прав та юридичних обов'язків, а в разі правопорушення притягує винну особу до адміністративної чи іншої юридичної відповідальності;

8) не належать до адміністративно-правових відносини між публічною адміністрацією та об'єктами публічного управління, якщо вони не засновані на праві [40].

Таким чином, адміністративно-правові відносини, що виникають щодо електронного цифрового підпису, відбивають вплив адміністративно-правових норм на поведінку суб'єктів, які використовують

електронний цифровий підпис, та об’єктів публічного управління, через що між ними виникають сталі правові зв’язки публічновладного характеру. Іншими словами, адміністративно-правова норма містить абстрактну конструкцію адміністративно-правового відношення. Сутність такої конструкції полягає в тому, що адміністративно-правова норма від імені держави визначає належну поведінку кожного зі своїх адресатів. Вона встановлює обов’язкові правила, за якими відбувається «спілкування». Ці правила формуються у вигляді взаємних прав і обов’язків [73].

Отже, адміністративно-правові відносини з використанням електронного цифрового підпису – це суспільні відносини, які виникають, змінюються і припиняються тільки завдяки електронному цифровому підпису, отриманому за результатом криптографічного перетворення набору електронних даних, що дає змогу підтвердити його цілісність та ідентифікувати підписувача, урегульовуються нормами адміністративного права, зокрема зовнішнім виразом якого є Закон України від 22.05.2003 №852-IV «Про електронний цифровий підпис» [123; 136].

На думку І Верес, електронний підпис є набором даних в електронній формі, який виконує функції ідентифікації особи підписувала й засвідчення волевиявлення його волі. Електронний цифровий підпис виконує ще одну додаткову функцію – підтвердження цілісності даних в електронній формі. За умови використання електронного цифрового підпису з посиленим чи без посиленого сертифіката, електронного підпису одноразовим ідентифікатором, аналогу власноручного підпису письмова форма договору є дотриманою [22].

У будь-якому суспільстві існують різноманітні відносини між окремими особами та різними об’єднаннями людей. Усі вони до певної міри упорядковані, організовані, значна частина з них регулюється нормами права. Головне призначення норм права – бути регулятором суспільних відносин. Регулюючи ті чи інші відносини, воно надає їм правового характеру, правової, юридичної форми. У результаті цього вони

й стають правовими. Тим самим у загальному розумінні адміністративно-правові відносини – це суспільні відносини, урегульовані нормами адміністративного права [3; 39].

На наш погляд, електронний цифровий підпис не може функціонувати без глобальної системи Інтернет. На думку Р. Еннан, інтернет-відносини – це суспільні відносини в кіберпросторі, учасники яких є носіями суб'єктивних прав та обов'язків у мережі Інтернет. Це особливі суспільні відносини, які виникають у результаті впливу норм інформаційного, комп'ютерного, міжнародного та інших галузей права, міжнародних договорів на поведінку суб'єктів цих відносин. Це новий тип суспільних відносин, що виникають, змінюються та припиняються в кіберпросторі. Це не лише правові, фактичні, етичні відносини – це складні соціальні зв'язки особливої правової, інформаційної та технічної природи [52; 147].

Суспільні відносини в мережі Інтернет можуть бути як правовими, так і неправовими. У свою чергу інтернет-правовідносини – це особливі відносини, що виникають в результаті впливу норм інформаційного, міжнародного та інших галузей права на поведінку людей в цьому середовищі. Інтернет-правовідносини є різновидом інформаційних правовідносин, які виникають, змінюються і припиняються у віртуальному просторі й регулюються нормами різних галузей права. Як і будь-які інші правовідносини, правовідносини в мережі Інтернет включають у себе певний набір елементів (суб'єкт, об'єкт та зміст). Тому перспективними для подальших досліджень є виявлення та дослідження особливостей суб'єкта та об'єкта інтернет-правовідносин, а також питання структури окремих видів таких правовідносин, без яких вони не можуть відбутися [13].

Таким чином, у вузькому розумінні адміністративно-правові відносини з використанням електронного цифрового підпису – це суспільні відносини, які виникають, змінюються і припиняються тільки

завдяки електронному цифровому підпису, отриманому за результатом криптографічного перетворення набору електронних даних, що дає змогу підтвердити його цілісність та ідентифікувати підписувача; вони врегульовуються нормами адміністративного права, зокрема зовнішнім виразом якого є Закон України від 22.05.2003 № 852-IV «Про електронний цифровий підпис» [123].

Загальною ознакою для всіх видів адміністративно-правових відносин, зокрема і тих, що здійснюються з використанням електронного цифрового підпису, є те, що як мінімум однією зі сторін є суб'єкт публічної адміністрації, наділений владною компетенцією. Крім того адміністративно-правові відносини з використанням електронного цифрового підпису характеризуються такими особливостями:

– вони нерозривно пов'язані з адміністративно-правовими нормами, виникають і здійснюються на їх основі;

– основною їх метою є забезпечення прав та свобод людини і громадянина, нормальне функціонування громадянського суспільства та держави;

– вони врегульовують широке коло суспільних відносин між публічною адміністрацією та об'єктами публічного управління – особами, які отримують, або/та користуються електронним цифровим підписом;

– адміністративно-правові відносини з використанням електронного цифрового підпису є переважно адміністративно-сервісними;

– вони мають свідомо-вольовий характер;

– адміністративно-правові відносини з використанням електронного цифрового підпису охороняються державою, яка сприяє здійсненню суб'єктивних публічних прав та юридичних обов'язків, а в разі правопорушення притягує винних осіб до адміністративної чи іншої юридичної відповідальності;

– не належать до адміністративно-правових відносини з використанням електронного цифрового підпису між публічною

адміністрацією та об’єктами публічного управління, якщо вони не засновані на нормах адміністративного права [39].

На наш погляд, структура адміністративно-правових відносин з використанням електронного цифрового підпису є класичною, вона характеризується взаємопов’язаністю всіх її складових компонентів, якими є суб’єкти, об’єкти, зміст правовідносин та юридичні факти.

Суб’єкти правовідносин – це учасники адміністративно-правових відносин, які мають суб’єктивні права та юридичні обов’язки й наділені специфічними юридичними властивостями. Іншими словами, до суб’єктів адміністративно-правових відносин належать як суб’єкти публічної адміністрації, так і об’єкти публічного управління [39].

Центральний засвідчувальний орган визначається Кабінетом Міністрів України. Він виконує такі функції:

– формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів;

– блокує, скасовує та поновлює посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів;

– веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів;

– веде акредитацію центрів сертифікації ключів;

– отримує та перевіряє інформацію, необхідну для їх акредитації;

– забезпечує цілодобово доступ засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;

– зберігає посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів;

– надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов’язаних з використанням електронного цифрового підпису [123].

Це 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 і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства [124].

До повноважень Кабінету Міністрів України у сферах електронних довірчих послуг та електронної ідентифікації належить такі:

– здійснення державної політики у сферах електронних довірчих послуг та електронної ідентифікації;

– визначення пріоритетних напрямів розвитку сфер електронних довірчих послуг та електронної ідентифікації;

– координація діяльності органів, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації, крім Національного банку України;

– прийняття у межах своїх повноважень нормативно-правових актів у сферах електронних довірчих послуг та електронної ідентифікації;

– державна підтримка розвитку сфер електронних довірчих послуг та електронної ідентифікації;

– організація міжнародного співробітництва у сферах електронних довірчих послуг та електронної ідентифікації;

– здійснення інших повноважень у сферах електронних довірчих послуг та електронної ідентифікації, визначених законом.

Забезпечення державного регулювання сфер електронних довірчих послуг та електронної ідентифікації здійснюється Кабінетом Міністрів України з урахуванням вимог національних, міжнародних та європейських стандартів [124].

Відповідно до Постанови Кабінету Міністрів України від 28 жовтня 2004 р. №1451 «Про затвердження Положення про центральний засвідчувальний орган» на Міністерство юстиції України покладено виконання функцій центрального засвідчувального органу, оскільки одним з основних завдань Міністерства юстиції України є виконання функцій центрального засвідчувального органу шляхом забезпечення створення умов для функціонування засвідчувальних центрів органів виконавчої влади або інших державних органів та центрів сертифікації ключів відповідно до Положення про Міністерство юстиції України, затвердженого Постановою Кабінету Міністрів України від 2 липня 2014 р. №228. Технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється державним підприємством «Національні інформаційні системи», яке визначено адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу відповідно до наказу Міністерства юстиції України від 19 жовтня 2015 р. №2025/5 «Деякі питання функціонування центрального засвідчувального органу» [166].

Так, відповідно до Постанови Кабінету Міністрів від 2 липня 2014 р. № 228 Міністерство юстиції виконує функції центрального засвідчувального органу системи електронного цифрового підпису, а саме:

– проводить реєстрацію, акредитацію засвідчувальних центрів та центрів сертифікації ключів, повторну акредитацію та скасування акредитації засвідчувальних центрів та акредитованих центрів сертифікації ключів, отримує та перевіряє інформацію, необхідну для цього;

– видає, переоформлює, анулює відповідні свідоцтва та видає дублікати;

– забезпечує діяльність постійно діючої комісії з акредитації засвідчувальних центрів та центрів сертифікації ключів;

– генерує пари ключів (особистий та відкритий ключі) центрального засвідчувального органу;

– формує і видає посилені сертифікати відкритих ключів засвідчувальним центрам та центрам сертифікації ключів;

– формує посилені сертифікати власних відкритих ключів центрального засвідчувального органу;

– блокує, скасовує та поновлює сертифікати відкритих ключів засвідчувальних центрів і центрів сертифікації ключів у випадках, передбачених законом, про що інформує орган контролю;

– зберігає посилені сертифікати відкритих ключів засвідчувальних центрів, центрів сертифікації ключів, акредитованих центрів сертифікації ключів, що припинили діяльність;

– надає послугу з постачання передачі сигналів точного часу для формування та проведення перевірки позначки часу;

– погоджує розроблені центрами сертифікації ключів, акредитованими центрами сертифікації ключів порядки синхронізації часу із Всесвітнім координованим часом (UTC);

– веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів відкритих ключів засвідчувальних центрів, центрів сертифікації ключів, акредитованих центрів сертифікації ключів та здійснює їх розповсюдження (публікацію);

– веде Реєстр суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом;

– забезпечує цілодобово доступ засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів і відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;

– надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов'язаних з використанням електронного цифрового підпису;

– розглядає заяви і скарги щодо неналежного функціонування центрів та подає відповідні пропозиції органу контролю;

– повідомляє органу контролю про обставини, які перешкоджають діяльності центрального засвідчувального органу;

– здійснює інші визначені законом повноваження, необхідні для забезпечення функціонування центрального засвідчувального органу;

забезпечує розроблення норм, стандартів і технічних регламентів у сфері електронного цифрового підпису;

– забезпечує здійснення відповідно до законодавства технічного регулювання у сфері електронного цифрового підпису;

– здійснює організаційні заходи щодо застосування електронного цифрового підпису [132].

Акредитований центр сертифікації ключів (АЦСК) – це центр сертифікації ключів, акредитований в установленому порядку, є акредитованим центром сертифікації ключів. Порядок акредитації та вимоги, яким має відповідати акредитований центр сертифікації ключів, установлюються Кабінетом Міністрів України [123].

В умовах сьогодення АЦСК зокрема є: Інформаційно-довідковий департамент ДФС «Акредитований центр сертифікації ключів Інформаційно-довідкового департаменту ДФС» [120; 144]; Державне підприємство «Інформаційний центр» Міністерства юстиції України «Акредитований центр сертифікації ключів державного підприємства «Інформаційний центр» Міністерства юстиції України [151]; Державне підприємство «Головний інформаційно-обчислювальний центр Державної адміністрації залізничного транспорту України»; «Акредитований центр сертифікації ключів державного підприємства «Головний інформаційно-обчислювальний центр Державної адміністрації залізничного транспорту України»; Генеральний штаб Збройних Сил України «Акредитований центр сертифікації ключів Збройних Сил»; Державне підприємство «Українські спеціальні системи»; «Акредитований центр сертифікації ключів державного підприємства «Українські спеціальні системи»; Публічне акціонерне товариство «Комерційний банк «Приватбанк»;

«Акредитований центр сертифікації ключів Публічного акціонерного товариства «Комерційний банк «Приватбанк»; Товариство з обмеженою відповідальністю «Арт-мастер»; «Акредитований центр сертифікації ключів «Masterkey» ТОВ «Арт-мастер» [145].

Споживачі електронного цифрового підпису:

1) органи публічної влади, що надають адміністративні послуги, які практично отримати без ЕЦП неможливо: єдині та державні реєстри Мін'юсту; електронні послуги Мін'юсту; система електронної взаємодії органів виконавчої влади; система добору арбітражних керуючих; ЄДЕБО Міністерства освіти та науки України; електронна звітність Державної служби статистики України; петиції Президенту України; Загальнодержавний портал державних закупівель; Національне агентство з питань запобігання корупції; електронні послуги Мінсоцполітики; призначення житлової субсидії; Портал електронних послуг пенсійного фонду України; Єдиний державний реєстр МВС України; електронні адміністративні послуги Міністерство внутрішніх справ України; електронні послуги Міністерства екології та природних ресурсів України; електронні послуги Державної архітектурно-будівельної інспекції України; Міністерство соціальної політики «Послуга призначення допомоги при народженні дитини»; електронні послуги Державного земельного кадастру; Єдиний портал адміністративних послуг; електронний сервіс «Електронний кабінет платника»; Особистий кабінет львів'янина; Пілотний проект iGov.org.ua; Єдиний веб-портал використання публічних коштів; електронний суд; он-лайн будинок юстиції; автоматизована система «Реєстр територіальних громад»; подання боржниками та організаторами аукціонів відомостей про справи про банкрутство; Особистий кабінет для мешканців міста Дніпра; Реєстр аграрних розписок та ін. [151];

2) будь-які інші особи приватного чи публічного права, які використовують електронний цифровий підпис для забезпечення

бізнесових чи публічних цілей (наприклад, Публічне акціонерне товариство «Українська залізниця», Публічне акціонерне товариство КБ «ПРИВАТБАНК»).

Підписувачі – це власники особистих ключів, фізичні або юридичні особи, які використовують їх для завірення своїх підписів в електронній формі для досягнення власних – як приватних, так і публічних потреб.

Таким чином, до основних суб'єктів адміністративно-правових відносин із використанням електронного цифрового підпису належать:

– центральний засвідчувальний орган (Міністерство юстиції України);

– акредитовані центри сертифікації ключів (зокрема Акредитований центр сертифікації ключів Інформаційно-довідкового департаменту ДФС, Акредитований центр сертифікації ключів державного підприємства «Інформаційний центр» Міністерства юстиції України);

– споживачі електронного цифрового підпису та підписувачі.

Суб'єкти адміністративно-правових відносин із використанням електронного цифрового підпису вступають у них з метою задоволення своїх інтересів і потреб, які опосередковують об'єкти адміністративно-правових відносин. Об'єктом адміністративно-правових відносин є те матеріальне або нематеріальне благо, на використання чи охорону якого спрямовано суб'єктивні права та юридичні обов'язки учасників адміністративно-правових відносин, а також певні дії, заради яких суб'єкти вступають в адміністративно-правові відносини. Об'єктом адміністративно-правових відносин може бути все, що здатне служити здійсненню публічних інтересів. Об'єкти адміністративного права поділяються на нематеріальні особисті блага людини (життя і здоров'я, честь і гідність, недоторканність, безпеку, свободу пересування та ін.) та матеріальні – предмети матеріального світу, створені природою чи людиною [39].

До останніх належить електронний цифровий підпис. Згідно із Законом України від 22.05.2003 № 852-IV «Про електронний цифровий підпис» електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних; електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Крім того в аналізованому Законі урегульовано інші суспільні відносини у сфері електронного цифрового підпису. Вимоги до сертифіката ключа прописано у ст. 6 Закону України від 22 травня 2003 р. № 852-IV «Про електронний цифровий підпис» [123]. Щодо суб'єктів адміністративного права, які використовують електронний цифровий підпис, то він використовується для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів, а саме для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. При цьому використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, установленого законом для вчинення правочинів у письмовій формі [123].

Невід'ємним елементом адміністративно-правових відносин є їх зміст як сукупність суб'єктивних публічних прав і обов'язків. Кожний із вище зазначених суб'єктів адміністративно-правових відносин із використанням електронного цифрового підпису мають свою адміністративні обов'язки і права. Юридичний обов'язок – це передбачені для зобов'язаної особи та забезпечені можливістю державного примусу вид і міра необхідної поведінки, які потрібно виконувати в інтересах уповноваженої особи, що має відповідні публічні суб'єктивні права.

У цілому юридичні обов'язки налічують чотири основні компоненти:

1) обов'язок здійснювати певні дії чи утримуватися від них (підписував зобов'язаний зберігати особистий ключ у таємниці);

2) обов'язок відреагувати на законні вимоги уповноваженого суб'єкта;

3) обов'язок нести відповідальність за невиконання цих вимог;

4) обов'язок не перешкоджати уповноваженому суб'єкту користуватися тим благом, на яке він має право [39].

Для прикладу візьмемо обов'язки підписувача, який зобов'язаний: зберігати особистий ключ у таємниці; надавати центру сертифікації ключів дані для засвідчення чинності відкритого ключа; своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа. У свою чергу він має право вимагати скасування, блокування або поновлення свого сертифіката ключа; оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку [123].

Таким чином, невід'ємним елементом адміністративно-правових відносин із використанням електронного цифрового підпису є їх зміст як сукупність суб'єктів адміністративно-правових відносин із використанням електронного цифрового підпису, які у цій сфері мають свої адміністративні обов'язки і права.

Усе вищевикладене дає можливість сформулювати такі висновки щодо поняття та змісту адміністративно-правових відносин із використанням електронного цифрового підпису:

1) у вузькому розумінні адміністративно-правові відносини з використанням електронного цифрового підпису – це суспільні відносини, які виникають, змінюються і припиняються завдяки електронному цифровому підпису, отриманого за результатом криптографічного перетворення набору електронних даних, що дає змогу підтвердити його

цілісність та ідентифікувати підписувача, і які врегульовуються нормами адміністративного права;

2) структура адміністративно-правових відносин із використанням електронного цифрового підпису є класичною – вони характеризується взаємопов'язаністю всіх її складових компонентів, якими є суб'єкти, об'єкти та зміст правовідносин;

3) до основних суб'єктів адміністративно-правових відносин із використанням електронного цифрового підпису належать: центральний засвідчувальний орган (Міністерство юстиції України); акредитовані центри сертифікації ключів, зокрема Акредитований центр сертифікації ключів Інформаційно-довідкового департаменту ДФС, Акредитований центр сертифікації ключів державного підприємства «Інформаційний центр» Міністерства юстиції України; споживачі електронного цифрового підпису та підписувачі;

4) об'єктом адміністративно-правових відносин у сфері використання електронного цифрового підпису є об'єктивно існуюче та законодавчо закріплене матеріальне інтелектуальне право (електронний цифровий підпис, а також діяння, які здійснюють з ним підписувачі і споживачі, а також суб'єкти публічної адміністрації на основі реалізації норм адміністративного права;

5) зміст адміністративно-правових відносин у сфері використання електронного цифрового підпису – це сукупність суб'єктів адміністративно-правових відносин із використанням електронного цифрового підпису, які в цій сфері мають свої адміністративні обов'язки і права.

Отже, адміністративно-правові відносини у сфері використання електронного цифрового підпису в широкому розумінні – це форма соціального прогресу як взаємодія спеціальної публічної адміністрації, що легалізує електронний цифровий підпис, підписувачів і споживачів електронного цифрового підпису на підставі адміністративно-правових

норм із метою більш ефективного забезпечення прав, свобод і законних інтересів фізичних і юридичних осіб, нормального функціонування громадянського суспільства і держави, учасники якої несуть адміністративні обов’язки та мають суб’єктивні права.

1.2 Адміністративно-правова природа електронного цифрового підпису

В Україні практично електронний цифровий підпис використовується в різноманітних сферах життєдіяльності, а саме: у банківській сфері, прикордонній службі, органах виконавчої влади (поліції) тощо. Проте розвинуті технологічні пристрої дають змогу незаконним шляхом підробити письмовий підпис, і тому на його заміну доречно використовувати саме електронний цифровий підпис, який дає змогу з великою ймовірністю виключити можливість незаконного підроблення документа та будь-які незаконні дії.

Проте, незважаючи на захищеність використання такого підпису, на сьогодні є значна небезпека з боку хакерів, тобто кіберзлочинність, яка нині існує майже в усіх країнах, розвивається зі своїм розвитком і методами; також розвиваються і шляхи подолання цих проблем, що зроблено для запобігання володіння чужим ключем: якщо зловмисник заволодіє чужим ключем, він може потенційно від імені справжнього власника здійснювати неправомірні дії – наприклад, проводити певні грошові транзакції, змінювати записи в базах даних тощо.

У таких випадках актуальним є виявлення та опис внутрішніх засад цього феномену, який практично вже використовується фізичними і юридичними особами, що підвищують ефективність своєї управлінської праці за допомогою захищених криптологічними засобами й такими, що постійно модернізуються, новими технологіями.

Електронний цифровий підпис на сьогодні є найбільш сучасним і безпечним типом електронного підпису. Він застосовується відповідно до чинних законодавчих вимог і використовується в найрізноманітніших сферах українського суспільства: від електронного протоколу, який складає національна поліція України, – до використання його в банківській сфері. Електронний цифровий підпис дав змогу замінити звичайний підпис, захистивши його від злочинних посягань і використання з недобросовісною метою для отримання певної вигоди.

Міжнародна практика використання засобів електронного цифрового підпису свідчить про поширене в розвинених країнах ужиття нормативних і технічних заходів щодо захисту особистих ключів від несанкціонованого використання. Найбільш надійним варіантом такого захисту є захищений носій особистих ключів. Він має вбудовані апаратно-програмні засоби, що забезпечують захист даних від несанкціонованого доступу, зокрема від ознайомлення із значенням параметрів особистих ключів та їх копіювання [16].

В Україні юридична природа електронного цифрового підпису містяться в нормах права. Це зокрема:

1) міжнародно-правові джерела: Конвенція ООН про використання електронних повідомлень у міжнародних договорах; Регламент ЄС від 23.07.2014р. «Про електронну ідентифікацію та довірчі служби для електронних операцій на внутрішньому ринку»; Директива 95/46/ЄС від 24.10.1995 р. «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»; Директива 97/66/ЄС від 15.12.1997 р. «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в елекомунікаційному секторі»; Директива 2002/58/ЄС від 12.07.2002 р. «Про обробку персональних даних та захист сектору електронних комунікацій» (Директива про секретність та електронні комунікації); Регламент Європейського парламенту та Ради ЄС № 45/2001 від 18.12.2001 р. «Про захист фізичних осіб, що стосується обробки

персональних даних установами і органами Європейського Співтовариства і щодо вільного переміщення таких даних»; Директива 2005/28/ЄС від 08.04.2005 р., що встановлювала принципи та детальні настанови належної клінічної практики, які стосуються досліджуваних лікарських засобів для вживання людиною, та вимог надання дозволу на виготовлення або імпорт таких продуктів; Рішення та рекомендації створеної згідно зі статті 29 Директиви 95/46/ЄС в 1996 р. постійно діючої Робочої групи з метою гармонізації європейського права в сфері захисту персональних даних та консультацій, а також рішення та рекомендації наглядових органів країн – учасниць ЄС;

2) вітчизняні джерела: а) закони: «Про електронний цифровий підпис»; «Про електронні документи та електронний документообіг»; «Про обов'язковий примірник документів»; «Про Національну програму інформатизації»; «Про телекомунікації»; «Про Національну систему конфіденційного зв'язку»; «Про захист інформації в інформаційно-телекомунікаційних системах»; б) підзаконні нормативно-правові акти: Наказ Адміністрація державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації». Наказ Міністерства юстиції України та Міністерства фінансів України від 09.10.2015 р. №1918/5/869 «Про інформаційну взаємодію між Єдиним державним реєстром юридичних осіб та фізичних осіб-підприємців та інформаційними системами Державної фіскальної служби України, обмін документами в електронній формі»; Розпорядження Голови Верховної Ради України від 19.05.2015 р. №698 «Про першочергові заходи з впровадження електронного документообігу у Верховній Раді України»; Наказ Вищого адміністративного суду України від 20.01.2015 р. № 3 «Про реалізацію проекту щодо обміну електронними документами між судом та учасниками судового процесу»; Рішення Національної комісії з цінних

паперів та фондового ринку від 28.08.2014 р. №1120 «Про затвердження Порядку обміну електронними документами Національної комісії з цінних паперів та фондового ринку та Центрального депозитарію цінних паперів»; Наказ Міністерства доходів і зборів від 31.12.2013 р. № 898 «Про затвердження форматів та Порядку подання документів в електронній формі для проведення електронної перевірки»; Постанова Кабінету Міністрів Українивід 17 липня 2009 р. № 733 «Про електронний обмін службовими документами в органах виконавчої влади» та інші.

Оновлення нормативно-правової бази України щодо створення спеціальних юридичних норм сприятиме ефективному впровадженню та функціонуванню електронного документообігу та електронного цифрового підпису. Воно здійснюється постійно. Так, для регулювання правовідносин у сфері інформаційних технологій Верховна Рада України ухвалила певну кількість законів: «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про обов'язковий примірник документів», «Про Національну програму інформатизації», «Про телекомунікації», «Про Національну систему конфіденційного зв'язку», «Про захист інформації в інформаційно-телекомунікаційних системах». Так, Закон України «Про електронну комерцію» передбачає три види електронних підписів: електронний цифровий підпис, електронний підпис одноразовим ідентифікатором, аналог власноручного підпису [126].

Проте основним Законом, яким регулюються адміністративно-правові відносини між особами, є Закон України «Про електронний цифровий підпис», що визначає певні адміністративно-правові аспекти. Так, правовий статус електронного цифрового підпису визначається тим, що такий підпис за правовим статусом дорівнюється до власноручного підпису (печатки) в разі, якщо: електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису; під час перевірки використовувався посилений сертифікат ключа, чинний на момент

накладення електронного цифрового підпису; особистий ключ підписувача відповідає відкритому ключу, зазначеному в сертифікаті.

Основне юридичне призначення електронного цифрового підпису – це забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. Електронний цифровий підпис використовується лише фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Хоч електронний цифровий підпис має специфічний вид використання й не змінює порядку підписання договорів та інших документів, установленого законом для вчинення правочинів у письмовій формі, він має таку ж юридичну силу, як і письмовий підпис [123].

Наріжним каменем застосування електронного цифрового підпису в електронному документообігу є те, що визначається не лише правовий статус такого підпису, але й електронних документів загалом, обов'язковим реквізитом яких є ЕЦП, а підпис дорівнюється до власноручного підпису (печатки) тільки у випадку виконання трьох умов.

Дві з трьох умов вимагають використання посиленого сертифікату, який є українським ноу-хау і не визнаний міжнародним та Європейським законодавством, якими визначається удосконалений електронний підпис та кваліфікований сертифікат, що є міжнародними умовами визнання цифрового підпису еквівалентним власноручному та вимоги до яких дещо інші, а також не відображені у стандартах «X.5091» [77; 143]. При цьому треба зазначити, що законодавство ЄС на відміну від українського під електронним підписом розуміє не тільки ідентифікацію автора, а й достовірність/цілісність самих підписаних даних.

Термін ЕЦП Закону України є більш слабким за визначення «удосконалений електронний підпис» у Директиві ЄС, де той визнається еквівалентним власноручному, оскільки для ЕЦП відсутня ключова вимога щодо забезпечення можливості автору підпису тримати під своїм повним

контролем засіб створення підпису. Крім того, обов'язкові вимоги до «безпечного механізму створення підпису» Директиви ЄС відрізняються від вимоги до «надійного засобу електронного цифрового підпису» за Законом України, як об'єкта, який має сертифікат відповідності виключно українського походження [102].

Електронний цифровий підпис має свою законодавчу базу, де прописуються захисні механізми, які з більшою можливістю виключають імовірність злочинних посягань, і тому цифрові підписи використовують цифровий ідентифікатор на основі сертифікату, виданого акредитованим органом сертифікації або постачальником довірчого сервісу, тому під час цифрового підписування документа підписувач однозначно прив'язує підпис до себе.

Цифровий підпис створений, захищений та забезпечений найвищими рівнями безпеки. При цьому підписувач у вигляді суб'єкта має повне право вимагати скасування, блокування або поновлення свого сертифіката ключа; оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку. Скасування, блокування та поновлення посильного сертифікату ключа має здійснювати Акредитований центр сертифікації ключів у разі: закінчення строку чинності сертифіката ключа, після подання заяви власника ключа або його уповноваженого представника, припинення діяльності юридичної особи – власника ключа, смерті фізичної особи – власника ключа або оголошення його померлим за рішенням суду, визнання власника ключа недієздатним за рішенням суду, надання власником ключа недостовірних даних, компрометації особистого ключа.

Скасування і блокування посиленого сертифіката ключа набирає чинності лише з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати та часу здійснення цієї операції. Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника.

Підписувач зобов'язаний: зберігати особистий ключ у таємниці, надавати центру сертифікації ключі в дані згідно з вимогами законодавства [123].

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму. Електронний документ не може бути застосовано як оригінал документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів; в інших випадках, передбачених законом [138].

Чинний закон України «Про електронний цифровий підпис» дає визначення електронного цифрового підпису – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [123].

Наукова природа електронного цифрового підпису базується на категоріях криптографії та криптоперетворення.

Криптогра́фія (від грецького *κρυπτός* – «прихований» і *gráphein* – «писати») – наука про математичні методи забезпечення конфіденційності, цілісності й автентичності інформації. Розвинулась вона з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей [26].

Криптографія – це практика і вивчення методів безпечного спілкування в присутності третіх осіб (так званих противників). У більш загальному понятті мова йде про побудову та аналіз протоколів, які дозволяють подолати вплив противників і які пов'язані з різними аспектами у сфері інформаційної безпеки – такими як конфіденційність

даних, цілісність даних, автентифікація і безвідмовність. Сучасна криптографія поєднує принципи математики, інформатики та електротехніки. Застосування криптографії включає банківські карти, комп'ютерні паролі й електронну комерцію [43].

В криптографичній термінології вихідне повідомлення називають відкритим текстом (plaintext або cleartext). Зміна вихідного тексту так, щоб скрити від інших його склад, називають шифруванням (encryption). Зашифроване повідомлення називають шифротекстом (ciphertext). Процес, у якому з шифротексту видаляється відкритий текст, називають дешифруванням (decryption). Переважно в процесі шифрування й дешифрування використовується деякий ключ (key), і алгоритм забезпечує, що дешифрування можна зробити, лише знаючи ключ [85].

Завдання криптографії, тобто таємна передача, виникає тільки для інформації, яка потребує захисту. тобто ця інформація містить таємницю або захищається, є приватною, конфіденційною, секретною. Для найбільш типових ситуацій такого типу, які часто зустрічаються, уведено навіть спеціальні поняття: державна таємниця; військова таємниця; комерційна таємниця, юридична таємниця; лікарська таємниця тощо [9; 84].

На думку низки науковців, сучасні криптографічні системи мають задовольняти таким основним вимогам: вихідний текст із шифрованого тексту може бути відтворений виключно із використанням ключа дешифрування; послідовний перебір усіх імовірних ключів дешифрування з метою відновлення вихідного тексту потребує великого часу обчислень або призводить до неприйнятно високих затрат для здійснення таких обчислень; інформація про алгоритм, що використовувався для шифрування, не має позначитись на стійкості системи шифрування до зламування; несуттєві зміни шифрувального ключа мають призводити до значних змін шифрограми того самого тексту; елементи структури алгоритму шифрування не мають змінюватись; додаткові біти, які в процесі шифрування додаються в повідомлення, мають бути надійно

закриті в зашифрованому тексті; не має існувати простих залежностей між ключами, які послідовно використовуються в шифруванні; довільний ключ із множини використовуваних ключів має забезпечувати надійність системи шифрування; алгоритми шифрування й дешифрування мають допускати як апаратну, так і програмну реалізацію, при цьому зміни довжин ключів не мають спричиняти якісне погіршення алгоритмів [54; 62].

Криптоперетворення – це сукупність операцій шифрування та дешифрування даних [86]. А. Дегтярьов класифікує криптографічну генезу на такі етапи: перший – етап донаукової криптології (до 1949 р.); другий – етап наукової криптології із секретними ключами (з 1949 р. по сімдесяті роки); третій – етап наукової криптології з використанням ЕОМ (із сімдесятих по сьогодні). Аналізуючи наукову природу електронного цифрового підпису, слід описати алгоритми шифру, які використовуються в цифровому підписі. Алгоритми шифрування поділяють на класичні та сучасні, нас безпосередньо цікавить сучасні алгоритми шифрування. Сучасні у свою чергу поділяються на симетричні (заміна) та асиметричні (перестановка) [43].

Симетричне шифрування потокового шифру кожного символу відкритого тексту зашифрується незалежно від інших. Головною проблемою створення потокового шифру є створення послідовності, що шифрує. У використанні потокових шифрів вони можуть вироблятися як на передавальному, так і на прийомному кінцях лінії зв’язку. За симетричного шифрування блокових шифрів відкритий текст розбивається на блоки фіксованої довжини й зазнає шифрування. Причому кожний блок зашифровується своїм шифром, але алгоритм перемішування залишається однаковим для всіх блоків. На цьому принципі побудовано багато шифрів, включаючи американський стандарт DES [43].

Симетричні алгоритми шифрування – спосіб шифрування, в якому для шифрування і дешифрування застосовується один і той же

криптографічний ключ. До винаходу схеми асиметричного шифрування єдиним чинним способом було симетричне шифрування. Ключ алгоритму має зберігатися в секреті обома сторонами. Алгоритми шифрування і дешифрування даних широко застосовуються в комп'ютерній техніці в системах приховування конфіденційної і комерційної інформації від некоректного використання сторонніми особами. Головним принципом у них є умова, що той, хто приймає, заздалегідь знає алгоритм шифрування, а також ключ до повідомлення, без яких інформація є всього лише набором символів, що не мають сенсу.

Симетричні криптоалгоритми виконують перетворення невеликого (1 біт або 32-128 біт) блоку даних залежно від ключа таким чином, що прочитати оригінал повідомлення можна, тільки знаючи цей секретний ключ. Симетричні криптоалгоритми діляться на скремблери та блокові шифри. Скремблерами називаються програмні або апаратні реалізації алгоритму, що дозволяють шифрувати побітно безперервні потоки інформації. Сам скремблер становить набір бітів, що змінюються на кожному кроці за певним алгоритмом. Після виконання кожного чергового кроку на його виході з'являється біт, що шифрує, – або 0, або 1, що накладається на поточний біт інформаційного потоку операцією XOR («побітне виключаюче АБО»).

Основним недоліком алгоритмів скремблювання є їхня нестійкість до фальсифікації. Блокові шифри в ході своєї роботи роблять перетворення блоку вхідної інформації фіксованої довжини й одержують результуючий блок того ж обсягу, але не доступний для прочитання сторонніми особами, що не володіють ключем. Таким чином, схему роботи блокового шифру можна описати функціями Z=EnCrypt(X,Key) і X=DeCrypt(Z,Key). Ключ Key є параметром блокового алгоритму і становить собою деякий блок двійкової інформації фіксованого розміру. Вихідний (X) і зашифрований (Z) блоки даних також мають фіксовану розрядність, рівну між собою, але необов'язково рівну довжині ключа [85].

Асиметричними криптоалгоритмами вважається криптосистема з відкритим ключем. Для шифрування повідомлення використовується відкритий ключ, а при дешифруванні – закритий. Тобто, знаючи ключ шифрування й зашифрований текст, неможливо відновити вихідне повідомлення; При порушенні конфіденційності робочої станції зловмисник довідається тільки про «закритий» ключ: це дозволяє йому читати всі повідомлення, що приходять абонентові k, але не дозволяє видавати себе за нього при відправленні листів; в асиметричних системах кількість існуючих ключів пов'язане з кількістю абонентів лінійно [43].

Асиметричні алгоритми шифрування – це такі алгоритми, які використовують різні ключі для шифрування та розшифрування даних. Головне досягнення асиметричного шифрування полягає в тому, що воно дозволяє людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналі цілком відпала. Процедура шифрування обрана так, що вона незворотна навіть по відомому ключу шифрування. Тобто, знаючи ключ шифрування й зашифрований текст, неможливо відновити вихідне повідомлення – прочитати його можна тільки за допомогою другого ключа – ключа дешифрування. А коли так, то ключ шифрування для відправлення листів якій-небудь особі можна взагалі не приховувати – знаючи його, однаково неможливо прочитати зашифроване повідомлення. Тому ключ шифрування називають в асиметричних системах «відкритим ключем», а от ключ дешифрування одержувачеві повідомлень необхідно тримати в секреті – він називається «закритим ключем». Алгоритми шифрування й дешифрування створюються так, щоб, знаючи відкритий ключ, неможливо було обчислити закритий ключ [85].

Окрім того під час надання кваліфікованих електронних довірчих послуг використовуються кваліфіковані сертифікати електронного підпису, кваліфіковані сертифікати електронної печатки та кваліфіковані

сертифікати автентифікації веб-сайту. Кваліфіковані сертифікати відкритих ключів обов'язково мають містити:

1) позначку, що сертифікат відкритого ключа виданий як 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, 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 серія 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,

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);

14) ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації веб-сайту).

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 мають впливати на інтероперабельність і визнання кваліфікованих електронних підписів. Правочин, учинений 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 [124].

В Україні для звичайних потреб (не для спеціальних державних служб) використовується зворотній асиметричний криптоалгоритм, коли підписувач володіє особистим закритим ключем і ставить свій підпис на програмний засіб, а перевіряється адресатом за допомогою відкритого ключа. Підписувач, який володіє особистим ключем та ставить свій підпис

на програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення або перевірки електронного цифрового підпису, повністю захищає себе як суб'єкт, який перебуває у правовому колі, від недобросовісних втручань.

Отже, наукова природа електронного цифрового підпису базується на категоріях криптографії та криптоперетворення, які дозволяють подолати вплив противників і які пов'язані з різними аспектами у сфері інформаційної безпеки, таких як конфіденційність даних, цілісність даних, аутентифікація і безвідмовність. Електронний цифровий підпис вимагає правового (зокрема адміністративно-правового) та технічного (організаційно-правого) захисту особистих ключів від несанкціонованого використання.

Однак, як показують матеріали Єдиного державного реєстру судових рішень за останні 2 роки, електронний цифровий підпис був об'єктом адміністративно-правової суперечки понад 30 000 разів [53]. Наприклад, рішенням Господарського суду м. Києва від 11.03.2014 у справі №910/361/14 задоволено позов Публічного акціонерного товариства Комерційний банк «ПриватБанк» і присуджено до стягнення з Фізичної особи-підприємця (далі – ФОП) на користь банку 50 000,00 грн. заборгованості за кредитом, 32 218,38 грн. – процентів за користування кредитом, 7 200,00 грн. – комісії, 12 421,61 грн. – пені, 2 036,80 грн. – судового збору.

Постановою Київського апеляційного господарського суду від 12.06.2017 у цій справі задоволено апеляційну скаргу ФОП і скасовано вищезазначене рішення Господарського суду м. Києва. Натомість прийнято нове рішення, яким відмовлено Банку в задоволенні позовних вимог та стягнуто з нього на користь ФОП 2 240,48 грн. судового збору за подання апеляційної скарги. Водночас банк не погодився з таким рішенням апеляції і звернувся з касаційною скаргою до тоді ще Вищого

господарського суду України. Останній в цій справі прийняв позицію апеляції [156].

Загальна судова практика з питань визнання електронних документів як доказів у цивільних і господарських справах, ще не є поширеною, оскільки може існувати рівно настільки, наскільки розвиваються самі відносини щодо використання електронних документів у цивільних та господарських відносинах [49]. При цьому найбільш часто предметом позову було доведення чи спростування виключності достатності електронного цифрового підпису директора та печатки юридичної особи як юридичного факту, який не підлягає сумніву. При цьому треба зазначити, що, користуючись казуїстичними невідповідностями в чинному законодавстві, адміністративний суд, як правило, не підтверджує достовірності юридичного факту.

Від такого стану речей потерпають банківські установи та бюджет України, а приватні фізичні та юридичні особи змушені під час взаємодії з органами публічної влади часто дублювати електронний цифровий підпис із паперовим його варіантом. Тим самим вітчизняне суспільство поступово і небезболісно пристосувалось до новітніх технологій. У процесі розроблення, виробництва та експлуатації засобів КЗІ беруть участь і взаємодіють між собою замовники; розробники; виробники; організації, що експлуатують засоби КЗІ; організації, що проводять сертифікаційні випробування (експертні роботи); постачальники ключових документів.

В інструкції із забезпечення безпеки експлуатації засобів криптографічного захисту інформації вказуються: права та обов’язки осіб, відповідальних за забезпечення безпеки експлуатації засобу КЗІ; права та обов’язки користувачів засобів КЗІ; порядок забезпечення безпеки засобу КЗІ під час його встановлення, експлуатації, виведення з експлуатації, ремонту, знищення, а також у разі порушення функціонування інформаційно-телекомунікаційної системи; порядок обліку засобів КЗІ; питання проведення тестування засобів КЗІ та їх резервування в системі;

дії персоналу в умовах надзвичайних ситуацій, стихійного лиха та підозри компрометації ключів; порядок проведення контролю за станом забезпечення безпеки засобів КЗІ; порядок допуску в приміщення, у яких установлені засоби КЗІ; порядок знищення засобів КЗІ.

В інструкції щодо порядку генерації ключових даних і поводження (облік, зберігання, знищення) із ключовими документами вказуються: опис ключової системи та ключових документів; термін дії ключових даних, ключових документів; порядок генерації ключових даних, їх запису на носії ключової інформації; порядок обліку, зберігання носіїв ключової інформації та їх знищення; особливості повторного використання носіїв ключової інформації; особливості використання ключових даних за призначенням та їх знищення [109].

З 2014 року в країнах-учасницях ЄС використовується розширений електронний підпис «eIDAS», який відповідає кільком вимогам, зокрема: підписувач має бути однозначно ідентифікований та пов'язаний з підписом; підписувач повинен мати єдиний контроль над своїм ключем, який використовувався для створення електронного підпису; підписувач має бути здатний визначити, чи було змінено супровідні дані після підписання повідомлення; у тому випадку, якщо супровідні дані були змінені, підпис має бути визначним недійсним [177]. Так, 2014 року прийнято Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС., який набрав чинності 01 липня 2016 року.

На гармонізацію з положеннями Регламенту № 910 eIDAS було розроблено Проект Закону України «Про електронні довірчі послуги» №4685. Практично весь текст Регламенту № 910 eIDAS був перенесений до нього. Метою законопроекту є реформування законодавства в сфері електронного цифрового підпису з урахуванням досвіду ЄС, розвиток

єдиного простору довіри на основі системи електронних довірчих послуг, визнання в Україні електронних довірчих послуг, що надаються іноземними постачальниками. Таким чином, українці зможуть користуватися електронними послугами не тільки у своїй країні, але і з-за кордону. Наприклад, замовити дублікат посвідчення водія з будь-якої європейської країни ще до повернення в Україну. Проект Закону визначає поняття «автентифікації» (п. 1 ст. 1), «електронної довірчої послуги» (п.8 ст.1), «електронної ідентифікації» (п. 9 ст. 1), «електронної печатки» (п.10 ст.1), електронної позначки часу (п. 11 ст. 1), «електронного підпису» (п.12 ст.1), «ідентифікації особи» (п. 22 ст. 1), «кваліфікованого електронного підпису» та відповідної «печатки» (п. 24, 25 ст. 1), «постачальника електронних довірчих послуг» (п. 35 ст. 1), «удосконаленого електронного підпису» (п. 49 ст. 1) та інші [24].

Згідно з проектом Закону, електронна довірча послуга – це послуга, що надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють постачальнику електронних довірчих послуг. Передбачається три рівня електронної ідентифікації:

1) високий (використання кваліфікованих електронних підписів і печаток);

2) середній (використання вдосконалених електронних підписів і печаток);

3) низький рівні довіри до використовуваних засобів електронної ідентифікації [24].

Цей проект Закону було підписано Президентом України та вступить у дію в листопаді 2018 р., він полегшує транскордонне використання онлайн-послуг, створює умови для безпечної електронної ідентифікації та автентифікації, а також взаємного визнання ключових компонентів транскордонних цифрових послуг, таких як електронна ідентифікація, електронні підписи, електронні документи та послуги, визначає основні

принципи державного регулювання у сферах електронних довірчих послуг та електронної ідентифікації.

Документом також запроваджується адміністративна послуга щодо включення юридичних та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку, а також установлюється порядок ведення такого списку. Крім того визначається процедура незалежної оцінки відповідності для ЕДП і можливість використання зазначеними особами у своїй діяльності як національних, так і міжнародних стандартів [118].

З 17.01.2006 Науково-виробнича фірма «Українські національні інформаційні системи» (УНІС) може виконувати функції центру сертифікації ключів електронного цифрового підпису. Це перша організація, що отримала акредитацію Центру сертифікації ключів електронного цифрового підпису. УНІС працює з сертифікатами міжнародного стандарту X.509 v3. Для створення електронного цифрового підпису використовуються стандарти ДСТУ 4145-2002, ГОСТ 34.310-95 та ГОСТ 34.311-95 [59].

Усе вищевикладене дає можливість сформулювати такі висновки щодо адміністративно-правової природи електронного цифрового підпису в Україні:

1) наукова природа електронного цифрового підпису базується на категоріях криптографії та криптоперетворення, які дозволяють подолати вплив противників і пов’язані з різними аспектами у сфері інформаційної безпеки, таких як конфіденційність даних, цілісність даних, автентифікації і безвідмовності;

2) електронний цифровий підпис вимагає правового (зокрема адміністративно-правового) та технічного (організаційно-правого) захисту особистих ключів від несанкціонованого використання;

3) законодавством України визначено, що електронний цифровий підпис – це вид електронного підпису, отриманого за результатом

криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його юридичну цілісність та ідентифікувати підписувача;

4) в Україні для звичайних потреб (не для спеціальних державних служб) використовується зворотній асиметричний криптоалгоритм, коли підписувач володіє особистим закритим ключем і ставить свій підпис на програмний засіб, а перевіряється адресатом за допомогою відкритого ключа;

5) норми адміністративного права, які визначають юридичну природу електронного цифрового підпису, зосереджені в таких основних європейських і вітчизняних джерелах: 1) міжнародно-правові джерела: Конвенція ООН про використання електронних повідомлень у міжнародних договорах (2005); Регламент ЄС від 23.07.2014 «Про електронну ідентифікацію та довірчі служби для електронних операцій на внутрішньому ринку»; 2) вітчизняні джерела: а) закони: «Про електронний цифровий підпис (спеціальний)»; «Про електронні документи та електронний документообіг»; «Про електронний цифровий підпис»; «Про обов'язковий примірник документів»; «Про Національну програму інформатизації»; «Про телекомунікації»; «Про Національну систему конфіденційного зв'язку»; «Про захист інформації в інформаційно-телекомунікаційних системах»; б) підзаконні нормативно-правові акти: Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації»;

6) основне юридичне призначення електронного цифрового підпису – це забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів;

7) Наріжним каменем застосування електронного цифрового підпису в електронному документообігу є те, що визначається не лише правовий

статус такого підпису, але й електронних документів загалом, обов'язковим реквізитом яких є ЕЦП, а підпис дорівнюється до власноручного підпису (печатки) тільки у випадку виконання трьох умов.

8) допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму;

9) загалом в Україні використовується розширений електронний підпис «eIDAS» ЄС, згідно з яким підписував має бути однозначно ідентифікований та пов'язаний з підписом; мати єдиний контроль над своїм ключем, має бути здатний визначити, чи було змінено супровідні дані після підписання повідомлення; у тому разі, якщо супровідні дані були змінені, підпис визнається недійсним.

Отже, адміністративно-правова природа електронного цифрового підпису в Україні полягає в тому, що він, базуючись на науковій природі математичних категорій криптографії та криптоперетворення, коли завдяки об'єктивній юридичній регламентації через норми адміністративного права забезпечує адміністративно-правовий та організаційно-правовий захист особистих ключів підписувачів від несанкціонованого використання (через використання закритого ключа) підвищує ефективність управлінської діяльності органів публічної влади та зручності користуванням приватних осіб, прирівнюється до власноручного підпису (печатки) і не може заперечуватися виключно на підставі того, що має електронну форму.

1.3 Фактичний зміст адміністративно-правових відносин у сфері електронного цифрового підпису

Адміністративно-правові відносини наповнюють усю правову матерію суспільства. Будь-які суспільні відносини стають адміністративно-правовими, якщо врегульовуються нормами адміністративного права. Однак урегулювання має бути об'єктивно обґрунтованим, відображати

соціальний прогрес, і в жодному разі не погіршувати чинні права, свободи і законні інтереси приватних осіб.

Тлумачний словник української мови трактує термін «зміст» у таких значеннях: 1) суть, внутрішня особливість чого-небудь; 2) певні властивості, характерні риси, які відрізняють дане явище, предмет від подібних явищ, предметів і т. ін.; 3) розумна основа, мета, призначення чого-небудь [152]. Чимало вчених визначають, що юридичний зміст відбиває передбачені нормами права реальні можливості стосовно здійснення суб'єктивних прав та юридичних обов'язків, тоді як фактичний – фактичну поведінку, у межах якої реалізуються суб'єктивні права та юридичні обов'язки суб'єктів правовідносин [66].

Професор В. Авер'янов уважає, що адміністративно-правові відносини – це врегульовані нормами адміністративного права суспільні відносини, в яких їх сторони (суб'єкти) взаємозв'язані й взаємодіють через здійснення суб'єктивних прав і обов'язків, установлених і гарантованих відповідними адміністративно-правовими нормами [1].

На думку професора І. Голосніченка, адміністративно-правові відносини – це система прав та обов'язків органів виконавчої влади, посадових осіб і службовців, громадян та інших суб'єктів, а також взаємозв'язок між ними в результаті здійснення державної виконавчої влади та відповідальності у сфері державного управління [41].

Професор В. Галунько адміністративно-правові відносини характеризує такими особливостями: вони нерозривно пов'язані з адміністративно-правовими нормами, виникають і здійснюються на їх основі; основною їх метою є забезпечення прав та свобод людини і громадянина, нормальне функціонування громадянського суспільства та держави; вони врегульовують широке коло суспільних відносин між публічною адміністрацією та об'єктами публічного управління; провідною рисою адміністративно-правових відносин є їх публічна природа, вони виникають з ініціативи будь-якої сторони, при цьому згода іншої сторони,

як правило, не є обов'язковою; адміністративно-правові відносини є переважно виконавчо-розпорядчими: у вузькому розумінні суб'єкти публічного управління наділені владною компетенцією, а об'єкти зобов'язані виконувати їх законні вимоги; поряд із цим за широкого підходу сторони адміністративно-правових відносин завжди мають суб'єктивні права та юридичні обов'язки, які взаємопов'язані між собою: кожному суб'єктивному праву однієї сторони відповідає юридичний обов'язок іншої, і навпаки; вони мають свідомо-вольовий характер, адже держава через видання відповідних адміністративно-правових норм виражає свою волю народу України, учасники цих відносин здійснюють своє волевиявлення, усвідомлюють значення своїх дій та можуть нести за них відповідальність; адміністративно-правові відносини охороняються державою, яка сприяє здійсненню суб'єктивних публічних прав та юридичних обов'язків, а в разі правопорушення притягує винну особу до адміністративної чи іншої юридичної відповідальності; не належать до адміністративно-правових відносини між публічної адміністрацією та об'єктами публічного управління, якщо вони не засновані на праві. Загалом структура адміністративно-правових відносин характеризується взаємопов'язаністю всіх її складових компонентів, якими є суб'єкти, об'єкти, зміст правовідносин та юридичні факти [39].

На думку А. Іванищука, за своїм змістом адміністративно-правове забезпечення діяльності судової гілки влади є складним і ємним комплексним інститутом адміністративного права, який наповнений численними вертикальними й горизонтальними зв'язками, поєднує однорідні суспільні відносини: систему адміністративно-правового забезпечення (правотворчість, правозастосування, правоохоронну діяльність), має свою структуру (засоби й типи правового регулювання), механізм адміністративно-правового забезпечення (джерела, принципи, тлумачення норм адміністративного права, адміністративно-правові відносини, статус суб'єктів адміністративного права, індивідуальні

адміністративні акти, методи, режими, процедури, ефективність адміністративно-правового забезпечення) та напрямки адміністративно-правового забезпечення діяльності судової гілки влади [57; 61].

З метою оптимізації системи центральних органів виконавчої влади видано Указ Президента України від 9 грудня 2010 року № 1085/2010 «Про оптимізацію системи центральних органів виконавчої влади» [139], де саме й було передбачено електронний документообіг. Проблема переходу від паперового до «електронного» документообігу постає сьогодні перед органами публічної влади. Упровадження «електронного» документообігу дозволяє поліпшити контроль над рухом і виконанням документів, значно спростити і прискорити доступ до інформації і, як наслідок, підвищити ефективність процесів управління [117]. Це важливо для держави, а тому Урядом України передбачено роботи із забезпечення «електронного» документообігу в органах державної влади всіх рівнів і ухвалено Закон України «Про Національну програму інформатизації» [139].

Розглядаючи це питання, потрібно звернутись до короткого історичного ракурсу виникнення електронних систем у світі.

Поява перших «електронних» обчислювальних машин (ЕОМ) у середині минулого століття безпосередньо пов’язана з потребою здійснення складних математичних обчислень. Розвиток технічних засобів раптово швидко дав змогу розширити сферу функціонального застосування ЕОМ за межі обчислювальних задач і використовувати їх для автоматизації технологічних процесів у виробництві, а також напрямів людської діяльності, пов’язаних з опрацюванням інформації. У середині 80-х років розвиток технічних засобів автоматизації одержав потужний імпульс, викликаний успіхами в мікроелектронних технологіях: унаслідок створення персонального комп’ютера потужні засоби опрацювання інформації стали доступні масовому користувачеві [50].

Термін «електронний документ» з’явився приблизно на початку 1990-х рр. у США, але у вітчизняному документознавстві він почав

активно використовуватися лише 2003 року, коли було ухвалено Закон України «Про електронні документи та електронний документообіг» і «Про електронний цифровий підпис», які на законодавчому рівні врегулювали можливість використання електронного документа з його обов'язковим реквізитом – електронним цифровим підписом – як офіційного документа, що дало початок становленню офіційного електронного діловодства в організаціях (установах і на підприємствах) України [88].

У процесі глобалізації ринку, зі зростанням темпів розвитку компаній колишні методи ведення традиційного документообігу стають непридатними. Потреба запровадження системи єдиних міжнародних стандартних номерів (ISBN) для документів була усвідомлена ще в середині 1960-х років минулого століття. Сьогодні індекси ISBN (а також ISSN, ISMN, ISAN тощо) уже мають фундаментальне значення для видавничої справи та інформаційної галузі взагалі [154].

Проте епоха онлайнових комунікацій висунула нові виклики у сфері стандартизації видавничої справи, зокрема виникла потреба розроблення системи реєстрації універсальних стандартних ідентифікаторів для онлайнових інформаційних ресурсів. Стандартизація «електронного» документообігу за допомогою ISBN подібних ідентифікаторів пов'язана з низкою проблем, адже електронні ресурси суттєво відрізняються від традиційних як за формальними ознаками, так і за механізмом їх видання [154].

У 90-ті рр. минулого століття документообіг та обмін інформацією здійснювалися за допомогою факсів, з використанням телефонів або електронної пошти. Алгоритми автоматичної обробки повідомлень стали основою технології взаємного обміну «електронними» документами (Electronic Document Interchange – EDI) між автоматизованими системами управління виробничих та торговельних компаній. З настанням «Інтернет-епохи» навіть невеликі компанії-провайдери отримали реальні можливості

конкуренції з власниками VAN, використовуючи online-зв'язок. Відчувши конкуренцію, власники VAN у свою чергу налагодили використання шлюзів Інтернет і почали нарешті обслуговувати дрібні фірми. Проте можливість відмовитися від дорогих VAN є привабливою, і більшість компаній усе ж планують перехід на мережу Інтернет і розширювану мову розмітки (extensible markup language) – XML. Основне значення дешевих інтернет-систем для EDI полягає в тому, що вони об'єднують усіх учасників «електронного» документообігу, дозволяючи використовувати повні дані для планування [169].

У середині 90-х успішно впроваджувалися перші програмні комплекси, які були досить гнучкими для того, щоб задовольнити потреби практично будь-якого замовника. Технологія створення системи передбачала два етапи: перший – розробку уніфікованого ядра, а другий – підгонку процесів під потреби конкретної організації. Такі програми для «електронного» документообігу коштували набагато дешевше від своїх попередників, а також вирішували проблеми масштабованості [148].

У вересні 1996 року Європейська економічна комісія ООН розробила рекомендацію про використання стандарту UN/EDIFACT, що мала забезпечити узгоджені дії урядів з упровадження UN/EDIFACT як єдиного міжнародного стандарту для «електронного» обміну даними між державними органами управління і компаніями в усіх економічних секторах у світових масштабах, зокрема України. Над упровадженням стандартів EDIFACT працювали державні та комерційні структури, проте широкому застосуванню EDI в Україні перешкоджала відсутність сервіс-провайдерів EDI. Вартість оплати послуг зв'язку спеціальних мереж VAN, які забезпечували передання даних по стандартах EDI, є високою [107].

У жовтні 1997 року, було розроблено універсальний цифровий ідентифікатор об'єктів Digital Object Identifier (DOI). Система DOI створена для ідентифікації будь-якого змісту в цифровому середовищі (причому сам зміст необов'язково має бути цифровим: DOI

розшифровується як «цифровий ідентифікатор об’єкта», а не як «ідентифікатор цифрового об’єкта») [183].

Оригіналом електронного документа вважається електронний примірник документа з обов’язковими реквізитами, зокрема з електронним підписом автора або підписом, дорівненим до власноручного підпису відповідно до Закону України «Про електронний цифровий підпис». Термін «електронний підпис» було вперше вжито Європейською Комісією у переробленому проекті Директиви ЄС 1999/93/ EG. Електронний підпис є обов’язковим реквізитом електронного документа, який використовується для ідентифікації автора та підписувача електронного документа іншими суб’єктами електронного документообігу. Накладанням електронного підпису завершується утворення електронного документа [27].

Першим спеціальним Законом, що встановив «правовий статус електронного цифрового підпису та врегулював відносини, що виникають при використанні ЕЦП», став Закон України «Про електронний цифровий підпис» від 22 травня 2003 року. Крім того деякі положення про електронний підпис були включені в Закон України «Про платіжні системи та переказ грошей в Україні» від 5 квітня 2001 і Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року. Під електронним цифровим підписом слід розуміти дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації особи, яка підписала ці дані.

Електронний підпис є обов’язковим реквізитом електронного документа, і його накладенням завершується створення такого документа. Тому електронно-цифровий підпис може використовуватись не лише для підписання адміністративно-правових документів, а й цивільно-правових.

У цілому можна виділити такі технології електронної ідентифікації: біометрія, паролі і ключі, симетрична й асиметрична криптографія.

Найбільш подібна власноручному підпису біометрія, оскільки вона дозволяє ідентифікувати особу, яка підписала електронний документ, завдяки встановленню тотожності між раніше відібраними зразками прояву фізіологічних властивостей особи з тими, якими вона характеризується в момент підписання документа.

Проте про підписання документа за допомогою біометрії можна говорити з певною умовністю. З технічної точки зору біометрія не дозволяє підписати електронний документ шляхом накладення на нього певного знака, а лише забезпечує доступ до закритої системи документообігу з подальшою фіксацією інформації про особу, яка такий доступ отримала, яка створила і яка відправила електронний документ.

Сьогодні використовуються такі технології біометричної ідентифікації, як контроль голосу, динаміка набору тексту на клавіатурі, геометрія долоні, сканування сітківки ока тощо. На відміну від традиційного власноручного підпису біометрія не може бути використана для підписання документів без попередньої домовленості сторін, що використовують такі документи.

До першого використання біометрії для ідентифікації електронного документа сторони мають визначити систему закритого документообігу, установити вид і порядок відбору зразків прояву фізіологічних властивостей, відібрати зразки, увести їх у систему, установити порядок визначення тотожності між відібраними зразками і характеризують особу в момент входу в систему. Технологія електронної ідентифікації особи за допомогою ключів і паролів заснована на встановленні тотожності між використаним особою ключем і введеної в систему інформацією (паролем) до раніше узгоджених сторонами ключем і паролем. Як і в біометрії, ключ і пароль не дозволяють підписати документ у традиційному розумінні, а лише надають можливість ідентифікувати особу під час входу в закриту систему документообігу, де така особа має право створювати, відправляти, отримувати і зберігати електронні документи [123].

Документи, які були підписані електронним цифровим підписом, мають таку ж юридичну силу, як і звичайний письмовий підпис. Якщо паперовий документ може бути підписаний звичайною шариковою ручко, то в цифровому світі, зокрема Інтернеті, все набагато складніше. Для того щоб забезпечити можливість підписання електронних документів, було розроблено спеціальні технології, названі за аналогією електронним підписом. Специфічність електронного – цифрового – підпису, його відмінність від власноручного обумовили потребу розробки і прийняття спеціального законодавства, що регулює порядок використання новітньої програмних засобів ідентифікації електронних документів [173].

Статус кваліфікованого надавача електронних довірчих послуг юридичні особи, фізичні особи підприємці набувають із дня внесення відомостей про них до Довірчого списку на підставі рішення центрального засвідчувального органу або засвідчувального центру (у разі надання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів) [124]. Також при реєстрації «електронного» документа, яка проводиться після його створення, потрібно перевіряти обов’язкові реквізити, зокрема реєстраційний індекс і дата реєстрації «електронного» документа не є складовими цього документа – на них як на дані не накладався «електронний» цифровий підпис, яким підписано «електронний» документ.

У разі встановлення порушень 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; зміну 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 контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг; набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом [124].

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 контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

– набрання законної сили рішенням суду про скасування самопідписаного сертифіката електронної печатки центрального засвідчувального органу. 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. Скасований кваліфікований сертифікат відкритого ключа поновленню не підлягає [124].

Поряд із цим було розроблено Закон України «Про Національну програму інформатизації». Інформатизація органів державної влади – це організаційний соціально-економічний і науково-технічний процес створення оптимальних умов для функціонування і реалізації прав і повноважень органів державної влади і забезпечення інформаційних потреб суб'єктів, які з ними взаємодіють, на основі формування і використання державних інформаційних ресурсів та відповідно до статті 5; головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави, основними завданнями є:

– формування правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних передумов розвитку інформатизації;

– застосування та розвиток сучасних інформаційних технологій у відповідних сферах суспільного життя України;

– формування системи національних інформаційних ресурсів;

– створення загальнодержавної мережі інформаційного забезпечення науки, освіти, культури, охорони здоров'я тощо;

– створення загальнодержавних систем інформаційно-аналітичної підтримки діяльності державних органів та органів місцевого самоврядування;

– підвищення ефективності вітчизняного виробництва на основі широкого використання інформаційних технологій;

– формування та підтримка ринку інформаційних продуктів і послуг;

– інтеграція України у світовий інформаційний простір [137].

На сьогодні активно електронні системи застосовуються в правоохоронних органах. Наприклад, у Міністерстві внутрішніх справ України ведуться роботи з розроблення та впровадження системи «електронного» документообігу, автоматизованої системи, до складу якої входить комплексна система захисту інформації з підтвердженою відповідністю. Так, активно з 1 січня 2016 року громадянам України службами ДМС МВС видаються біметричні документи. Біометричними називають документи, що посвідчують особу та містять електронний носій інформації, на якому записано інформацію про біометричні дані власника документа з метою його ідентифікації. Передбачається, що такі документи найбільш захищені від підробок та виключають можливість користування ними будь-якою особою, окрім власника.

Головна ідея впровадження більш захищених документів, які забезпечують ідентифікацію особи, – це суттєве підвищення захищеності суспільства від проявів злочинності та міжнародного тероризму. Понад 90 країн із 193 держав-членів ООН уже видають такі документи, ще понад 20 готові до впровадження таких документів у найближчі роки. Для захисту інформації на електронному носії використовуються новітні технології, що робить підробку електронних документів практично неможливою. У разі крадіжки чи втрати такого паспорта зловмисники не зможуть скористатися ним. Для зчитування інформації, наприклад на кордоні, будуть використовуватись автоматизовані контрольно-пропускні системи для власників біометричних паспортів. Це, по-перше, виключить суб’єктивність і можливість зловживань під час проходження контролю, а по-друге – зменшить час, необхідний на таке проходження. Подорожі до країн, які використовують автоматичні пропускні системи, стали зручними, без виснажливих черг. Аналогічно будуть створені умови, необхідні для спрощення та прискорення внутрішньодержавних процедур надання адміністративних послуг, які передбачають ідентифікацію особи [106].

Особливістю є те, що бланк паспорта громадянина України для виїзду за кордон з безконтактним електронним носієм. У праву частину обкладинки імплантовано безконтактний електронний носій, який відповідає вимогам стандарту ISO/IEC 14443A щодо запису і зчитування даних та вимогам ІКАО, що встановлюються до електронних документів. Сторінка даних виготовляється з багатошарового полімерного матеріалу (полікарбонат) і розміщується між лівою частиною форзаца та першою паперовою сторінкою. Бланк паспорта скріплюється замкненим швом, нитками із захисними властивостями, що набувають червоного свічення під дією джерела ультрафіолетового опромінення. Законом України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» передбачено перелік інформації, що вноситься до біометричних документів [17; 26].

З метою покращання цієї роботи Постановою Кабінету Міністрів України від 30 листопада 2016 р. № 869 розроблено «Порядок внесення засобів електронного цифрового підпису до безконтактного електронного носія, що міститься в паспорті громадянина України, та надання послуг електронного цифрового підпису з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм». Цей Порядок визначає з урахуванням вимог законів України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», «Про електронний цифровий підпис», законодавства у сфері електронного цифрового підпису та криптографічного захисту інформації, міжнародних стандартів та рекомендацій Міжнародної організації цивільної авіації (ІКАО) механізм здійснення операцій із внесення надійних засобів електронного цифрового підпису, зокрема засобів шифрування, до безконтактного електронного носія, який імплантовано в паспорт громадянина України, їх використання та надання послуг електронного

цифрового підпису з використанням паспорта громадянина України у формі картки [111].

6 грудня 2017 року в Україні запустили електронну послугу системи «Трембіта», що пов'язана з державною реєстрацією договорів земельної оренди. Інформаційна система забезпечить сучасне робоче середовище для адміністраторів центрів надання адміністративних послуг, дозволить управляти роботою з документами в електронному вигляді та надавати доступ до даних у державних реєстрах. Крім того інформаційна система стане системою, що працюватиме онлайн та частково в автономному режимі й управлятиметься ІТ-фахівцями дистанційно. Процедура закупівлі системи здійснюється як частина Програми «U-LEAD з Європою» та спільно фінансується Європейським Союзом і його державами-членами – Данією, Естонією, Німеччиною, Польщею та Швецією [63].

Отже, можемо стверджувати, що фактично наявні можливості криптологічних технологій є такими, що надають можливість практично використовувати для користі фізичних і юридичних осіб технологію електронного цифрового підпису. Це є класичним прикладом переростання специфічних за своєю основою суспільно-технічних відносини в адміністративно-правову площину, що зумовлює нові вимоги до безпеки особистих даних і зручності їх використання.

Висновки до розділу 1

1. Адміністративно-правові відносини, що виникають з приводу електронного цифрового підпису, характеризуються такими особливостями:

1) вони нерозривно пов'язані з адміністративно-правовими нормами, виникають і здійснюються на їх основі;

2) основною їх метою є забезпечення прав та свобод людини і громадянина, нормальне функціонування громадянського суспільства та держави;

3) вони регулюють широке коло суспільних відносин між публічною адміністрацією та об'єктами публічного управління;

4) провідною рисою адміністративно-правових відносин є їх публічна природа, вони виникають з ініціативи будь-якої сторони, при цьому згода іншої сторони, як правило, не є обов'язковою;

5) адміністративно-правові відносини є переважно виконавчо-розпорядчими: у вузькому розумінні суб'єкти публічного управління наділені владною компетенцією, а об'єкти зобов'язані виконувати їх законні вимоги; поряд із цим за широкого підходу сторони адміністративно-правових відносин завжди мають суб'єктивні права та юридичні обов'язки, які взаємопов'язані між собою: кожному суб'єктивному праву однієї сторони відповідає юридичний обов'язок іншої й навпаки;

6) вони мають свідомо-вольовий характер, адже держава через видання відповідних адміністративно-правових норм виражає свою волю народу України, учасники цих відносин здійснюють своє волевиявлення, усвідомлюють значення своїх дій та можуть нести за них відповідальність;

7) адміністративно-правові відносини охороняються державою, яка сприяє здійсненню суб'єктивних публічних прав та юридичних обов'язків, а в разі правопорушення притягує винну особу до адміністративної чи іншої юридичної відповідальності;

8) не належать до адміністративно-правових відносини між публічної адміністрацією та об'єктами публічного управління, якщо вони не засновані на праві.

2. Доведено, що наукова природа електронного цифрового підпису базується на категоріях криптографії та криптоперетворення, які дозволяють подолати вплив противників і пов'язані з різними аспектами у

сфері інформаційної безпеки, таких як конфіденційність даних, цілісність даних, аутентифікація і безвідмовність. Електронний цифровий підпис вимагає правового (зокрема адміністративно-правового) та технічного (організаційно-правого) захисту особистих ключів від несанкціонованого використання;

3. Виявлено, що в Україні для звичайних потреб (не для спеціальних державних служб) використовується зворотній асиметричний крипто-алгоритм, коли підписувач володіє особистим закритим ключем і ставить свій підпис на програмний засіб, а перевіряється адресатом за допомогою відкритого ключа.

4. Доведено, що норми адміністративного права, які визначають юридичну природу електронного цифрового підпису зосереджені в таких основних європейських та вітчизняних джерелах:

1) міжнародно-правові джерела: Конвенція ООН про використання електронних повідомлень у міжнародних договорах (2005); Регламент ЄС від 23.07.2014 «Про електронну ідентифікацію та довірчі служби для електронних операцій на внутрішньому ринку»;

2) вітчизняні джерела: а) закони: «Про електронний цифровий підпис (спеціальний)»; «Про електронні документи та електронний документообіг»; «Про електронний цифровий підпис»; «Про обов'язковий примірник документів»; «Про Національну програму інформатизації»; «Про телекомунікації»; «Про Національну систему конфіденційного зв'язку»; «Про захист інформації в інформаційно-телекомунікаційних системах»; б) підзаконні нормативно-правові акти: Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації»;

5. Підкреслено, що наріжним каменем застосування електронного цифрового підпису в електронному документообігу є те, що визначається

не лише правовий статус такого підпису, але й електронних документів загалом, обов’язковим реквізитом яких є ЕЦП, а підпис дорівнюється до власноручного підпису (печатки) тільки у випадку виконання трьох умов.

6. Зроблено висновок, що в Україні використовується розширений електронний підпис «eIDAS» ЄС, згідно з яким підписувач має бути однозначно ідентифікований та пов’язаний з підписом; мати єдиний контроль над своїм ключем, бути здатним визначити, чи було змінено супровідні дані після підписання повідомлення; у тому разі, якщо супровідні дані були змінені, підпис визнається недійсним.

7. Доведено, що фактично існуючі можливості криптологічних технологій є такими, що надають можливість практично використовувати для користі фізичних і юридичних осіб електронний цифровий підпис. Це є класичним прикладом переростання специфічних за своєю основою суспільно-технічних відносини в адміністративно-правову площину, що зумовлює нові вимоги до безпеки особистих даних і зручності їх використання.

РОЗДІЛ 2
ЮРИДИЧНИЙ ЗМІСТ АДМІНІСТРАТИВНО-ПРАВОВИХ ВІДНОСИН З ВИКОРИСТАННЯМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В УКРАЇНІ

2.1 Суб'єкти адміністративно-правових відносин у сфері електронного цифрового підпису в Україні

Незважаючи на захищеність використання такого підпису, на сьогодні існує значна небезпека з боку хакерів, тобто кіберзлочинність, яка нині існує майже в усіх країнах, розвивається зі своїм розвитком і методами; також розвиваються і шляхи подолання цих проблем, що зроблено для запобігання володіння чужим ключем: якщо зловмисник заволодіє чужим ключем, він може потенційно від імені справжнього власника здійснювати неправомірні дії – наприклад, проводити певні грошові транзакції, змінювати записи в базах даних тощо.

У таких випадках актуальним є виявлення та опис суб'єктів адміністративно-правових відносин у сфері електронно-цифрового підпису, які надають різноманітні адміністративні послуги в цій сфері та здійснюють виконавчо-розпорядчу діяльність, що підвищує ефективність корисної роботи за допомогою захищених криптологічними засобами й такими, що постійно модернізуються, новими технологіями.

На слушну думки В. Шуби, структура адміністративно-правових відносин, що виникають у діяльності органів прокуратури, складається з таких елементів: суб'єктів адміністративно-правових відносин, яких визначено як індивідуальних чи колективних осіб, фізичних чи юридичних, одні з яких, як правило, наділені владними повноваженнями (правами та обов'язками), що реалізуються ними у сфері владної управлінської діяльності стосовно інших суб'єктів, які визначено як

поведінку учасників цих відносин, тобто суб'єктів (дії, утримання від дій), які можуть мати як зовнішній, так і внутрішньоорганізаційний характер; зміст адміністративно-правових відносин, які визначено як вид і міру можливої (дозволеної) та належної (необхідної) поведінки, що передбачені адміністративно-правовими нормами, перебувають у тісному взаємозв'язку, тобто є взаємозалежними і забезпечуються державою [171].

Учені-адміністративісти невід'ємним юридичним елементом адміністративно-правових відносини визначають суб'єкти таких відносин. Ряд учених уважають, що суб'єкти правовідносин – це учасники адміністративно-правових відносин, які мають суб'єктивні права та юридичні обов'язки й наділені специфічними юридичними властивостями. Іншими словами, до суб'єктів адміністративно-правових відносин належать як суб'єкти публічної адміністрації, так і об'єкти публічного управління.

Об'єкти правовідносин – це те, на що спрямовано інтереси суб'єктів, з приводу чого останні вступають в адміністративно-правові відносини. Між цими елементами існує нерозривний зв'язок. Суб'єкти адміністративно-правових відносин вступають у них з метою задоволення своїх інтересів і потреб, які опосередковують об'єкти адміністративно-правових відносин. Виникнення у суб'єктів взаємних прав і обов'язків можливе лише на підставі настання певних юридичних умов юридичних фактів, закріплених у гіпотезах адміністративно-правових норм. Суб'єкти завжди вступають у правові відносини заради задоволення різних матеріальних, економічних, культурних, політичних або інших інтересів і потреб. Для досягнення цієї мети суб'єкти адміністративно-правових відносин здійснюють певні дії, спрямовані на досягнення корисного для них результату. Цей результат і є об'єктом адміністративно-правових відносин [39; 97].

Якщо говорити про інформаційне забезпечення діяльності недержавних громадських організацій, то воно має сприяти:

– підвищенню оперативності та якості роботи з інформацією;

– створенню умов для переходу від традиційної паперової до непаперової технології;

– створенню необхідних умов для підвищення автоматизації в роботі з інформацією і зниження трудових витрат на рутинні операції;

– підвищенню достовірності створюваної інформації;

– виключенню дублювання при отриманні інформації;

– забезпеченню централізованого зберігання інформації, підготовленої в електронній формі, включаючи графічну, а також усі супутні матеріали з можливістю організації логічного узгодження інформації, що належить до одного напряму пошуку за тематичним набором реквізитів;

– забезпеченню єдиного порядку індивідуальної й сумісної роботи з інформацією та ін. [98].

О. Брель уважає, що суб'єктами інформаційних відносин є: фізичні особи; фізичні особи – підприємці; юридичні особи; об'єднання громадян; суб'єкти владних повноважень; держава. Суб'єктами інформаційних відносин можуть бути також інші держави, їх фізичні та юридичні особи, міжнародні організації та особи без громадянства [20].

Адміністративно-правові відносини є різновидом правових відносин, а тому характеризуються їх загальними ознаками. Складовими частинами адміністративно-правових відносин є: суб'єкти, об'єкти та юридичні факти. Учасники адміністративно-правових відносин мають конкретні права та обов'язки і є суб'єктами правовідносин.

До суб'єктів адміністративно-правових відносин можна віднести:

– державні органи (органи законодавчої, виконавчої та судової влади, прокуратури, адміністрації державних підприємств і установ);

– структурні підрозділи органів держави, посадових осіб державних органів; власника (представника, менеджера, уповноваженого власника);

– об'єднання громадян, кооперативи, органи самоврядування, самодіяльні організації;

– громадян України, іноземних громадян, осіб без громадянства. Передумовою вступу названих суб'єктів у конкретні адміністративно-правові відносини є наявність у них правоздатності та дієздатності [6].

Відповідно до Закону України «Про електронні довірчі послуги» до суб'єктів відносин у сфері електронних довірчих послуг, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації, належать: користувачі електронних довірчих послуг; надавачі електронних довірчих послуг; органи з оцінки відповідності; засвідчувальний центр; центральний засвідчувальний орган; орган контролю [124].

Згідно зі статтею 2 Закону України від 22.05.2003 № 852-IV «Про електронний цифровий підпис» суб'єктами правових відносин у сфері послуг електронного цифрового підпису є: підписувач; користувач; центр сертифікації ключів; акредитований центр сертифікації ключів; центральний засвідчувальний орган; засвідчувальний центр органу виконавчої влади або іншого державного органу; орган контролю [123].

Розглянемо кожного з них. Підписувач – це особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку представляє, накладає електронний цифровий підпис під час створення електронного документа. Він має відповідно до статті 7 права та обов'язки підписувача, а саме має право: вимагати скасування, блокування або поновлення свого сертифіката ключа; оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку. Підписувач зобов'язаний: зберігати особистий ключ у таємниці; надавати центру сертифікації ключів дані згідно з вимогами статті 6 Закону для засвідчення чинності відкритого ключа; своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа [123].

Особливих вимог до підписувача законодавством України не встановлено. Лише вказано, що встановлення фізичної особи здійснюється за паспортом громадянина України (паспортом громадянина іншої країни з

нотаріально засвідченим перекладом українською мовою, посвідкою про тимчасове/постійне проживання, посвідченням біженця або паспортом громадянина України для виїзду за кордон з відміткою про постійне місце проживання в іноземній державі).

Адміністратор реєстрації приймає рішення про відмову в реєстрації в разі:

– відсутності необхідних для ідентифікації та реєстрації документів;

– відсутності в заявника/відповідальної особи документів, які засвідчують її особу та повноваження;

– подання неналежно засвідчених копій документів;

– подання документів/копій документів, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення, написи олівцем або мають пошкодження, унаслідок чого їх текст (фото) неможливо прочитати (розпізнати);

– невідповідності даних, що визначені в поданих документах, фактичним даним заявника (підписувача);

– ненадання контактного номеру телефону та/або діючої електронної адреси;

– ненадання достатньої кількості конвертів для носіїв ключової інформації підписувачів (у разі звернення довіреної особи (представника);

– ненадання запитів на формування посилених сертифікатів відповідальною особою;

– відсутності носіїв для запису ключової інформації в підписувача на момент реєстрації;

– з інших обґрунтованих підстав.

У разі відмови в реєстрації один примірник реєстраційної картки з додатками та позначкою адміністратора реєстрації про відмову із зазначенням підстав повертається заявнику, а другий з такою ж позначкою залишається у ВПР. АЦСК ІДД ДФС має право відмовити в реєстрації в разі, якщо підписувач є ув’язненим або засудженим та утримується в

слідчому ізоляторі або відбуває покарання в установах виконання покарань [25].

До користувачів належать органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори прав на нерухоме майно, державні реєстратори юридичних осіб, фізичних осіб – підприємців і громадських формувань, нотаріуси для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа. Державні реєстратори прав на нерухоме майно, державні реєстратори юридичних осіб, фізичних осіб – підприємців і громадських формувань, нотаріус також використовують лише захищені носії особистих ключів [131].

Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності Кабінетом Міністрів України. Порядок застосування електронного підпису, зокрема електронного цифрового підпису, у банківській системі України та суб'єктами переказу коштів визначається Національним банком України. Так, постановою від 14.08.2017р. № 78 «Про затвердження Положення про застосування електронного підпису в банківській системі України» до суб'єктів, належать Національний банк України, банки України, клієнти та контрагенти банків України. Контрагент банку – будь-яка юридична чи фізична особа, яка має з банком відносини фінансового характеру [131].

З метою взаємодії органів державної влади та значного покращення роботи Міністерством юстиції України було розроблено «Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, який затверджено наказом від 11.11.2014 № 1886/5». Цим Законом передбачено, що установи, в яких упроваджено системи електронного документообігу, застосовують електронний цифровий підпис типу «електронний цифровий підпис з повним набором даних перевірки», вимоги до якого визначаються наказом

Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованим у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710. Установи застосовують електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису. Організація роботи з електронними документами, що містять службову інформацію, здійснюється в порядку, визначеному чинним законодавством [113].

Окрім того Постановою Кабінету Міністрів визначено уповноважені суб'єкти, визначені в Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» – як такі, що мають право видачі паспорта громадянина України, здійснюють представництво центру в порядку, передбаченому Цивільним кодексом України, актами МВС та регламентом роботи центру.

На уповноважених суб'єктів, що здійснюють представництво центру, покладається відповідальність за невиконання чи неналежне виконання своїх обов'язків згідно із законодавством у сфері електронного цифрового підпису.

Уповноважені суб'єкти, що здійснюють представництво центру, надають такі послуги електронного цифрового підпису та виконують такі процедури:

– приймання від осіб, які досягли вісімнадцятирічного віку та отримують паспорт громадянина України з імплантованим безконтактним електронним носієм, заяв про реєстрацію в центрі як підписувачів та укладання договорів про надання послуг електронного цифрового підпису;

– ідентифікація особи;

– надання в користування надійних засобів електронного цифрового підпису та засобів шифрування, внесених до паспортів громадянина України з імплантованим безконтактним електронним носієм;

– надання допомоги під час генерації ключів [111].

Електронний цифровий підпис застосовується в обов'язковому порядку при поданні декларацій. Особам, уповноваженим на виконання функцій держави або місцевого самоврядування, для заповнення на офіційному веб-сайті Національного агентства з питань запобігання корупції декларацій необхідно мати ключ електронного цифрового підпису. Згідно з Положенням Закону України від 14 жовтня 2014 року №1700-VII «Про запобігання корупції», особи, уповноважені на виконання функцій держави або місцевого самоврядування, зобов'язані щорічно до 1 квітня подавати шляхом заповнення на офіційному веб-сайті Національного агентства декларації за минулий рік за встановленою формою. Для подання декларації суб'єкт декларування має використовувати особистий ключ електронного цифрового підпису, отриманий для виконання своїх службових обов'язків. Разом із цим особи, які припинили діяльність, пов'язану з виконанням функцій держави або місцевого самоврядування, протягом звітного року отримують послуги ЕЦП як фізичні особи, а не як посадові особи органу державної влади, органу місцевого самоврядування, підприємства, установи або організації державної форми власності [141].

Державна фіскальна служба України надає послугу електронного цифрового підпису суб'єктам декларування на безоплатній основі. Для отримання ЕЦП для подання декларації за звітний період суб'єкту декларування слід звернутись до спеціально призначеної відповідальної особи відповідного органу державної влади, місцевого самоврядування, підприємств, установ та організацій державної форми власності та надати: копію паспорта підписувача, засвідчену підписом власника; копію картки платника податків, засвідчену підписом власника. За наявності в паспорті

громадянина України реєстраційного номера облікової картки платника податків, замість копії картки платника податків може бути подана копія сторінки паспорта громадянина України з відповідною відміткою, засвідчена підписом власника. Якщо через релігійні переконання фізична особа відмовилась від реєстраційного номеру облікової картки платника податків, додатково подається копія сторінки паспорту з відміткою про таку відмову [141].

Також у зв'язку з тим, що в межах послуг електронного цифрового підпису не передбачено надання носіїв ключової інформації, генерація особистих ключів підписувачів виконується на носії суб'єкта декларування (змінні флеш-носії, оптичні носії CD/DVD, захищені носії ключової інформації тощо). Тому суб'єкту декларування потрібно надати спеціально призначеній відповідальній особі відповідного органу державної влади, місцевого самоврядування, підприємств, установ та організацій державної форми власності також і носій ключової інформації [там само].

Особистий ключ має властивості прихованого файлу і відображається, якщо у налаштуваннях папок активовано функцію відображення прихованих файлів. Строк дії посилених сертифікатів відкритих ключів становить два роки з моменту їх формування [там само].

Документом, який засвідчує чинність і належність відкритого ключа підписувачу, є сертифікат відкритого ключа. Сертифікат видається центром сертифікації ключів. Центром сертифікації ключів може бути юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі.

Обслуговування фізичних та юридичних осіб здійснюється центром сертифікації ключів на договірних засадах. Центр сертифікації ключів має право: надавати послуги електронного цифрового підпису та обслуговувати сертифікати ключів; отримувати та перевіряти інформацію,

необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо в юридичної або фізичної особи чи в її уповноваженого представника. Центр сертифікації ключів зобов'язаний:

– забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;

– забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;

– установлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;

– своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених Законом;

– своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;

– перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;

– цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;

– вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

– забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

– забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

– надавати консультації з питань, пов’язаних з електронним цифровим підписом.

Зберігання особистих ключів підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються [123].

За критерієм владних повноважень суб’єкти адміністративно-правових відносин у сфері електронного цифрового підпису слід поділити на владних (суб’єктів публічної адміністрації) та невладних. До невладних суб’єктів належать підписувач і користувач послуг електронного цифрового підпису, до владних – Акредитований центр сертифікації ключів. Перед тим як дати характеристику суб’єктам владних і невладних повноважень, необхідно дати визначення кожному з них. Невладним суб’єктом є підписувач – це фізична або юридична особа, яка на законних підставах володіє особистим ключем і від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис на електронний документ та користується послугами електронного цифрового підпису, що надає їй Центр [116].

Ще одним невладним суб’єктом є користувач – певна особа, яка користується інформаційними послугами для одержання інформації чи рішення певних завдань [133]. Суб’єктом владних повноважень є акредитований центр сертифікації ключів – це акредитований державою в установленому порядку орган, що надає послуги з надання ЕЦП з одночасним постачанням захищених носіїв ключової інформації або з використанням власних носіїв заявників типу USB-флеш-накопичувач [26].

Акредитований центр сертифікації ключів має право: надавати послуги електронного цифрового підпису та обслуговувати виключно посилені сертифікати ключів; отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо у юридичної або фізичної особи чи її представника. Акредитований центр сертифікації ключів має виконувати

всі зобов'язання та вимоги, установлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису. Порядок акредитації та вимоги, яким має відповідати акредитований центр сертифікації ключів, установлюються Кабінетом Міністрів України [123].

Також одним із важливих суб'єктів є центральний засвідчувальний орган, що визначається Кабінетом Міністрів України. Він формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів, блокує, скасовує та поновлює посилені сертифікати ключів засвідчувальних центрів і центрів сертифікації ключів, веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів, веде акредитацію центрів сертифікації ключів, отримує та перевіряє інформацію, необхідну для їх акредитації; забезпечує цілодобово доступ засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали, зберігає посилені сертифікати ключів засвідчувальних центрів і центрів сертифікації ключів, надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов'язаних із використанням електронного цифрового підпису [123].

Постановою Кабінету Міністрів України від 06 серпня 2014 року №311 «Про утворення територіальних органів Державної фіскальної служби та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України» утворено юридичну особу публічного права – Інформаційно-довідковий департамент ДФС, який став правонаступником Інформаційно-довідкового департаменту Міндоходів. У складі Інформаційно-довідкового департаменту ДФС функціонує Акредитований центр сертифікації ключів, метою діяльності якого є безкоштовне надання

послуг електронного цифрового підпису органам державної влади, органам місцевого самоврядування, підприємствам, установам та організаціям усіх форм власності, іншим суб'єктами господарської діяльності та фізичним особам.

Робота АЦСК ІДД забезпечується сучасним програмно-технічним комплексом, у складі якого використовуються унікальні програмно-апаратні рішення, які забезпечують високий рівень надійності захисту інформації. До послуг ЕЦП, які надаються АЦСК ІДД, належать:

– реєстрація заявників; надання в користування надійних засобів ЕЦП;

– допомога при генерації відкритих та особистих ключів;

– обслуговування посилених сертифікатів ключів заявників, що включає сертифікацію відкритих ключів заявників, розповсюдження та зберігання посилених сертифікатів ключів, управління статусом посилених сертифікатів ключів та розповсюдження інформації про статус сертифікатів ключів;

– надання послуги фіксування часу; консультативні послуги у сфері ЕЦП за зверненням підписувачів [119].

Ідентифікація іноземців здійснюється відповідно до законодавства. 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 видання кваліфікованого сертифіката відкритого ключа.

Кваліфікований надавач електронних довірчих послуг під час формування та видання 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 [124].

Відповідно до статті 10 Закону України «Про електронний цифровий підпис» Засвідчувальний центр використовується для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям. Засвідчувальний центр щодо групи центрів сертифікації ключів, зазначених у частині першій цієї статті, має ті ж функції та повноваження, що й центральний засвідчувальний орган стосовно центрів сертифікації ключів. Засвідчувальний центр відповідає вимогам, установленим законодавством для акредитованого центру сертифікації ключів. Засвідчувальний центр реєструється, засвідчує свій відкритий ключ і акредитується в центральному засвідчувальному органі. Національний банк України має право створити Засвідчувальний центр для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації центрів сертифікації ключів [123].

Статтею 12 передбачений орган контролю, функції якого здійснює спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації. Орган контролю перевіряє дотримання вимог Закону центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів. У разі невиконання або неналежного виконання обов'язків та виявлення порушень вимог, установлених законодавством для центру сертифікації ключів, засвідчувального центру, орган контролю дає розпорядження

центральному засвідчувальному органу про негайне вжиття заходів, передбачених законом [123].

Таким органом відповідно до постанови Кабінету Міністрів України «Про затвердження Положення про центральний засвідчувальний орган» від 28 жовтня 2004 року № 1451 зі змінами, внесеними Постановою Кабінету Міністрів України від 05.10.2011 № 1022, на Міністерство юстиції України покладено виконання функцій центрального засвідчувального органу. Одним з основних завдань Міністерства юстиції України є виконання функцій центрального засвідчувального органу шляхом забезпечення створення умов для функціонування засвідчувальних центрів органів виконавчої влади або інших державних органів та центрів сертифікації ключів відповідно до Положення про Міністерство юстиції України, затвердженого Постановою Кабінету Міністрів України від 02 липня 2014 року № 228.

Технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється державним підприємством «Національні інформаційні системи», яке визначено адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу відповідно до наказу Міністерства юстиції України від 19.10.2015 №2025/5 «Деякі питання функціонування центрального засвідчувального органу». До послуг обслуговування сертифікатів ключів центрів належать такі: формування, повторне формування, блокування, скасування та поновлення сертифікатів ключів Центрів, консультування центрів щодо надання Адміністратором ІТС ЦЗО послуг з обслуговування сертифікатів ключів.

Для одержання послуг центри подають до Адміністратора ІТС ЦЗО заяву, запит на формування сертифіката ключа Центру та інші документи в порядку та за формою, визначеними Регламентом роботи центрального засвідчувального органу та іншими нормативно-правовими актами, що регулюють відносини у сфері використання ЕЦП [166].

Таким чином, адміністративно-правовий статус суб'єктів адміністративно-правових відносин у сфері електронного цифрового підпису в Україні, які за своєю юридичною природою є публічними або приватними особами, наділені нормами адміністративного права різними за формулою правового регулювання суб'єктивними адміністративними обов'язками і правами коли суб'єкти публічної адміністрації (центральний засвідчувальний орган і акредитовані центри сертифікації ключів) надають адміністративні послуги та здійснюють виконавчо-розпорядчу діяльність, а приватні особи (споживачі та підписувачі) отримують адміністративні послуги, користуються всіма можливостями електронного цифрового підпису та можуть піддаватися адміністративній відповідальності за порушення режиму використання і зберігання електронних ключів.

Таким чином, суб'єкти адміністративно-правових відносин у сфері електронно-цифрового підпису характеризуються такими особливостями:

1) учасники адміністративно-правових відносин належать до владних суб'єктів владних повноважень і невладних;

2) адміністративні відносини між суб'єктами виникають с приводу електронно цифрового підпису;

3) усі суб'єкти владних і невладних повноважень мають певні права і обов'язки, які виникають з приводу електронно-цифрового підпису та закріплені в чинному законодавстві;

4) владний суб'єкт забезпечує цілодобово доступ засвідчувальних центрів і центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;

5) користувач – це певна особа, яка користується інформаційними послугами для одержання інформації чи вирішення певних завдань.

Отже, суб'єкти адміністративно-правових відносин у сфері електронно-цифрового підпису – це учасники адміністративно-правових відносин у сфері електронно-цифрового підпису, які мають суб'єктивні

права та юридичні обов'язки й наділені специфічними юридичними властивостями щодо надання повної юридичної легітимності електронно-цифровому підпису та можливостей використання його підписувачем і користувачем як тотожного аналогу письмового підпису.

2.2 Об'єкти адміністративно-правових відносин у сфері електронного цифрового підпису в Україні

Соціальний прогрес надає фізичним і юридичним особам усе більше можливостей для підвищення ефективності праці, відповідно й стандартів життя і відпочинку людства. Останнім часом вагомим кроком у розвитку світового суспільства є практичне використанні різноманітних «крипто»технологій, які в силу того, що стають найбільш важливими для великої кількості осіб, починають регулюватися нормами права, зокрема нормами адміністративного права.

Серед криптологічних технологій найбільшого практичного застосування отримав електронний цифровий підпис, що зумовлює нові вимоги до безпеки особистих даних і зручності їх використання.

Проте незважаючи на захищеність використання такого підпису, на сьогодні існує значна небезпека з боку хакерів, тобто кіберзлочинність, яка нині існує майже в усіх країнах, розвивається зі своїм розвитком і методами; також розвиваються і шляхи подолання цих проблем, що зроблено для запобігання володіння чужим ключем: якщо зловмисник заволодіє чужим ключем, він може потенційно від імені справжнього власника здійснювати неправомірні дії – наприклад, проводити певні грошові транзакції, змінювати записи в базах даних тощо.

Такі вагомі суспільні відносини все більше регулюються нормами права, зокрема адміністративними. Відповідно суспільні відносини у сфері цифрового електронного підпису об'єктивно стають адміністративно-правовими, що потребують утвердження та розвитку. Невід'ємним

елементом адміністративно-правових відносин у сфері електронного цифрового підпису є відповідні об’єкти. Саме заради цього суб’єкти цих відносин і вступають в них, задовольняючи свої законні, права та законні інтереси. Усі ці чесноти, які врегульовуються на основі норм адміністративного права, вимагають також подальшого розвитку й удосконалення. Суспільні відносини у сфері електронно-цифрового підпису врегульовуються численними нормами адміністративного права, тим самим вони є адміністративно-правовими відносинами, які характеризуються внутрішнім складом, до якого входять суб’єкти, об’єкти і зміст.

У теорії права під об’єктом правовідносин розуміють те, з приводу чого виникає та існує саме правове відношення. Так, управлена особа може претендувати на надання їй іншою стороною якогось майна (грошей, речей тощо), володіти і розпоряджатися якимись цінностями й ін. [55].

На загальнонауковому рівні слід зазначити, що об’єкт – це науковий простір, у межах якого проводиться дослідження; частина об’єктивної реальності, що на певному етапі стає предметом практичної та теоретичної діяльності людини. На думку вчених, завжди слід пам’ятати, що над об’єктом дослідження не здійснюють жодних перетворювальних дій, об’єкт дослідження є лише джерелом інформації для дослідника [163].

Кожен об’єкт має шанс стати предметом, тобто тією частиною пізнаної дійсності, про яку сформовано знання і яку можна вивчати, якою можна оперувати у своїй діяльності; трансформація об’єкта на предмет означає перехід суб’єкта від пізнання об’єкта до його практичного перетворення [60; 153]. Так, професор В. Галунько вважає, що об’єктом адміністративно-правових відносин може бути все, що здатне служити здійсненню публічних інтересів. У цій ролі можуть бути права людини і громадянина, право власності й послуги інших осіб [39].

Професор Ю. Битяк визначає, що об’єктом адміністративно-правових відносин є поведінка людей, а саме їх дії, за допомогою яких

реалізуються передбачені адміністративно-правовими нормами обов'язки і права учасників даних відносин. Ці дії можуть бути пов'язані зі здійсненням завдань державного управління (наприклад, видання індивідуального акта управління), особистими нематеріальними благами (наприклад, гідність людини), реалізацією суб'єктивних обов'язків і прав (наприклад, право на оскарження в суді дій посадових осіб і органів виконавчої влади), матеріальними предметами [15].

Схожу точку зору мають А. Комзюк і В. Бевзенко, які зазначають, що об'єктом правовідносин є те, з приводу чого вони виникають, на що націлені. Адміністративні процесуальні правовідносини виникають у зв'язку з потребою захисту й поновлення порушених, невизнаних, оспорюваних прав та інтересів. Об'єктом адміністративних процесуальних правовідносин є суперечка про право. Загальний об'єкт поділяється на окремі підвиди. Зазначено, що об'єктом правовідносин, пов'язаних із порушенням адміністративної справи, в суді є відкриття провадження у справі, подальший розгляд та вирішення публічноправової суперечки [75].

Об'єкт – це те, заради чого виникають правовідносини. Об'єктом адміністративно-правових відносин є поведінка учасників управлінських відносин (дії, утримання від дій). Дії учасників управлінських відносин можуть здійснюватися заради різноманітних правових інтересів. Це можуть бути речі, матеріальні цінності, продукти духовної творчості, особисті нематеріальні блага, а саме здоров'я, гідність людини, моральність тощо. Так, якщо об'єктом правовідносин є поведінка учасників (наприклад, передання державного майна від одного органу управління іншому), то предметом адміністративних правовідносин будуть об'єкти матеріального характеру, тобто майно, речі.

Підставою виникнення, зміни або припинення адміністративно-правових відносин є юридичні факти. Це дії та події. Під діями розуміють факти, які виникають за волею людей. Вони можуть бути як правомірними, так і неправомірними. Адміністративно-правові відносини

характеризуються всіма ознаками правових відносин, але крім цього мають деякі особливості:

1) адміністративно-правові відносини складаються у сфері управління, тобто в повсякденній практичній реалізації завдань і функцій держави щодо здійснення управління господарським, соціально-культурним будівництвом, адміністративно-політичною сферою;

2) в усіх відносинах однією зі сторін обов'язково є орган виконавчої влади (державного управління), орган місцевого самоврядування або громадська організація, наділена державно-владними повноваженнями;

3) адміністративно-правові відносини – це особливий зв'язок між їх учасниками, один із яких за даних обставин має право вимагати від іншого такої поведінки, яку передбачено адміністративно-правовою нормою;

4) адміністративно-правові відносини можуть виникнути за ініціативою будь-якого суб'єкта адміністративного права, згода іншої сторони не є обов'язковою умовою для їх виникнення.

У цілому адміністративно-правовим відносинам притаманні дві найважливіші ознаки: з одного боку – це форми соціальних відносин, оскільки в них обов'язково беруть участь люди чи їх об'єднання, а з іншого – форми організаційних відносин, у процесі реалізації яких розв'язуються завдання управлінської діяльності [6; 105].

Об'єктом адміністративно-правових відносин є те матеріальне або нематеріальне благо, на використання чи охорону якого спрямовано суб'єктивні права та юридичні обов'язки учасників адміністративно-правових відносин, а також певні дії, заради яких суб'єкти вступають в адміністративно-правові відносини. Об'єктом адміністративно-правових відносин може бути все, що здатне служити здійсненню публічних інтересів. Об'єкти адміністративного права поділяються на нематеріальні особисті блага людини (життя і здоров'я, честь і гідність, недоторканність, безпеку, свободу пересування та ін.) та матеріальні – предмети матеріального світу, створені природою чи людиною [39].

У своєму дослідженні А. Іванищук вважає, що об'єкти адміністративно-правового регулювання та адміністративно-правового забезпечення у сфері судової гілки влади співпадають. Це конституційно-правові норми, які визначають теоретико-правові засади функціонування судової гілки влади, гарантії забезпечення яких покладаються на публічну адміністрацію через реалізацію норм адміністративного права. Об'єктом адміністративно-правового забезпечення судової гілки влади в широкому розумінні є суспільні відносини, які виникають у сфері забезпечення публічною адміністрацією належних умов для здійснення правосуддя суддями, надання адміністративних послуг фізичним і юридичним особам у системі судової гілки влади; у вузькому розумінні – це конституційно-правові норми, що визначають теоретико-правові засади функціонування судової гілки влади [61].

На думку М. Савюк, інформаційне суспільство як об'єкт адміністративно-правових відносин – це різноманітні блага у формі ефективного виявлення, фіксації та переробки інформації, технологій (персональні комп'ютери, інформаційні послуги та ін.), виробництва знань (наука, мистецтво, освіта та ін.), публічних технологій (електронний уряд, самоврядування, партії та вибори), інформаційної економіки (інформаційні товари й послуги – освіта, правова система, видавнича сфера, ЗМІ, комп'ютерне виробництво), культури інформаційного суспільства (цивілізованих правил надання, сприймання та користування інформацією), які становлять публічну цінність для споживачів інформаційних ресурсів, а також діяння суб'єктів публічної адміністрації стосовно забезпечення права фізичних та юридичних осіб на інформацію, свободи інформації та законних інтересів фізичних і юридичних осіб в інформаційному суспільстві, що здійснюється на основі адміністративно-правових норм [150].

На думку Р. Мельника, під час користування публічними установами (об'єктами), а також у межах юридичних суперечок, які виникають між

органом місцевого самоврядування (органом виконавчої влади) та громадянином, необхідно розрізняти два рівні. Перший рівень стосується допуску громадян до користування публічними установами (об'єктами). Тут вирішується питання про існування взагалі права на користування публічною установою (об'єктом), відповідь на яке завжди здійснюється, виходячи з норм публічного (адміністративного) права. Такі норми зосереджуються в нормативних актах (положеннях), які гарантують (надають) приватним особам право доступу до публічних установ (об'єктів) [75]. У свою чергу А. Машков уважає, що об'єктом правовідносин є реальне благо, на використання або охорону якого спрямовані суб'єктивні права та юридичні обов'язки учасників (суб'єктів) правовідносин [96].

До останніх належить електронний цифровий підпис. Згідно із Законом України від 22.05.2003 № 852-IV «Про електронний цифровий підпис» електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних; електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Крім того в аналізованому Законі урегульовано інші суспільні відносини у сфері електронного цифрового підпису. Вимоги до сертифіката ключа прописано в ст. 6 Закону України від 22 травня 2003 р. № 852-IV «Про електронний цифровий підпис». Щодо дій суб'єктів адміністративного права, які здійснюють використання електронного цифрового підпису, то він використовується для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням

електронних документів, а саме для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. При цьому використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, установленого законом для вчинення правочинів у письмовій формі [123].

Постановою Кабінету Міністрів України від 28.10.2004р. №1452 затверджено «Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності», де вказано, що установа застосовує електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису, що має бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від спеціально уповноваженого центрального органу виконавчої влади у сфері криптографічного захисту інформації, та наявності посилених сертифікатів відкритих ключів у своїх працівників-підписувачів. Установа застосовує електронний цифровий підпис для вчинення правочинів за участю інших юридичних та фізичних осіб лише за наявності в них посилених сертифікатів відкритих ключів [112].

У правовому регулюванні розрізняють норми права: 1) матеріальні (первинний регулятор суспільних відносин) – закріплюють права і обов’язки суб’єктів права, на підставі яких можливо вирішити справу за суттю (право на сумлінну конкуренцію); 2) процесуальні (вторинний регулятор суспільних відносин) – містять правила про порядок реалізації норм матеріального права та вирішення справи за суттю (порядок розслідування злочину, порядок виклику свідків у суд).

Призначення норм процесуального права – установити «регламент» (фр. règlement від лат. regula – «правило») здійснення прав або виконання обов’язків, закріплених у матеріальних нормах; сприяти досягненню

результату, передбаченого нормою матеріального права; реалізовувати право на захист. Ознаки норм матеріального права:

1) регулюють фактичні зв'язки, що є змістом процесуального права;

2) є більш динамічними за процесуальні;

3) зумовлені матеріальними обставинами суспільного життя;

4) мають на меті забезпечувати права і свободи людини, упорядковувати відносини в суспільстві, встановлювати правопорядок;

5) мають регулятивну, правоохоронну і правозахисну дію;

6) адресуються всім суб'єктам права;

7) скасовуються в офіційному порядку [104].

У юридичній літературі зазначено, що норми матеріального права створені з метою закріплення прав та обов'язків суб'єктів чи визначення правил поведінки суб'єктів, які вступають у відносини в реальному суспільному житті, прагнучи досягнення своїх життєвих інтересів і потреб. Наприклад, це норми, що об'єднуються в галузі матеріального права та визначають статус суб'єктів, зміст їхніх прав і обов'язків, порядок утворення та функціонування, структуру і компетенцію юридичних осіб, закріплюють форму власності, структуру правовідносин та інших юридичних конструкцій тощо.

На думку деяких науковців, термін «матеріальне право» використовують для позначення правових норм, за допомогою яких держава прямо впливає на суспільні відносини та регулює їх. Інші вчені вважають, що матеріальне право регулює предметні («матеріальні») відносини. До галузей матеріального права, зазвичай зараховують конституційне, цивільне, адміністративне, кримінальне, трудове, сімейне, фінансове, земельне, міжнародне, водне, лісне (природоохоронні) та інші нормативно-правові комплекси [176].

До об'єктів права інтелектуальної власності належать (ст.420 ЦК): літературні та художні твори; комп'ютерні програми; компіляції даних (бази даних); виконання; фонограми, відеограми, передачі (програми)

організацій мовлення; наукові відкриття; винаходи, корисні моделі, промислові зразки; компонування (топографії) інтегральних мікросхем; раціоналізаторські пропозиції; сорти рослин, породи тварин; комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення; комерційні таємниці.

Суб'єктами права інтелектуальної власності є: творець (творці) об'єкта права інтелектуальної власності (автор, виконавець, винахідник тощо) та інші особи, яким належать особисті немайнові та (або) майнові права інтелектуальної власності відповідно до цього Кодексу, іншого закону чи договору. Суб'єктом права інтелектуальної власності перш за все є творець такого результату. Творцем може бути лише фізична особа, юридичні ж особи можуть стати суб'єктами права інтелектуальної власності на підставі закону [110].

Усі суб'єкти права інтелектуальної власності можна поділити на первинних і похідних. До перших належать лише творці результату інтелектуальної діяльності. Окремою категорією суб'єктів є роботодавці, у яких виникає право інтелектуальної власності на об'єкти, які створені при виконанні службових обов'язків. Так, у разі коли об'єкт інтелектуальної власності створено при виконанні трудового договору, то право на нього належить як працівникові, що створив об'єкт, так і роботодавцю, у той же час сторони можуть визначити інший порядок. Якщо об'єкт інтелектуальної власності створено в результаті участі кількох осіб, то всі вони є суб'єктами права інтелектуальної власності, а саме співавторами [110].

Норми, що охороняють творчий результат, постійно змінюються й ускладнюються під впливом науково-технічного прогресу, який безперервно породжує нові форми відтворення та розповсюдження інтелектуального продукту. Результати творчої діяльності прийнято поділяти на дві великі групи залежно від того, до якої сфери творчості вони належать. Від цього залежать й особливості правового режиму їх

охорони. До першої групи належать результати художньої творчості – літературні, музичні, хореографічні твори, а також образотворчого мистецтва, аудіовізуальні твори, наукові та інші подібні твори. До другої – результати технічної творчості – технічні пристрої, машини, механізми, інструменти, транспортні засоби, обладнання, споруди, нові речовини, рішення у сфері конструювання, нові способи та технології виробництва, досягнення селекції тощо. Зазначені результати творчої діяльності отримали спільну назву, яка підкреслює природу їх походження, – об'єкти інтелектуальної власності [19].

Правові норми, які регулюють суспільні відносини у сфері створення та використання результатів творчої діяльності, утворюють окрему підгалузь цивільного права – право інтелектуальної власності, яка включає декілька інститутів: авторське право та суміжні права, патентне право, інститут правових засобів індивідуалізації учасників цивільного обігу, їх товарів та послуг. Інститут авторського права та суміжних прав охороняє результати художньої творчості – твори науки, літератури та мистецтва (об'єкти авторського права), а також об'єкти, які створюються з метою їх розповсюдження – виконання творів, фонограми та відеограми, програми теле- та радіомовлення (об'єкти суміжних прав) використання та оформлення прав на результати науково-технічної творчості людини. Вони охороняються після спеціального оформлення прав і отримання охоронного документа – патенту або свідоцтва [19].

Виокремлення двох названих інститутів базується на особливостях правової охорони об'єктів авторського права та промислової власності, які пов'язані зі специфікою творчого процесу створення цих об'єктів та умовами їх використання.

По-перше, патентне право, на відміну від авторського права, спрямоване на охорону не художньої форми виразу ідей, думок чи понять, а на охорону самої сутності цієї ідеї, тобто змісту творчого технічного

(технологічного) рішення. Останнє може бути реалізоване в певному пристрої, механізмі, виробі, речовині тощо.

По-друге, для патентного права характерна обов'язковість формального визнання технічної (технологічної) ідеї охороноздатним об'єктом. Це здійснюється Держдепартаментом інтелектуальної власності, що діє у складі Міністерства освіти і науки України. З цією метою Департамент забезпечує функціонування системи експертизи заявок на об'єкти інтелектуальної власності, здійснює державну реєстрацію об'єктів та видає охоронні документи.

По-третє, об'єктам патентного права притаманна об'єктивна повторюваність, бо ідентичні технічні або технологічні рішення можуть бути створені кількома особами незалежно один від одного [19].

До них належить і електронний ключ – певний набір символів (цифр, букв, знаків), який формується комп'ютерною програмою з використанням генератора випадкових чисел. Ця інформація міститься в файлі або зберігається на паперовому носії. Особисті ЕК є секретними і зберігаються тільки в підприємства (доступ до них забезпечується паролем). За допомогою особистого ЕК і певного алгоритму підприємство створює ЕЦП, розшифрувати яку можна відкритими ключами. Такі ЕК підтверджуються сертифікатами, які видає центр сертифікації ключів, а доступ до них мають усі зацікавлені особи. Наприклад, створивши той чи інший звіт, підприємство підписує його за допомогою особистого ЕК. Отримавши звіт, ГФС, Пенсійний фонд або органи статистики відкритим ЕК підтверджують, що звіт підписаний саме цим підприємством [175].

Однак адміністративні відносини можуть виникати тільки між суб'єктами адміністративного права: це, по-перше, реальні учасники адміністративно-правових відносин, які володіють адміністративно-правовим статусом і беруть участь в організації держаного управління; по-друге – одна зі сторін публічної управлінської діяльності, яка наділена відповідною компетенцією, повноваженнями, наданими законодавством;

по-третє, вони можуть бути конкретними учасниками адміністративно-правових відносин, у які вони вступають за власним бажанням або в силу обов'язку (громадяни, посадові особи) [6].

Ознаки суб'єктів адміністративного права:

– володіння відповідно до приписів адміністративно-правових норм здатністю мати або реалізовувати (безпосередньо або через представника) права та юридичні обов'язки у сфері державного управління, тобто володіння адміністративною правосуб'єктністю;

– володіння потенційною можливістю реально брати участь в адміністративно-правових відносинах;

– зовнішня самостійність у реалізації своїх прав та обов'язків у сфері державного управління.

Слід розмежовувати поняття «суб'єкти адміністративного права» і «суб'єкти адміністративних правовідносин». Суб'єкт права може визначатись абстрактно в загальному вигляді. Суб'єкт правовідносин завжди конкретний. Суб'єкт права не завжди є суб'єктом правовідносин. Останнім він стає з моменту реалізації своїх прав та обов'язків у сфері виконавчої влади [6].

Статтею 422 Цивільного кодексу не встановлено підстав виникнення (набуття) права інтелектуальної власності, а лише визначено, що «право інтелектуальної власності виникає (набувається) з підстав, установлених цим Кодексом, іншим законом чи договором». Право інтелектуальної власності на результат творчої діяльності виникає внаслідок його створення, якщо такий об'єкт відповідає вимогам закону, а саме він має бути новим, утіленим в матеріальний об'єкт, придатним для використання, та відповідати іншим вимогам встановленим законодавством [167].

Тобто реалізуючи свої права та обов'язки у сфері цифрового підпису суб'єкти задовольняють свої права, свободи, інтереси і потреби як споживачі і підписувачі, що визначається межами юридичних норм і регулюється в ході адміністративної діяльності суб'єктів публічної

адміністрації та може захищатися від порушення засобами адміністративного примусу. Наприклад, підписувач – це особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку представляє, накладає електронний цифровий підпис після надання в користування засобів електронного цифрового підпису, може під час створення електронного документ вимагати скасування, блокування або поновлення свого сертифіката ключа; оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку [123]. Тобто має право на отримання, володіння, користування, а у подальшому – розпорядження електронним цифровим підписом за своїм баченням.

Центр сертифікації ключів виконує такі функції:

– надає послуги електронного цифрового підпису та обслуговує сертифікати ключів;

– отримує та перевіряє інформацію, необхідну для реєстрації підписувача й формування сертифіката ключа безпосередньо у юридичної або фізичної особи чи в її уповноваженого представника;

– забезпечує захист інформації в автоматизованих системах відповідно до законодавства;

– забезпечує захист персональних даних, отриманих від підписувача, установлює під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;

– своєчасно скасовує, блокує та поновлює сертифікати ключів, попереджає підписувача та додає в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;

– перевіряє законність звернень про скасування, блокування та поновлення сертифікатів ключів і зберігає документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;

– цілодобово приймає заяви про скасування, блокування та поновлення сертифікатів ключів;

– веде електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

– забезпечує цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

– забезпечує зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

– надає консультації з питань, пов’язаних з електронним цифровим підписом [123].

Акредитований центр сертифікації ключів: надає послуги електронного цифрового підпису та обслуговує виключно посилені сертифікати ключів; отримує та перевіряє інформацію, необхідну для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо в юридичної або фізичної особи чи її представника; негайно скасовує сформований ним посилений сертифікат ключа в разі: закінчення строку чинності сертифіката ключа; подання заяви власника ключа або його уповноваженого представника; припиняє діяльність юридичної особи – власника ключа у разі смерті фізичної особи – власника ключа або оголошення його померлим за рішенням суду; визнає власника ключа недієздатним за рішенням суду; надання власником ключа недостовірних даних; компрометації особистого ключа [там само].

Центральний засвідчувальний орган: формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів із дотриманням вимог Закону; блокує, скасовує та поновлює

посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів; веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів; веде акредитацію центрів сертифікації ключів, отримує та перевіряє інформацію, необхідну для їх акредитації; забезпечує цілодобово доступ засвідчувальних центрів і центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали; зберігає посилені сертифікати ключів засвідчувальних центрів і центрів сертифікації ключів; надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов'язаних із використанням електронного цифрового підпису; негайно скасовує посилений сертифікат ключа центру сертифікації ключів, засвідчувального центру в разі: припинення діяльності з надання послуг електронного цифрового підпису; компрометації особистого ключа [123].

Окрім того, Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно блокують посилений сертифікат ключа: у разі подання заяви власника ключа або його уповноваженого представника; за рішенням суду, що набрало законної сили; у разі компрометації особистого ключа. Скасування і блокування посиленого сертифіката ключа набирає чинності з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати та часу здійснення цієї операції. Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника [124].

Що стосується особливостей застосування електронного цифрового підпису, то органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності,

державні реєстратори прав на нерухоме майно, державні реєстратори юридичних осіб,фізичних осіб – підприємців та громадських формувань, нотаріуси для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа. Державні реєстратори прав на нерухоме майно, державні реєстратори юридичних осіб, фізичних осіб – підприємців та громадських формувань, нотаріуси також використовують лише захищені носії особистих ключів. Інші юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, сформованим центром сертифікації ключів, а також використовувати електронний цифровий підпис без сертифіката ключа [123].

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються електронними цифровими підписами без сертифіката ключа, визначається суб'єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах. У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, а також для забезпечення цілісності електронних даних та ідентифікації юридичної особи як підписувача під час надання адміністративних та інших послуг в електронній формі, здійснення інформаційного обміну з іншими юридичними особами, на електронний документ накладається ще один електронний цифровий підпис юридичної особи, спеціально призначений для таких цілей [там само].

Таким чином, об'єкт адміністративно-правових відносин у сфері електронного цифрового підпису в Україні є об'єктивно існуючим явищем матеріального інтелектуального права, похідним від суб'єктів адміністративного права як складова формального змісту адміністративно-правових відносин, існує з метою задоволення прав, свобод, інтересів і потреб споживачів і підписувачів, визначається межами юридичних норм,

регулюється в ході адміністративної діяльності суб'єктів публічної адміністрації.

Отже, об'єкт адміністративно-правових відносин у сфері електронного цифрового підпису в Україні є об'єктивним явищем матеріального інтелектуального права, похідним від суб'єктів адміністративного права як складова формального змісту адміністративно-правових відносин, існує з метою задоволення прав, свобод, інтересів і потреб споживачів і підписувачів, визначається межами юридичних норм, регулюється в ході адміністративної діяльності суб'єктів публічної адміністрації та захищається від порушень засобами адміністративного примусу.

2.3 Зміст адміністративно-правових відносин у сфері електронного цифрового підпису в Україні

В умовах сучасного суспільства наша держава набуває необхідних законодавчих змін для реалізації свого потенціалу, у нашому випадку – українські державні й недержавні органи використовують електронно-цифровий підпис як заміну звичайного письмового підпису, а сучасне законодавство постійно змінюється і модернізується в напрямку європейського законодавства, серед якого доцільно виділити міжнародно-правові джерела – Конвенцію ООН про використання електронних повідомлень у міжнародних договорах (2005); Регламент ЄС від 23.07.2014 «Про електронну ідентифікацію та довірчі служби для електронних операцій на внутрішньому ринку».

Поступово модернізуються й вітчизняні джерела – закони «Про електронний цифровий підпис (спеціальний)»; «Про електронні документи та електронний документообіг»; «Про електронний цифровий підпис»; «Про обов'язковий примірник документів»; «Про Національну програму інформатизації»; «Про телекомунікації»; «Про Національну систему

конфіденційного зв'язку»; «Про захист інформації в інформаційно-телекомунікаційних системах»; підзаконні нормативно-правові акти – Наказ Адміністрація державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації», інші нормативно-правові акти. Ці акти зосереджують свою юридичну силу і на правових відносинах, які виникають з приводу електронно-цифрового підпису.

Зміст – це сукупність елементів, аспектів, властивостей, зв'язків і тенденцій, що складають певний предмет, процес, явище. Проте не в його найзагальнішому вигляді, а в такому, що реалізується в кожному окремому предметі (групі предметів) на певному етапі розвитку, за певних умов. Згідно з діалектикою «зміст» і «форма» перебувають в органічній єдності, є співвідносними поняттями, які відображають дві взаємозалежні, суперечливі складові (елементи) буття предмета, явища, процесу [172]. Тлумачний словник української мови трактує термін «зміст» у таких значеннях: сутність, внутрішня особливість чого-небудь; певні властивості, характерні риси, які відрізняють певне явище, предмет від подібних явищ, предметів і т. ін.; розумна основа, мета, призначення чого-небудь [152].

У теорії права визначено, що зміст правовідносин – це передбачена нормами права сукупність суб'єктивних прав та юридичних обов'язків суб'єктів правовідносин. Розрізняють юридичний і фактичний зміст правовідносин. Юридичний зміст правовідносин – це передбачена нормами права реальна можливість суб'єктів правовідносин щодо здійснення суб'єктивних прав та юридичних обов'язків. Фактичний зміст правовідносин – це фактична поведінка суб'єктів правовідносин, у межах якої реалізуються їхні суб'єктивні права та юридичні обов'язки.

Юридичний і фактичний зміст не тотожні. Перший – значно ширший за другий і містить невизначену кількість можливостей. Наприклад,

реально особа може вступити на навчання до одного або двох вищих навчальних закладів за умови успішного складання вступних іспитів і тим самим реалізувати один із варіантів свого суб'єктивного права (фактичний зміст) [21].

Суб'єктивне право належить лише уповноваженому суб'єкту, який реалізує його на свій розсуд, тобто суб'єкт завжди може відмовитися від використання свого суб'єктивного права, крім випадків, коли суб'єктивне право збігається з юридичним обов'язком. Суб'єктивні права містять такі варіанти можливої поведінки уповноваженого суб'єкта:

– право здійснювати певні дії, тобто реалізувати свої інтереси;

– право вимагати певних дій від зобов'язаного суб'єкта;

– право вимагати відновлення порушеного права, тобто звертатися до компетентних державних органів за захистом суб'єктивного права і примусового забезпечення юридичного обов'язку;

– право користуватися певним соціальним благом.

Залежно від характеру та стадії реалізації того чи іншого суб'єктивного права на перший план у ньому може виходити одна із зазначених можливостей – як правило, перша. У цілому ж усі вищеназвані елементи становлять зміст і структуру суб'єктивного права [101]. Суб'єктивне право не може здійснюватися його носієм довільно, незалежно від інших правових норм. Реалізуючи своє суб'єктивне право, суб'єкт правовідносин діє на основі і в межах чинних правових норм.

Юридичний обов'язок постає як особливий, передбачений чинним законодавством вид поведінки зобов'язаної особи стосовно уповноваженої особи [101]. Юридичні обов'язки передбачають такі варіанти можливої поведінки зобов'язаного суб'єкта: здійснювати певні дії на користь уповноваженого суб'єкта; зобов'язання утримуватися від здійснення дій, що суперечать інтересам інших суб'єктів; вимагати здійснення або нездійснення тих чи інших дій від інших суб'єктів; нести юридичну

відповідальність за невиконання чи неналежне виконання передбачених правовою нормою дій.

Юридичний обов'язок установлюється як в інтересах уповноваженого суб'єкта, так і в інтересах держави в цілому, яка є гарантом їхнього здійснення. На відміну від суб'єктивного права, відмовитися від виконання юридичного обов'язку не можна, тому що відмова від виконання або неналежного виконання є підставою для юридичної відповідальності. Залежно від того, який вид поведінки передбачений диспозицією правової норми, юридичні обов'язки поділяються на активні (учинення позитивних дій в інтересах уповноваженого суб'єкта) і пасивні (невчинення заборонних дій). Юридичні обов'язки, як і суб'єктивні права, суворо персоніфіковані, тобто вони адресовані не абстрактній особі чи особам, а покладаються на конкретного суб'єкта чи суб'єктів визначених, конкретних правовідносин. Суб'єктивні права і юридичні обов'язки тісно пов'язані між собою, вони є взаємозалежними і відповідають один одному [65].

Л. Коваль визначав, що основним завданням адміністративного права є правове регулювання організаційних, управлінських відносин у суспільстві (адміністративна діяльність) та правоохоронна діяльність держави [68]. А. Макаренко вважає, що адміністративно-правові відносини – це урегульовані нормами адміністративного права суспільні відносини, в яких їхні сторони (суб'єкти) взаємопов'язані й узаємодіють унаслідок здійснення суб'єктивних прав і обов'язків, установлених і гарантованих відповідними адміністративно-правовими нормами [91].

В. Галунько визначив, що адміністративно-правові норми врегульовують відносини між публічною адміністрацією та фізичними особами; публічною адміністрацією та юридичними особами, які не мають владного статусу, та фізичними особами зі спеціальним невладним статусом; між вищими та нижчими органами й посадовими особами публічної адміністрації. Тим самим загальним для всіх видів

адміністративно-правових відносин є те, що як мінімум однією зі сторін є суб'єкт публічної адміністрації, наділений народом України владною компетенцією [39].

Виходячи із зазначеного, М. Горбач визначає, що підґрунтям (основою) адміністративно-правового статусу суб'єктів права є норми адміністративного права, зовнішнім виразом яких є джерела адміністративного права, що визначають правосуб'єктність, адміністративні обов'язки і права та адміністративну відповідальність суб'єктів адміністративного права. Дослідниця вказує, що майже всі вчені до змісту адміністративно-правового статусу відносять права, свободи та обов'язки суб'єктів адміністративного права. Права – це інтереси певного суб'єкта адміністративно-правових відносин, які полягають в користуванні й вільному розпоряджанні соціальними благами й цінностями, а також дозволяють користуватися основними свободами у встановлених законом межах. Відповідно обов'язком є сукупність зобов'язань одного суб'єкта адміністративного права щодо інших, що є певною органічною необхідністю, яка узгоджує особисті й суспільні інтереси. Таким чином, права й обов'язки як комплексні елементи адміністративно-правового статусу виділяють його цілісну складову, без жодного з елементів якого він не може існувати [42].

Суб'єктивне право – це гарантована правом і законом міра можливої або дозволеної поведінки особи, яка належить суб'єкту незалежно від того, перебуває він у правових відносинах з іншими суб'єктами чи ні. Саме тому до суб'єктивних прав належать фундаментальні демократичні права і свободи. Суб'єктивне право завжди належить уповноваженій особі, яка має певний інтерес – матеріальний, духовний, політичний, сімейний тощо. Для задоволення цього інтересу й існує соціальна цінність надання певних правових можливостей. Можлива поведінка щодо реалізації певного інтересу становить зміст суб'єктивного права і заснована на бажанні

уповноваженої особи. Межі бажаної поведінки чітко окреслені нормами позитивного права [165].

Т. Мацелик вказує та відносить до ознак суб'єктивного права наявність влади, інтерес і воля. Виділяє суб'єктивне публічне право, яке є різновидом суб'єктивного права, якому притаманні ознаки останнього. Особливості суб'єктивного публічного права полягають у залежності від публічного інтересу, у процедурі набуття та втрати права, у юридичних гарантіях їх реалізації та захисту [95].

Р. Мельник під поняттям «влада» розуміє реалізовану здатність суб'єкта влади впливати на рішення, дії чи бездіяльність фізичних і юридичних осіб та визначати юридичну долю об'єктів неживої природи. Зазначений вплив може здійснюватися у відкритий (безпосередньо) або прихований (опосередковано) спосіб. Влада характеризується такими особливостями: суверенітетом, який означає незалежність реалізації публічної влади від бажання чи небажання об'єктів влади; загальністю, яка означає, що публічна влада поширює свій вплив на все суспільство або його частину; авторитетністю, тобто її визначенням суспільством та його членами; фінансовою забезпеченістю, яка досягається за рахунок установлення податків, зборів та інших обов'язкових платежів; нормативним регулюванням суспільних відносин, що виявляється в можливості публічної влади видавати загальнообов'язкові правила поведінки; вольовим характером впливу, який виявляється в тому, що вплив публічної влади має внутрішній, духовний аспект, тобто заснований на волі суб'єкта реалізації влади [97].

Чимало науковців, досліджуючи теорію адміністративного права, державну владу характеризують: 1) можливістю оперативно ухвалювати рішення, оскільки процедури, які використовуються у сфері функціонування державної влади, є значно простішими порівняно з процедурами законотворчості та судочинства, що забезпечує швидкість вирішення завдань, які ставляться перед такою гілкою влади;

2) можливістю користуватися всім обсягом державновладних повноважень, визначених у законі, зокрема правом застосування прямого примусу; 3) розпорядництвом. Так, виконавча влада не лише виконує закони, ухвалені законодавчою владою, а й видає власні – підзаконні нормативні акти (наприклад, постанови Кабінету Міністрів, накази центральних органів виконавчої влади тощо), тобто видає обов'язкові для виконання розпорядження; 4) самостійністю, яка полягає в можливості виконавчої влади самостійно, тобто без погодження із законодавчою та судовою владою, ухвалювати рішення та забезпечувати їх виконання [97].

Державні службовці зобов'язані додержуватися Конституції та інших актів законодавства України, забезпечувати ефективну роботу відповідних органів, не допускаючи при цьому порушень прав і свобод людини й громадянина, безпосередньо виконувати покладені на них службові обов'язки, зберігати державну таємницю, інформацію про громадян, що стала їм відома під час виконання обов'язків державної служби, постійно вдосконалювати організацію своєї роботи та підвищувати професійну кваліфікацію [14].

Професор В. Галунько вважає, що адміністративні права – це комплекс природних і визначених адміністративним законодавством юридичних можливостей суб'єктів права – як позитивного, так і негативного спрямування. Адміністративні права суб'єкта публічної адміністрації – це прописана адміністративним законодавством міра дозволеної поведінки щодо виконання поставлених обов'язків стосовно забезпечення прав, свобод і законних інтересів невладних фізичних і юридичних осіб, та публічного інтересу держави й суспільства в цілому [7].

Законом України «Про державну службу» від 10.12.2015 № 889-VIII передбачено принципи, правові та організаційні засади забезпечення публічної, професійної, політично неупередженої, ефективної, орієнтованої на громадян державної служби, що функціонує в інтересах

держави й суспільства. Відповідно до статті 7 Закону державний службовець має право на повагу до своєї особистості, честі та гідності, справедливе й шанобливе ставлення з боку керівників, колег та інших осіб; чітке визначення посадових обов'язків; належні для роботи умови служби та їх матеріально-технічне забезпечення; оплату праці залежно від займаної посади, результатів службової діяльності, стажу державної служби та рангу; відпустки, соціальне та пенсійне забезпечення відповідно до законодавства; професійне навчання, зокрема за державні кошти; просування по службі з урахуванням професійної компетентності та сумлінного виконання своїх посадових обов'язків; участь у професійних спілках з метою захисту своїх прав та інтересів; участь у діяльності об'єднань громадян, крім політичних партій у певних випадках; оскарження в установленому законом порядку рішень про накладення дисциплінарного стягнення, звільнення з посади державної служби, а також висновку, що містить негативну оцінку за результатами оцінювання його службової діяльності; захист від незаконного переслідування з боку державних органів та їх посадових осіб у разі повідомлення про факти порушення вимог законодавства; отримання від державних органів, підприємств, установ та організацій, органів місцевого самоврядування необхідної інформації з питань, що належать до його повноважень, у випадках, установлених законом; безперешкодне ознайомлення з документами про проходження ним державної служби, зокрема з висновками щодо результатів оцінювання його службової діяльності; проведення службового розслідування за його вимогою з метою зняття безпідставних, на його думку, звинувачень або підозри [121].

Центр сертифікації ключів має право: надавати послуги електронного цифрового підпису та обслуговувати сертифікати ключів; отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо в юридичної або фізичної особи чи в її уповноваженого представника [123].

Національний банк України має право створити Засвідчувальний центр для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації центрів сертифікації ключів [123]. Головним органом у системі центральних органів виконавчої влади з формування та забезпечення реалізації державної правової політики, політики з питань банкрутства та використання електронного цифрового підпису, з формування та забезпечення реалізації політики у сфері архівної справи, діловодства та створення і функціонування державної системи страхового фонду документації, у сфері виконання кримінальних покарань, у сфері захисту персональних даних, у сфері організації примусового виконання рішень суддів та інших органів (посадових осіб) з питань державної реєстрації речових прав на нерухоме майно та їх обтяжень, з питань державної реєстрації юридичних осіб та фізичних осіб-підприємців з питань реєстрації (легалізації) об'єднань громадян, інших громадських формувань, статутів, друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності є Мін'юст України [100].

Мін'юст відповідно до покладених на нього завдань має право:

1) залучати в установленому порядку спеціалістів центральних та місцевих органів виконавчої влади, підприємств, установ та організацій (за погодженням з їх керівниками), учених, представників інститутів громадянського суспільства (за згодою) до розгляду питань, що належать до компетенції Міністерства;

2) отримувати безоплатно від міністерств, інших центральних та місцевих органів виконавчої влади, органів місцевого самоврядування необхідні для виконання покладених на нього завдань інформацію, документи і матеріали, зокрема від органів статистики – статистичні дані;

3) користуватися відповідними інформаційними базами даних державних органів, державною системою урядового зв'язку та іншими технічними засобами;

4) скликати наради, утворювати комісії, зокрема постійно діючі та робочі групи, проводити наукові конференції, семінари з питань, що належать до компетенції Міністерства [132].

О. Марченко визначає, що адміністративні права Міністерства юстиції України – це сукупність загальнообов'язкових, нормативно визначених правил щодо дій посадових осіб та органів Міністерства юстиції України, за допомогою яких відбувається виконання завдань і повноважень для досягнення належного рівня функціонування державної правової політики в системі органів виконавчої влади [93].

При цьому треба зазначити, що в нашому випадку більшість суб'єктивних прав спеціальної публічної адміністрації є зобов'язальними перед споживачами електронного цифрового підпису та зобов'язаними надавати їм визначені нормами адміністративного права адміністративні послуги. Однак у деяких випадках прямого порушення споживачами заборонних норм адміністративного права суб'єкт публічної адміністрації набуває суб'єктивне право діяти владно і застосувати щодо нього засоби адміністративного примусу [135].

Що стосується суб'єктів персональних даних, то вони мають право:

– знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, установлених законом;

– отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

– на доступ до своїх персональних даних;

– отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про

те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

– висувати вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

– пред’являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем і розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

– на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв’язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність і ділову репутацію фізичної особи;

– звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

– застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

– вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

– відкликати згоду на обробку персональних даних;

– знати механізм автоматичної обробки персональних даних; на захист від автоматизованого рішення, яке має для нього правові наслідки [135].

Окрім того 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 [124].

Пропозиція укласти електронний договір, її прийняття (акцепт) може бути надана шляхом: надсилання електронного повідомлення особі, яка зробила пропозицію укласти електронний договір; заповнення формуляра заяви (форми) про прийняття такої пропозиції в електронній формі; вчинення дій, що вважаються прийняттям пропозиції укласти електронний договір, якщо зміст таких дій чітко роз'яснено в інформаційній системі, в якій розміщено таку пропозицію, і ці роз'яснення логічно пов'язані з нею (тобто фактично шляхом учинення конклюдентних дій) [51].

Підписання електронного правочину пов'язується з використанням таких засобів: електронного підпису або електронного цифрового підпису відповідно до Закону України «Про електронний цифровий підпис», за умови використання засобу електронного цифрового підпису всіма сторонами електронного правочину; електронного підпису одноразовим ідентифікатором, який являє собою дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору; аналога власноручного підпису (факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, іншого аналога власноручного підпису) за письмовою згодою сторін, у якій мають міститися зразки відповідних аналогів власноручних підписів [51].

Також кваліфіковані надавачі електронних довірчих послуг мають право: надавати електронні довірчі послуги з дотриманням вимог 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 оцінювання 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 з переліку стандартів, визначеного Кабінетом Міністрів України, крім сфери спеціального зв'язку [124].

Однак права не можуть існувати без обов'язків, які тісно між собою пов'язані. Відповідно до академічного тлумачного словника української мови «обов'язок» – це те, чого треба беззастережно дотримуватися, що слід безвідмовно виконувати відповідно до вимог суспільства або виходячи з власного сумління [152]. Так, юридичні обов'язки – це передбачена правовою нормою і забезпечена можливістю державного примусу міра належної поведінки зобов'язаного суб'єкта, яку він мусить здійснити в інтересах уповноваженого суб'єкта. Він постає як особливий, передбачений чинним законодавством вид поведінки зобов'язаної особи стосовно уповноваженої особи.

Існують такі варіанти можливої поведінки зобов'язаного суб'єкта: здійснювати певні дії на користь уповноваженого суб'єкта; зобов'язання утримуватися від здійснення дій, що суперечать інтересам інших суб'єктів; вимагання здійснення або нездійснення тих чи інших дій від інших суб'єктів; несення юридичної відповідальності за невиконання чи неналежне виконання передбачених правовою нормою дій. Юридичний обов'язок установлюється як в інтересах уповноваженого суб'єкта, так і в інтересах держави в цілому, яка є гарантом їхнього здійснення. На відміну від суб'єктивного права, відмовитися від виконання юридичного обов'язку не можна, тому що відмова від виконання або неналежного виконання є підставою для юридичної відповідальності [65;114].

Законом України «Про державну службу» визначено, що державний службовець зобов'язаний: 1) дотримуватися Конституції та законів

України, діяти лише на підставі, у межах повноважень та у спосіб, що передбачені Конституцією та законами України; 2) дотримуватися принципів державної служби та правил етичної поведінки; 3) поважати гідність людини, не допускати порушення прав і свобод людини та громадянина; 4) з повагою ставитися до державних символів України; 5) обов'язково використовувати державну мову під час виконання своїх посадових обов'язків, не допускати дискримінації державної мови та протидіяти можливим спробам її дискримінації; 6) забезпечувати в межах наданих повноважень ефективне виконання завдань і функцій державних органів; 7) сумлінно і професійно виконувати свої посадові обов'язки; 8) виконувати рішення державних органів, накази (розпорядження), доручення керівників, надані на підставі та у межах повноважень, передбачених Конституцією та законами України; 9) додержуватися вимог законодавства у сфері запобігання і протидії корупції; 10) запобігати виникненню реального, потенційного конфлікту інтересів під час проходження державної служби; 11) постійно підвищувати рівень своєї професійної компетентності та вдосконалювати організацію службової діяльності; 12) зберігати державну таємницю та персональні дані осіб, що стали йому відомі у зв'язку з виконанням посадових обов'язків, а також іншу інформацію, яка відповідно до закону не підлягає розголошенню; 13) надавати публічну інформацію в межах, визначених законом [121].

Відповідно до Закону «Про державну таємницю» від 21.01.1994 №3855-XII державна таємниця – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може зашкодити національній безпеці України. Державні службовці, яким може бути надано допуск до державної таємниці, зобов'язані: не допускати розголошення будь-яким способом державної таємниці, яка їм довірена або стала відомою у зв'язку з виконанням службових обов'язків; не брати участі в діяльності політичних партій та громадських організацій,

діяльність яких заборонена в порядку, установленому законом; не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України; виконувати вимоги режиму секретності; додержуватися інших вимог законодавства про державну таємницю [122].

На користувачів електронних довірчих послуг покладаються такі зобов'язання:

– 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 [123].

Також 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 веб-сайту; впровадження, підтримання в актуальному стані та публікацію

на своєму веб-сайті реєстру чинних, блокованих і 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; 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 контролюючого органу 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 у разі його компрометації; постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів; внесення коштів на поточний рахунок із 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 заподіяна користувачам таких послуг чи третім особам внаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов’язань; наймання працівників, які володіють

необхідними для надання кваліфікованих електронних довірчих послуг знаннями, досвідом і кваліфікацією, у тому числі 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 контролюючого органу 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. Обов'язкові вимоги до кваліфікованих надавачів електронних довірчих послуг, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України [124].

Центр сертифікації ключів зобов'язаний:

– забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;

– забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;

– установлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;

– своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених цим Законом;

– своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;

– перевіряти законність звернень про скасування,блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;

– цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;

– вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

– забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

– забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

– надавати консультації з питань, пов’язаних з електронним цифровим підписом.

Зберігання особистих ключів підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються. Акредитований центр сертифікації ключів має виконувати всі зобов’язання та вимоги, установлені законодавством для центру сертифікації ключів, та додатково зобов’язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису [123].

Однак з метою недопущення чинного законодавств**а** у сфері електронних довірчих послуг встановлено державний нагляд (контроль). Одним із вагомих, відносно самостійних методів адміністративного права є контроль як вид адміністративної діяльності, який полягає в тому, що суб’єкт контролю здійснює перевірку й облік того, як контрольований об’єкт виконує покладені на нього завдання та реалізує свої функції. Основне призначення державного контролю полягає у виявленні невідповідності його об’єкта тим чи іншим правомірним оціночним

критеріям для подальшого застосування адекватних заходів реагування [39; 140].

Заходи державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг здійснюються відповідно до Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності». Орган контролю здійснює такі планові заходи державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг:

– перевірку кваліфікованого надавача електронних довірчих послуг (його відокремлених пунктів реєстрації) або надання запиту до органу з оцінювання відповідності щодо проведення процедури оцінювання відповідності кваліфікованого надавача електронних довірчих послуг за його власний рахунок для підтвердження того, що він та електронні довірчі послуги, які ним надаються, відповідають вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, що ними надаються;

– перевірку засвідчувального центру.

Протягом місяця з дня генерації центральним засвідчувальним органом пар ключів та формування відповідних самопідписаних сертифікатів електронних печаток центрального засвідчувального органу орган контролю проводить позапланову перевірку центрального засвідчувального органу щодо захисту інформації у програмно-технічному комплексі центрального засвідчувального органу. У разі виявлення порушень вимог, установлених законодавством для центрального засвідчувального органу, орган контролю інформує Кабінет Міністрів України про виявлені порушення та пропонує центральному засвідчувальному органу шляхи їх усунення. Щороку до 1 квітня орган контролю готує та подає до Кабінету Міністрів України звіт про оцінку діяльності суб’єктів відносин у сфері електронних довірчих послуг щодо дотримання вимог законодавства [124].

На сьогодні існує така класифікація атак на схеми ЕЦП: атака з використанням відкритого ключа (той, хто зламує, володіє відкритим ключем і набором підписаних повідомлень); атака на основі поширених повідомлень (той, хто зламує, володіє лише допустимим підписами набору електронних документів, що йому відомі, але не обраними ним); адаптивна атака на основі обраних повідомлень (той, хто зламує, може одержати підписи електронних документів, що він обирає).

Кожна з атак має визначену мету, кожну з яких можна віднести до відповідного класу: повний злам цифрового підпису (той, хто зламував, отримує таємний ключ та повністю зламує алгоритм); універсальна підробка цифрового підпису (знаходження алгоритму, аналогічного алгоритму підпису, що дозволяє підробляти електронний підпис на будь-якому електронному документі); вибіркова відбірка цифрового підпису (можливість підробляти підписи для документів, обраних тим, хто зламує); екзистенціальна підробка цифрового підпису (можливість отримання допустимого підпису хоча б для одного випадково обраного документу).

Найбільш небезпечною є адаптивна атака на основі обраних повідомлень, тому її в першу чергу потрібно перевіряти на крипостійкість, якщо немає якихось особливих умов. При безпомилковій реалізації сучасних алгоритмів ЕЦП отримання закритого ключа алгоритму є практично неможливим завдяки обчислювальній складності завдання, на якому заснований ЕЦП. Набагато більш імовірним є екзистенціальна відбірка або вибіркова.

На практиці застосування ЕЦП дозволяє виявити або запобігти таким діям порушника: відмова одного з учасників від авторства документу; модифікація прийнятого електронного документа; підробка документа; нав’язування повідомлень у процесі передачі – той, хто зламує, перехоплює повідомлення та модифікує їх. Проте є і такі порушення, від яких неможливо захистити систему обміну повідомленнями, – це повтор передачі повідомлення і фальсифікація часу відправлення повідомлення.

Протидія цим порушенням може засновуватися на використанні тимчасових вставок і суворому обліку вхідних повідомлень [11].

З метою недопущення витоку інформації та інших порушень необхідне створенням комплексної системи захисту інформації .Порядок створення такої комплексної системи захисту інформації регламентується «Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» та низкою нормативних документів Державної служби технічного захисту інформації Служби безпеки України. Так, відповідно до п. 16 «Правил» комплексна система захисту інформації призначається для захисту інформації від: витоку технічними каналами; несанкціонованих дій з інформацією, зокрема з використанням комп'ютерних вірусів; спеціального впливу на засоби обробки інформації.

Захист інформації від витоку технічними каналами та її убезпечення від спеціального впливу мають забезпечуватися в системі в разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації. Захист інформації від несанкціонованих дій, зокрема від комп'ютерних вірусів, має забезпечуватися в усіх системах [45; 136].

Шкода, заподіяна користувачеві електронних довірчих послуг надавачами електронних довірчих послуг, засвідчувальним центром, центральним засвідчувальним органом чи органом контролю, підлягає відшкодуванню в повному розмірі в установленому законом порядку. Особи, винні в порушенні вимог Закону або нормативно-правових актів, що регулюють діяльність у сфері електронних довірчих послуг, несуть кримінальну, адміністративну та цивільно-правову відповідальність згідно із законом. Суперечки, що виникають у сфері електронних довірчих послуг, вирішуються в порядку, установленому законом [124].

За останні роки збільшилася кількість правопорушень і злочинів, пов’язаних саме з компрометацією та незаконним використанням особистих ключів електронних підписів. Переважна більшість злочинів із використанням особистого ключа електронного підпису скоєні внаслідок явної компрометації особистого ключа самим підписувачем. Саме підписувачі створюють умови для компрометації особистого ключа й подальшого його незаконного використання.

Здебільшого такі злочини здійснюються в банківській сфері, а також в галузі нотаріату та реєстрації юридичних осіб. Прикладом є низка кримінальних справ, фігуранти яких, будучи банківськими працівниками, нехтували правилами політик банківської безпеки, під різними приводами заволодівали особистими ключами цифрових підписів своїх колег або підлеглих та організували схеми незаконного заволодіння коштами клієнтів банків [81].

К. Архіпова вказує, що на сьогодні більшість учених правові визначення комп’ютерної злочинності трактують як злочини, що прямо або побічно пов’язані з ЕОМ, які складаються з серії незаконних актів, що відбуваються за допомогою електронної обробки даних або проти неї. Інші під «комп’ютерною злочинністю» розуміють будь-які дії, пов’язані з незаконним втручанням у майнові права, які виникають у зв’язку з використанням ЕОМ. Треті вкладають у це визначення всі умисні й протиправні дії, що призводять до спричинення ущербу майну, державі, іншим суб’єктам і створення яких стало можливим завдяки електронній обробці інформації.

Комп’ютерні злочини становлять велику безпеку для інформаційних систем. Це пов’язано з тим, що вразливістю інформаційних систем можуть скористатися не тільки злочинці та терористичні угрупування, а й окремі особистості. А електронний цифровий підпис – реквізит електронного документа, призначений для захисту даного електронного документа від підробки, одержаний у результаті криптографічного перетворення

інформації з використанням закритого ключа електронного цифрового підпису, що дозволяє ідентифікувати власника сертифікату ключа підпису, а також установити відсутність несанкціонованих змін або підміни інформації в електронному документі. Електронний цифровий підпис в електронному документі є рівнозначним підпису, що ставиться власноруч на паперовому документі, якщо виконуються такі умови: сертифікат ключа підпису, що відноситься до цього електронного цифрового підпису, не втратив сили (діє) на момент перевірки або на момент підписання електронного документу за наявністю доказів, що визначають момент підписання; підтверджено достовірність електронного цифрового підпису в електронному документі; електронний цифровий підпис використовується відповідно до відомостей, які є в сертифікаті ключа підпису [11].

Кримінальний кодекс містить низку статей, що передбачають кримінальну відповідальність, а саме: стаття 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації»; стаття 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»; стаття 362 «Несанкціоновані дії з інформацією, яка оброблюється 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»; стаття 363 «Порушення правил експлуатації електронно-обчислювальних

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється» [83].

У разі встановлення правопорушень в адміністративній сфері відповідальність передбачено Кодексом України про адміністративні правопорушення. Це міститься в главах: 12 «Адміністративні правопорушення в галузі торгівлі, громадського харчування, сфери послуг, в галузі фінансів і підприємницькій діяльності»; 13-А «Адміністративні правопорушення, пов'язані з корупцією», а також у статтях 186-3 «Порушення порядку подання або використання даних державних статистичних спостережень»; 188-3 «Ухилення від виконання законних вимог посадових осіб центрального органу виконавчої влади, що реалізує державну політику у сфері державного контролю за додержанням законодавства про захист прав споживачів»; 188-31 «Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України»; 188-39 «Порушення законодавства у сфері захисту персональних даних»; 188-40 «Невиконання законних вимог Уповноваженого з прав людини»; 188-47 «Порушення встановленого законом порядку отримання інформації з Єдиного державного реєстру»; 195-5 «Незаконне зберігання спеціальних технічних засобів негласного отримання інформації», 212-2 «Порушення законодавства про державну таємницю»; 212-3 «Порушення права на інформацію та права на звернення»; 212-5 «Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію»; 212-6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем» та інші. За вчинення зазначених адміністративних правопорушень передбачено адміністративні стягнення: штраф; конфіскація незаконного тиражу продукції, який став знаряддям

вчинення або безпосереднім об’єктом адміністративного правопорушення [69].

Що стосується цивільної відповідальності, то це одна з форм (видів) юридичної відповідальності, суть якої полягає в примусовому впливові на порушника цивільних прав і обов’язків шляхом застосування щодо нього санкцій, які тягнуть за собою додаткові невигідні майнові наслідки. Цивільна відповідальність установлюється законом або договором сторін, має компенсаційний характер, оскільки мета її – поновити порушені майнові права кредитора. Настає за умови невиконання або неналежного виконання зобов’язання, протиправності поведінки порушника, заподіяння шкоди, прямого причинного зв’язку між поведінкою порушника і заподіяними збитками, а також вини. Цивільна відповідальність може бути частковою (кожний відповідає в розмірі своєї частки), солідарною (один за всіх і всі за одного, як правило, при скоєнні злочину), субсидіарною (додаткова матеріальна відповідальність – скажімо, батька за дитину у віці від 15 до 18 років), змішаною, коли враховується вина не лише порушника, а й потерпілого. Без вини несе відповідальність лише володілець джерел підвищеної небезпеки [174].

Основою є підпис особи, який має виконувати три основні функції: фіксацію волевиявлення особи завдяки її вираженню в певній об’єктивній формі; ідентифікацію підписанта за рахунок оригінальності підпису та можливості його верифікації та підтвердження цілісності підписаного тексту завдяки нерозривній пов’язаності підпису із текстом. Тільки за таких умов можливе доказування допущеної вини в цивільному праві.

У своєму дослідженні І. Верес вважає, що електроні підписи доцільно класифікувати договори в електронній форми за видами електронного підпису: 1) договори з електронним цифровим підписом, підтвердженим сертифікатом відкритого ключа; 2) договори з електронним цифровим підписом, підтвердженим посиленим сертифікатом відкритого ключа; 3) договори з іншими електронними підписами [22].

Відповідно до Закону України «Про електронний підпис» іншими електронними підписами є електронний підпис одноразовим ідентифікатором та аналог власноручного підпису. Доцільно законодавчо передбачити, що за умови використання всіх трьох видів електронних підписів письмова форма договору є дотриманою й відповідні документи можуть бути доказами під час розгляду спорів у судах. Однак необхідно передбачити, в яких саме випадках можуть використовуватися сторонами окремі види електронних підписів. У ст.5 Закону України «Про електронний цифровий підпис» зазначено, що органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори прав на нерухоме майно, державні реєстратори юридичних осіб, фізичних осіб-підприємців і громадських формувань, нотаріуси для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа. Доцільно розширити сферу використання електронного цифрового підпису з посиленим сертифікатом, зокрема у випадках, передбачених ч.2 ст.1 Закону України «Про електронну комерцію» [22]. Ми погоджуємось з такою точкою зору.

Отже, зміст адміністративно-правових відносин у сфері використання електронного цифрового підпису – це сукупність суб'єктивних прав та юридичних обов'язків суб'єктів адміністративно-правових відносин із використанням електронного цифрового підпису, коли кожному суб'єктивному праву одного суб'єкта права кореспондується юридичний обов'язок іншого й навпаки.

Таким чином, юридичні адміністративні обов'язки і права суб'єктів публічної адміністрації та підписувачів і споживачів електронного цифрового підпису, коли юридичним обов'язкам суб'єктів публічної адміністрації щодо забезпечення ідентифікації сертифіката ключа та відповідного особистого ключа, захисту інформації та персональних даних, доступу користувачів до сертифікатів ключів, відповідають

встановленому адміністративним законодавством праву отримати від них якісні й своєчасні адміністративні послуги стосовно електронного цифрового підпису. Визначено, що користувачів і підписувачів, які є приватними особами, мають негативно визначені права згідно із загальною забороною норм адміністративного права із незначною кількістю обмежень у вигляді зобов'язання зберігати особистий ключ у таємниці.

Висновки до розділу 2

1. Визначено специфічні особливості суб'єктів адміністративно-правових відносин у сфері електронно-цифрового підпису: вони за своєю юридичною природою можуть мати адміністративно-правовий статус суб'єктів публічної адміністрації або приватних осіб; виникають с приводу електронного цифрового підпису; наділені нормами адміністративного права суб'єктивними адміністративними обов'язками і правами; суб'єкти публічної адміністрації надають у цій сфері адміністративні послуги та здійснюють виконавчо-розпорядчу діяльність; приватні особи, що отримують адміністративні послуги, користуються усіма можливостями електронного цифрового підпису та можуть піддаватися адміністративній відповідальності за порушення режиму використання і зберігання електронних ключів.

2. З'ясовано, що до основних суб'єктів адміністративно-правових відносин із використанням електронного цифрового підпису належать: центральний засвідчувальний орган (Міністерство юстиції України); акредитовані центри сертифікації ключів, що отримали акредитацію, зокрема Акредитований центр сертифікації ключів Інформаційно-довідкового департаменту ДФС, Акредитований центр сертифікації ключів державного підприємства «Інформаційний центр» Міністерства юстиції України; споживачі та підписувачі електронного цифрового підпису.

3. Доведено, що суб’єкти адміністративно-правових відносин із використанням електронного цифрового підпису вступають у них з метою задоволення своїх прав, свобод, інтересів і потреб, які опосередковують об’єкти адміністративно-правових відносин. Визначено, що такою метою є однозначна юридична ідентифікації клієнтів фізичної чи юридичної особи, що надає їм можливість дистанційно за допомогою інформаційних систем і глобальної системи Інтернет здійснювати різноманітні юридичні дії як публічного, так і приватного характеру в різних місцях країни та за її межами. Сфера застосування електронного цифрового підпису суб’єктами адміністративного права є надзвичайно широкою (від отримання офіційної електронної довідки до дистанційного управління компанією) і постійно розширюється.

4. Визначено, що адміністративними діями суб’єктів публічної адміністрації у сфері електронного цифрового підпису в Україні є, по-перше, надання приватним особам (споживачам і підписувачам електронного цифрового підпису) адміністративних послуг у цій сфері, щоб вони могли комфортно і безпечно отримувати, продовжувати термін і відмовлятися від електронних ключів, користуватися ними в усіх сферах публічного і приватного життя. Дії споживачів та підписувачів електронного цифрового підпису можуть мати як публічноправову (наприклад, у випадку здачі податкової звітності), так і приватноправову природу; по-друге – здійснення публічного адміністрування цифровим електронним підписом, коли спеціальні суб’єкти публічної адміністрації здійснюють увесь перелік передбачених адміністративним законодавством заходів, пов’язаних зі здійсненням організаційно-правових, технічних, організаційно-технічних, техніко-безпекових і організаційно-безпекових заходів для того, щоб система електронного цифрового підпису надійно працювала і задовольняла споживачів та підписувачів.

5. Визначено, що зміст у системі адміністративно-правових відносин у сфері електронного цифровий підпису полягає в тому, що кожному

суб’єктивному адміністративному праву одного суб’єкта адміністративного права встановлюється нормами адміністративного права юридичний обов’язок іншого і навпаки.

6. Виявлено сутнісну різницю змісту адміністративно-правових відносин суб’єктів владних повноважень і приватних осіб. Для перших домінантом є адміністративні обов’язки, а їх адміністративні права мають додатковий забезпечувальний характер і надаються адміністративним законодавством виключно тією мірою, що їм мінімально необхідна для ефективного виконання поставлених перед ними завдань.

7. Виділено такі адміністративні обов’язки суб’єктів публічної адміністрації: надавати адміністративні послуги щодо електронного цифрового підпису; забезпечувати однозначну ідентифікацію сертифіката ключа та відповідного особистого ключа підписувачу, захист інформації та персональних даних, цілодобовий доступ користувачів до сертифікатів ключів; своєчасно скасовувати, блокувати та поновлювати сертифікатів ключів. По виконанні зазначеного спеціальні суб’єкти публічної адміністрації мають адміністративні права стосовно отримання та перевірки інформації, яка необхідна для реєстрації підписувача і формування посиленого сертифіката ключа; перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів.

8. Доведено стосовно користувачів і підписувачів, які є приватними особами, що їх адміністративні права визначаються позитивно, хоча й отримали певне формальне оформлення, однак згідно з теорією права мають визначатися негативно згідно з першим принципом правового регулювання «дозволено усе крім того, що прямо заборонено законом». При цьому перелік таких заборони є дуже незначним – наприклад, що підписував зобов’язаний зберігати особистий ключ у таємниці.

РОЗДІЛ 3.
УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВИХ ВІДНОСИН З ВИКОРИСТАННЯМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ В УКРАЇНІ

3.1 Зарубіжний досвід використання електронного цифрового підпису

Розвиток в Україні інформаційно-комунікаційних технологій зумовлює особливе значення саме електронних інформаційних ресурсів як таких, що є найбільш зручною та ефективною, з точки зору користування, формою представлення інформації. На сьогодні важливою вимогою вступу України до Європейського Союзу є приведення законодавства до норм ЄС. З цією метою було ухвалено в Україні Закон України «Про електронний цифровий підпис», який визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при його використанні [123].

Реалізацію державної політики щодо електронного документообігу покладено на Кабінет Міністрів України та інші органи виконавчої влади в межах повноважень, визначених законом. Відповідно до Закону України «Про електронні документи та електронний документообіг» державне регулювання у сфері електронного документообігу спрямоване на реалізацію єдиної державної політики електронного документообігу; забезпечення прав і законних інтересів суб'єктів електронного документообігу; нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення електронних документів.

Уведення в дію законодавства щодо надання юридичної сили електронному документу та електронному цифровому підпису дає можливість створювати системи обміну електронними документами, які не

потребують дублювання паперовими і значно знижують фінансові витрати та витрати робочого часу в органах державної влади та управління. Особливо актуальним процес упровадження електронного документообігу є під час упровадження програми «Електронний уряд», адже підвищується якість надання державних послуг і прозорість системи відносин «громадянин – держава», «підприємство – держава». З метою визначення основних організаційно-правових засад електронного документообігу та використання електронних документів було ухвалено Закон України «Про електронні документи та електронний документообіг» [125].

Директива 1999/93/ЄС Європейського парламенту та Ради «Про систему електронних підписів, що застосовується в межах Співтовариства» від 13 грудня 1999 року засвідчує, що електронні підписи будуть використовуватись у великій кількості випадків, що мають своїм наслідком виникнення широкого спектру нових послуг та продукції, яка використовує електронні підписи; визначення такої продукції та послуг не має зводитись лише до видання та організації сертифікатів, але має також включати в себе будь-які інші послуги та продукцію, що використовує чи є допоміжною до електронних підписів, такі як послуги реєстрації, проставляння дати, довідкові послуги, послуги з підрахування чи послуги з надання консультацій стосовно електронних підписів.

Внутрішній ринок дає можливість постачальникам послуг щодо сертифікації розвивати свою транскордонну діяльність з метою досягти зростання їх конкурентоспроможності і таким чином надати споживачам та підприємцям нові можливості для безпечного обміну інформацією та ведення торгівлі електронним шляхом, незважаючи на кордони; з тим, щоб стимулювати надання в межах всього Співтовариства послуг щодо сертифікації через відкриті мережі; постачальник послуг по сертифікації має бути вільним з тим, щоб надавати свої послуги без попереднього отримання дозволу; отримання попереднього дозволу означає не лише отримання будь-якого дозволу, за допомогою якого зацікавлений

постачальник послуг щодо сертифікації має отримати рішення державних органів до того, як йому дозволять надавати свої послуги не лише з сертифікації, але й будь-які інші заходи, що мають таку ж силу [143]

На сьогодні багато країн світу (Австрія, Бельгія, Ірландія, Сінгапур, Таїланд, Фінляндія, Естонія, Данія, Люксембург, Франція, Німеччина, Іспанія, Італія та ін.) живуть уже у нових вимірах цифрового суспільства та економіки, запровадивши е-урядування, створивши урядові портали, запустивши електронні цифрові підписи, ID- та MobileID-карти, налагодивши взаємодію між органами державними влади, а найголовніше – між державою і громадянином. Закони про електронно-цифровий підпис ухвалено в Німеччині, Австрії, Франції, Індії, Ірландії, Республіці Корея, Литві, Польщі, Фінляндії, Естонії, Росії, Таїланді тощо. Наприкінці 1999 року в Євросоюзі було ухвалено Директиву про правові рамки використання цифрових підписів у Співтоваристві, в якій надано визначення електронного підпису, під яким розуміються дані в електронній формі, що прикладені або логічно поєднані з іншими електронними даними та слугують методом перевірки автентичності [178].

У більшості розвинених країн світу законодавство про електронний підпис ухвалено з метою прискорення торгівлі через Інтернет, а також електронного документообігу. Відповідно кожна країна підходить до цього питання, виходячи зі своїх власних критеріїв безпеки та контролю. На сьогодні відбувається певний розподіл:

1 категорія – країни, де статус електронного підпису прирівняний до статусу власноручного письмовій. До таких країн належать США, Канада, Велика Британія, Ірландія, Чилі, Швейцарія, Сінгапур, Португалія, Філіппіни, ОАЕ, Ірландія, Гонконг;

2 категорія – країни, де електронний підпис використовується, але не має настільки ж широкого статусу, як власноручний підпис на паперовому носії. Подібний статус застосування електронного підпису діє в Китаї, Чехії, Франції, Японії, Бельгії, Китаї, Індії. Юридично застосування

електронного підпису допустимо, а законодавство цих країн чітко визначає сфери застосування електронного підпису.

3 категорія – країни, де статус електронних підписів нечіткий. До таких країн можна віднести Аргентину, Австрію, Бразилію, Данію, Угорщину, Німеччину. У цих країнах використання електронного підпису безпосередньо залежить від засвідчувальних центрів. Електронні підписи при цьому не мають рівної юридичної сили з підписами на папері.

Провідна роль у розвитку правил електронного документообігу та електронного цифрового підпису у фінансовій сфері історично належить UNCITRAL і Раді Європи. Починаючи з 1997 року ООН рекомендувала національним урядам максимально враховувати положення типового закону UNCITRAL «Про електронну комерцію» (ухвалений на 29-й сесії UNCITRAL в Нью-Йорку, 28.05.1996-14.07.1996 р.) [128; 168]. Як результат тривалої роботи, в Європі ухвалено директиву ЄС «Про електронну комерцію». Обидва ці документи проголошують як основний принцип рівність правового статусу паперового й електронного документів. Це дозволяє застосовувати весь традиційний базовий юридичний багаж, напрацьований при використанні письмової (паперової) форми укладання контрактів і при використанні електронної форми. Крім того, вони уніфікують процедуру укладання контрактів в on-line, установлюють перелік інформації про сторони контракту, а також доводять позовну силу електронного контракту тощо [47].

Відповідно до типового закону UNCITRAL електронний документ означає інформацію, утворену, послану, отриману або збережену електронними, оптичними чи подібними засобами, включаючи електронний обмін даними (EDI1), електронну пошту, телеграми чи телекопіювання, але не обмежуючись ними. Ще одним цікавим моментом Правил UNCITRAL є те, що документ визнається оригіналом, якщо є достатня впевненість у цілісності інформації, починаючи з того часу, коли вона вперше створена в остаточній формі у вигляді електронного

документа або іншим способом. Іншими словами, Правила UNCITRAL визнають оригіналом будь-який документ, якщо тільки він зберігає цілісність інформації первинно створеного електронного документа.

Таке трактування дещо відрізняється від звичної інтерпретації оригіналу паперового документа, де оригінал може бути лише в одному примірнику, а повторні його екземпляри називаються або дублікатом 2, або копіями [103; 115]. Що стосується США, то базою для законів про електронні підписи стали два документи: «Модельний закон про електронні угоди» [184] та Закон 2000 року «Про електронні підписи в міжнародній і національній торгівлі» [179]. Законом «Про електронні підписи в міжнародній і національній торгівлі» [126] підтверджено законність «електронних» документів і «електронних» підписів у сфері внутрішньої й світової торгівлі. Відповідно до Закону «Про ліквідацію паперового документообігу в державних органах» [181] були визначені правила, за якими федеральні органи мають перейти на «електронний» документообіг і забезпечити доступ громадян до «електронних» документів.

У Німеччині правовий режим «електронних» документів, підписаних «електронними» підписами, регулюється актами про загальні умови використання «електронних» підписів. Так, Законом «Про цифрові підписи», прийнятим 2001 року [180] установлено систему визнання юридичної чинності за «електронними» підписами й регламентації обігу засобів створення й перевірки «електронних» підписів, а також передбачено систему провайдерів, що сертифікують. У такому разі мова йде про суворий порядок використання криптографії з відкритим або закритим ключем, технічні вимоги до органів, що сертифікують.

У Франції впровадження механізмів використання «електронних» підписів було здійснено шляхом внесення змін до Цивільного кодексу (ФЦК) щодо доведення здійснення угоди в писемній формі і ухвалення Декрету про електронний підпис, що розвиває положення Цивільного

кодексу. Згідно зі статтею 2 Декрету існує презумпція надійності такого підпису у випадку, коли він перевірений за допомогою «кваліфікованого електронного сертифіката», визначення якого схоже на надане в німецькому SigG. Тому, хоч і здається, що тільки технологія цифрового підпису сьогодні задовольняє вимогам Декрету, інші способи підписання не виключаються, за умови, що вони можуть гарантувати такий же рівень безпеки і використовують послуги незалежних сертифікаційних органів, що видають кваліфіковані сертифікати.

13 березня 2000 року французький уряд прийняв Закон, яким внесено зміни до глави VI Цивільного кодексу, що були спрямовані на створення загальних правил, які дозволили прирівняти юридичну силу «електронних» документів і підписів до власноручної форми у всіх сферах правовідносин. Відповідно до цих змін як письмові докази визнаються згідно зі ст. 1316 Цивільного кодексу «букви й цифри або будь-який інший знак або символ, значення якого може бути легко з’ясоване поза залежністю від способу створення й передачі». Для визнання дійсності такого аналога власноручного підпису висуваються дві традиційних вимоги: автентифікація особи, від якої виходить повідомлення, і підтвердження незмінності повідомлення. Таким чином, можна сказати, що позиція Франції більш ліберальна від тієї ж Німеччини, оскільки вона надає «електронним» документам такий самий рівень визнання їх юридичної чинності без «прив’язки» до конкретних технологічних засобів.

Незважаючи на те, що в цей час правила, висунуті до «електронних» підписів, задовольняє тільки технологія цифрового підпису, ці правила не обмежуються тільки цим видом автентифікації (англ. – «реальний» або «істинний»). На цей час немає готових до використання технологічно нейтральних засобів автентифікації, однак можливе їх прийняття в майбутньому, якщо вони відповідатимуть вимогам ФЦК і Декрету й будуть використовувати кваліфіковані сертифікати. У будь-якому разі місце для нововведень і їх конкуренції є.

Статтею 8 Декрету встановлено, що організації з сертифікації держав – нечленів ЄС – визнаються законом, якщо вони виконують вимоги Директиви про електронні підписи. Це означає, що вони мають відповідати вимогам французького закону й мають пройти акредитацію, як того вимагає Директива, або здобути сертифікати доручається акредитованому органу з сертифікації держави – члена ЄС, або що вони діють відповідно до міжнародного договору [18].

Що стосується Естонії, то послуги громадянам і послуги бізнесу мають п’ять рівнів: 1) інформування; 2) одностороння взаємодія; 3) двостороння взаємодія; 4) трансакція (у разі потреби); 5) персоналізація. Її стратегія розвитку інформаційного суспільства будується відповідно до «i2010:AEuropean Information Society for growth and employment» та «i2010 eGovernment action plan» (програма дій), затвердженої урядом Естонії, і залучає до своєї реалізації всі міністерства, державну канцелярію, наукові кола та інші організації. Водночас нова стратегія «Estonian Information Society Strategy 2013» була схвалена і затверджена 30 листопада 2006 р. урядом Естонії і вступила в силу 1 січня 2007 р.

Законодавчою основою електронного врядування в Естонії слугує «The Public Information Act» (PIA) (Закон про публічну інформацію), що був затверджений у листопаді 2000 р. і вступив в силу в червні 2001 р. Він стосується загальнодержавних і регіональних органів влади, юридичних осіб, що провадять соціальні послуги. Згідно з цим Законом будь-яка людина може звернутися до того чи іншого органу із запитом на отримання певної інформації, і в п’ятиденний термін їй мають відповісти. Відповіді реєструються. Інформація, що використовується для проведення наукових досліджень, надається безкоштовно. Також має бути забезпечений електронний доступ до цієї інформації та інші.

Заходами із захисту інформації займається Міністерство внутрішніх справ, Асоціація естонських міст та інші. Завдяки можливості ідентифікації особи через національну eID Card користувачі порталу

можуть заповнювати і подавати документи з електронним підписом, мають доступ до закритих для широкого загалу інформаційних баз, можуть здійснювати різноманітні операції з муніципальними та загально-державними органами державної влади (на сьогодні близько 60 установ і організацій). Кожен власник ідентифікаційної картки підписує та регулює створення й обслуговування електронних баз даних. Згідно з цим Законом створюється реєстр баз даних, він окреслює необхідний для них ступінь захисту. Основні суб'єкти розвитку електронного врядування в Естонії перебувають на центральному рівні [64].

В Італії існує декілька нормативних актів, присвячених «електронному» уряду й управлінню «електронними» документами. Так, у декреті президента Італії 1997 року, крім питань використання засобів «електронного» підпису (сертифікації ключів підпису, організації мережі сертифікаційних центрів), вирішено питання створення, передання, використання й зберігання «електронних» документів. 30 грудня 2010 року в Італії набула чинності нова редакція «Кодексу електронного уряду». Поряд із законодавчим декретом, що ввів принципи прозорості й підзвітності в державному управлінні, цей «Кодекс» вважається опорою процесу відновлення системи державного управління в Італії [149].

Канада стала одним зі світових лідерів постачання електронних послуг. Одним із найбільш вагомих аспектів є те, що програма розроблення електронного урядування «Уряд-онлайн» (Government Online (GOL) була підтримана на найвищому політичному та адміністративному рівні. Починаючи з 1997 р. прем'єр-міністри країни, міністри урядів наголошували на важливості та потребі створення е-урядування та підтримували курс на його поступове постійне впровадження. З жовтня 1999 р. після промови, яка відкрила засідання парламенту, GOL стала одним із ключових компонентів стратегії уряду Канади з надання різноманітних послуг своїм громадянам. Головною тезою промови стала така: «Уряд має стати взірцем у використанні інформаційних технологій та

мережі Інтернет. Нашою метою є до 2005 р. стати урядом, найближчим і найдоступнішим для своїх громадян, щоб канадці могли отримувати будь-яку інформацію та послуги від уряду в той час і з того місця, з якого вони забажають». Відтоді фінансування програми уряду GOL було закладено в усіх бюджетах країни на наступні роки [64].

У Великій Британії ринок електронної інформації – найбільший і був сформований одним із перших у ЄС. Основними законодавчими актами, що діють у королівстві, є Закон «Про захист даних». Відповідно до редакції 1984 року Закон декларує принципи захисту даних і регулює використання тільки автоматично обробленої інформації. Зазначений акт регулює автоматизовану обробку персональних даних як у публічному, так і в приватному секторах. Основний акцент у правовому регулюванні робиться на ретельно опрацьованій процедурі реєстрації й обробки персональних даних, нагляді й адміністративних приписах. 1998 року він одержав королівську санкцію, і відтоді сфера чинності Закону поширилася й на паперові документи.

Закон «Про захист інформації» був затверджений 2000 року й набрав чинності із січня 2005 року. Він закріплює право на доступ до публічних документів й інформації про діяльність державних органів. Одна з цілей цього Закону – зобов’язати державні органи розміщати в Інтернеті повідомлення про плани, строки й місце публікації з тих питань, які стануть доступними громадськості в певний час.

Закон «Про електронні комунікації» 2000 року був прийнятий, щоб установити норми, які полегшують використання «електронних» комунікацій і зберігання «електронних» даних. Закон був розроблений внаслідок імплементації двох Директив ЄС. Акт пропонує розширити рамки законодавчого визнання «електронних» підписів, які відповідають певним загальним критеріям і критерію функціональної еквівалентності. У Великій Британії крім законодавчих актів діє й низка національних стандартів з управління електронною документацією [18].

Уряд Великої Британії розпочав діяльність над удосконаленням своїх порталів з 2002 р. Уряд витрачає близько 208 млн. (€310 млн.) на розроблення та вдосконалення порталів щорічно. На сьогодні уряд проводить трансформацію всього лоту існуючих сайтів до єдиного порталу Directgov та паралельно використовує businesslink.gov.uk – для того щоб надати можливість громадянам та бізнесу більш вільно використовувати сервіси та послуги. Directgov уже протестований та затверджений урядом.

Таким чином, сьогодні кількість індивідуальних державних вебсайтів уже зменшена і ще буде зменшена до остаточного функціонування центрального порталу, що, безумовно, є бонусом для громадян. Electronic Signatures Regulations 2002 (Закон щодо електронного підпису) спрямований на побудову нової системи електронного підпису у приватній та публічній сферах, у комерції [64].

Що стосується країн Азії, то першою стала Малайзія, де був прийнятий Закон «Про цифровий підпис», що набув чинності з 1998 року та закріпив використання «електронних» документів і «електронного» підпису. Таким чином, для впровадження систем «електронного» документообігу з використанням «електронного» цифрового підпису в Україні необхідно враховувати всі прогалини, що існують в законодавчій базі, яка регламентує «електронний» документообіг в органах державної влади, органах місцевого самоврядування, установах та організаціях, і відповідним чином з урахуванням європейського досвіду внести корегування.

Отже, за рівнем легалізації електронного цифрового підпису (безпеки і контролю) здійснюється його юридична градація на три категорії: 1 категорія – країни, де статус електронного підпису прирівняний до статусу власноручного (США, Канада, Велика Британія, Ірландія, Чилі, Швейцарія, Сінгапур, Португалія, Ірландія, Гонконг); 2 категорія, де електронний підпис широко використовується, але не має повної тотожності власноручному підпису на паперовому носії (Китай,

Чехія, Франція, Японія, Бельгія, Китай, Індія); 3 категорія, де статус електронних підписів використовується в окремих сферах (Аргентина, Австрія, Бразилія, Данія, Угорщина). Провідна роль у розвитку правил електронного документообігу та електронного цифрового підпису історично належить UNCITRAL (Комісії ООН з права міжнародної торгівлі) і Раді Європи. В ЄС діє директива «Про електронну комерцію», яка проголошує рівність правового статусу паперового й електронного документів.

Також специфічними особливостями функціонування і використання електронного цифрового підпису в різних країнах є такі:

– у США прийнято Закон про ліквідацію паперового документообігу;

– у ФРН педантично визначено суворий порядок використання криптографії з відкритим або закритим ключем, технічні вимоги до органів, що сертифікують;

– у Франції формально впроваджено електронні підписи, що здійснювалось через зміни і доповнення до цивільного кодексу;

– в Італії існує декілька нормативних актів, присвячених «електронному» уряду й управлінню «електронними» документами;

– у Великий Британії основними законодавчими актами стосовно електронного цифрового підпису є закони про захист даних і захист інформації.

3.2 Удосконалення законодавства у сфері використання електронного цифрового підпису в Україні

Початок XXI століття відзначається стрімким розвитком комунікаційних та інформаційних систем, відбувається суттєва зміна способів виробництва, змінюється світогляд людей, внутрішні та міждержавні відносини у сфері економіки та торгівлі. Серед основних

тенденцій формування інформатизації суспільства в цілому, що стосується всіх сфер нашої повсякденної життєдіяльності, включаючи освіту, науку, медицину, економіку, державне управління, культуру, мистецтво, слід відзначити досить стрімкий розвиток глобальної мережі Інтернет. З появою глобальної мережі Інтернет кожен день усе більше й більше охоплював повсякденне життя людини та суспільства в цілому, аж поки не поглинув усі сфери. Адже зараз практично кожна людина користується Інтернетом для вирішення своїх соціально-побутових питань. Це оплата за комунальні послуги, розрахунки банківською карткою через. Тому із розвитком мережі виникли нові можливості до більш оперативного спілкування та комунікацій, укладання різного виду договорів.

Інтернет постає як гігантський посередник у торгівлі, через який можна продати й купити безліч товарів і послуг. Ця нова територія для ведення бізнесу надає широкі можливості відображення реальної економіки держави у віртуальному всесвіті. Бурхливий розвиток електронної комерції відкриває нові перспективи для ведення бізнесу. Можна стверджувати, що саме інтернет-комерція стане відправною точкою створення зовсім нових моделей ринкових відносин, абсолютно нових об’єднань партнерів і в підсумку – нової економіки. Дуже скоро Інтернет займе панівне місце в усіх сферах сучасного бізнесу, в якому працюють такі бізнес-моделі, які в реальному житті й уявити собі неможливо. З кожним днем він все активніше входить у ділове життя кожного, хто прагне процвітати і поліпшити економічну ситуацію в країні [158].

Кабінет Міністрів України планує здійснювати підготовку проектів рішень уряду та матеріалів до них в електронному вигляді. Згідно з Постановою № 608 від 18 серпня 2017 р. «Деякі питання підготовки проектів актів законодавства в електронній формі» проекти актів уряду та матеріали до них будуть готуватися в електронній формі із застосуванням електронного цифрового підпису. Проте крім випадків наявності

обґрунтованих підстав для їх підготовки в паперовій формі, таких як інформація з обмеженим доступом, у разі неможливості застосування матеріалів до відповідного проекту акта як оригіналів в електронній формі згідно з вимогами законодавства, у разі підготовки проекту акта з питань, пов'язаних із запобіганням виникненню надзвичайних ситуацій, ліквідації їх наслідків, або з інших питань, пов'язаних із виникненням загрози життю та/або здоров'ю населення, а також із невідкладних питань проведення антитерористичної операції та обороноздатності держави.

З цією метою було видано Наказ від 10.04.2013 р.№668/5 «Про затвердження Концепції реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг», де передбачалась подальша розбудова системи електронного цифрового підпису; створення на її основі єдиного простору довіри до електронних послуг; удосконалення та регулювання відносин, що виникають під час використання електронного цифрового підпису; створення умов для визнання юридичного статусу електронних документів, засвідчених електронним цифровим підписом, як аналога документів, складених у паперовій формі з власноручним підписом; вирішення завдань інтеграції України у світовий електронний інформаційний простір [129].

Також на рівні підзаконних нормативно-правових актів визначено потребу реформування законодавства у сфері електронного цифрового підпису, що зумовлено такими чинниками: недостатньою інформованістю громадян про можливість використання електронних документів як аналога документів, складених у паперовій формі з власноручним підписом; випадками невизнання юридичної значущості електронних документів і накладених електронних цифрових підписів, що призводить до недовіри фізичних та юридичних осіб до електронних послуг, які надаються з використанням електронного цифрового підпису; відсутністю правових засад до використання всіх можливостей інфраструктури

відкритих ключів для розбудови й ефективного функціонування електронних довірчих послуг, зокрема адміністративних послуг в електронному вигляді, електронного нотаріату, електронних закупівель, електронного документообігу, електронного архіву, електронного судочинства тощо; юридичною колізією окремих нормативно-правових актів, що регулюють функціонування інфраструктури відкритих ключів та надання послуг електронного цифрового підпису в Україні; відсутністю належної стандартизації інфраструктури відкритих ключів та надання послуг електронного цифрового підпису, а також органу оцінки відповідності державним стандартам і технічним регламентам функціонування інфраструктури відкритих ключів та послуг електронного цифрового підпису; недосконалістю нормативного регулювання державного контролю за діяльністю суб'єктів, які надають послуги з використанням електронного цифрового підпису, що призводить до надлишкового державного контролю за офіційно зареєстрованими суб'єктами, та існування тіньового ринку надання таких послуг, державний контроль якого не здійснюється; відсутністю в органі державної влади, що здійснює державне регулювання у сфері надання послуг електронного цифрового підпису, повноважень здійснювати державний нагляд у цій сфері; недостатністю рівня гармонізації термінології, що використовується в нормативно-правових актах, які регулюють сферу інфраструктури відкритих ключів та надання послуг з використанням електронного цифрового підпису, з термінологією, що використовується у відповідних міжнародних актах; відсутністю нормативно-правового регулювання визнання в Україні іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються при наданні юридично значимих електронних послуг [129].

Однак на сьогодні основні нормативні акти, які регламентують використання в України електронного цифрового підпису, – Закон України

«Про електронний цифровий підпис» [123] та Закон України «Про електронні документи та електронний документообіг» [125], ухвалені ще 2003 року, уже значно застаріли й потребують оновлення та змін, особливо що стосується адміністративних послуг і розширення сфери застосування електронного цифрового підпису. З метою вдосконалення державного регулювання у сфері електронного цифрового підпису, контролю за додержанням законодавства про електронний цифровий підпис, а також реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг потрібним є сутнісне розширення сфери його застосування, що має здійснюватися позитивними (переконання і заохочення) методами та негативними (адміністративно-попереджувальними) заходами загальної та спеціальної публічної адміністрації. Визнання в Україні іноземних електронних підписів та їх сертифікатів відкритих ключів використовуються при наданні юридично значущих електронних послуг резидентам.

До кінця 2018 року Урядом України планується запровадити 100 найбільш важливих послуг для громадян та бізнесу. Ключовими завданнями є реалізація єдиного порталу для надання всіх електронних послуг з одного місця, а також запровадження електронних договорів і популяризація всіх сервісів. Планується запровадження MobileID, що дозволить зробити електронну ідентифікацію більш масовою та популярною серед громадян. Ключовим завданнями залишається наповнення єдиного демографічного реєстру та видання ID-карток з ЕЦП, а також запровадження електронних довірчих послуг.

Відповідний законопроект, визначений Урядом як пріоритетний, перебуває у Верховній Раді. Планується розвивати загальнодоступні соціальні, громадські, медійні та комерційні проекти на базі відкритих даних. Також є потреба продовжувати заохочувати громадян і бізнес до участі в процесі формування політики та ухвалення управлінських рішень. В Україні вже доступні такі сервіси, як електронна петиція, громадський

бюджет, обговорення проектів актів, що дають можливість громадянам безпосередньо впливати на рішення.

Реалізація електронної взаємодії реєстрів залишається пріоритетним завданням. Розпочато запровадження кращого у світі рішення – естонської системи X-Road, яку попередньо Агентство з питань електронного урядування пілотувало з багатьма міністерствами. У вересні система проходить експертизу з безпеки і до кінця року планується її впровадження. Станом на вересень 2017 року всі центральні органи виконавчої влади та обласні держадміністрації на 80% обмінюються листування в електронній формі. Важливим завданням залишається створення електронного архіву та розвиток внутрішніх систем документообігу. Також Уряд затвердив склад Міжгалузевої ради з питань розвитку електронного урядування, до складу якої увійшли представники всіх Міністерств не нижче заступника Міністра. Цей орган має забезпечити єдину координацію реалізації Концепції, політичну волю та взаємне узгодження всіх завдань. Також планується впровадження міжнародного досвіду роботи з державними актами за принципом Digital by Default – усі акти КМУ проходитимуть додаткову цифрову експертизу, що передбачає цифровий спосіб реалізації описаного процесу як пріоритетний [160].

Виходячи з таких позицій вважаємо, що концептуально основними напрямками підвищення ефективності використання електронного цифрового підпису в Україні є такі:

1) сутнісне розширення сфери його застосування, що має здійснюватися позитивними (переконання і заохочення) методами та негативними (адміністративно-попереджувальними) заходами загальної та спеціальної публічної адміністрації;

2) посилення захищеності електронних систем від стороннього втручання хакерського й організаційного характеру;

3) покращення зручності користування електронним цифровим підписом;

4) захист норм адміністративного права у сфері електронного цифрового підпису адміністративними санкціями через установлення відповідної адміністративної відповідальності.

У першому випадку доцільним є розробити і прийняти на рівні розпорядження Кабінету Міністрів України нормативний акт «Концепція впровадження електронного цифрового підпису в усі сфери суспільного життя». При цьому за основу можна взяти положення Концепції розвитку електронного урядування в Україні, що затверджена Розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р., яка стосується сфери публічного управління. Запропонована нами концепція має сприяти розвитку вживання цифрового електронного підпису в різних сферах приватного і громадського життя, не пов'язаних із наданням адміністративних послуг. Іншими словами, на основі сприятливого інструментарію адміністративного права має бути створено механізм уживання цифрового електронного підпису в різних сферах життя.

Метою запропонованої концепції є визначення напрямків, механізмів і строків формування ефективної системи стимулювання вживання цифрового електронного підпису в різних сферах приватного і громадського життя, підвищення конкурентоспроможності вітчизняної економіки, стимулювання експорту продукції вітчизняних суб'єктів господарювання до країн-учасниць ЄС і розвитку громадянського суспільства.

Реалізація Концепції має здійснюється за такими основними принципами:

– цифровий за замовчуванням (забезпечення приватним особам можливості надавати комерційні послуги й отримувати публічні послуги, забезпечення міжвідомчої та між собою й публічними органами комунікації, як пріоритет, планування та реалізація будь-якої реформи, проекту чи завдання із застосуванням інформаційно-комунікаційних технологій);

– одноразове введення інформації (реалізація підходу, коли приватні особи лише один раз подають інформацію у відповідним чином сертифіковані реєстри при взаємодії між собою чи до органів влади, а у подальшому ця інформація повторно використовується для здійснення бізнесових операцій як підтверджена для громадських організацій інформація та для виконання інших повноважень, зокрема публічних, із дотриманням вимог захисту інформації та персональних даних);

– сумісність за замовчуванням (здійснення проектування та функціонування інформаційно-телекомунікаційних систем в органах влади відповідно до єдиних відкритих вимог і стандартів для забезпечення їх подальшої сумісності та електронної взаємодії та повторного використання; доступність та залучення всіх зацікавлених приватних осіб і суб'єктів громадянського суспільства; відкритість і прозорість; довіра та безпека) [79].

Шляхи і способи розв'язання проблеми. Повсякденне життя громадян, суб'єктів господарювання та громадянського суспільства стає дедалі все більш «цифровим», що передбачає високий рівень очікувань серед них щодо розвитку сучасних електронних форм взаємодії, прозорості та відкритості діяльності. Відповідно є потреба застосувати трансформаційний шлях, який пропонується в рамках цієї Концепції, що має революційний характер і робить акцент на посиленні функціональних можливостей використання цифрового електронного підпису та зниженні витрат суб'єктів господарювання, посиленні динамічності протидії корупції громадськими організаціями шляхом застосування сучасних інноваційних підходів, методологій та технологій (зокрема Інтернету речей, хмарної інфраструктури, Blockchain, Mobile ID, shareding economy, просування методики опрацювання даних великих обсягів (Big Data), нормативно-правового врегулювання принципів «цифровий за замовчуванням», «одноразове введення інформації» та «сумісність за замовчуванням», а також застосування перспективних форм організації

виконання завдань і проектів розвитку публічно-приватного партнерства) [79].

Для досягнення мети Концепції слід забезпечити виконання комплексних заходів за такими напрямами: модернізація методами переконання і заохочення приватних осіб на використання електронного цифрового підпису щодо розвитку взаємодії влади, громадян і бізнесу за допомогою інформаційно-комунікаційних технологій; модернізація комерційного управління через відповідні публічні ресурси (реєстри) за допомогою інформаційно-комунікаційних технологій.

Розвиток і підтримка доступних та прозорих, безпечних та некорупційних, найменш витратних, швидких та зручних електронних послуг дасть змогу покращити якість надання публічних послуг фізичним та юридичним особам, підвищити їх мобільність і конкуренто-спроможність, зменшити корупційні ризики та забезпечити, щоб електронні послуги обслуговували економіку майбутнього.

З урахуванням переваг технологій електронних послуг основними заходами із забезпечення розвитку електронного цифрового підпису має стати запровадження електронного цифрового підпису, зокрема адміністративних, в усіх сферах суспільного життя, а також надання інтегрованих електронних послуг за життєвими та бізнес-ситуаціями; реалізація принципу єдиного вікна («one-stop-shop») шляхом забезпечення розвитку та функціонування Єдиного державного порталу «Бізнес» і громадської діяльності як єдиної точки доступу фізичних та юридичних осіб до електронних послуг; розвиток електронних публічних закупівель, електронних договорів і рахунків, електронних аукціонів; стимулювання використання електронних послуг приватними особами [79].

За другим напрямком слід здійснити низку адміністративних роз’яснювальних заходів із користувачами і підписувачами стосовно виконання ними своїх зобов’язань зберігати особистий ключ у таємниці. Або у більш широкому форматі потрібно створити ефективну систему

протидії кіберзагрозам, їх попередження та усунення негативних наслідків; перегляд та конкретизацію повноважень суб'єктів забезпечення кібербезпеки; боротьбу з дезінформацією та деструктивною пропагандою з боку Російської Федерації; забезпечення захисту і розвитку кібернетичного простору України, а також конституційного права громадян на доступ до інформації; формування позитивного міжнародного іміджу України.

Актуальність формування дієвої системи забезпечення кібернетичної безпеки України зумовлена тим, що в сучасних глобалізаційних процесах значно зростає уразливість інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби обороноздатності та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури. Основним призначенням системи забезпечення кібербезпеки є сприяння в досягненні цілей кібернетичної безпеки, а тому основною функцією цієї системи можна визначити забезпечення збалансованого існування інтересів особи, суспільства і держави шляхом здійснення перевірок, діагностування, виявлення та ідентифікації, запобігання та припинення, мінімізації та нейтралізації дії внутрішніх і зовнішніх загроз і небезпек [44].

За третім напрямком слід розробити концепцію, програмне забезпечення, правові, технічні та організаційно-правові заходи щодо прив'язки ID-картки громадянина України, використання для цієї мети можливостей технологій NFC у смартфонах користувачів. ID-картка замінить паперовий паспорт, аби полегшити спілкування з державними органами та не збирати всілякі довідки для отримання послуг. Це станеться не завтра. Але саме так поступово, без ажіотажу Україна переходить до електронної системи урядування, прийнятої в багатьох державах світу.

Візуально ID-картка – це пластиковий документ розміром 8,56 см на 5,4 см, де про особу міститься і візуальна інформація, і така, що її можна прочитати лише на електронному носії. Візуально на самій картці можна

буде побачити назву держави; назву документа; прізвище та ім’я українською мовою та латинською транслітерацією, по батькові – лише українською; громадянство; дату народження; унікальний номер запису в Єдиному державному демографічному реєстрі а ін. Перехід на такий вид документа у всіх державах світу відбувався для запровадження електронного урядування. Про це ми вже говорили. Коли критична маса ID-карток буде значною, усі державні інституції будуть забезпечені обладнанням для зчитування інформації з електронних носіїв. Саме таким шляхом йшли інші держави, де введено такий документ. Окрім електронного урядування і наявності в ID-картці електронного підпису особи, що дозволить дистанційно отримувати послуги, упровадження таких карток є рекомендацією Єврокомісії та обов’язковим кроком для надання Україні безвізового режиму з ЄС [162].

Що стосується захисту норм адміністративного права у сфері електронного цифрового підпису адміністративними санкціями через установлення відповідної адміністративної відповідальності, то відповідний проект Закону України нами розроблений і представлений у додатку до дисертації.

Усе вищевикладене в цьому підрозділі дає можливість сформулювати такі висновки:

1) концептуально основними напрямками підвищення ефективності використання електронного цифрового підпису в Україні є: а) сутнісне розширення сфери його застосування, що має здійснюватися позитивними (переконання і заохочення) методами та негативними (адміністративно-попереджувальними) заходами загальної та спеціальної публічної адміністрації; б) посилення захищеності електронних систем від стороннього втручання хакерського і організаційного характеру; в) покращення зручності користування електронним цифровим підписом; г) захист норм адміністративного права у сфері електронного цифрового

підпису адміністративними санкціями через установлення відповідної адміністративної відповідальності;

2) доцільно розробити й ухвалити на рівні розпорядження Кабінету Міністрів України нормативний акт «Концепція впровадження електронного цифрового підпису в усі сфери суспільного життя»;

3) методами адміністративного переконання здійснити низку адміністративних роз'яснювальних заходів з користувачами і підписувачами стосовно виконання ними своїх зобов'язань зберігати особистий ключ у таємниці;

4) розробити концепцію, програмне забезпечення, правові, технічні та організаційно-правові заходи щодо прив'язки ID-картки громадянина України, використавши для цієї мети можливості технологій NFC у смартфонах користувачів;

5) доповнити КУпАП ст. 163-16 «Відмова надавати адміністративні послугу за електронним цифровий підписом» та ст. 163-17 «Неналежне зберігання особистого електронного цифрового ключа в таємниці, що призвело до його втрати або/та або використання сторонніми особами».

Отже, удосконалення законодавства у сфері використання електронного цифрового підпису в Україні має здійснюватися шляхом формування концептуальних положень і конкретних змін і доповнень до чинного законодавства стосовно підвищення ефективності використання цифрового підпису в Україні через розширення сфери його застосування, посилення захищеності, покращення зручності користування, захист санкціями через установлення відповідної адміністративної відповідальності. Це має реалізуватися в концепції впровадження електронного цифрового підпису в усі сфери суспільного життя, поєднання ID-картки громадянина України та можливостей технологій NFC у смартфонах користувачів і встановлення адміністративної відповідальності за відмову надавати адміністративні послуги за електронним цифровим підписом і неналежне його зберігання.

Висновки до розділу 3

1. Доведено, що переважна більшість демократичних правових держав живуть у новому вимірі інформаційного суспільства (Австрія, Бельгія, Ірландія, Сінгапур, Таїланд, Фінляндія, Естонія, Данія, Люксембург, Франція, Німеччина, Іспанія, Італія), коли цифрові технології ефективно використовуються в економіці, публічному управління та торгівлі. Інструментами реалізації зазначеного є запровадження е-урядування, електронні цифрові підписи, ID- та MobileID-карти. Спеціальні закони про електронно-цифровий підпис прийняті в Німеччині, Австрії, Франції, Індії, Ірландії, Республіці Корея, Литві, Польщі, Фінляндії, Естонії, Росії, Таїланді тощо.

2. Зроблено висновок, що в демократичних правових державах електронний цифровий є невід'ємним елементом інформаційного суспільства і широко використовується в усіх публічних і приватних сферах.

3. Виявлено, що за рівнем легалізації електронного цифрового підпису (безпеки і контролю) здійснюється його юридична градація на три категорії: 1 категорія – країни, де статус електронного підпису дорівняний до статусу власноручного (США, Канада, Велика Британія, Ірландія, Чилі, Швейцарія, Сінгапур, Португалія, Ірландія, Гонконг); 2 категорія, де електронний підпис широко використовується, але не має повної тотожності власноручному підпису на паперовому носії (Китай, Чехія, Франція, Японія, Бельгія, Китай, Індія); 3 категорія**,** де статус електронних підписів використовується в окремих сферах (Аргентина, Австрія, Бразилія, Данія, Угорщина).

4. З'ясовано, що провідна роль у розвитку правил електронного документообігу та електронного цифрового підпису історично належить UNCITRAL (Комісії ООН з права міжнародної торгівлі) і Раді Європи. В

ЄС діє директива «Про електронну комерцію», яка проголошує рівність правового статусу паперового й електронного документів.

5. Виявлено, що специфічними особливостями функціонування й використання електронного цифрового підпису в різних країнах є такі: у США прийнято Закон про ліквідацію паперового документообігу; у ФРН визначено суворий порядок використання криптографії з відкритим або закритим ключем, технічні вимоги до органів сертифікації; у Франції формально впровадження електронних підписів здійснювалось через зміни й доповнення до цивільного кодексу; в Італії існує декілька нормативних актів, присвячених «електронному» уряду й управлінню «електронними» документами; основними законодавчими актами щодо електронного цифрового підпису у Великий Британії є Закон про захист даних і захист інформації.

6. Концептуально визначено, що основними напрямками підвищення ефективності використання електронного цифрового підпису в Україні є: 1) сутнісне розширення сфери його застосування, що має здійснюватися позитивними (переконання і заохочення) методами та негативними (адміністративно-попереджувальними) заходами загальної та спеціальної публічної адміністрації; 2) посилення захищеності електронних систем від стороннього втручання хакерського й організаційного характеру; 3) покращення зручності користування електронним цифровим підписом; 4) захист норм адміністративного права у сфері електронного цифрового підпису адміністративними санкціями через установлення відповідної адміністративної відповідальності.

7. Запропоновано розробити й ухвалити на рівні розпорядження Кабінету Міністрів України нормативний акт «Концепція впровадження електронного цифрового підпису в усі сфери суспільного життя».

8. Запропоновано методами адміністративного переконання здійснити низку адміністративних роз’яснювальних заходів із

користувачами і підписувачами стосовно виконання ними своїх зобов’язань зберігати особистий ключ у таємниці.

9. Запропоновано розробити концепцію «Про програмне забезпечення, правові, технічні та організаційно-правові заходи щодо прив’язки ID-картки громадянина України», використавши з цією метою можливості технологій NFC у смартфонах користувачів.

10. Запропоновано доповнити КУпАП ст. 163-16 «Відмова надавати адміністративні послугу за електронним цифровий підписом» та ст. 163-17 «Неналежне зберігання особистого електронного цифрового ключа в таємниці, що призвело до його втрати або/та або використання сторонніми особами».

ВИСНОВКИ

У **висновках** на основі теорії адміністративного права, законодавства, досягнень публічної адміністрації наведено нове розв'язання наукового завдання стосовно розвитку засад та адміністративного інструментарію у сфері адміністративно-правових відносин з використанням електронного цифрового підпису в Україні, викладено найбільш важливі наукові та практичні результати, визначено наукові проблеми, для розв'язання яких можуть бути застосовані результати дослідження. Основі з них такі:

1. Доведено, що у вузькому розумінні адміністративно-правові відносини з використанням електронного цифрового підпису – це суспільні відносини, що врегульовуються нормами адміністративного права, виникають, змінюються і припиняються завдяки електронному цифровому підпису, отриманому у результаті криптографічного перетворення набору електронних даних, що дає змогу підтвердити його цілісність та ідентифікувати підписувача.

2. З'ясовано, що адміністративно-правова природа електронного цифрового підпису в Україні полягає у тому, що він, базуючись на науковій природі математичних категорій криптографії та криптоперетворення, завдяки об'єктивній юридичній регламентації через норми адміністративного права забезпечує адміністративно-правовий та організаційно-правовий захист особистих ключів підписувачів від несанкціонованого використання (через використання закритого ключа), підвищує ефективність управлінської діяльності органів публічної влади та зручність користування приватними особами, прирівнюється до власноручного підпису (печатки) і не може заперечуватися виключно на підставі того, що він має електронну форму.

3. Виявлено, що адміністративно-правові відносини, які виникають щодо електронного цифрового підпису відображають вплив адміністративно-правових норм на поведінку суб'єктів, які використовують електронний цифровий підпис та об'єктів публічного управління, через що між ними виникають сталі правові зв'язки публічно-владного характеру. Іншими словами, адміністративно-правова норма містить абстрактну конструкцію адміністративно-правового відношення. Сутність такої конструкції полягає в тому, що адміністративно-правова норма від імені держави визначає належну поведінку кожного зі своїх адресатів. Вона встановлює обов'язкові правила, за якими відбувається «спілкування». Ці правила формуються у вигляді взаємних адміністративних прав і обов'язків.

4. З'ясовано адміністративно-правовий статус суб'єктів адміністративно-правових відносин у сфері електронного цифрового підпису в Україні, які за своєю юридичною природою є публічними або приватними особами, наділені нормами адміністративного права різними за формулою правового регулювання суб'єктивними адміністративними обов'язками і правами, коли суб'єкти публічної адміністрації (центральний засвідчувальний орган і акредитовані центри сертифікації ключів, як центр сертифікації ключів) надають адміністративні послуги та здійснюють виконавчо-розпорядчу діяльність, а приватні особи (споживачі та підписувачі) отримують адміністративні послуги, користуються усіма можливостями електронного цифрового підпису та можуть притягуватися до адміністративної відповідальності за порушення режиму використання і зберігання електронних ключів.

5. Встановлено, що об'єкт адміністративно-правових відносин у сфері електронного цифрового підпису в Україні є об'єктивно існуючим явищем матеріально-інтелектуального права, похідним від суб'єктів адміністративного права, як складова формального змісту адміністративно-правових відносин, існує з метою задоволення прав,

свобод, інтересів і потреб споживачів і підписувачів, визначається межами юридичних норм, регулюється в ході адміністративної діяльності суб'єктів публічної адміністрації та захищається від порушення засобами адміністративного примусу.

6 З'ясовано адміністративні обов'язки і права суб'єктів публічної адміністрації, а також підписувачів і споживачів електронного цифрового підпису, коли юридичним обов'язкам суб'єктів публічної адміністрації щодо забезпечення ідентифікації сертифіката ключа та відповідного особистого ключа, захисту інформації та персональних даних, доступу користувачів до сертифікатів ключів, відповідає встановлене адміністративним законодавством право отримання від них якісних і своєчасних адміністративних послуг стосовно електронного цифрового підпису. Визначено, що користувачі і підписувачі, які є приватними особами мають негативно визначені права згідно із загальною забороною норм адміністративного права із незначною кількістю обмежень у вигляді зобов'язання зберігати особистий ключ у таємниці.

7. Здійснена компаративістична характеристика ефективного зарубіжного досвіду стосовно використання електронного цифрового підпису. В результаті чого виявлено, що переважна більшість демократичних правових держав функціонують у вимірі інформаційного суспільства, в яких цифрові технології ефективно використовуються в економіці, публічному управлінні та торгівлі, невід'ємним елементом яких є електронні цифрові підписи, що використовуються в усіх публічних і приватних сферах суспільного життя. Здійснено класифікацію електронного цифрового підпису за рівнем легалізації (безпеки і контролю) на три основні групи держав в яких: 1) статус електронного підпису прирівняний до статусу власноручного; 2) електронний підпис широко використовується, але не прирівнюється до власноручного; 3) електронний підпис використовується в окремих сферах. З'ясовано, що

в ЄС діє директива, яка проголошує рівність правового статусу паперового й електронного документів.

8. Удосконалено законодавство у сфері використання електронного цифрового підпису в Україні шляхом формування концептуальних положень і конкретних змін і доповнень до діючого законодавства стосовно підвищення ефективності використання цифрового підпису в Україні шляхом розширення сфери його застосування, посилення захищеності, покращення зручності користування, захисту санкціями через встановлення відповідної адміністративної відповідальності, що має реалізовуватися у концепції впровадження електронного цифрового підпису в усі сфери суспільного життя, поєднання ID-картки громадянина України та можливостей технологій NFC у смарфонах користувачів та встановленням адміністративної відповідальності за відмову надавати адміністративні послуги за електронним цифровим підписом та неналежне його зберігання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авер’янов В. Б. Адміністративне право України. підручник : у 2 т. Київ. *Юрид. Думка.* 2004. 584 с.

2. Авер’янов В. Б. Необхідність врахування євроінтеграційних вимог в умовах становлення нової української адміністративно-правової доктрини. *Правова держава*. 2010. Вип. 21. С. 183-191.

3. Адміністративне право України : підручник / Ю.П. Битяк, В.М. Гаращук, О.В. Дьяченко та ін. ; за ред. Ю.П. Битяка. Київ : *Юрінком Інтер*, 2005. 544 с.

4. Адміністративне право України. Академічний курс: підручник: / за ред. В.Б. Авер’янова. у 2 т. Т. 1: Загальна частина. Київ*: Юридична думка*, 2007. 592 с

5. Адміністративне право України. Загальне адміністративне право: навчальний посібник. За ред. В. В. Галунька. Херсон: *Грінь Д.С.*, 2015. 272 с.

6. Адміністративне право. URL. https:/ /sites. google. com/site/ igroupteamsite/ administrativne-pravo-ukraieni/ob-ekt-ta-zmist-administrativno-pravovih-vidnosin

7. Адміністративні права і обов’язки: словник термінів. Науково дослідний інститут публічного права. 2017. URL: http://sipl.com.ua/?p=4352/

8. Адміністративне право. Загальна частина. URL: https: //pidruchniki. com/ 14580906/ pravo /subyekti_ administrativnogo_ prava_ administrativnih_ pravovidnosin

9. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.. Основы криптографии: Учебное пособие. 3-е изд., *Москва*.: Гелиос АРВ, 2005.

10. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти: монографія, за заг. ред. Бандурки О. М.Харків: *Вид-во Ун-ту внутр. справ*, 2000.368 с.

11. Архіпова К.С. Кримінальне право та кримінологія. Підручник: URL. file:///C:/Users/Galunko/Downloads/jnn_2011_4-5_17%20(1).pdf

12. Архіпова К. С. Правовий режим використання електронного цифрового підпису в аспекті попередження правопорушень і злочинів. Юридична наука. 2011. №4-5. С.133-140.

13. Бааджи Н. Правова природа правовідносин у мережі Інтернет. *Часопис Цивілістики*. 2015. С. 112-116.

14. Битяк Ю. Адміністративне право: підручник. Нац. юрид. акад. України ім. Ярослава Мудрого. Харків: *Право*. 2010. 624 с.

15. Битяк Ю., Гаращук В., Зуй В. та ін. Адміністративне право: підручник. Харків: *Право*, 2012. 656 с.

16. Безпечність використання електронного цифрового підпису. INVESTGAZETA. 2016. URL: https://investgazeta.ua/blogs/bezpechnist-vikoristannya-elektronnogo-tsifrovogo-pidpisu.

17. Біометричний паспорт. URL: https:// uk.wikipedia. org/wiki/% D0%91%D1 %96%D0% BE%D0% BC%D0%B5 %D1%82%D 1%80%D0% B8%D1%87% D0%

18. Бойков А. Правове зебезпечення «електронного» документообігу в правоохоронних органах України. Дис. к-та ю.наук. 12.00.07. Київ. 2014. 214 с.

19. Борисова В.І. Право інтелектуальної власності України. URL: http: // web. Kpi .kharkov. ua/acem/wp-content /uploads/sites /16/2017/06/IV_nav_case _1.pdf-content /uploads/ sites/16/2017/06/IV_nav_case_1.pdf.

20. Брель О. С. Правове регулювання інформаційних відносин суб’єктів господарювання в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : Київ. 2012. 18 с.

21. Ведєрніков Ю. А. Теорія держави і права: Навч. посіб. Київ.: *Центр навчальної літератури*, 2005. 224 с.

22. Верес І. Правове регулювання цифрового підпису. URL. http://pgp-journal.kiev.ua/archive/2017/3/3.pdf

23. Верес І. Правове регулювання електронних підписів. *Цивільне право і процес*. 2007. № 3. С. 67-72.

24. Ви ще не використовуєте електронно-цифровий підпис? А виявляється, що і він вже «застарів»…URL. https:// www .kievskiysud.od.ua/press-department/all-news/3944-vi-shche-ne-vikoristovuete-elektronno-tsifrovij-pidpis-a-viyavlyaetsya-shcho-i-vin-vzhe-zastariv

25. Витяг з Регламенту Акредитованого центру сертифікації ключів інформаційно-довідкового департаменту ДФС. URL. https:/ /acskidd. gov. ua/ reglament

26. Вікіпедія. Акредитований центр сертифікації ключів.2018. URL: https: //uk. wikipedia. org/ wiki/

27. Вільна енциклопедія. Електронний_документ. 2001. URL. https:// uk. wikipedia. org/wiki/

28. Влада – бібліотека – громада: приєднуємося до електронного урядування : практичний посібник для бібліотек з надання послуг електронного урядування. уклад. Г. М. Гич, Т. О. Михайловська, О. М. Некипелова, А. Є. Цуканова. Миколаїв : *ФОП Швець В. Д.*, 2013. 120 с.

29. Волинка К. Г. Теорія Держави і права: навч. посіб. Київ: *МАУП*, 2003. 240 с.

30. Гавловский И. Содержание Административно-правовые отношения в сфере электронно-цифровой подписи/ Международный научно-практический журнал «*Право и Закон*». 2017. № 1. С. 89-93.

31. Гавловський І. Адміністративно-правові відносини у сфері електронно-цифрового підпису. *Науковий вісник публічного та приватного права*. 2016. №1. С. 189-194.

32. Гавловський І. Генеза виникнення електронного документообігу та цифрового підпису / Матеріали всеукраїнської науково-практичної конференції «Актуальні проблеми створення інтелектуальних і індустріальних парків»: м. Київ, 22 лютого 2016 р. Херсон, *Грінь Д.С.*, 2016. С. 126-130.

33. Гавловський І. Об'єкти адміністративно-правових відносин у сфері електронно-цифрового підпису. Науковий вісник Херсонського державного університету. *Серія «Юридичні науки»*. 2016. Випуск 6-2. Т. 1. С. 88-92.

34. Гавловський І. Поняття адміністративно-правового статусу суб'єктів адміністративного права. *Науковий вісник Ужгородського національного університету*. *Серія «Право»*. 2016. Випуск 41. Т. 3. С. 107-111.

35. Гавловський І. Поняття та зміст адміністративно-правових відносин з використанням електронного цифрового підпису. *Прикарпатський юридичний вісник*. 2015. № 3 (9). Т. 3. С. 183-187.

36. Гавловський І. Правове регулювання електронних документів та цифрового підпису. *Право, суспільство і держава: форми взаємодії*: Міжнародна науково-практична конференція, м. Київ, 13-14 січня 2017 р. Київ: *Центр правових наукових досліджень*, 2017. С. 79-82.

37. Гавловський І. Програмні інформаційні комплекси які використовуються в Україні. *Правове регулювання суспільних відносин: актуальні проблеми та вимоги сьогодення*: Матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 22-23 липня 2016 року. Запоріжжя: *Запорізька міська громадська організація «Істина»*, 2016. С.98-102.

38. Гавловський І. Суб'єкти адміністративно-правових відносини у сфері електронно-цифрового підпису. *Науковий вісник публічного та приватного права*. 2016. №2. С. 156-160.

39. Галунько В., Курило В., Короєд С. та ін. Адміністративне право України. Т.1. Загальне адміністративне право: навчальний посібник. Херсон: *Грінь Д.С*., 2015. 272 с.

40. Галунько В.В., Олефір В.І., Пихтін М.П. та ін Адміністративне право України : навч.посібник: у 2-х т.; за заг. ред. В.В. Галунька. Херсон : *ПАТ* «*Херсонська міська друкарня*» 2011. 320 с.

41. Голосніченко І. Адміністративне право України (основні категорії і поняття): навчальний посібник. Ірпінь, 1998. 126 с.

42. Горбач М. Адміністративно-правовий статус суб'єктів адміністративного права: теорія і практика: дис. канд. юрид. наук. 12.00.07. Київ, 2017. 215 с.

43. Дегтярьов А. Методи сучасної криптографії. Криптографія: загальні визначення, класифікація.асиметричні та симетричні криптоалгоритми, їх порівняння. URL: https://dehtyarov09.wordpress.com/2014/03/16/криптографія-загальні-визначення-кл-2/

44. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. 2017. URL: http://stratcom.co.ua/sistema-zabezpechennya-kiberbezpeki-sutnist-ta-priznachennya

45. Договірні відносини в системі Інтернет. URL: http:// ndipzir.org.ua/wp-content/uploads/2017/07/Yefremova/2_2.pdf

46. ДСТУ 2732:2004. Національний стандарт України. *Діловодство й архівна справа*. URL: http: //law.leschishin.org/nor024.php

47. Е-демократія: правовий аспект. URL: http:/ /www. library. vn.ua/publications/ 2006/E-demokrat11/E-dem11_1.html

48. Електронна демократія: сутність та основні етапи. *Вітчизняний і зарубіжний досвід впровадження електронного урядування*: зб. матеріалів наук.-практ. кон. Київ. 2008. С.85-88.

49. Електронний документ: чи має він на сьогодні доказову основу? URL:http://business-rost.com.ua/news/news-ucraina/elektronii-dokument-chi-ma-v-n-na-sogodn-dokazovu-osnovu.html

50. Електронний документообіг, тенденції та перспективи / М.Б.Величкевич, Н. В. Мітрофан, Н. Е. Кунанець. Вісн. Нац. ун-ту "Львів. політехніка". 2010. № 689. С. 44-53.

51. Електронний реєстр суб'єктів, які надають послуги, пов'язані з ЕЦП.RUL.: http://czo.gov.ua/ca-registry

52. Еннан Р. Правове регулювання відносин у мережі Інтернет. *Право: Проблеми і перспективи розвитку в Україні*. 2011. URL: http:// aphd. Ua /publication-173/

53. Єдиний державний реєстр судових рішень. 2016. URL: http://reyestr.court.gov.ua/Page/1778

54. Ємець В., Мельник А. , Попович Р. Сучасна криптографія . Основні поняття Львів : *БаК*, 2003. 144 с.

55. Єрмоленко В. Об'єкт у структура правовідносин. *Юридична Україна*. 2004. № 1. С.11-15.

56. Женченко М.І. Методика оформлення бібліографічних посилань на електронні ресурси в наукових статтях. *Наукові записки Інституту журналістики*. 2011. № 43. С. 119–126.

57. Запорожець М. П. Адміністративно-правове забезпечення діяльності місцевих загальних судів України: автореф. дис. на здобуття ступеня канд. юрид. наук : спец. 12.00.07. Харків, 2004. 20 с.

58. Зарубіжний досвід упровадження електронного урядування / авт. кол. : Т. Камінська, А. Камінський, М. Пасічник та ін. ; за заг. ред. С.А.Чукут. Київ., 2008. 200 с.

59. Застосування електроного цифрового підпису. URL. http://www.bestreferat.ru/referat-143072.html

60. Іванищук А. А. Поняття об’єкту адміністративно-правового регулювання у сфері судової гілки влади. *Форум права*. 2012. № 4. С. 399-403.

61. Іванищук А. Адміністративно-правове регулювання діяльності судової гілки влади: теорія і практика. Монографія. Київ: *Університет "Україна*". 2014. 356 с.

62. Ігнатович О.А. Методи підвищення ефективності компонентів безпеки комп’ютерних систем з використанням маскуючих елементів текстових та біметричних даних. Дис. на здобуття канд. тех. наук. 05.13.05. Львів. 2016. 173с.

63. Інформаційна система, яка розробляється EGOV4Ukraine, забезпечить до 400 ЦНАПів цифровими технологіями. URL. https:/ /decentralization. gov. ua/ news/8074

64. Камінська Т., Камінський А. та ін. Зарубіжний досвід упровадження електронного урядування. Київ. 2008. 200с.

65. Кириченко В., Куракін О. Теорія держави і права. навчальний. посібник. Київ: *Центр навчальної літератури*, 2010. 264 с.

66. Ківалов С. В., Біла Л. Р. Адміністративне право України (2-ге вид., перероб. і доп) Одеса. *Юрид. літ-ра*. 2002. 312 с.

67. Клименко І.В. Линьов К.О. Технології електронного документообігу: навч. пос. Київ. *Центр сприяння інституційному розвитку державної служби*, 2006. 192 с.

68. Коваль Л. Адміністративне право України. Київ, 1994. 208 с.

69. Кодекс України про адміністративні правопорушення. *Верховна Рада України*. 2017. URL. http: //zakon5. rada. gov. ua/ laws/show/80731-10/page14

70. Коломоєць Т. Адміністративне право України. Академічний курс: підручник. Київ: Юрінком Інтер. 2011. 576 с.

71. Коломоєць Т.О., Пиріжкова Ю.В., Армаш Н.О. та ін. Адміністративне право України : підручник; за заг. ред. Т.О. Коломоєць. Київ. : *Істина*, 2010. С. 19.

72. Коломоєць Т. Адміністративне право України. Академічний курс: підручник. Київ. *Юрінком Інтер*. 2011. 576 с.

73. Колпаков В.К. Адміністративне право України: навчальний посібник. Київ: *Юрінком Інтер*, 2004. 544 с.

74. Колпаков В. Адміністративно-правові відносини: поняття і види. Юридичний науковий електронний журнал. 2013. URL: http://www.lsej.org.ua/ 1_2013/ukr/Kolpakov.pdf

75. Комзюк А., Бевзенко В., Мельник Р. Адміністративний процес України: Навч. посіб. Київ. *Прецедент*, 2007. 531 с.

76. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года. *Офіційний вісник України*. 2011. №1. Ст. 1994.

77. Конвенция Организации Объединенных Наций об использовании электронных сообщений в международных договорах от 23.11.2005. *Верховна Рада України*. URL: http://zakon2.rada.gov.ua/laws/show/995_e71

78. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

79. Концепція розвитку електронного урядування в Україні. Затверджена Розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р.

80. Косовець О.О. Правове регулювання електронного документообороту. *Вісник Московського університету*. Серія 11. Право. 1997. №4. С.46-60.

81. Костенко О. В. Компроментація особистого ключа електронного підпису(правовий аспект). URL. kompрometatsiya- osobistogo- klyucha- elektronnogo -pidpisu -pravoviy-aspekt.pdf

82. Кривошеїн П.П. Адміністративно-правове регулювання будівництва в Україні. 12.00.07 Дис. на здобуття ступеня канд. юрид. наук : спец. 12.00.07. 2017 URL: http://sipl.com.ua/wp-content/uploads/ 2017/05/% D0%9A%D1% 80% D0%B8% D0%B2%D0%BE%D1%88%D0%B5%D1%97%D0%BD-%D0%

83. Кримінальний кодекс. *Верховна Рада України*. URL http://zakon2.rada.gov.ua/laws/show/2341-14/page2

84. Криптографічні_засоби_захисту_інформації URL: http:/ /ua-referat. com /Криптографічні_засоби_захисту_інформації

85. Криптогрпфія загальні визначення, класифікація. Асиметричні та симетричні криптоалгоритми.їх порівняння. URL https:/ /dehtyarov 09.wordpress. com/2014/03/16/криптографія-загальні-визначення-кл-2/

86. Криптоперетворення. Академік. URL: https: //ukrainian_explanatory. academic.ru/74669/%D0%BA%D1%80%D0%B8%D0%BF%D1

87. Курило В. Адміністративні правовідносини у сільському господарстві України: автореф. дис... д-ра юрид. наук: 12.00.07. Київ, 2008. 39 с

88. Лаба О. В. Основні етапи розвитку електронного діловодства. *Бібліотекознавство. Документознавство. Інформологія*. 2011. №3. С.16-19.

89. Лопатін С. Адміністративно-правові відносини у сфері забезпечення права громадян на інформацію: автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2010. 20 с.

90. Любченко Д., Кургаєва І. Адміністративно-правові відносини у сфері забезпечення фінансової безпеки держави. *Науковий вісник Національної академії внутрішніх справ*. .№ 6. 2011. С. 49-55.

91. Макаренко А. Адміністративне право. Навчальний посібник. Київ. *КНЕУ*, 2008. 264 с.

92. Маруховський О. О. Політичні аспекти зарубіжних концепцій інформаційного суспільства : автореф. дис. на здобуття наук. ступеня канд. політ. наук .23.00.01. Ін-т політ. і етнонац. дослідж. ім. І.Ф. Кураса НАН України. Київ. 2008. 20с.

93. Марченко О. Адміністративно-правовий статус Міністерства юстиції України. автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2017. 18с.

94. Матвійчук В.К., Ілларіонов В.М. Впровадження інформаційно коммунікаційних технологій як додатковий засіб підвищення якості освіти (на прикладі юридичного факультету). URL: http:/ /legal. nam.edu.ua/journal/n-4-5-2011.pdf

95. Мацелик Т. Суб'єктивне публічне право як юридичний феномен. *Юридичний вісник. Повітряне і космічне право*. 2011. № 3. С. 67-71.

96. Машков А. Теорія держави і права: підручник. Київ: Дакор. 2015. 492 с.

97. Мельник Р., Бевзенко В. Загальне адміністративне право. Навч. посібн. Київ: *Baime*. 2014. 376 с.

98. Мерзляк А. В., Боклаг В. А. Інформаційне забезпечення державного управління земельними ресурсами України: монографія. Запоріжжя : *Вид-во КПУ*, 2010.152 с.

99. Методичний комп'ютерний посібник. Електрон. Дані і прогр. Харків: *Основа*, 2011. URL: http://unbib.mk.ua/index.php/2015-02-09-13-48-46/85-2015-02-09-12-57-54/2014-2016-10-03-08-42-00.html

100. Міністрество Юстиції України: Офіційний портал. URL. https:// pidruchniki. com/ 1539100656114 /pravo/ ministerstvo_ yustitsiyi_ukrayini_ struktura_ osnovni_zavdannya_povnovazhennya

101. Молдован В. В. Основи держави і права: Курс лекцій. Київ. *Юмана*, 1996. 176 с

102. Науково-практичний коментар до Закону України «Про електронний цифровий підпис. 2009. URL:

http://cesaris.itsway.kiev.ua/public /Downloads/ Science-practic %20 comment% 20for %20 Law% 20about %20Electr %20 Signature. pdf

103. Новицький А.М. Електронний документообіг як елемент забезпечення правового регулювання становлення інститутів інформаційного суспільства. *Науковий вісник Національного університету ДПС України* (економіка, право), 4(63) 2013. С.13-20

104. Норми матеріального і процесуального права. Особливість процедурних норм матеріального права. URL: https:// pidruchniki. com/1858102143108/ pravo/normi _materialnogo_ protsesualnogo_ prava_ osoblivist _protsedurnih_ norm_ materialnogo_ prava

105. Об'єкт та зміст адміністративно-правових відносин. Державне управління як різновид соціального управління та його ознаки. URL: https://lektsii.org/8-59792.html

106. Обмін паперових паспортів громадянина Україна на документи нового зразка не є обов'язковим.:URL. https://tsn.ua/politika/ukrayinci-zmozhut-obminyati-ninishni-pasporti-na-novi-id-kartki-koli-ta-yak-ce-zrobiti-512977.html

107. Пелехата О.Г. Розвиток стандартів електронного обміну даних у web-технологіях. *Вісник ХДАК*. 2011. № 33. С. 66–73.

108. Поліщук І. О. Електронне урядування в Україні: проблеми та перспективи / І. О. Поліщук, В. К. Лур'є. Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". *Серія : Соціологія. 2016*. № 3. С. 229-230.

109. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141. URL: http://zakon5.rada.gov.ua/laws/show/z0862-07

110. Поняття права інтелектуальної власності. Суб'єкти і об'єкти права інтелектуальної власності. Підстави виникнення права

інтелектуальної власності. *Захист права інтелектуальної власності*. URL. https:// pidruchniki. com/1088040554719 /pravo/ponyattya_ prava_ intelektualnoyi_ vlasnosti_ subyekti_ obyekti_ prava_intelektualnoyi_vlasnosti

111. Порядок внесення засобів електронного цифрового підпису до безконтактного електронного носія, що міститься в паспорті громадянина України, та надання послуг електронного цифрового підпису з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм. URL. https://www.kmu.gov.ua/ua/npas/249551811

112. Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності. URL. https://www.kmu.gov.ua/ua/npas/10243597

113. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, який затверджено наказом від 11.11.2014 № 1886/5

114. Посадова інструкція керівника апарату місцевого загального суду : затверджена наказом ДСА України від 19.06.2011. *Судова гілка влади*: офіційний веб-портал. 2011. URL: http:pl.dn.court.gov.uasud0542236, с. 107.

115. Правила UNCITRAL - Model Law on Electronic Commerce of the United Nations Commission on International Trade Law (Типовий закон ЮНСІТРАЛ «Про електронну комерцію» 1996 р. (з додатковою статтею 5 bis, прийнятою у 1998 р.).URL: https://dtkt.com.ua/show/1cid0201.html

116. Правила оформлення Регламенту роботи центрів сертифікації ключів банків України. Постанова. 2010 № 284 *Офіційний вісник України*. офіційне від 22.11.2010 р., № 87, стор. 51, стаття 3080, код акта 53384/2010

117. Правова відповідальність за порушення у сфері документаційного забезпечення управління.. URL:http://ua-referat .com/%

D0%9F% D1%80% D0%B0% D0%B2%D0 %BE% D0%B2 %D0%B0_ %D0%B2%D 1%96%D0%B4%

118. Президент підписав «Про електронні довірчі послуги» URL. http:/ /www. president.gov.ua/news/prezident-pidpisav-zakon-pro-elektronni-dovirchi-poslugi -44298

119. Про акредидований центр сертифікації ключів. URL. https://acskidd.gov.ua

120. Про АЦСК. Офіційний веб-сайт. 2017. URL: https://acskidd.gov.ua/

121. Про державну службу: Закон України від 17.11.2011 № 4050-VI втратив чинність від 31.12.2015. *Відомості Верховної Ради України*. 2012. № 26. Ст.273.

122. Про державну таємницю: Закон України від 21.01.1994 №3855XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.

123. Про електронний цифровий підпис. Закон України від 22.05.2003 № 852-IV. *Відомості Верховної Ради України*. 2003. № 36. ст. 276.

124. Про електронні довірчі послуги. Закон України. *Верховна Рада України* URL. http://zakon2.rada.gov.ua/laws/show/2155-19

125. Про електронні документи та електронний документообіг. Закон України. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275.

126. Про електронні підписи. типовий закон Комісії ООН по праву та міжнародній торгівлі (ЮНСІТРАЛ), 2001 р. URL. http:// www. uncitral. Org /uncitral/ ru/

127. Про електронну комерцію: Закон України від 3 верес. 2015 р. №675-VIII .*Відом. Верхов. Ради України*. 2015. №45.

128. Про електронну комерцію: Типовий (модельний) закон UNCITRAL Draft Model Lawon Electronic Commerce URL: http:// www. uncitral. Org /english/ text /electcom

129. Про затвердження Концепції реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг. Наказ від 10.04.2013 р. №668/5. URL. http:// zakon3. rada. gov. ua/ laws/show/v668-323-13

130. Про затвердження Концепції реформування законодавства у сфері використання інфраструктури відкритих ключів та надання електронних довірчих послуг. Наказ від 10.04.2013 р.№668/5 .URL. http:/ /zakon3. rada. gov. ua/laws/ show/v668-323-13

131. Про затвердження Положення про застосування електронного підпису в банківській системі України. Постанова Правління Національного банку № 78 від 14.08.2017р. URL. http://zakon3.rada.gov.ua/laws/show/v0078500-17

132. Про затвердження положення Про Міністерство юстиції України. Постанова Кабінету Міністрів. URL. http://zakon5.rada.gov.ua/laws/show/228-2014-п

133. Про затвердження типових форм первинного обліку науково-інформаційної діяльності та Інструкції про порядок їх використання і застосування. *Офіційний вісник України* від 03.12.1998 р., № 46, стор. 69, стаття 1705, код акта 6331/1998.

134. Про затвердження Типової інструкції з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади: Постанова Кабінету Міністрів України від 30.11.2011 № 1242. *Офіційний вісник України*. офіційне видання. 2011. № 94. С 172

135. Про захист персональних даних. Закон України. Відомості Верховної Ради України. 2010. № 34. Ст. 481

136. Про інформацію: Закон України від 2.10.1992. *Відомості Верховної Ради*. 1992. № 48.

137. Про Національну програму інформатизації: Закон України від 4.02.1998 № 74/98-ВР. *Відомості Верховної Ради України*. 1998. № 27–28. Ст. 181.

138. Про Національну систему конфіденційного зв'язку. Закон від 10.01.2002 № 2919-III. *Відомості Верховної Ради України*. 2002. №15. Ст.103.

139. Про оптимізацію системи центральних органів виконавчої влади. Указ Президента України від 9 грудня 2010 року № 1085/2010.

140. Про основні засади державного нагляду (контролю) у сфері господарської діяльності. Закон України від 5 квітня 2007 р. № 877-V URL.: http:/ /zakon2. rada. gov. ua/laws/main/a#Find

141. Про отримання ключа для електронного цифрового підпису для заповнення електронних декларацій URL. http://novadoba.com.ua/34643-pro-otrymannya-klyucha-elektronnogo-cyfrovogo-pidpysu-dlya-zapovnennya-elektronnykh-deklaraciy-za-2016-rik.html

142. Про першочергові завдання щодо впровадження новітніх інформаційних технологій: Указ Президента України від 20 жовтня 2005 р. № 1497/2005. *Урядовий кур'єр*. 2005. № 207.

143. Про систему електронних підписів, що застосовується в межах Співтовариства. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 р.URL. http://zakon3.rada.gov.ua/laws/show/994_240

144. Про утворення територіальних органів Державної фіскальної служби та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України. Постанова Кабінету Міністрів України від 6 серпня 2014 р. № 311. URL: http://zakon5.rada.gov.ua/laws/show/311-2014-%D0%BF

145. Процедура отримання електронних ключів. Державне підприємство «Інфоресурс». *Офіційний веб-сайт*. 2016. URL: https:/ /www. inforesurs. gov. ua/ uploads/files/1431698839_procedura-otrimannya-elektronnogo-cifrovogo-pdpisu.pdf

146. Радько Д. Адміністративно-правові відносини за участю фінансових компаній: автореф. дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2011. 20 с.

147. Рассолов И. М. Интернет право. Рассолов. Москва: *Юнити*, 2004. 143с

148. Розвиток електронного документообігу. URL: http://www.me-doc.com.ua/razvitie_edo/?&lang=ukr.

149. Рысков О. Управление документами в европейских странах : обзор нормативной бази . делопроизводство. 2006. № 4. С. 8–14.

150. Савюк М.Ф. Адміністративно-правові засади інформаційного суспільства. Дис. на здобуття наукового ступеня к.ю.н. 12.00.07. *Відкритий міжнародний університет «Україна»*. Київ.2016.208 с.

151. Системи, в яких працює ЕЦП АЦСК органів юстиції України. Акредитований центр сертифікації ключів державного підприємства. *Офіційний веб-сайт*. 2017. URL: https://ca.informjust.ua/partnership

152. Словник української мови в 11 т. АН УРСР. Інститут мовознавства. Київ. *Наукова думка* 1970 – 1980. 671 с.

153. Словник. За ред. В. І. Войтка. Київ.: *Головн. вид. видавн. об'єд. "Вища школа"*, 1982. С. 108.

154. Солов'яненко Д. Цифровий ідентифікатор об'єкта (DOI): ISBN суспільства знань. Бібліотечний вісник.2009. № 4. С. 3–15

155. Станіслав Лур'є. Безпечність використання електронного цифрового підпису. URL: https:// investgazeta.ua/ blogs/bezpechnist-vikoristannya-elektronnogo-tsifrovogo-pidpisu

156. Судова практика. URL. http:// blog. Liga .net/ user/ kvengrinyak/ article/ 29683 .

157. Теорія держави і права : модульний курс / В.М. Кириченко, О.М. Куракін. Київ : *Центр учбової літератури*, 2010. 264 с.

158. Тиханський В.В. Електронний цифровий підпис як інструмент цифрової держави. URL. http://www.dy.nayka.com.ua/?op=1&z=1128]

159. Тодчук О. І. Система електронного документообігу з використанням електронно-цифрового підпису в пенсійному фонді України. *Вісник східноукраїнського національного університету імені Володимира Даля*. 2012. № 14. С. 132-138.

160. Уряд схвалив ключові напрями е-декларування в Україні до 2020р. URL. https:/ /nachasi. com/2017/ 09/20/ kontseptsiya-rozvytku-e-uryaduvannya/

161. Урядовий портал. URL. https://www.kmu.gov.ua/ua/npas/250287124

162. Усе що треба знати про ID-картки URL. http://tvoemisto.tv/news/use_shcho_treba_znaty_pro_idkartku_migratsiyna_sluzhba_vidpovila_na_naypopulyarnishi_zapytannya_lvivyan_83798.html

163. Фіцула М. Педагогіка: навчальний посібник. Київ. *Академвидав*. 2009. 560 с.

164. Харківської державної академії культури. Збірник наукових праць. За заг. ред. В. М. Шейка. Випуск 3. Харків, ХДАК, URL: http://www.uk.x-pdf.ru/5informatika/1340664-32-harkivskoi-derzhavnoi-akademii -kulturi-zbirnik-naukovih-prac-zagalnoyu-redakci-yu-sheyka-zasnovano-1999-vipusk-ha.php

165. Цвік М. Загальна теорія держави і права: підручник для студ. юрид. спец. вищ. навч. закладів освіти. Національна юридична академія України ім. Ярослава Мудрого. Харків: *Право*. 2002. 432 с

166. Центральний засвідчувальний орган. Офіційний веб-сайт. 2017. URL: https://czo.gov.ua/

167. Цивільний кодекс України. *Верховна Рада України*. URL. http://zakon2.rada.gov.ua/laws/show/435-15/page

168. Цифрова легітимність: основні факти про електронний підпис. URL: http://bigenergy.com.ua/statti/rzne/905-cifrova-legitimnist-osnovni-fakti-pro-elektronnij -pidpis.html

169. Черников А. Бизнес по EDImrn правилам. Компьютерное Обозрение. 2002. № 25. URL: http://ko.com.ua/node/10315

170. Шевченко Е. Визначення поняття адміністративно-правових відносин з урахуванням пріоритетного значення та ролі в них суб'єкта адміністративного права (на прикладі адміністративного суду). *Форум права*. 2011. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2011_1_180.pdf

171. Шуба В. Адміністративно-правові відносини в діяльності органів прокуратури України: загальнотеоретичні аспекти: автореф. дис... канд. юрид. наук: 12.00.07. Харків, 2007. 20 с.

172. Щерба С. Філософія. підручник. Київ: *Кондор*. 2011. 548

173. Юридическая сила электронной подписи. *Юридична практика*. Газета Українських юристів. URL: http:/ /pravo. ua/ article. php? id= 10003334

174. Юридичний словник-довідник. URL. http:// www. subject. com.ua/parvo /dict/1200.html

175. Як відобразити в обліку витрати на електронні ключі. URL. http://rnba.com.ua/Ua/2016/10/kak-otrazit-v-uchete-rasxody-na-elektronnye-klyuchi/

176. Ясіновська А. Кодекси матеріального права: деякі теоретичні аспекти file:///C:/Users/Galunko/Downloads/Vlnu_yu_2014_59_8.pdf

177. Dawn M. Advanced Electronic Signatures for eIDAS. Cryptomathic. Retrieved 7 June 2016.

178. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013 , 19/01/2000. P. 0012 – 0020.URL : / www.eur-lex. europa. eu/ Lex UriServ /LexUriServ.do?uri=CELEX:31999 L0093:EN:HTML

179. Electronic Signatures in Global and National Commerce Act, 2000. URL: www.law.upenn.edu/bll/ulc /ulc_final.htm

180. Federal Republic of Germany, «Signature Law Passes Bundesrat and Can Take Effect Without Delay» (March 2001). Bundesregierung Background

Information – Germany in the Global Economy, Fr 2001/03/09.URL: http:// www.iid.de/iukdg/eval VIB2Referente-nentwurfenglisch.pdf

181. Government Paperwork Elimination Act (GPEA) of 1980 URL: http: // www.whitehouse. gov/omb/fedreg_gpea

182. Havlosky I. Administrative and legal nature of electronic digital signature / Visegrad journal on human rights. 2016. № 6/2. P. 62-66.

183. Paskin, N. Digital Object Identifier (DOI®). Encyclopedia of Library and Information Sciences: Third Edition. URL:www.doi.org/overview/080625DOI-ELIS-Paskin.pdf

184. Uniform Electronic Transactions Act, 1999 UETA. URL: http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Гавловський І. А. Адміністративно-правові відносини у сфері електронно-цифрового підпису. *Прикарпатський юридичний вісник.* 2015. № 3. Том 4. С. 167-171.

2. Гавловський І. А. Об’єкти адміністративно-правових відносин у сфері електронно-цифрового підпису. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2015. Випуск 33. Ч. 2. С. 84-89.

3. Гавловський І. А. Адміністративно-правова природа електронного цифрового підпису. *Науковий вісник публічного та приватного права.* 2016. Випуск 2. Том 4. С. 134-138.

4. Гавловский И. А. Зарубежный опыт электронной цифровой подписи. *Право и Политика.* 2017. № 1. С. 55-58 (Кыргызская Республика).

5. Гавловський І. А. Поняття та зміст адміністративно-правових відносин з використанням електронного цифрового підпису. *Науковий вісник Херсонського державного університету.* Серія «Юридичні науки». 2017. Випуск 2. Т. 4. С. 112-117.

6. Гавловский И. А. Содержание административно-правовых отношений в сфере электронно-цифровой подписи. *Право и Закон.* 2017. № 4. С. 67-70 (Кыргызская Республика).

7. Гавловський І. А. Суб’єкти адміністративно-правових відносини у сфері електронно-цифровий підпису. *Науковий вісник публічного та приватного права.* 2018. Випуск 1. Том 1. С. 122-127.

які засвідчують апробацію матеріалів дисертації:

8. Гавловський І. А. Генеза виникнення електронного документообігу та цифрового підпису. *Сучасне державотворення та правотворення: питання теорії та практики:* матер. Міжнар. наук.-практ. конф. (м. Одеса, Україна, 11-12 груд. 2015 р.). Одеса: ГО «Причорноморська фундація права», 2015. С. 86-90.

9. Гавловський І. А. Програмні інформаційні комплекси, які використовуються в України. *Особливості розвитку публічного та приватного права в Україні:* матер. Міжнар. наук.-практ. конф. (м. Харків, 15-16 лип. 2016 року). Харків: ГО «Асоціація аспірантів-юристів», 2016. С. 23-26.

10. Гавловський І. А. Правове регулювання електронних документів та цифрового підпису. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи:* матер. Міжнар. наук.-практ. конф. (м. Київ, 10-11 берез. 2017 р.). К.: Центр правових наукових досліджень, 2017. С. 57-60.

Додаток Б

Соціологічне опитування

БЛАНК

соціологічного опитування громадян з питань використання електронного цифрового підпису в Україні

Шановний респонденте!

Вашій увазі надається бланк соціологічного опитування щодо проблем використання електронного цифрового підпису в Україні. Опитування є анонімним, відповідно просимо Вас надати правдиві відповіді. На кожне питання треба надати однозначну відповідь «Так» або «Ні» в графі навпроти шляхом постановки позначки (наприклад, «+» або «-»). Якщо однозначної відповіді немає, питання пропускається.

Результати Вашої активної громадянської позиції будуть використані для розроблення рекомендацій стосовно вдосконалення застосування та використання електронного цифрового підпису в Україні.

Дякуємо Вам за участь!

Таблиця 1

Чи знаєте Ви про існування електронного цифрового підпису в Україні?	
ТАК	НІ
Чи Ви користуєтесь електронним цифровим підписом ?	
ТАК	НІ
На Вашу думку, чи необхідно змінити чинне законодавство про використання електронного цифрового електронного підпису ?	

ТАК	НІ
Чи необхідна додаткова реклама про застосування електронного цифрового підпису	
ТАК	НІ

БЛАНК

соціологічного опитування громадян з питань

використання електронного цифрового підпису в Україні

Вибірковим анкетуванням у два етапи було опитано 544 респонденти. Час проведення анкетування – друге півріччя 2017 року та пере півріччя 2018 року.

Таблиця 2

Чи знаєте Ви про існування електронного цифрового підпису в Україні?	
ТАК	НІ
102 або 47%	442 або 53%
Чи Ви користуєтесь електронним цифровим підписом ?	
ТАК	НІ
34 або 6%	510 або 94%
На Вашу думку, чи необхідно змінити чинне законодавство про використання електронного цифрового електронного підпису ?	
ТАК	НІ
72 або 13%	472 або 86%
Чи необхідна додаткова реклама про застосування електронного цифрового підпису	
ТАК	НІ
455 або 83%	89 або 16%

Додаток В

Проект

З А К О Н У У К Р А Ї Н И

«Про внесення змін до Кодексу України про адміністративні правопорушення відносно відповідальності в галузі торгівлі, громадського харчування, сфері послуг, в галузі фінансів і підприємницькій діяльності»

Верховна Рада України п о с т а н о в л я є:

Внести до Кодексу України про адміністративні правопорушення (80731-10) (Відомості Верховної Ради УРСР, 1984 р., додаток до № 51, ст. 1122) такі зміни:

Главу 12

Адміністративні правопорушення в галузі торгівлі, громадського харчування, сфері послуг, у галузі фінансів і підприємницькій діяльності

Доповнити

Статтею 163-16 «Відмова надавати адміністративні послуги за електронним цифровим підписом»

викласти в такій диспозиції:

ч. 1 : «Відмова надавати адміністративні послуги за електронним цифровим підписом, –

тягне за собою накладення штрафу від тридцяти до сорока неоподатковуваних мінімумів доходів громадян».

2. Цей Закон набирає чинності з дня його опублікування.

Голова
Верховної Ради України А.В. ПАРУБІЙ

Проект

З А К О Н У У К Р А Ї Н И

«Про внесення змін до Кодексу України про адміністративні правопорушення щодо відповідальності в галузі торгівлі, громадського харчування, сфері послуг, у галузі фінансів і підприємницькій діяльності»

Верховна Рада України п о с т а н о в л я є:

Внести до Кодексу України про адміністративні правопорушення (80731-10) (Відомості Верховної Ради УРСР, 1984 р., додаток до № 51, ст. 1122) такі зміни:

Главу 12

Адміністративні правопорушення в галузі торгівлі, громадського харчування, сфері послуг, в галузі фінансів і підприємницькій діяльності

Доповнити

Статтею 163-17 «Неналежне зберігання особистого електронного цифрового ключа в таємниці, що призвело до його втрати або/та використання сторонніми особами».

та викласти в такій диспозиції:

ч. 1 : «Неналежне зберігання особистого електронного цифрового ключа в таємниці, що призвело до його втрати або/та використання сторонніми особами, –

тягне за собою накладення штрафу від тридцяти до сорока неоподатковуваних мінімумів доходів громадян».

2. Цей Закон набирає чинності з дня його опублікування.

Голова
Верховної Ради України А.В. ПАРУБІЙ

Додаток Г

ЗАТВЕРДЖУЮ

Директор
Науково-дослідного інституту
публічного права,
доктор юридичних наук, професор

В.В. Галунько
«26» грудня 2017р.

А К Т

про впровадження результатів дисертаційного дослідження на здобуття наукового ступеня кандидата юридичних наук Гавловського Ігоря Анатолійовича у науково-дослідну діяльність Науково-дослідного інституту публічного права

Комісія у складі: завідувача відділу науково-правових експертиз та законопроектних робіт – кандидата юридичних наук Куркової К.М., наукового співробітника відділу науково-правових експертиз та законопроектних робіт Глобенка І.О., склала цей акт про те, що матеріали дисертації Гавловського Ігоря Анатолійовича на тему «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» мають необхідний теоретичний рівень і практичну значимість та використовуються у науково-дослідній роботі наукових відділів Науково-дослідного інституту публічного права під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем адміністративно-правових відносин з використанням електронного цифрового підпису в Україні та удосконалення законодавства у цій сфері та використовуються Інститутом в межах реалізації теми науково-дослідницької роботи Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0115U005495).

ВИСНОВОК

Результати дисертації Гавловського Ігоря Анатолійовича на тему «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» на здобуття наукового ступеня кандидата юридичних наук вважати впровадженими в наукову діяльність Науково-дослідного інституту публічного права під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем адміністративно-правових відносин з використанням електронного цифрового підпису в Україні та удосконалення законодавства у цій сфері.

Члени комісії:

завідувач відділу
науково-правових експертиз
та законопроектних робіт,
кандидат юридичних наук — **К. М. Куркова**

науковий співробітник
відділу науково-правових експертиз
та законопроектних робіт — **І.О. Глобенко**

Додаток Ґ

ЗАТВЕРДЖУЮ
Директор Інституту права
та післядипломної освіти
Міністерства юстиції України,
д.ю.н., заслужений юрист України
К.І. Чижмарь
від 11 січня 2018 р.

АКТ
упровадження результатів дисертаційного дослідження на здобуття наукового ступеня кандидата юридичних наук Гавловського Ігоря Анатолійовича на тему «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» у правозастосовну діяльність Інституту права та післядипломної освіти Міністерства юстиції України

Комісією, у складі першого заступника директора Журавльова Д.В. та заступника директора – завідувача навчально-методичного кабінету підвищення кваліфікації Головченко Л.М., було розглянуто результати використання матеріалів дисертаційного дослідження на тему «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» Гавловського Ігоря Анатолійовича. Під час обговорення наданих матеріалів комісією було констатовано, що окремі положення вказаного вище дослідження було впроваджено в правозастосовну діяльність Інституту права та післядипломної освіти Міністерства юстиції України, а саме для розроблення методичних рекомендацій щодо вдосконалення адміністративно-правових відносин з використанням електронного цифрового підпису в Україні.

ВИСНОВОК

Результати дисертаційного дослідження на тему «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» Гавловського Ігоря Анатолійовича вважати впровадженими у правозастосовну діяльність Інституту права та післядипломної освіти Міністерства юстиції України.

Члени комісії:
Перший заступник директора Журавльов Д.В.

Заступник директора – завідувач
навчально-методичного кабінету
підвищення кваліфікації Головченко Л.М.

Додаток Д

ЗАТВЕРДЖУЮ
Заступник директора з навчальної роботи Інституту права та суспільних відносин Відкритого міжнародного університету розвитку людини «Україна»
к.ю.н. І. Орловська
від 25 2017 р.

АКТ

впровадження результатів дисертаційного дослідження на здобуття наукового ступеня кандидата юридичних наук Гавловського Ігоря Анатолійовича на тему «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» у навчальний процес кафедри цивільного, господарського, адміністративного права та правоохоронної діяльності Інституту права та суспільних відносин Відкритого міжнародного університету розвитку людини «Україна»

Комісією кафедри було розглянуто результати використання матеріалів дисертаційного дослідження на тему: «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» Гавловського Ігоря Анатолійовича. Під час обговорення наданих матеріалів комісією було констатовано, що окремі положення дослідження було використано в розробленні лекційних курсів з дисципліни «Проблеми теорії адміністративного права», при підготовці відповідних підручників, навчальних посібників.

ВИСНОВОК: результати дисертаційного дослідження на тему: «Адміністративно-правові відносини з використанням електронного цифрового підпису в Україні» Гавловського Ігоря Анатолійовича, вважати впровадженими в навчальний процес кафедри цивільного, господарського, адміністративного права та правоохоронної діяльності Інституту права та суспільних відносин Відкритого міжнародного університету розвитку людини «Україна» з дисципліни «Проблеми теорії адміністративного права».

Члени комісії:

Заступник директора з профорієнтаційної та методичної роботи Інституту права та суспільних відносин — **О. О. Фаст**

Доцент кафедри конституційного права та теоретико-правових дисциплін Інституту права та суспільних відносин — **Є. В. Сердюк**