https://doi.org/10.31891/2219-9365-2025-83-51
УДК 004.056

ЧЕШУН Віктор
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ПЕТЛЯК Наталія
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
ТІТОВА Віра
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: titovav@khmnu.edu.ua

ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЇ АТРИБУТИВНОГО ЦИФРОВОГО ПІДПИСУ В УКРАЇНІ

Метою даної роботи є аналіз положень законів та нормативно-правових документів України, які регулюють використання електронного підпису, на відповідність вимогам щодо впровадження технології цифрового підпису на основі особистих атрибутів підписувача як суб'єкта персональних даних. Аналіз проведено для визначення відповідності запропонованого варіанту реалізації технології вимогам законодавства України щодо обробки і зберігання персональних даних підписувача, які можуть входити до складу цифрового підпису на основі атрибутів.

Ключові слова: захист інформації, електронний цифровий підпис, атрибути користувача, правове регулювання.

CHESHUN Viktor, KLOTS Yurii, PETLIAK Nataliia, TITOVA Vira
Khmelnytskyi National University

LEGAL REGULATION OF ATTRIBUTIVE DIGITAL SIGNATURE TECHNOLOGY IN UKRAINE

The purpose of this work is to analyze the provisions of laws and regulatory documents of Ukraine, which regulate the use of electronic signatures, for compliance with the requirements for the implementation of digital signature technology based on the personal attributes of the signatory as a subject of personal data. The analysis was carried out to determine the compliance of the proposed version of the implementation of the technology with the requirements of the legislation of Ukraine regarding the processing and storage of the signer's personal data, which can be included in the digital signature based on attributes. The article discusses the main provisions of digital signature technology based on personal attributes, provides a classification of attributes used to form a signature, and analyzes the differences between a cryptographic electronic digital signature and a signature on attributes. To analyze the features of digital signature technology based on personal attributes, a method of formalized representation of various classes of attributes in a mathematical model is provided, and a signature synthesis scheme based on a formalized representation of the signer's personal attributes is presented. It was determined that the attribute digital signature technology provides maximum flexibility and adaptability to the signer's needs and can be both an alternative to the cryptographic electronic digital signature technology and its addition. The digital signature technology based on the personal attributes of the signer also increases the security and accuracy of the signer's identification, since not one, but an arbitrary number of attributes of different classes is used to identify the person. In order to determine the possibility of applying the attribute digital signature technology in the legal field of Ukraine, a comparative study of the basic provisions of the technology and the requirements of the current laws was conducted. The article proves the possibility of introducing electronic digital signature technology in Ukraine based on the attributes of the signatory person in accordance with current legislation and other regulatory documents. It was determined that the adaptation of the laws and standards of Ukraine to the normative legal documents of the European Union plays not the least role in creating the necessary conditions for this.

Keywords: information protection; digital signature; user attributes; legal regulation

Стаття надійшла до редакції / Received 11.07.2025
Прийнята до друку / Accepted 14.08.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Розвиток інформаційних технологій в останні десятиліття зумовлює стрімкий та невпинний рух суспільства у напрямку цифрової трансформації і відіграє важливу роль у поширенні та вдосконаленні нових систем та сервісів, до числа яких відноситься і електронний цифровий підпис (ЕЦП)[1].

Початково системи ЕЦП використовувалися переважно в обмеженому колі сфер, таких як фінансовий сектор та урядові структури. Зі зростанням світового обсягу електронної комунікації і транзакцій, вони стали необхідним елементом в багатьох галузях і застосунках, включаючи фінанси, медицину, урядові послуги, електронну комерцію та багато інших [2,3,4].

Впровадження ЕЦП сприяло збільшенню швидкості та зручності електронних процесів, а також забезпечило високий рівень довіри між їх учасниками процесів [5].

Технологія ЕЦП не є сталою і зазнає трансформації та перебуває у постійному розвитку. Вдосконалення криптографічних алгоритмів, покращення методів аутентифікації та зростання швидкості обробки даних сприяють збільшенню ефективності та безпеки ЕЦП. Подальший розвиток інформаційних технологій, таких як блокчейн та розумні контракти, може відкрити нові можливості для застосування ЕЦП, покращуючи їх безпеку, автентичність та надійність [2,6].

Альтернативним напрямком розвитку технологій ЕЦП є збільшення їх універсальності як щодо сфер застосування, так і щодо гнучкості та адаптованості формату підпису відповідно потребам або бажанням підписувача. Одним із перспективних напрямків у наданні ЕЦП нових властивостей і можливостей є технологія створення підпису на основі особових атрибутів, що впроваджується і поширюється в країнах ЄС та США [7,8,9].

Завдяки застосуванню нових принципів системи ЕЦП можуть стати ще більш інтегрованими та універсальними в цифровому світі, де зручність та ефективність сервісів, захист даних та конфіденційність інформації, відповідність операцій законодавчій та нормативній базі характеризуються високим пріоритетом, що робить актуальними дослідження в цій сфері.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Цифровий підпис це інструмент, який відіграє важливу роль у сучасному цифровому світі.

Перш за все, ЕЦП – це технологічний механізм, який дає змогу електронно підписувати документи або інші електронні повідомлення. ЕЦП використовується для підпису електронних документів, що надає їм правову силу, еквівалентну традиційному паперовому підпису. Це дозволяє ефективно здійснювати різноманітні операції в електронному форматі, такі як укладання угод, підтвердження транзакцій та підписання документації [4].

ЕЦП забезпечує важливі засади безпеки в електронному середовищі. Ігнорування ЕЦП – одна з найбільш поширених слабких сторін систем електронного документообігу [10,11]. В класичному варіанті в основі ЕЦП лежить криптографічна технологія, що забезпечує конфіденційність, цілісність та автентичність інформації. Вона гарантує, що інформація не буде підроблена або змінена після підпису, оскільки будь-яка модифікація документа призведе до недійсного підпису. Це особливо важливо в сферах, де велике значення має достовірність та непорушність даних, наприклад, у фінансовій сфері або у сфері медичної інформації.

ЕЦП також допомагає вирішувати проблеми ідентифікації користувачів в мережі Інтернет, завдяки чому можливе здійснення безпечних автентифікованих операцій, таких як підписання електронних листів, входу до систем та здійснення фінансових транзакцій тощо.

У цілому, ЕЦП відіграє надважливу роль у забезпеченні безпеки, достовірності та ефективності в електронному середовищі, роблячи його набагато більш зручним і безпечним для всіх учасників.

З іншої сторони, сфери застосування класичних технологій ЕЦП, визначені їх безпосереднім призначенням, є досить вузькими, а сам ЕЦП є малоінформативним, жорстко залежним від алгоритмів формування і неадаптивним до побажань і потреб підписувача. При формуванні, накладанні і перевірці ЕЦП підписувач і верифікатор потребують послуг акредитованих центрів сертифікації ключів і не мають змоги ні сформувати ЕЦП власноруч, ні отримати з нього інформацію про підписувача.

Альтернативним напрямком розвитку технологій цифрового підпису є формування сигнатури підпису на основі даних підписувача (персональних даних тощо), що робить підпис безпосередньо пов'язаним з особою автора та максимально інформативним для верифікатора [12]. Сам підписувач при цьому постає як автор та власник підпису подібно до ручного підпису. Такий підхід сприяє створенню систем електронного підпису, де персональні атрибути підписувача використовуються для створення унікального цифрового підпису, який забезпечує відмінну індивідуалізацію та ідентифікацію підписувача.

Поняття і базова ідеологія підписів із застосуванням атрибутів були визначені в роботі [13] і отримало подальший розвиток в [14], де підпис із застосуванням атрибутів описується як «універсальний примітив, що дозволяє стороні підписувати повідомлення з детальним контролем над ідентифікаційною інформацією».

Огляд наявних рішень з реалізації технології АЕЦП дозволяє відзначити наявність як суто теоретичних рішень, прикладом якого може слугувати проєкт ABCJTrust [15] так і повноцінних діючих сервісів, прикладом якого є проєкт Yivi [16]. Існуючі реалізації технології АЕЦП відрізняються своїм основним призначенням та, відповідно, функціоналом. Порівняльні дані щодо можливостей окремих варіантів реалізації технології АЕЦП наведено в таблиці 1.

Таблиця 1

Функціональні особливості типових систем АЕЦП

№	Технологія	Аутентифікація	Сигнатура ЕЦП	Децентралізація	Відкритий код	Робоча версія
1	YIVI	+	+	+	+	+
2	DECODE	+	-	-	+	+
3	Schluss	+	-	-	+	+
4	Serto	+	-	+	+	-
5	Sovrin	+	-	+	+	+
6	SelfKey	+	-	+	+	+

Базові принципи атрибутивного ЕЦП (АЕЦП) суттєвою мірою відрізняються від класичного криптографічного ЕЦП [9,17]:

– цифровим підписом вважається будь-яке розкриття даних про особу, навіть якщо це розкриття не дозволяє ідентифікувати підписувача і є відповіддю на елементарне питання. Прикладом такого розкриття може бути звичне користувачам інтернет-сервісів питання про повноліття користувача (тобто, чи є користувачу 18 років);

– хоча АЕЦП і може застосовуватись для підписання електронних документів та в ряді традиційних для криптографічних ЕЦП застосувань, його призначення є ширшим і передбачає використання технології АЕЦП в будь-яких сервісах, що передбачають розкриття особових даних підписувача. Прикладом може бути заповнення анкетних або реєстраційних даних в електронному сервісі на запит постачальника товарів або послуг, замовлення яких здійснюється підписувачем;

– АЕЦП не повинен містити надлишкових даних про підписувача, крім дійсно необхідних;

– сигнатура АЕЦП повинна бути максимально гнучкою і адаптованою до потреб підписувача;

– формування сигнатури АЕЦП повинне бути повністю підконтрольним підписувачу;

– атрибути для формування, накладання і перевірки АЕЦП не повинні передаватись третій довіреній стороні, тобто, мають експлуатуватись за призначенням тільки підписувачем і одержувачем (верифікатором) підпису.

Значною мірою перелічені вимоги до АЕЦП визначаються можливістю використання в підписі атрибутів, що є персональними даними підписувача, обробка яких регламентується на законодавчому рівні.

В роботах [18,19] розглядаються проблемні аспекти впровадження і використання технології АЕЦП. Особлива увага приділяється дослідженню відповідності технології АЕЦП нормативним документам та законам ЄС, зокрема, вимогам Загального регламенту про захист даних ЄС (GDPR) [20].

Для України технологія АЕЦП є новою. Наявні дослідження [2,21,22] питань правового регулювання ЕЦП в Україні акцентуються на розгляді традиційних технологій і не враховують особливостей АЕЦП. В зв'язку з цим, застосування технології АЕЦП потребує як урахування технічних особливостей її реалізації, так і дослідження проблем правового регулювання технології законодавством України

Основні положення технології атрибутивного цифрового підпису

Аналіз відповідності технології АЕЦП діючим законам та регулятивним актам, першочергово, потребує урахування особливостей запропонованої реалізації самої технології.

В роботах [23,24] представлено опис реалізації технології АЕЦП у формі мобільного додатку з можливістю формування сигнатури підпису та застосування в довірчих електронних послугах для розкриття атрибутів замовника надавачу послуг.

Технологія базується на класифікації атрибутів, які можуть бути використані при формуванні сигнатури атрибутивного підпису.

Проведений в [24] аналіз дозволив виділити три типових категорії атрибутів, що можуть використовуватись в АЕЦП:

ідентифікаційні атрибути;

неідентифікаційні атрибути;

контекстуальні атрибути.

В математичній моделі [24] технології атрибутивного цифрового підпису зазначені класи атрибутів представлені трьома множинами:

$$\mathrm{IA}:\{\mathrm{IA}_1,\ \mathrm{IA}_2,\ldots,\mathrm{IA}_i,\ldots,\mathrm{IA}_k\} \tag{1}$$

$$\mathrm{NIA}:\{\mathrm{NIA}_1,\ \mathrm{NIA}_2,\ldots,\mathrm{NIA}_j,\ldots,\mathrm{NIA}_m\} \tag{2}$$

$$\mathrm{CA}:\{\mathrm{CA}_1,\ \mathrm{CA}_2,\ldots,\mathrm{CA}_l,\ldots,\mathrm{CA}_n\} \tag{3}$$

де IA – множина ідентифікаційних атрибутів $IA_i \in IA$ підписувача; NIA – множина неідентифікаційних атрибутів $NIA_j \in NIA$ підписувача; CA – множина контекстуальних атрибутів $CA_l \in CA$ підписувача або підпису.

Формування цифрового підпису в примітивах математичної моделі технології до вибору елементів множин $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$, які відповідають потребам-побажанням підписувача, та поєднання їх у єдину двійкову послідовність – вектор (сигнатуру) цифрового підпису із застосуванням атрибутів ABDS (attribute-based digital signature):

$$ABDS = \left\{ IA_i \,\middle|\, IA_i \in IA \right\} \cup \left\{ NIA_j \,\middle|\, NIA_j \in NIA \right\} \cup \left\{ CA_i \,\middle|\, CA_i \in CA \right\} \qquad (4)$$

Сигнатура ABDS разом з хеш-сигнатурою відкритого тексту може піддаватися криптографічному шифруванню (закриттю) і додаватися до відкритого тексту. Можливе використання атрибутивного цифрового підпису у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта.

Ці дві перспективи роблять можливим використання технології цифрового підпису в системах електронного документообігу більш широкими, а саму технологію гнучкішою і універсальнішою.

Правове регулювання технології атрибутивного цифрового підпису

В дослідженнях [2,21,22] питань правового регулювання ЕЦП в Україні акцент робиться на трьох складових нормативно-правових документів:

– Закон України «Про електронний цифровий підпис» [25];

– Закону України «Про електронні довірчі послуги» [26] (Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [27]);

– Закони України та інші нормативні документи, що регулюють застосування ЕЦП в різних сферах та видах діяльності (Закон України «Про електронні документи та електронний документообіг»[28], Закон України «Про електронну комерцію» [29], «Положення про застосування електронного підпису та електронної печатки» [30] тощо).

Закон України «Про електронний цифровий підпис» 2003 року (з 2018 року втратив чинність) містить перше законодавчо затверджене визначення ЕЦП – «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». За положеннями цього Закону ЕЦП отримує таку ж юридичну силу, як особистий підпис громадянина на паперовому носії. Подальший розгляд ЕЦП в Законі ведеться в аспекті саме криптографічно генерованого алгоритмами асиметричного шифрування коду, що принципово не задовольняє ідеології формування і використання АЕЦП, хоча технологія АЕЦП і не заперечує можливість використання криптографічного ЕЦП і, в окремих реалізаціях, передбачає поєднання обох підходів [19].

Введення у 2015 році в дію Закон України «Про електронні довірчі послуги» (з 2022 року Закон України «Про електронну ідентифікацію та електронні довірчі послуги») супроводжується введенням нового визначення електронного підпису – «електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис». З урахуванням наданого в Законі визначення електронних даних, як «будь-яка інформація в електронній формі», цим законом відкривається можливість визнання легітимності АЕЦП. Зазначена в [2] узгодженість Закону з Регламентом Європейського Союзу «Про електронну ідентифікацію, верифікацію та довірчі послуги» (eIDAS – electronic IDentification, Authentication and trust Services) [31] зумовила єдність підходів до регулювання питань надання довірчих послуг та можливості застосування технології АЕЦП в Україні і ЄС в розрізі положень цих документів.

Аналіз Законів та нормативних документів України, що регулюють застосування ЕЦП в різних сферах та видах діяльності, дозволяє дійти висновку про відсутність суперечностей у розгляді електронного підпису в цих актах та в технології АЕЦП: Закон України «Про електронні документи та електронний документообіг» при підтвердженні оригінальності документу електронним підписом посилається (стаття 7) на вимоги до підпису до Закону України "Про електронну ідентифікацію та електронні довірчі послуги"; Закон України «Про електронну комерцію» в статті 12, ідентифікуючи підпис у сфері електронної комерції, спирається на вимоги законів України «Про електронні документи та електронний документообіг» та «Про електронну ідентифікацію та електронні довірчі послуги»; в «Положенні про застосування електронного підпису та електронної печатки» дається власне визначення простого електронного підпису (ЕП) – «будь-який вид ЕП, крім кваліфікованого ЕП, цифрового власноручного підпису, удосконаленого ЕП з кваліфікованим сертифікатом, удосконаленого ЕП, ЕП Національного банку», що не суперечить принципам технології АЕЦП тощо.

Слід зазначити, що, хоча розглянуті документи і закони передбачають широкий спектр варіантів реалізації електронних підписів, що відповідає потребам технології АЕЦП, вони не забезпечують нормативно-правове регулювання всіх аспектів технології.

Технологія АЕЦП базується на використанні особових атрибутів підписувача, частина з яких апріорі визначена як ідентифікаційні атрибути особи (персональні дані), що зумовлює потребу урахування при реалізації технології вимог Закону України «Про захист персональних даних» [32]. Проведені дослідження свідчать про відповідність реалізованих в технології АЕЦП механізмів зазначеному Закону:

– відповідно до пункту 6 статті 6 Закону, технологією АЕЦП «не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди»;

– згідно статті 11 Закону, підставою для обробки персональних даних «є згода суб'єкта персональних даних на обробку його персональних даних», передбачена неможливістю надання атрибутів підписанта володільцю даних для обробки ніким, окрім самого суб'єкта персональних даних (реалізується механізмами аутентифікації підписанта та вибору-затвердження атрибутів для формування АЕЦП);

– у відповідності до статті 13 Закону в технології АЕЦП «зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них», оскільки атрибути зберігаються тільки на особистому гаджеті суб'єкта персональних даних, захищені механізмами криптографічного закриття та багатофакторної аутентифікації і є безпосередньо підконтрольними тільки суб'єкту;

– отримання гарантовано достовірних атрибутів від емітентів базується на праві суб'єкта персональних даних «на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними» згідно пункту 6 статті 16 Закону;

– виконання вимоги пункту 3 статті 6 Закону, за якою «склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки», контролює сам суб'єкт персональних даних, оскільки жоден атрибут не може бути включений до АЕЦП без згоди підписувача тощо.

Удосконалення системи нормативно-правового регулювання технології АЕЦП є очікуваним при подальшій імплементації стандартів і законів ЄС в Україні, зокрема, при повноцінному запровадженні Загального регламенту про захист даних ЄС в електронних послугах України. Хоча Закон України «Про захист персональних даних» значною мірою узгоджений з GDPR, визнання Регламенту GDPR обов'язковим до дотримання при наданні електронних послуг в Україні і запровадження механізму сертифікації GDPR-CARPA [33] дозволить значно підвищити ефективність застосування технології АЕЦП і уникнути ризиків несанкціонованого розкриття особових атрибутів суб'єкта персональних даних через недосконалість нормативно-правового забезпечення.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Проведений аналіз положень Законів та нормативних документів України, якими регулюється питання використання електронних підписів, дозволив дійти висновку, що вони не вступають в протиріччя з вимогами реалізації технології цифрового підпису на основі особових атрибутів, що створює можливості для впровадження і використання зазначеної технології в електронних сервісах. Не в останню чергу створенню необхідних для впровадження технології цифрового підпису на основі особових атрибутів правових умов сприяло узгодження Законів і стандартів України та ЄС, і саме в цьому напрямку автори вбачають перспективи подальшого вдосконалення інструментів нормативно-правового регулювання технології цифрового підпису на основі особових атрибутів, зокрема, через визнання Загального регламенту про захист даних (GDPR) обов'язковим до дотримання при наданні електронних послуг в Україні і запровадження механізму сертифікації GDPR-CARPA.

Література

1. Olokundun M. COVID-19 Pandemic and Antecedents for Digital Transformation in the Workplace: A Conceptual Framework / M. Olokundun, S. Ibidunni, M. Ogbari, H. Falola, O. Salau // Open Access Maced J Med Sci. – 2021. – №9. P.41-46.

2. Новосад Р.В. Правовий статус електронного підпису в Україні: від ідеї до реалізації / Р.В. Новосад // Право та державне управління. – 2023. – № 3. – С. 112–116.

3. Політанський В.С. Теоретико-правові засади системи електронного документообігу в Україні / В.С. Політанський //Право і суспільство. – 2021. – № 1. С.22-27.

4. Cavus N. The Importance of Digital Signature in Sustainable Businesses: A Scale Development Study. / Nadire Cavus, Nuriye Sancar. // Sustainability. – 2023. – №15(6), 5008. – P.1-15.

5. Smith J. Sign me up , log me in , let me begin: the rise of digital signatures [Electronic resource] / John Smith // Watson Farley & Williams Article. – 2020. – Available from: https://surl.lu/kmcyup. (Accessed 23.06.2025). – Screen title.

6. Sancar N. Determining the awareness of users towards E-signature: A scale development study / N. Sancar, N. Cavus // AIP Conf. Proc. 2325. – 2021. – Article ID: 020038.

7. Zhenjie Huang. Secure server-aided attribute-based signature with perfect anonymity for cloud-assisted systems / Zhenjie Huang, Zhiwei Lin // Journal of Information Security and Applications. – 2022. – №65: 103066.

8. Ke Gu. Traceable attribute-based signature / Ke Gu, Keming Wang, Lulu Yang // Journal of Information Security and Applications. – 2019. – №49. – Article ID 102400.

9. Sucasas V. Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services / Victor Sucasas, Georgios Mantas, Maria Papaioannou, Jonathan Rodriguez // IEEE Transactions on Cloud Computing. – 2023. – Vol.11, №.1. – P.168-184.

10. Rauniyar K. Role of FinTech and innovations for improvising digital financial inclusion / K. Rauniyar // Int. J. Innov. Sci. Res. Technol. – 2021. – №6. – P.1419-1424.

11. Varshney P.S. Digital signatures / P.K. Varshney, A. Kukreja, S. Dewan // J. IITM Journal of Management and IT. – 2020. – №11. – P.86–90.

12. Belguith S. Analysis of attribute-based cryptographic techniques and their application to protect cloud services. / Sana Belguith, Nesrine Kaaniche, Mohammad Hammoudeh // Transactions on emerging telecommunications technologies. – 2022. – №33 (3). P.1-20.

13. Shanqing G. Attribute-based signature scheme ./ Guo Shanqing, Zeng Yingpei // In 2008 International Conference on Information Security and Assurance (ISA 2008). IEEE. – 2008. – P. 509-511.

14. Hemanta K Maji. Attribute-based signatures / Hemanta K Maji, Prabhakaran M., Rosulek Mike // In Cryptographers' track at the RSA conference. Springer. – 2011. – P.376-392.

15. ABC4Trust Attribute-based Credentials for Trust [Electronic resource] – Available from: https://surl.li/ntalnm – (Accessed 20.06.2025). – Screen title.

16. How Yivi works? [Electronic resource] Available from: http://surl.li/qnohm. – (Accessed 20.06.2025). – Screen title.

17. Lei He. Attribute-Based Proxy Signature Scheme Supporting Flexible Threshold Predicate for UAV Networks / Lei He, Yong Gan, Yanhua Zhang // Electronics. – 2023. – №12(23). – Article ID: 4854.

18. Panse T. Attribute Based Signature Architecture for Transferring Digital Document / Trishna Panse, Prashant Panse // Medi-Caps University Research Article. – 2022 – P.1-21.

19. Blazy O. Anonymous attribute-based designated verifier signature / O. Blazy, L. Brouilhet, E. Conchon, M. Klingler // Journal of Ambient Intelligence and Humanized Computing. – 2022. – № 68 (9). P. 6233-6244.

20. Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 4.5.2016. 88 p.

21. Ватаманюк-Зелінська У.З. Перспективи використання електронного цифрового підпису в державних структурах / У.З. Ватаманюк-Зелінська , В.С. Сушко // Ефективна економіка. – 2020. – №7.

22. Святошнюк А.Л. Щодо особливостей використання електронного цифрового підпису при укладенні цивільно-правових договорів у мережі інтернет / А.Л. Святошнюк // Вісник Одеського національного університету. Серія: Правознавство. – 2023. – №25-2 (37). – С.21-24.

23. Чешун В. Модель Технології цифрового підпису на основі особових атрибутів. / В. Чешун, Я. Рижий, Д. Чешун, О. Чешун // Вісник Хмельницького національного університету. Технічні науки. – 2025. – № 1 (347). – С. 401-404.

24. Рижий Я.О. Технологія цифрового підпису з використанням атрибутів в системах електронного документообігу / Я.О. Рижий, М.М. Мельник, В.М. Стецюк// Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної НП Інтернет конференції. – 2023. – С.223-225.

25. Про електронний цифровий підпис [Електронний ресурс]: Закон України від 22.05.2003 № 852-IV: станом на 07.11.2018р.. – Режим доступу : https://zakon.rada.gov.ua/laws/show/852-15#Text.

26. Про електронні довірчі послуги [Електронний ресурс] : Закон України від 05.10.2017 № 2155-VIII. Редакція від 01.12.2022р. – Режим доступу : https://kodeksy.com.ua/pro_elektronni_dovirchi_poslugi.htm

27. Про електронну ідентифікацію та електронні довірчі послуги [Електронний ресурс] : Закон України від 05.10.2017 № 2155-VIII. Редакція від 18.12.2024. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2155-19#Text.

28. Про електронні документи та електронний документообіг [Електронний ресурс] : Закон України від 22.05.2003 № 851-IV. Редакція від 31.12.2023. – Режим доступу : https://zakon.rada.gov.ua/laws/show/851-15#Text.

29. Про електронну комерцію [Електронний ресурс] : Закон України від 03.09.2015 № 675-VIII. Редакція від 01.01.2024. – Режим доступу : https://zakon.rada.gov.ua/laws/show/675-19#Text .

30. Про затвердження Положення про використання електронного підпису та електронної печатки [Електронний ресурс] : Постанова Національного банку України; Положення, Стандарт від 20.12.2023 № 172. – Режим доступу : https://zakon.rada.gov.ua/laws/show/v0172500-23#n20.

31. eIDAS Regulation [Electronic resource] – An official website of the European Union. – Available from: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation – (Accessed 25.06.2025).

32. Про захист персональних даних [Електронний ресурс] : Закон України від 01.06.2010 № 2297-VI. Редакція від 14.06.2025. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2297-17#Text.

33. GDPR-CARPA. Gdpr-certified assurance report-based processing activities. [Electronic resource] – Available from: https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/lu-gdpr-carpa-certificationscheme.pdf – (Accessed 25.06.2025).

References

1. Olokundun M. COVID-19 Pandemic and Antecedents for Digital Transformation in the Workplace: A Conceptual Framework / M. Olokundun, S. Ibidunni, M. Ogbari, H. Falola, O. Salau // Open Access Maced J Med Sci. – 2021. – №9. P.41-46.

2. Novosad R.V. Pravovyi status elektronnoho pidpysu v Ukraini: vid idei do realizatsii / R.V. Novosad // Pravo ta derzhavne upravlinnia. – 2023. – № 3. – S. 112–116.
3. Politanskyi V.S. Teoretyko-pravovi zasady systemy elektronnoho dokumentoobihu v Ukraini / V.S. Politanskyi //Pravo i suspilstvo. – 2021. – № 1. S.22-27.
4. Cavus N. The Importance of Digital Signature in Sustainable Businesses: A Scale Development Study. / Nadire Cavus, Nuriye Sancar. // Sustainability. – 2023. – №15(6), 5008. – S. 1-15.
5. Smith J. Sign me up , log me in , let me begin: the rise of digital signatures [Electronic resource] / John Smith // Watson Farley & Williams Article. – 2020. – Available from: https://surl.lu/kmcyup. (Accessed 23.06.2025). – Screen title.
6. Sancar N. Determining the awareness of users towards E-signature: A scale development study / N. Sancar, N. Cavus // AIP Conf. Proc. 2325. – 2021. – Article ID: 020038.
7. Zhenjie Huang. Secure server-aided attribute-based signature with perfect anonymity for cloud-assisted systems / Zhenjie Huang, Zhiwei Lin // Journal of Information Security and Applications. – 2022. – №65: 103066.
8. Ke Gu. Traceable attribute-based signature / Ke Gu, Keming Wang, Lulu Yang // Journal of Information Security and Applications. – 2019. – №49. – Article ID 102400.
9. Sucasas V. Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services / Victor Sucasas, Georgios Mantas, Maria Papaioannou, Jonathan Rodriguez // IEEE Transactions on Cloud Computing. – 2023. – Vol.11, №.1. – P.168-184.
10. Rauniyar K. Role of FinTech and innovations for improvising digital financial inclusion / K. Rauniyar // Int. J. Innov. Sci. Res. Technol. – 2021. – №6. – P.1419-1424.
11. Varshney P.S. Digital signatures / P.K. Varshney, A. Kukreja, S. Dewan // J. IITM Journal of Management and IT. – 2020. – №11. – P.86–90.
12. Belguith S. Analysis of attribute-based cryptographic techniques and their application to protect cloud services. / Sana Belguith, Nesrine Kaaniche, Mohammad Hammoudeh // Transactions on emerging telecommunications technologies. – 2022. – №33 (3). P.1-20.
13. Shanqing G. Attribute-based signature scheme ./ Guo Shanqing, Zeng Yingpei // In 2008 International Conference on Information Security and Assurance (ISA 2008). IEEE. – 2008. – P. 509-511.
14. Hemanta K Maji. Attribute-based signatures / Hemanta K Maji, Prabhakaran M., Rosulek Mike // In Cryptographers' track at the RSA conference. Springer. – 2011. – P.376-392.
15. ABC4Trust Attribute-based Credentials for Trust [Electronic resource] – Available from: https://surl.li/ntalnm – (Accessed 20.06.2025). – Screen title.
16. How Yivi works? [Electronic resource] Available from: http://surl.li/qnohm. – (Accessed 20.06.2025). – Screen title.
17. Lei He. Attribute-Based Proxy Signature Scheme Supporting Flexible Threshold Predicate for UAV Networks / Lei He, Yong Gan, Yanhua Zhang // Electronics. – 2023. – №12(23). – Article ID: 4854.
18. Panse T. Attribute Based Signature Architecture for Transferring Digital Document / Trishna Panse, Prashant Panse // Medi-Caps University Research Article. – 2022 – P.1-21.
19. Blazy O. Anonymous attribute-based designated verifier signature / O. Blazy, L. Brouilhet, E. Conchon, M. Klingler // Journal of Ambient Intelligence and Humanized Computing. – 2022. – № 68 (9). P. 6233-6244.
20. Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 4.5.2016. 88 p.
21. Vatamaniuk-Zelinska U.Z. Perspektyvy vykorystannia elektronnoho tsyfrovoho pidpysu v derzhavnykh strukturakh / U.Z. Vatamaniuk-Zelinska , V.S. Sushko // Efektyvna ekonomika. – 2020. – №7.
22. Sviatoshniuk A.L. Shchodo osoblyvostei vykorystannia elektronnoho tsyfrovoho pidpysu pry ukladenni tsyvilno-pravovykh dohovoriv u merezhi internet / A.L. Sviatoshniuk // Visnyk Odeskoho natsionalnoho universytetu. Seriia: Pravoznavstvo. – 2023. – №25-2 (37). – S.21-24.
23. Cheshun V. Model Tekhnolohii tsyfrovoho pidpysu na osnovi osobovykh atrybutiv. / V. Cheshun, Ya. Ryzhyi, D. Cheshun, O. Cheshun // Herald of Khmelnytskyi National University. Technical Sciences. – 2025. – № 1 (347). – S. 401-404.
24. Ryzhyi Ya.O. Tekhnolohiia tsyfrovoho pidpysu z vykorystanniam atrybutiv v systemakh elektronnoho dokumentoobihu / Ya.O. Ryzhyi, M.M. Melnyk, V.M. Stetsiuk// Elektronni informatsiini resursy: stvorennia, vykorystannia, dostup. Zbirnyk materialiv Mizhnarodnoi NP Internet konferentsii. – 2023. – S.223-225.
25. Pro elektronnyi tsyfrovyi pidpys [Elektronnyi resurs]: Zakon Ukrainy vid 22.05.2003 № 852-IV: stanom na 07.11.2018r.. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/852-15#Text.
26. Pro elektronni dovirchi posluhy [Elektronnyi resurs] : Zakon Ukrainy vid 05.10.2017 № 2155-VIII. Redaktsiia vid 01.12.2022r. – Rezhym dostupu : https://kodeksy.com.ua/pro_elektronni_dovirchi_poslugi.htm
27. Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy [Elektronnyi resurs] : Zakon Ukrainy vid 05.10.2017 № 2155-VIII. Redaktsiia vid 18.12.2024. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/2155-19#Text.
28. Pro elektronni dokumenty ta elektronnyi dokumentoobih [Elektronnyi resurs] : Zakon Ukrainy vid 22.05.2003 № 851-IV. Redaktsiia vid 31.12.2023. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/851-15#Text.
29. Pro elektronnu komertsiiu [Elektronnyi resurs] : Zakon Ukrainy vid 03.09.2015 № 675-VIII. Redaktsiia vid 01.01.2024. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/675-19#Text .
30. Pro zatverdzhennia Polozhennia pro vykorystannia elektronnoho pidpysu ta elektronnoi pechatky [Elektronnyi resurs] : Postanova Natsionalnoho banku Ukrainy; Polozhennia, Standart vid 20.12.2023 № 172. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/v0172500-23#n20.
31. eIDAS Regulation [Electronic resource] – An official website of the European Union. – Available from: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation – (Accessed 25.06.2025).
32. Pro zakhyst personalnykh danykh [Elektronnyi resurs] : Zakon Ukrainy vid 01.06.2010 № 2297-VI. Redaktsiia vid 14.06.2025. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/2297-17#Text.
33. GDPR-CARPA. Gdpr-certified assurance report-based processing activities. [Electronic resource] – Available from: https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/lu-gdpr-carpa-certificationscheme.pdf – (Accessed 25.06.2025).