НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ ОСОБОВИХ АТРИБУТІВ

Віктор Чешун
Хмельницький національний університет
Юрій Кльоц
Хмельницький національний університет
Віра Тітова
Хмельницький національний університет
Наталія Петляк
Національний авіаційний університет

DOI 10.24917/9788368020861.27

Abstract

The purpose of the article 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 subject of personal data. The article provides a description of the basic provisions of digital signature technology based on personal attributes, provides a classification of attributes used to form a signature, and analyzes the differences between cryptographic EDS and signature on attributes. The authors proved the possibility of implementing digital signature technology based on personal attributes in Ukraine in accordance with current laws 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, electronic digital signature, user attributes, legal regulation.

Вступ

Розвиток інформаційних технологій в останні десятиліття зумовлює 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).

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 [1, 2]. Впровадження ЕЦП сприяло збільшенню швидкості та зручності електронних процесів, а також забезпечило високий рівень довіри між учасниками цих процесів.

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 [1].

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 [3,4].

Таким чином, у майбутньому 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.

Технології класичного і атрибутивного цифрового підпису

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.

ЕЦП забезпечує важливі засади безпеки в електронному середовищі. Ігнорування ЕЦП – одна з найбільш поширених слабких сторін систем електронного документообігу [5]. 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 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 неадаптовним 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. 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 [6] і отримало подальший розвиток в [7], де підпис із застосуванням атрибутів описується як «універсальний примітив, що дозволяє стороні підписувати повідомлення з детальним контролем над ідентифікаційною інформацією».

Базові принципи атрибутивного ЕЦП (АЕЦП) суттєвою мірою відрізняються від класичного криптографічного ЕЦП:

- 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.

Огляд наявних рішень з реалізації технології АЕЦП дозволяє відзначити наявність як суто теоретичних рішень, прикладом якого може слугувати проєкт ABCJTrust [8], так і повноцінних діючих серівсів, прикладом якого є проєкт Yivi [9]. Існуючі реалізації технології АЕЦП відрізняються своїм основним призначенням та, відповідно, функціоналом. Порівняльні дані щодо можливостей окремих варіантів реалізації технлогії АЕЦП наведено в таблиці 1.

Таблиця 1. Функціональні особливості типових систем АЕЦП

№ з/п	Техно-логія	Аутентифі-кація	Сигнатура ЕЦП	Децентралі-зація	Відкритий код	Робоча версія
1	YIVI	+	+	+	+	+
2	DECODE	+	–	–	+	+
3	Schluss	+	–	–	+	+
4	Serto	+	–	+	+	–
5	Sovrin	+	–	+	+	+
6	SelfKey	+	–	+	+	+

В роботах [10, 11] представлено опис вітчизняної реалізації технології АЕЦП у формі мобільного додатку з можливістю формування сигнатури підпису та застосування в довірчих електронних послугах для розкриття атрибутів замовника надавачу послуг, але при виконанні проєкту постало питання узгодженості рішень із діючими законами та регулятивними актами.

Нормативно-правове забезпечення технології ЕЦП і АЕЦП

Аналіз відповідності технології АЕЦП діючим законам та регулятивним актам, першочергово, потребує аналізу і класифікації атрибутів, які можуть бути використані при формуванні сигнатури атрибутивного підпису.

Проведений в [11] аналіз дозволив виділити три типові категорії атрибутів, що можуть використовуватись в АЕЦП:

- ідентифікаційні атрибути;
- неідентифікаційні атрибути;
- контекстуальні атрибути.

Ідентифікаційні атрибути однозначно дозволяють ідентифікувати особу без додаткових уточнень. До ідентифікаційних атрибутів відносяться: відбиток пальця; малюнок сітківки ока; ПІБ; підпис особи (рукописний); ідентифікаційний код; серія-номер паспорта; серія-номер диплома; офіційний псевдонім (який однозначно пов'язаний з особою); ідентифікатор (номер або серія-номер) посвідчення з місця роботи тощо.

Як неідентифікаційні атрибути визначаються такі дані особи, які в певному аспекті ідентифікують особу, але не дозволяють однозначно її ідентифікувати без додаткових уточнень, оскільки можуть належати певному колу осіб або мають масове розповсюдження. До неідентифікаційних атрибутів можна віднести: ім'я; по батькові; розповсюджене прізвище; освіту; фах; місце роботи; посаду; неідентифікуючий особу псевдонім (широко розповсюджений або такий, що відомий тільки довіреній особі або обмеженому колу довірених осіб); дату народження; вік; дату видачі паспорту (будь-якого іншого документа тощо); орган, що видав паспорт (будь-який інший документ тощо) та інші.

Якщо ідентифікаційні атрибути служать для точної ідентифікації особи, то неідентифікаційні атрибути містять певну особисту інформацію підписувача без прямої ідентифікації його особи. Особливістю неідентифікаційних атрибутів є можливість отримання шляхом їх комбінування ідентифікаційного атрибуту.

Як контекстуальні атрибути підпису розглядаємо такі характеристики або ж параметри, які визначаються або можуть змінюватися залежно від конкретного контексту чи поточних обставин. В контексті ідентифікації особи ці атрибути надають додаткову інформацію про користувача, яка може бути корисною для точнішої та надійнішої ідентифікації підписувача в певному середовищі чи ситуації. До контекстуальних атрибутів можна віднести: часові параметри накладання ЕЦП (дата, час, день тижня, місяць тощо); геолокаційні параметри накладання ЕЦП (геолокаційні координати, адреса або складові адреси, установа або офіс з можливістю уточнення їх місцезнаходження тощо); тип пристрою, задіяного для накладання цифрового підпису; дані автентифікації під час входу в систему; права та повноваження підписувача; роль підписувача у певному контексті тощо.

В [11] надано опис технології формування сигнатури АЕЦП із ідентифікаційних, неідентифікаційних та контекстуальних атрибутів, в якій основна

увага акцентується на забезпеченні гнучкості, адаптивності та мультиатрибутності цифрового підпису. Зазначені принципи передбачають надання підписувачу можливості формувати цифровий підпис з довільної кількості атрибутів та визначати їх склад за власним побажанням або у відповідності до потреб.

В дослідженнях [1, 12, 13] питань правового регулювання ЕЦП в Україні акцент робиться на трьох складових нормативно-правових документів:

- Закон України «Про електронний цифровий підпис» [14];
- Закону України «Про електронні довірчі послуги» [15]; (Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [16]);
- Закони України та інші нормативні документи, що регулюють застосування ЕЦП в різних сферах та видах діяльності (Закон України «Про електронні документи та електронний документообіг» [17], Закон України «Про електронну комерцію» [18], «Положення про застосування електронного підпису та електронної печатки» [19] 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 в собі поєднання обох підходів [7].

Введення у 2015 році в дію закону Закону 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 [1] узгодженість Закону з Регламентом Європейського Союзу «Про електронну ідентифікацію, верифікацію та довірчі послуги» (eIDAS – electronic IDentification, Authentication and trust Services) [20] 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 зазначеної 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» [21]. 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 (GDPR) [22] 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 [23] дозволить значно підвищити ефективність застосування технології АЕЦП і уникнути ризиків несанкціонованого розкриття особових атрибутів суб'єкта персональних даних через недосконалість нормативно-правового забезпечення.

Висновки

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.

Список літератури

1. Р.В. Новосад (2023). *Правовий статус електронного підпису в Україні: від ідеї до реалізації*, Право та державне управління, № 3, pp. 112–116.
2. В.С. Політанський (2021). *Теоретико-правові засади системи електронного документообігу в Україні,* Право і суспільство., № 1, pp. 22–27.
3. Ke Gu, K. Wang, L. Yang (2019). *Traceable Attribute-Based Signature*, Journal of Information Security and Applications, vol. 49, article ID 102400, electronic resource: https://www.sciencedirect.com/science/article/abs/pii/S2214212616303106 (date of access: 11.02.2024).
4. V. Sucasas, G. Mantas, M. Papaioannou, J. Rodriguez (2023). *Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services*, IEEE Transactions on Cloud Computing, vol.11, № 1, pp. 168–184.
5. K. Rauniyar (2021). *Role of FinTech and innovations for Improvising Digital Financial Inclusion*, Int. J. Innov. Sci. Res. Technol., № 6, pp. 1419–1424.
6. G. Shanqing, Z. Yingpei (2008). *Attribute-Based Signature Scheme*, 2008 International Conference on Information Security and Assurance (ISA 2008), pp. 509–511.
7. H.K Maji, M. Prabhakaran, M. Rosulek, *Attribute-Based Signatures*, Cryptographers' Track at the RSA Conference, Springer, pp. 376–392.
8. *ABC4Trust Attribute-based Credentials for Trust*, electronic resource: https://abc-4trust.eu/download/ABC4Trust-OnePager-About-ABC4Trust.pdf (date of access: 11.02.2024).
9. *How Yivi works?*, electronic resource: http://surl.li/qnohm (date of access: 11.02.2024).
10. Я.О. Рижий, та ін. (2023). *Класифікація атрибутів особи і формування цифрового підпису на їх основі*, Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». – Хмельницький, pp. 252–256.
11. Я.О. Рижий, М.М. Мельник, В.М. Стецюк (2023). *Технологія цифрового підпису з використанням атрибутів в системах електронного документообігу*, Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції, pp. 223–225.
12. У. З. Ватаманюк-Зелінська, В. С. Сушко (2020). *Перспективи використання електронного цифрового підпису в державних структурах*, Ефективна економіка, № 7, Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=8043 (дата звернення: 12.02.2024).
13. А. Л. Святошнюк (2023). *Щодо особливостей використання електронного цифрового підпису при укладенні цивільно-правових договорів у мережі інтернет*, Вісник Одеського національного університету. Серія: Правознавство, том 25, Випуск 2 (37), pp. 21–24.
14. *Про електронний цифровий підпис*, Закон України від 22.05.2003 № 852-IV: станом на 7.11.2018 р., режим доступу: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення: 10.02.2024).

15. *Про електронні довірчі послуги*, Закон України від 05.10.2017 № 2155-VIII, режим доступу: https://kodeksy.com.ua/pro_elektronni_dovirchi_poslugi.htm (дата звернення: 10.02.2024).
16. *Про електронну ідентифікацію та електронні довірчі послуги*, Закон України від 05.10.2017 № 2155-VIII, Редакція від 01.01.2024, режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 10.02.2024).
17. *Про електронні документи та електронний документообіг*, 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 (дата звернення: 10.02.2024)
18. *Про електронну комерцію*, 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 (дата звернення: 10.02.2024).
19. *Про затвердження Положення про використання електронного підпису та електронної печатки*, Постанова Національного банку України; Положення, Стандарт від 20.12.2023 № 172, режим доступу: https://zakon.rada.gov.ua/laws/show/v0172500-23#n20 (дата звернення: 10.02.2024).
20. *eIDAS Regulation*, An official website of the European Union, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (дата звернення: 11.02.2024).
21. *Про захист персональних даних*, Закон України від 01.06.2010 № 2297-VI. Редакція від 27.10.2022, режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.02.2024).
22. 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, p. 88, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата звернення: 12.02.2024).
23. GDPR-CARPA. Gdpr-Certified Assurance Report-Based Processing Activities, https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/lu-gdpr-carpa-certificationscheme.pdf (дата звернення: 12.02.2024).

Uniwersytet Komisji Edukacji Narodowej w Krakowie
Prace Monograficzne 1213

UNIVERSITY OF THE NATIONAL EDUCATION COMMISSION, KRAKOW

PROBLEMS OF SCIENTIFIC, TECHNICAL AND LEGAL SUPPORT FOR CYBERSECURITY IN THE MODERN WORLD

MONOGRAPH
edited by Serhii Semenov, Mateusz Muchacki

Krakow 2024

Recenzenci:
prof. dr hab. inż. Jerzy Korostil
dr hab. inż. Stanisław Rajba, prof. UBB

Redaktor prowadzący: Natalia Majoch
Korekta tekstów w języku angielskim: Katarzyna Ryrych-Korczyńska
Korekta tekstów w języku ukraińskim: Oleg Aleksejczuk
Korekta tekstów w języku polskim: Natalia Majoch
Projekt okładki: Janusz Schneider
Projekt typograficzny i skład: Stanisław Tuchołka | panbook.pl

ISSN 2450-7865
ISBN 978-86-68020-86-1
e-ISBN 978-86-68020-87-8
DOI 10.24917/9788668020861

Wydawnictwo Naukowe UKEN
30–084 Kraków, ul. Podchorążych 2
tel./faks 12 662-63-83, tel. 12 662-67-56
e mail: wydawnictwo@up.krakow.pl
http:/ www.wydawnictwoup.pl

CONTENT