DOI: 10.18372/2225-5036.31.21163

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ДОВГОСТРОКОВОЇ ПЕРЕВІРКИ ЕЛЕКТРОННИХ ПІДПИСІВ

Андрій Охріменко[1], Олександр Стокіпний[2], Влад Ковтун[3]

[1]Маріупольський державний університет, м. Київ, Україна
[2] Державний університет «Київський авіаційний інститут», м. Київ, Україна
[3] Національний технічний університет «Харківський політехнічний інститут», м. Київ, Україна

ОХРІМЕНКО Андрій, к.т.н.
Рік та місце народження: 1990, м. Васильків, Київська обл., Україна
Освіта: Національний авіаційний університет, 2012
Посада: старший викладач кафедри системного аналізу та інформаційних технологій, Маріупольський державний університет
Наукові інтереси: криптографія, інфраструктура відкритих ключів, оптимізація криптографічних перетворень, безпека інформаційних систем
Публікації: понад 60 наукових праць, статті в фахових та міжнародних виданнях, патенти на корисну модель, авторські свідоцтва.
E-mail: a.okhrimenko@mu.edu.ua
ORCID 0000-0001-8270-2863

СТОКІПНИЙ Олександр, к.т.н.
Рік та місце народження: 1979, м. Гадяч, Полтавська обл., Україна
Освіта: Харківський військовий університет, 2002
Посада: доцент кафедри інтелектуальних кібернетичних систем, Державний університет «Київський авіаційний інститут»
Наукові інтереси: криптографія, ефективна реалізація криптографічних алгоритмів, розробка високонавантажених систем, архітектури сучасних програмних систем.
Публікації: понад 20 наукових праць, статті в фахових та міжнародних виданнях, авторські свідоцтва.
E-mail: oleksandr.stokipnyi@kai.edu.ua
ORCID 0009-0007-4346-9684

КОВТУН Владислав, к.т.н.
Рік та місце народження: 1978, смт. Петрове, Кіровоградська обл., Україна
Освіта: Харківський військовий університет, 2000
Посада: доцент кафедри програмної інженерії та інтелектуальних технологій управління, Національний технічний університет «Харківський політехнічний інститут»
Наукові інтереси: криптографія, алгебраїчні криві, ефективна реалізація криптографічних перетворень, прикладна математика, аналіз та алгебра
Публікації: понад 60 наукових праць, статті в фахових та міжнародних виданнях, патенти на корисну модель, авторські свідоцтва.
E-mail: vladislav.kovtun@gmail.com
ORCID 0000-0002-4303-3510

Анотація. *У статті досліджуються методи забезпечення довгострокової перевірки електронних підписів у сучасних системах електронного документообігу та архівах. Проаналізовано проблеми втрати чинності підписів у часі, зокрема через закінчення терміну дії сертифікатів, недоступність сервісів перевірки статусу сертифікатів та втрату стійкості криптографічних алгоритмів. Розглянуто стандарти та механізми довгострокового зберігання. Запропоновано підхід до побудови систем LTV з урахуванням вимог довгострокового зберігання електронних документів.*

Ключові слова: *електронний підпис, геш, довгострокова перевірка, PKI, XAdES, CAdES, PAdES, позначка часу, блокчейн, архівне зберігання*

Вступ. Довіра до електронних документів є важливим викликом в сучасному інформаційному суспільстві. При переході на електронні документи виникає необхідність забезпечити їх автентичність та цілісність протягом багатьох років. В окремих сферах важливо, щоб навіть через десятиліття електронні документи могли слугувати

достовірними джерелами, як і їх паперові аналоги. Тобто, необхідно мати можливість достовірно встановити, що документ є справжнім, цілісним, створеним та підписаним у заявлений час. Завдяки криптографічним методам гарантується автентичність підписанта та цілісність документа, проте довіра до електронного документу має зберігатись протягом усього необхідного часу його зберігання. Для забезпечення цього процесу необхідно застосовувати різні методи і підходи, як технологічні так і організаційні.

Для контролю цілісності електронних документів зазвичай використовують геш-функції. Одним із методів забезпечення автентичності електронного документу є використання електронних підписів. Проте сам лише електронний підпис, в його класичному розумінні, не може забезпечити довіру до електронного документу в довгостроковому періоді [1]. Підпис, який дійсний сьогодні, завтра може стати недійсним за кількома причинами. По-перше, сертифікати відкритих ключів мають обмежений строк дії, крім того, їх можуть відкликати. У разі завершення строку дії сертифікату або його відкликання при перевірці підписів, що були створені з використанням цих ключів можуть виникнути проблеми (навіть якщо в документ не були внесені зміни). По-друге, в процесі перевірки підпису необхідно звертатись до сервісу OCSP чи до списку відкликаних сертифікатів (CRL) щоб впевнитись, що на момент підпису сертифікат відкритого ключа був дійсним. CRL підписаний ключами центру сертифікації, який його видав, а відповіді від сервісу OCSP підписані ключами самого сервісу OCSP. Відповідно, сертифікати ключів сервісу OCSP та центру сертифікації теж мають хоч і більший, ніж у сертифікатів користувачів, але цілком скінченний термін дії. Тому при завершенні терміну дії цих сертифікатів, а також при недоступності OCSP/CRL також виникнуть проблеми. По-третє, криптографічні алгоритми гешування та цифрового підпису можуть стати непідтримуваними чи ненадійними. Також проблемами можуть стати неможливість побудувати та перевірити весь ланцюжок сертифікатів від сертифіката підписувача до довіреного кореневого сертифіката центра сертифікації, а також відсутність підтвердження, що підпис був дійсним на момент додавання документу до архіву [2].

Отже потрібно зафіксувати факт того, що підпис був дійсним на момент додавання документу до архіву, а також зберегти підтвердження цього факту на тривалий час – це є необхідною умовою юридичної значущості електронних документів. Тому недостатньо мати лише геш документа чи електронний підпис, потрібно мати додатково метадані, використовувати формати і протоколи, що надають додаткову інформацію про документ – коли і ким він був підписаний та доданий до архіву, які операції проводились з цим документом. Такі метадані є підтвердженням, що з моменту додавання до архіву вміст документу не модифікувався.

Довгострокова перевірка

Довгострокова перевірка (Long-Term Validation, LTV) це набір методів та підходів, що направлені на забезпечення можливості перевірки електронних підписів через тривалий час після його створення. Для забезпечення LTV відбувається вбудовування чи додавання до підписаного документа всіх даних, необхідних для підтвердження його дійсності в майбутньому, зокрема: позначки часу (timestamp), інформації про статус сертифіката підписанта на момент підписання (відповіді OCSP або CRL) та інших допоміжних даних (наприклад усіх необхідних сертифікатів) [3]. Завдяки цьому звичайний електронний підпис перетворюється на самодостатній об'єкт, який можна перевірити протягом тривалого часу. Позначка часу фіксує геш двійкових даних з додаванням дати і часу та підписується ключами довірчого сервісу позначок часу (TSA). Позначка часу може створюватися для даних, які підписуються, чи для самого підпису, тим самим забезпечуючи незаперечний доказ існування відповідно даних чи самого підпису в конкретний момент часу [4].

Довгострокова перевірка цифрових даних регулюється низкою міжнародних та європейських стандартів. ETSI EN 319 102 визначає процедури створення та перевірки розширених електронних підписів AdES та описує повну модель перевірки підпису, включно з довгостроковою перевіркою [5] та протокол перевірки [6]. ETSI EN 319 421 «Policy and Security Requirements for Trust Service Providers issuing Time-Stamps» містить вимоги до служб засвідчення часу (TSA), зокрема до точності джерела часу, до захисту ключів TSA, до формату позначки часу тощо. ETSI EN 319 422 «Time-stamping protocol and time-stamp token profiles» описує формат позначки часу, різні алгоритмічні профілі, підтримку нових геш-алгоритмів та посилених штампів. IETF RFC 4998 та RFC 6283 стандарти з серії Long-Term Archive and Notary Services, що описують синтаксис запису доказів (Evidence Record Syntax, ERS) існування цифрових даних та їх цілісності. Для успішного довготривалого зберігання недостатньо лише криптографічних засобів, потрібні ще й організаційні заходи. Міжнародний стандарт OAIS (ISO 14721) описує модель відкритого архіву інформації, де визначені концепції інформаційних

пакетів, метаданих і процесів збереження. Стандарт ISO 16363 (Audit and Certification of Trustworthy Digital Repositories) встановлює критерії, за якими архіви можуть перевірятись на надійність. Де-факто міжнародний стандарт PREMIS (Preservation Metadata: Implementation Strategies) описує формат метаданих для довгострокового збереження.

Формати електронних підписів

Для забезпечення LTV повинні використовуватися спеціальні формати підписів AdES (Advanced Electronic Signature), які визначають як зберігати підпис та пов'язані дані всередині файлу або окремо.

Формат підписів на основі CMS (Cryptographic Message Syntax) CAdES [7] підходить для будь-яких двійкових даних і часто використовується для відкріплених підписів (файли .p7s). Формат X-Long у CAdES відповідає профілю LT та включає усі дані для перевірки: повний набір необхідних сертифікатів, відповіді OCSP/CRL тощо. В останніх редакціях стандарту CAdES [7] також передбачено формат CAdES-A, що відповідає рівню LTA, яким передбачається додавання архівних позначок часу.

Формат підписів XAdES для даних, що представлені в XML [8]. Базові профілі XAdES-B/BES забезпечують підпис та базові атрибути, XAdES-T додає позначку часу. Рівні XAdES-C і XAdES-X додають відповідно сертифікати і відповіді OCSP. XAdES-LT містить повний набір даних для довгострокової перевірки (всі необхідні сертифікати, OCSP/CRL, позначки часу). XAdES-LTA (Long Term with Archive) додає ще й архівну позначку часу поверх усього набору даних (timestamp, який ставиться після того, як підпис вже містить усі дані).

Формат підписів для PDF-документів PAdES (PDF Advanced Electronic Signature) має профілі підпису, що стандартизовані ETSI і ISO [9]. PAdES-LTV означає, що PDF-файл містить всі елементи, потрібні для довгострокової перевірки підписів у ньому. Після підписання PDF, у нього вбудовується підпис в форматі PKCS#7 з повним набором даних для перевірки (відповідає рівню B-LT). Далі на весь документ додається архівна позначка часу (відповідає рівню B-LTA).

З технічної точки зору основною відмінністю між цими трьома типами підпису та їх форматами є метод вбудовування даних підпису. PAdES безперешкодно інтегрується з програмами для перегляду PDF (наприклад Adobe Acrobat), CAdES використовується для ширшої сумісності, а XAdES використовує XML для динамічних середовищ. З точки зору безпеки, всі три стандарти підтримують довгострокову перевірку (LTV) та сумісні з eIDAS [7-9].

Архівні довірчі послуги

Хоча спеціалізовані формати електронних підписів і дозволяють збільшити час гарантованої їх перевірки, проте для більш тривалого зберігання лише їх використання недостатнє.

Для більш тривалого зберігання необхідно використовувати спеціалізовані сервіси або певний набір процедур, що забезпечують так звану повторна перевірку, в результаті якої періодично оновлюються докази автентичності електронних документів з метою продовження довіри до них і автоматизованої можливості їх перевірки (без втручання експертів). До основних методів відносять повторний підпис, повторне створення позначки часу, засвідчення печаткою [10-12].

Метод повторного підпису або перепідпису використовується за деякий час до закінчення терміну дії сертифікату ключів, якими підписувався документ. Відповідальна особа вручну, чи технологічне програмне забезпечення автоматично, створює новий електронний підпис або електронну печатку на вже підписаний документ (чи набір даних), тим самим підтверджуючи, що на момент перепідпису попередній підпис був дійсним.

Метод повторного створення позначки часу використовується для накладання нової позначки часу на існуючу стару позначку, на існуючий документ або підпис. Додаванням нової позначки часу засвідчується, що на момент її видачі попередня позначка часу (підпис чи набір даних) була дійсна. Таким чином можна сформувати ланцюжок архівних позначок часу, коли геш документу з позначкою часу використовується для отримання нової позначки часу декілька разів підряд.

При повторному підписанні чи повторній видачі позначки часу кожен наступний підпис чи позначка часу подовжує на деякий час довіру до електронного документу. При цьому можуть використовуватись нові більш стійкі криптографічні алгоритми, більші довжини ключів тощо.

Дещо схожим до повторного підпису є метод засвідчення печаткою. При передачі на архівне зберігання електронного документа до архівної організації на вже підписаний документ (чи набір даних) додатково накладається електронна печатка архіву з метою засвідчити незмінність даних, тим самим підтверджується що від моменту прийому документу архівом його цілісність контролюється. В подальшому цей документ може перепідписуватись ключами архіваріуса або повторно накладатись електронна печатка.

Паралельно з оновленням підписів та позначок часу архівні системи повинні вести журнали всіх операцій. Такі журнали можуть бути предметом криптографічного захисту. Наприклад, записи журналу часто зчеплюються через геш-ланцюжок, коли кожен новий запис в журналі включає геш чи код автентифікації повідомлень (MAC) попереднього запису. Таким чином досягається незмінність журналу, при спробі вилучити чи замінити запис в журналі ламається контроль цілісності всіх наступних записів. Крім того, геш останнього запису в журналі або геш самого журналу може підписуватись для фіксації його стану зовнішнім сервісом довірчих послуг. При проведенні аудиту можна буде впевнитись, що всі дії над електронним документом зафіксовані в журналі, а журнал не піддавався сторонньому впливу.

Блокчейн

Інтеграція технології блокчейн у механізмі довгострокової перевірки електронних підписів та дозволяє зменшити залежність від централізованих сервісів довіри (надавачів електронних довірчих послуг), зокрема служб TSA [13]. Блокчейн забезпечує незмінність записів та можливість перевірки факту існування документа у певний момент часу за допомогою механізмів гешування та зчеплення блоків. Дані про електронний документ, його геш, електронний підпис та протокол перевірки [6] електронного підпису під час додавання до блокчейну, можуть формувати транзакції публічного блокчейну (наприклад, Ethereum чи інший, який має певну довіру у суспільстві) чи приватного блокчейну (наприклад, коли один чи кілька вузлів розгорнуто і контролюються незалежно інституціональними установами: нотаріус та юридична компанія), тим самим довіра базується на консенсусі мережі цього блокчейну. Після запису до блокчейну документ може зберігатися без додаткових дій (без перепідпису, чи додаткових позначок часу). Також блокчейн ідеально підходить для доведення факту існування документу (Proof of existence, POE), його незмінності, автентичності та ступеня довіри при додаванні.

Незважаючи на явні переваги, блокчейн не може повністю замінити інфраструктуру відкритих ключів, оскільки не забезпечує функцій ідентифікації підписувача та перевірки статусу сертифікатів. Крім того, юридичний статус поки чітко не визначений, блокчейн лише гарантує цілісність даних, але не їх юридичну прив'язку до конкретної особи. Це можливо компенсувати за рахунок впровадження протоколів перевірки підпису [6] електронного документу та додаванням їх разом з документом до архіву. Серед недоліків при використанні публічних блокченів є: невисока швидкість транзакцій, через необхідність підтвердження її розподіленими вузлами; компрометація математичного апарату блокчейну; захоплення контролю над блокчейном групою осіб. Тому використання спеціалізованих приватних блокчейнів, розгорнутими в межах певної установи, із залученням кількох інституціональних установ (юридичних компаній, консалтингових компаній та нотаріусів) є більш доцільною. Спеціалізований блокчейн не матиме велику кількість документів і велику кількість розподілених вузлів, тому використання геш-функції для зчеплення записів не є безпечним. Для забезпечення безпеки пропонується використовувати MAC замість геш-функції, невелику кількість вузлів (5-7) та для кожного вузла власний ключ MAC і адміністративно-технічними обмеженням на створення нового вузла (дозволить контролювати розширення спеціалізованого блокчейну). Крім того, у випадку компрометації математичного апарату MAC існує можливість послідовної міграції вузлів спеціалізованого приватного блокчейну на інші, більш стійкі криптографічні алгоритми MAC.

Таким чином, найбільш перспективним є гібридний підхід, у якому блокчейн використовується як додатковий рівень: доказу існування документу, його цілісності та протокол перевірки електронного підпису під час додавання до блокчейну.

Гібридний підхід до побудови систем LTV

Враховуючи розглянуті вище методи і підходи пропонується гібридне системне рішення, що підтримує вимоги довготривалого збереження та перевірки, а також враховує рекомендації міжнародних і галузевих стандартів, перспективні напрямки і кращі практики.

1. Перед занесенням електронного документу до архіву має виконуватись перевірка електронного підпису. У випадку, якщо цей підпис не LT чи LTA, система має розширювати його до рівня LT чи LTA, придатного для довгострокового зберігання, шляхом збагачення додатковою інформацією, такою як сертифікати і статуси цих сертифікатів, позначки часу на момент додавання.
2. До документу додається електронний підпис в форматі LTA відповідальної особи (архіваріуса) та/або печатка установи для підтвердження прийняття електронного документу на архівне зберігання.
3. Метадані документу мають зберігатись у БД разом із самим документом, а геш-

образ документу, геш-образ протоколу перевірки, протокол перевірки електронного підпису [6], тощо, зберігаються у окремій БД із зчепленими блоками на основі MAC.

4. Використовується приватний блокчейн з невеликою кількістю розподілених вузлів (5-7), де для кожного вузла використовується власний ключ MAC. Вузли блокчейну розгорнуто у кількох незалежних установах (юридичних компаніях, консалтингових компаніях, нотаріусів), які володіють власними ключами MAC та забезпечують незалежність і контроль цілісності власних вузлів блокчейну. Впроваджено адміністративно-технічні обмеження на додавання нових вузлів такого блокчейну і видалення існуючих (юридична компанія чи нотаріус припинив свою діяльність).
5. Для перевірки цілісності електронного документу і протоколу його перевірки [6], необхідно використовувати розподілений режим перевірки, що базується на консенсусі - результату перевірки отриманому від більшості вузлів. Кілька вузлів архіву отримують запити на отримання протоколу перевірки електронного документу за його гешем, далі виконують пошук відповідних записів за геш-образами у БД блокчейну, повертають результати до центрального сервісу, який приймає рішення щодо цілісності і автентичності електронного документу за отриманими результатами. Щоб підробити дані, необхідно скомпрометувати більше половини вузлів блокчейну.
6. Регулярна та автоматична перевірка цілісності ланцюжків записів у БД блокчейну з занесенням результатів до самого блокчейну, дозволяє зменшити можливість підробки таких документів і прискорити отримання результату перевірки.
7. Виконується перевірка електронного підпису архіваріуса та/або печатки установи.
8. За розкладом, в автоматичному режимі, виконується додавання архівної позначки часу до електронного підпису архіваріуса та/або печатки установи з використанням підходів, які були описані раніше. Можливе використання алгоритмів підпису, що забезпечують або такий самий рівень захисту, або більший.
9. Забезпечення більшого рівня захисту можливе за рахунок використання алгоритмів підпису із більшою довжиною ключа і більшим розміром геш-образу, із більшим розміром MAC, чи взагалі, з використанням постквантових алгоритмів підпису. Допускається дублювання підписів, як з використанням класичного алгоритму підпису з більшою довжиною ключа, так і з постквантовим алгоритмом підпису. Це зумовлено тим, що більшість постквантових алгоритмів підпису не пройшли перевірку часом.

Використання такої гібридної моделі поєднання класичного архіву з елементами блокчейну та приватного блокчейну з використанням MAC має підвищити довіру до даних протягом великого проміжку часу та надійність рішення в цілому.

Висновки. Перехід до використання виключно електронних документів потребує використання механізмів і принципів довгострокового зберігання електронних документів. Перевірка електронних підписів є критично важливими для забезпечення достовірності та юридичної значущості електронних документів через роки і десятиліття. Забезпечення довгострокової автоматичної перевірки електронних підписів є комплексною задачею, яка виходить за межі класичної криптографічної перевірки підпису та потребує врахування часових, інфраструктурних і архівних аспектів. Базові електронні підписи не гарантують можливості перевірки у довгостроковій перспективі через закінчення терміну дії сертифікатів, недоступність сервісів перевірки статусу сертифікатів та поступову втрату стійкості криптографічних алгоритмів.

Проаналізовано підходи, закладені у стандартах ETSI для форматів CAdES, XAdES та PAdES, які передбачають використання розширених профілів підпису (зокрема LT та LTA), що дозволяють забезпечити довгострокову автоматичну перевірку шляхом включення до підпису повного набору додаткових даних, зокрема сертифікатів, даних про їх статус та позначок часу. Встановлено, що саме додавання цих даних до електронного підпису документу дозволяє здійснювати перевірку підпису незалежно від зовнішніх сервісів у майбутньому.

Показано, що ключовим елементом довгострокової перевірки є наявність доказу того, що підпис був дійсним саме на момент додавання

до архіву. Існування такого доказу досягається шляхом використання додаткових підписів архівної установи і архіваріуса, додаткових архівних позначок часу, фіксації статусів сертифікатів під час підписання та протоколу перевірки підпису під час додавання до архіву. Додатково встановлено, що для забезпечення стійкості до криптографічної деградації необхідним є застосування механізмів архівного підпису (LTA), які передбачають періодичне оновлення доказових даних класичними криптографічними алгоритмами з більшими довжинами ключа та використання нових постквантових криптографічних алгоритмів.

Окремо встановлено, що сучасні технології, зокрема приватний блокчейн, можуть використовуватись як додатковий інструмент забезпечення доказу існування та цілісності даних, підвищення стійкості до нових криптографічних вразливостей. Крім того зменшує загальне навантаження на архівну систему з перепідписами та підвищує захисту від можливого втручання людини у процес зберігання електронного документу. Подальше підвищення ефективності приватного блокчейна можливе за рахунок додавання вузлів, створення регламенту перевірки цілісності вузлів блокчейну за розкладом, які винесені в інші інституційні установи, та розробки відповідного регламенту додавання нових і видалення існуючих вузлів приватного блокчейну.

Таким чином, запропонований підхід до побудови систем довгострокової перевірки електронних підписів, що поєднує стандартизовані механізми ETSI з перевірки підписів, формування звітів про перевірку, архівні профілі поширених форматів підписів та сучасні інструменти забезпечення цілісності і автентичності даних, дозволяє забезпечити надійність, відтворюваність та юридичну значущість електронних документів протягом тривалого часу.

Джерела

1. Entrust. What Is Long-Term Validation and Why Is It Important for Digital Signatures? URL: https://www.entrust.com/resources/learn/what-is-long-term-validation
2. Brzica H., Herceg B., Stančić H. Long-term preservation of validity of electronically signed records. INFuture 2013.
3. European Commission. Digital Signature Service (DSS). URL: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html
4. RFC 3161. Time-Stamp Protocol (TSP).
5. ETSI EN 319 102-1 V1.4.1 (2024-06). Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
6. ETSI EN 319 102-2 V1.4.2. Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report
7. ETSI EN 319 122-1. CAdES digital signatures.
8. ETSI EN 319 132-1. XAdES digital signatures.
9. ETSI EN 319 142-1. PAdES digital signatures.
10. RFC 4810. Long-Term Archive Service Requirements.
11. ETSI TS 119 511. Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
12. Lekkas D., Gritzalis D. Cumulative notarization for long-term preservation of digital signatures. Computers & Security. Volume 23, Issue 5, 2004, Pages 413-424.
13. Tomasz Hyla, Jerzy Pejaś. Long-term verification of signatures based on a blockchain. https://www.sciencedirect.com/science/article/abs/pii/S0045790618327381

Okhrimenko A., Stokipnyi O., Kovtun V. Methods for ensuring long-term validation of electronic signatures

Abstract. *The article investigates methods for ensuring the long-term validation of electronic signatures in modern electronic document management systems and archives. It analyzes the problems of signature validity loss over time, specifically due to certificate expiration, the unavailability of certificate status checking services, and the loss of robustness in cryptographic algorithms. Standards and mechanisms for long-term preservation are examined. An approach to building LTV (Long-Term Validation) systems is proposed, considering the requirements for the long-term preservation of electronic documents.*

Keywords: *electronic signature, hash, long-term validation, PKI, XAdES, CAdES, PAdES, timestamp, blockchain, archival storage.*

Охріменко Андрій, кандидат технічних наук, старший викладач кафедри системного аналізу та інформаційних технологій Маріупольського державного університету
Andrii Okhrimenko, PhD, Senior Lecturer at the Department of Systems Analysis and Information Technologies, Mariupol State University**.**

Стокіпний Олександр, кандидат технічних наук, доцент кафедри інтелектуальних кібернетичних систем Державний університету «Київський авіаційний інститут»
Oleksandr Stokipnyi, PhD, Associate Professor at the Department of Intelligent Cybernetic Systems, State University "Kyiv Aviation Institute".

Ковтун Владислав, кандидат технічних наук, доцент кафедри програмної інженерії та інтелектуальних технологій управління Національного технічного університету «Харківський політехнічний інститут»
Vladyslav Kovtun, PhD, Associate Professor at the Department of Software Engineering and Intelligent Management Technologies, National Technical University "Kharkiv Polytechnic Institute".