Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Технологія використання цифрового підпису
в системах електронного документообігу
Назва теми

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.190167.22.01.21 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Рижий Я.О.
Підпис

Керівник доц., к.т.н, доцент _____ Орленко В.С.
Підпис

Нормоконтролер старший викладач _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Кльоц Ю.П.
Підпис

11 12 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рижому Ярославу Олександровичу
Прізвище, ім'я, по батькові студента

1. Тема проєкту (роботи) Технологія використання цифрового підпису в системах електронного документообігу

Керівник роботи Орленко Вікторія Сергіївна
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проєкту (роботи) Підвищення ефективності технології використання цифрового підпису в системах електронного документообігу

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Дослідження технологій використання цифрового підпису в системах електронного документообігу. Постановка задачі дослідження. Математична модель технології ЕЦП. Алгоритмічна реалізація технології ЕЦП. Апробація технології ЕЦП. Висновки.

5. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри Кб		

6. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка алгоритмів і технологій, їх аналіз	16.10.2023	
6	Робота над розділом 4 – апробація запропонованих рішень	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих \результатів; оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент _____ Я.О.Рижий
Підпис Ініціали, прізвище

Керівник проєкту (роботи) _____ В.С. Орленко
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Технологія використання цифрового підпису в системах електронного документообігу

Автор роботи: Рижий Ярослав Олександрович

Керівник роботи: к.т.н., доц. Орленко Вікторія Сергіївна

Загальний обсяг роботи: 85 сторінок, 13 рисунків, 1 таблиця, 2 додатки, 58 посилань.

Ключові слова: захист інформації, електронний цифровий підпис, атрибути користувача, система електронного документообігу.

Кваліфікаційна робота присвячена визначенню базових теоретичних положень та алгоритмічній реалізації технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу.

В роботі здійснено ідентифікацію та класифікацію атрибутів для реалізації технології цифрового підпису в системах електронного документообігу, визначено спосіб формалізованого представлення різних класів атрибутів в математичній моделі та презентовано схему синтезу сигнатури підпису, розроблені алгоритми та рольові схеми реалізації технології, здіснео апробацію отриманих результатів Запропонована технологія використання цифрового підпису в системах електронного документообігу базується на принципах гнучкості, адаптивності та мультиатрибутності електронного цифрового підпису.

25.11.2023

ANNOTATION

Theme of qualification work: Digital signature technology in electronic document management systems

Author of the work: Ryzhyi Yaroslav Oleksandrovych

Mentor: Ph.D. Orlenko Viktoriia Serhiivna

Total volume of work: 85 pages, 13 figures, 1 tables, 2 appendices, 58 links.

Keywords: information protection, electronic digital signature, user attributes, electronic document management system.

The qualification work is devoted to the definition of the basic theoretical provisions and algorithmic implementation of the digital signature technology using the signatory's personal attributes in electronic document management systems.

In the work, the identification and classification of attributes for the implementation of digital signature technology in electronic document circulation systems was carried out, the method of formalized representation of various classes of attributes in a mathematical model was determined, and the signature synthesis scheme was presented, algorithms and role schemes for the implementation of the technology were developed, and the results were tested. signature in electronic document management systems is based on the principles of flexibility, adaptability and multi-attribute electronic digital signature.

25.11.2023

ЗМІСТ

ВСТУП

Сучасний світ невпинно рухається в напрямку цифрової трансформації, змінюючи спосіб, яким ми працюємо і спілкуємося. У цьому контексті системи електронного документообігу стають ключовим інструментом для забезпечення ефективного обміну даними та документами між організаціями, установами та приватними особами [1,2].

Системи електронного документообігу є невід'ємною складовою сучасного підприємства чи організації. Вони дозволяють значно зменшити витрати часу та ресурсів, пов'язаних з обробкою, зберіганням та передачею паперових документів. Вони сприяють автоматизації рутинних процесів, забезпечуючи швидкий доступ до необхідної інформації в будь-який час і в будь-якому місці.

У зв'язку з розвитком роботи на віддалених робочих місцях, системи електронного документообігу дозволяють забезпечити ефективний обмін документами в реальному часі, незалежно від місцезнаходження користувачів. Це сприяє підвищенню продуктивності та зручності роботи, що є особливо важливим у сучасному глобалізованому світі [3].

Загалом, системи електронного документообігу стають необхідним інструментом для підвищення ефективності роботи, поліпшення безпеки даних та сприяють зручній комунікації між організаціями та працівниками. Враховуючи швидкий темп технологічного розвитку, впровадження та вдосконалення цих систем стає критично важливим для підтримки конкурентоспроможності та інноваційного розвитку сучасних підприємств і установ.

Системи електронного документообігу також сприяють і поліпшенню безпеки даних [4,5]. Вони дозволяють керувати доступом до конфіденційної інформації, забезпечуючи шифрування даних та механізми перевірки цілісності. Це допомагає запобігти несанкціонованому доступу до важливих даних та зменшити ризик витоку інформації.

Використання передових технологій безпеки в системах електронного документообігу є важливою умовою для забезпечення надійного захисту

конфіденційної інформації та забезпечення безпечного обміну даними між організаціями та приватними особами [6-8].

Актуальність роботи полягає в тому, щоб в умовах постійного і незупинного зростання кількості загроз інформаційної безпеки загалом і в системах електронного документообігу зокрема запропонувати технологія використання цифрового підпису в системах електронного документообігу більш широкого застосування і зрозумілого нефаховому користувачу формату.

Ця кваліфікаційна робота присвячена визначенню базових положень та алгоритмічній реалізації технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу.

Мета кваліфікаційної роботи полягає у вдосконаленні і розширенні можливостей технології використання цифрового в системах електронного документообігу та інших електронних сервісах з авторизацією користувачів за рахунок застосування у сигнатурі підпису особових атрибутів підписанта.

Об'єктом дослідження є процеси захищеної авторизації користувачів інформаційних послуг систем електронного документообігу.

Предметом дослідження є технології формування електронного цифрового підпису в електронних сервісах та системах електронного документообігу з адаптованою потребам підписанта структурою сигнатури.

Щоб реалізувати програму досліджень необхідно:

а) виявити перспективні напрямки та способи вдосконалення технології використання цифрового підпису в системах електронного документообігу, що можуть бути використані у підвищенні її ефективності;

б) визначити основні положення технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу;

в) розробити математичну модель технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу;

г) здійснити алгоритмічну реалізацію технології;

д) провести апробацію дієвості прийнятих теоретичних і алгоритмічних рішень технології.

В основі методів дослідження лежать базові положення інформаційної безпеки, теорії ідентифікації та аутентифікації, криптографії, теорії множин.

Наукова новизна отриманих результатів:

1. Визначено спосіб формування мультиатрибутивної адаптивної сигнатури цифрового підпису в термінах запропонованої математичної моделі;

2. Удосконалено технологію електронного цифрового підпису систем електронного документообігу забезпеченням гнучкості формування сигнатури підпису із застосуванням атрибутів та її адаптивності до потреб підписанта.

Практична значимість отриманих результатів полягає у визначенні положень і розробці алгоритмів технології використання цифрового підпису в системах електронного документообігу більш широкого застосування і зрозумілого нефаховому користувачу формату.

Публікації. За темою магістерської роботи підготована до видання 1 стаття у фаховому журналі та опубліковано 3 тези доповідей на Всеукраїнській і міжнародній науково-практичній конференції.

1 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ВИКОРИСТАННЯ ЦИФРОВОГО ПІДПИСУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1.1 Системи електронного документообігу як об’єкт захисту

Системи електронного документообігу є важливою складовою діяльності сучасних фірм і організацій, яка сприяє оптимізації бізнес-процесів, покращенню ефективності та забезпеченню безперервного потоку документів та інформації. Впровадження систем електронного документообігу дозволяє прискорити обробку документів, зменшити час, необхідний для їх обробки, та забезпечити швидкий доступ до необхідної інформації [1]. Використання систем електронного документообігу дозволяє знизити витрати на паперову документацію, друкування, зберігання та розсилку, що сприяє збереженню ресурсів і зменшенню витрат на бізнес-процеси. Системи електронного документообігу дозволяють зручно та надійно зберігати всі документи та дані, що дозволяє підтримувати легкий доступ до них та забезпечити їх безпеку [2].

Використання систем електронного документообігу дозволяє забезпечити точність даних та документів, а також здійснювати контроль за їхнім рухом та обробкою. Такі системи сприяють полегшенню комунікації між співробітниками та партнерами, забезпечуючи швидкий та ефективний обмін документами та інформацією [3].

Системи електронного документообігу допомагають фірмам підвищити продуктивність, ефективність та точність своєї діяльності, забезпечуючи безперебійний обмін даними та документами і відповідаючи сучасним вимогам бізнесу [4].

Системи електронного документообігу є важливим об'єктом захисту в організаціях, оскільки містять велику кількість конфіденційної інформації та важливих даних, які потребують надійного захисту від різноманітних кіберзагроз [3,5,6].

Системи електронного документообігу часто містять конфіденційну інформацію. Забезпечення конфіденційності таких даних є критично важливим

аспектом їх захисту [6-8]. Конфіденційна інформація, яка зберігається у системах електронного документообігу, є важливим активом для організацій і фірм, оскільки вона може містити чутливі дані, що вимагають особливого захисту від несанкціонованого доступу. Деякі типи конфіденційної інформації, які можуть зберігатися у системах електронного документообігу, включають [2,7,10]:

– фінансові дані – фінансові звіти, бюджетні плани, операційні дані та інша фінансова інформація, яка є конфіденційною для організації;

– правові документи – контракти, угоди, договори, ліцензії, юридичні документи та інші правові матеріали, які вимагають особливого захисту від несанкціонованого доступу;

– персональні дані – інформація про співробітників, клієнтів, партнерів, така як особисті дані, контактна інформація, медична інформація тощо;

– комерційна інформація – торговельні секрети, рекламні стратегії, маркетингові плани, дослідження ринку та інші комерційні дані, які приховуються від конкурентів;

– стратегічні плани – інформація щодо стратегічних планів, розробки продуктів, розширення бізнесу та інші конфіденційні плани, які можуть мати значний вплив на діяльність організації.

Важливо забезпечити, щоб дані в системі електронного документообігу не піддавалися несанкціонованій модифікації або пошкодженню під час трансляції чи зберігання. Важливим аспектом захисту систем документообігу є забезпечення безперебійного доступу до даних є, оскільки недоступність важливих документів може призвести до серйозних проблем для бізнесу [2].

Системи електронного документообігу повинні бути захищені від широкого спектру кіберзагроз, таких як віруси, зломи, фішинг, DDoS-атаки та інші шкідливі дії, спрямовані на порушення безпеки даних [11]. Також системи електронного документообігу повинні бути об'єктом постійного аудиту та моніторингу з метою виявлення можливих загроз та вразливостей у реальному часі[12].

Проведені дослідження показали, що системи електронного документообігу,

як і будь-які інші інформаційні системи, мають свої слабкі місця, які можуть бути вразливими перед різноманітними загрозами [6,12,13]:

– відсутність ефективних заходів з кібербезпеки, що може призвести до можливості несанкціонованого доступу до конфіденційної інформації або зміни даних без дозволу;

– слабкі місця у мережевій інфраструктурі, які створюють можливість реалізації кібератак, що можуть призвести до перебоїв у роботі системи електронного документообігу;

– використання слабких методів аутентифікації та авторизації можуть викликати проблеми з безпекою, оскільки недоброзичливі сторони можуть отримати доступ до важливих даних;

– використання слабкого шифрування може зробити дані уразливими перед атаками з перехопленням даних або зловживанням даними;

– недосконаліть підготовки персоналу щодо кібербезпеки та правил безпеки може створити можливості для соціального інжинірингу та інших видів атак, які використовують людський фактор;

– вади системи резервного копіювання можуть призвести до втрати важливих даних у разі виникнення непередбачуваних ситуацій, таких як технічні збої або кібератаки;

– ігнорування цифрового електронного підпису документів може призвести до різних негативних наслідків, особливо у випадках, коли безпека та валідність документів є критичними аспектами.

1.2 Електронний цифровий підпис як елемент захисту систем електронного документообігу

Електронний цифровий підпис (ЕЦП) – це технологічний механізм, який дозволяє вам електронно підписувати документи або інші електронні повідомлення [14]. Ігнорування ЕЦП – одна з найбільш поширених слабких сторін систем

електронного документообігу [13,15].

Відсутність ЕЦП може призвести до недостатньої захищеності процесу ідентифікації відправника документа, що в свою чергу може відкрити двері для шахрайства або підробки. Без ЕЦП може бути складно визначити, чи документ був змінений після його створення, що може призвести до невпевненості в щодо правдивості даних між компаніями або сторонами. У багатьох юрисдикціях, відсутність ЕЦП може призвести до недійсності електронних документів, які потребують правового підтвердження та достовірності [16]. Існує ризик порушення конфіденційності даних, оскільки за відсутності ЕЦП немає надійного засобу для перевірки автентичності документа та відправника. Відсутність ЕЦП також може призвести до затримок у процесі перевірки та схвалення документів, оскільки необхідно використовувати альтернативні методи перевірки їх достовірності.

Потенційним рішенням проблем кібербезпеки систем електронного документообігу є використання цифрових підписів [17].

Традиційне використання підписів (власноручних рукописних) часто пов’язують з гарантією неспростовності, цілісності та автентичності різних видів угод, у формі контрактів тощо. Однак, цілісність документа не може бути гарантована використання власноручних підписів – є можливість підмінити сторінки або підправити електронний текст.

Цифровий світ став і залишається на підйомі, тому логічною ідеєю постало перенести цю практику підписів в цифровий світ. Вперше концепція цифрових підписів введена Діффі та Хеллманом [18] як теоретизована схема цифрового підпису, однак у їх статті лише припущено, що така схема теоретично існує. Автори запропонували, щоб кожен користувач оприлюднював відкритий (загальнодоступний ключ), який використовується в схемі для перевірки підпису, але зберігаючи при цьому секретний (конфіденційний) ключ, який використовується у схемі для створення підпису. У схемі цифрового візування підпис користувача для певного повідомлення є таким значенням, яке залежить як від цього повідомлення, так і від конфіденційного ключа підписанта, ще й таким чином, що будь-хто може перевірити підпис автора за допомогою

загальнодоступного ключа підписанта. Хоча перевірити підпис за допомогою загальнодоступного ключа підписанта легко, підробити підпис документа важко, оскільки конфіденційний ключ, як це виходить з назви, є секретним і обов'язковим для фальсифікації підпису.

Алгоритм RSA, представлений Rivest з колегами [19], давав вже практичний, але початково досить примітивний варіант цифрового підпису.

Незважаючи на те, що власноручні рукописні підписи існують уже досить давно і є досить прості у використанні, цифровий варіант відрізняється від них і має деякі основні і супутні технічні проблеми. Цифрові підписи вимагають, щоб підписант (власник підпису або той, хто підписує документ) обов'язково мав пару власних ключів – конфіденційний і загальнодоступний. Ці два ключі є математичними операндами, зворотними один одному, що поєднує їх унікальним зв'язком. Це дозволяє скасовувати операцію (наприклад, результат підписання документа), виконану за допомогою конфіденційного (закритого) ключа, за допомогою загальнодоступного (відкритого) ключа. Тобто, конфіденційний ключ використовується лише для підпису, тоді як загальнодоступний ключ використовується для підтвердження справжності цифрового підпису.

Безпека процесу підписання залежна від того, щоб конфіденційний ключ був доступний лише підписанту, і жодному іншому. Як ця властивість безпеки є гарантована, одержувач підписаного документу може бути впевнений, що лише справжній підписант зі своїм особистим ключем був здатен підписати електронний документ або повідомлення, файл тощо.

Одночасно через цей механізм забезпечується безпека властивостей інформаційної безпеки щодо неспростування та автентичності, оскільки підписант є унікальним власником конфіденційного ключа і тому не може заборонити власноручно зроблену дію накладання підпису (невідмовність) і персонально може бути пов'язаний із вмістом (автентичність).

Іншою властивістю, яку гарантує застосування технологій ЕЦП, є цілісність. Має бути обчислювально неможливим, щоб для пари різних документів створювався той самий цифровий контрольний вміст після застосування технології

ЕЦП. Більшість сучасних схем ЕЦП гарантують, що навіть однобітна зміна у вмісті електронного документу створювала зовсім інший ЕЦП. Кожна зміна, внесена до коду документа, розпізнається схемою верифікації та робить оригінальний цифровий підпис невідповідним коду документа, вимагаючи підписання даних повторно. Поняття цілісності, незаперечності та автентичності сукупно роблять використання ЕЦП універсальним інструментом кібербезпеки.

Електронний цифровий підпис є важливим елементом захисту в системах електронного документообігу, оскільки він гарантує автентичність документів, цілісність даних та їх недоторканість під час передачі та зберігання [6,20,21]. Використання цифрового електронного підпису у системах електронного документообігу є важливим елементом забезпечення кібербезпеки, конфіденційності та правової вірогідності електронних документів [21].

До переваг цифрового електронного підпису як елементу захисту систем електронного документообігу слід віднести [6,20-22]:

– ЕЦП дозволяє перевірити ідентичність особи, що підписує документ, забезпечуючи підтвердження авторства та автентичності документа;

– ЕЦП дозволяє виявити будь-які зміни в документі, забезпечуючи захист від несанкціонованих змін або пошкоджень;

– ЕЦП має юридичну силу та визнається в багатьох країнах як еквівалент паперового підпису, що робить його ефективним інструментом для укладання договорів та угод у цифровій формі;

– використання ЕЦП забезпечує високий рівень безпеки документів під час передачі та обробки;

– ЕЦП дозволяє швидко та ефективно підписувати документи без необхідності у використанні паперу та друкарської техніки;

– ЕЦП дозволяє визначити факт підпису та уникнути відмови від авторства документа;

– ЕЦП може бути дуже легко перевірений за допомогою комп'ютера або сервера одержувача;

– ЕЦП неможливо підробити;

– ЕЦП забезпечує високий рівень довіри та безпеки при обміні електронними документами.

– ЕЦП виступають як ключовий елемент у різноманітних типах цифрових сертифікатів інфраструктури відкритих ключів;

– ЕЦП має широкі можливості застосування, охоплюючи різноманітні сфери в Інтернеті – від файлів програмного забезпечення і документів у Microsoft Office до електронних листів та веб-сайтів.

1.3 Технології створення цифрового підпису в системах електронного документообігу

Створення цифрового підпису у системах електронного документообігу включає такі основні кроки [23,24]:

– вибір алгоритму цифрового підпису – обирається алгоритм, який відповідає вимогам безпеки та стандартам криптографії (популярними є алгоритми RSA, DSA, ECDSA тощо);

– генерація ключів – створюються публічний та приватний ключі за допомогою криптографічних алгоритмів (приватний ключ використовується для створення підпису, а публічний ключ – для його перевірки);

– хешування даних – дані, до яких потрібно створити підпис, проходять процес хешування, що дозволяє отримати унікальний хеш-код цих даних;

– шифрування хешу даних за допомогою приватного ключа – хеш даних шифрується за допомогою приватного ключа, створюючи цифровий підпис, який додається до документа;

– публікація публічного ключа – публічний ключ пов'язується з документом і надсилається разом з цифровим підписом, щоб інші користувачі могли перевірити його автентичність.

Ці кроки гарантують надійність та автентичність цифрових підписів у системах електронного документообігу, що є важливим елементом забезпечення кібербезпеки та надійності обміну електронними документами.

Схема створення ЕЦП (рисунок 1.1) [24] для електронного документа передбачає обчислення хеш-функції цього документа та подальше шифрування отриманого хеш-значення за допомогою секретного ключа відправника.

Рисунок 1.1 – Схема формування цифрового електронного підпису

Хеш-функція, що застосовується до електронного документа для його захисту, представляє собою унікальне числове значення, яке отримується з вихідного документа через застосування складного, але відомого алгоритму, відомого як хеш-функція. Результатом цього шифрування стає саме значення ЕЦП, яке включається в електронний документ і передається одержувачу.

Технологія сертифікації документів ЕЦП [14,23] відображена на рисунку 1.2.

Особливість хеш-функції полягає в тому, що вона чутлива до будь-яких змін, навіть мінімальних, в вихідному електронному документі. Іншими словами, навіть найменша зміна або спотворення хоча б одного символу у вихідному документі призводить до істотних змін у хеш-значенні. Крім того, хеш-функція так створена, що, по-перше, на основі хеш-значення неможливо відновити вихідний електронний документ, а по-друге, майже нереально знайти два різних електронних документи, які матимуть однакове хеш-значення.

Рисунок 1.2 – Технологія сертифікації документів з використанням цифрового електронного підпису

Таким чином, ЕЦП жорстко пов'язує зміст документа та секретний ключ для формування підпису та унеможливлює зміну документа без порушення відповідності цього підпису самому документу.

1.4 Технології створення цифрового підпису із застосуванням особових атрибутів

Здається, що традиційні цифрові підписи пропонують певною мірою ту саму функціональність підпису, що й підпис на основі атрибутів, коли він призначає одну пару ключів підпису для кожної ролі, під якою користувач хоче підписати. Подібно до того, як лікар дозволяє підписати свій відкритий ключ центру сертифікації медиків, за допомогою якого лікар може використовувати свій закритий ключ для підпису вмісту як лікар. Якщо ця сама особа (лікар) хоче підписати якийсь вміст, який не стосується його медичної експертизи, потрібна інша пара ключів під іншою роллю, наприклад. роль громадянина конкретної нації в купівлі будинку. Роль лікаря, а отже, пов’язана пара ключів, у цій ситуації нічого не варті. Ви можете бути лікарем в Україні, але ця особливість не дасть вам права візуватись у Німеччині. Таким чином, існує можливість використовувати

традиційні цифрові підписи для «рольового» підпису вмісту, але цей процес виснажливий, його важко масштабувати та це створює складні проблеми з керуванням ключами. Цифровий підпис із застосуванням атрибутів дозволяє користувачам підписувати вміст під різними ролями за допомогою однієї пари ключів.

Поняття підписів із застосуванням атрибутів було явно введено Shanqing і Yingpei [25]. Maji з однодумцями [26] продовжив цю роботу і описує підпис із застосуванням атрибутів як «універсальний примітив, що дозволяє стороні підписувати повідомлення з детальним контролем над ідентифікаційною інформацією».

Як описано Альпаром і Джейкобсом [27], повна ідентифікація себе часто не потрібна. Часто буває так, що постачальник послуг вимагає лише кілька особистих даних (атрибутів) користувача, щоб запропонувати певну послугу. Існуючий, але в основному теоретичний проєкт під назвою ABCJTrust, описаний в роботах [28-30], мав на меті розробити структуру під ідентифікатором ABC (Attribute-based Credentials – облікові дані на основі атрибутів) на основі існуючої технології використання атрибутів в системах електронного документообігу.

ABC4Trust – це проєкт, який фінансується Європейською Комісією та детально описаний в [31]. У документі Біксела [31] зазначено, що метою ABC4Trust є «вирішення проблеми об’єднання та взаємозамінності технологій, які підтримують надійні, але зберігають конфіденційність облікові дані на основі атрибутів». Проєкт представляє архітектурну структуру з підтвердженням концепції, яка вдосконалює так звані функції облікових даних із застосуванням атрибутів збереження конфіденційності (Privacy-ABC).

Подібним, але більш практичним проєктом є Yivi [32,33] – технологія, спрямована на реалізацію функціонального потенціалу облікових даних на основі атрибутів. Для впровадження облікових даних із застосуванням атрибутів Yivi (частково) покладається на систему ідентифікації Idemix, розроблену IBM Research [34]. Система IBM Idemix надає різні функціональні можливості для підтвердження володіння обліковими даними із застосуванням атрибутів та їхніми властивостями.

У порівнянні з ABC4Trust, Yivi використовується реально, а не лише теоретично. Ще однією перевагою Yivi над ABC4Trust є можливість підписувати

вміст за допомогою підписів ABS (Attribute-Based Signatures).

Отже, щоб пояснити проблему відсутності зрозумілих цифрових підписів, ми розглядаємо підпис на основі атрибутів, розроблений фондом Privacy by Design [35] у рамках проєкту Yivi (раніше відомого як IRMA). Схема реалізації технології цифрового підпису Yivi представлена на рисунку 1.3 [36].

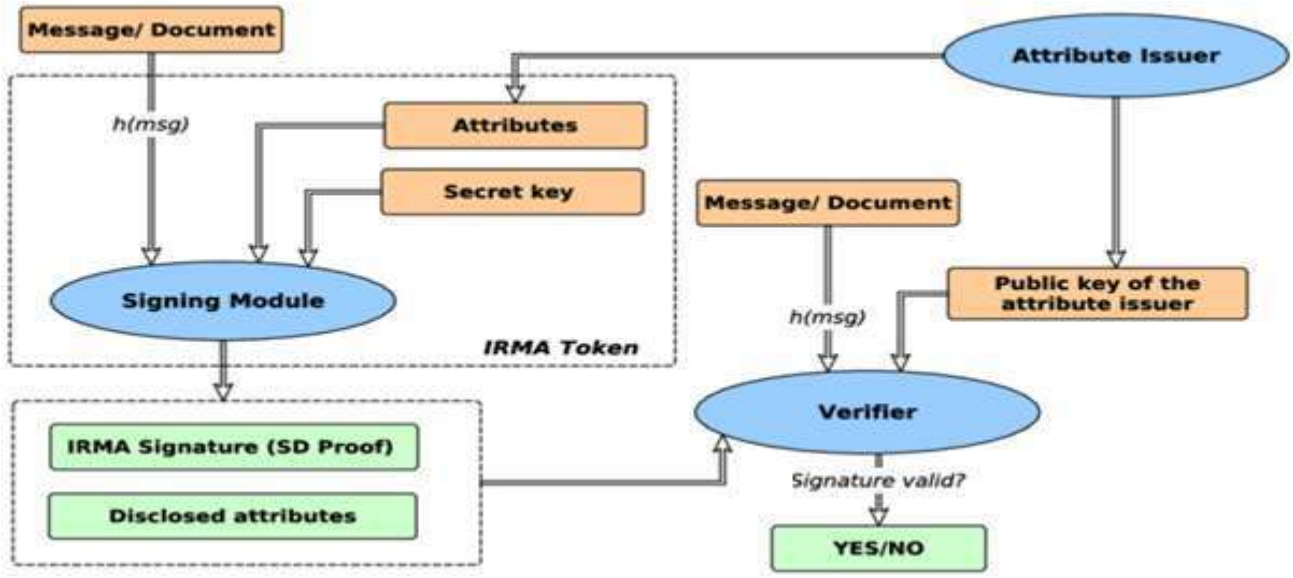


Рисунок 1.3 – Схема реалізації технології цифрового підпису Yivi-IRMA

Yivi використовує систему облікових даних із застосуванням атрибутів і розширює платформу ідентифікації за допомогою підписів на основі атрибутів. Перенесення функціональних можливостей облікових даних із застосуванням атрибутів у процесі аутентифікації в процес підписи.

Основні функції Yivi були зосереджені на аутентифікації за допомогою облікових даних на основі атрибутів, але з’явилася можливість перевести цю функцію на цифрові підписи. Це дозволило розробити нову систему, де користувачі можуть підписувати вміст за допомогою власних атрибутів. Оскільки Yivi дозволяє практично реалізувати підписи на основі атрибутів, проєкт функціонує як відповідна основа для розробки нового набору інструментів.

Деякі з питань, що стосуються систем, які претендують на конфіденційність, пов’язані з включенням файлів cookie для відстеження та використанням

центральної бази даних. IPMA не має ні того, ні іншого. Немає відстеження будь-якої діяльності Yivi або фонду Privacy by Design. Це означає, що щоразу, коли користувач розкриває атрибути або виконує певну дію в мобільному додатку Yivi, обмін даними здійснюється виключно між мобільним додатком Yivi та постачальником послуг. Немає проміжної третьої сторони, яка функціонує як точка доступу до конфіденційності. Існує також менше намірів робити це, оскільки фонд Privacy by Design налаштований як незахищений, і тому не зацікавлений у відстеженні активності користувачів для покращення потоку їх доходу. Інша проблема стосується використання центральної бази даних. Часто мобільні програми використовують центральну базу даних, яка знаходиться під контролем організації, яка розробляє програму. Мобільний додаток Yivi відрізняється тим, що йому не потрібна центральна база даних для зберігання атрибутів користувача. Усі облікові дані та відповідні атрибути зберігаються локально в мобільному додатку Yivi. Тому за безпеку атрибутів відповідає програма, а не центральна база даних.

Багато систем управління ідентифікацією організовані саме в централізованому вигляді, що створює найбільший комерційний інтерес для постачальників таких систем. Їм доступно не лише створювати та реалізовувати профілі всіх користувачів (з інформацією про те, хто, куди і коли входить, із якими даними), але також збирати оплату від довірених сторін за кожен етап аутентифікації. Це стає можливим завдяки їхньому посередництву, де вся комунікація протікає через їхні системи. Такий підхід дозволяє їм не лише контролювати, а і комерціалізувати кожен аспект ідентифікаційного процесу.

Типовим прикладом є система аутентифікації iDIN [38], впроваджена банками в Нідерландах. Під час аутентифікації через iDIN банк отримує змогу перевірити, куди відбувається вхід користувача: в магазин алкогольних напоїв, в психіатричну клініку, в специфічні заклади тощо. Банки гарантують, що не використовуватимуть цю інформацію для інших цілей, наприклад, при прийнятті рішення щодо видання іпотеки. З іншого боку, довірені сторони, такі як веб-магазини, повинні виплачувати банкам винагороду за кожен сеанс аутентифікації iDIN. Ці тарифи стають причиною серйозних обурень і скарг спільнот користувачів.

Yivi володіє децентралізованою структурою, де атрибути зберігаються тільки локально, на пристрої користувача, уникнувши централізованого зберігання в системах посередника ідентифікації.

Рисунки 1.4 і 1.5 взято з веб-сайту Privacy by Design Foundation [37]. Вони демонструють різницю між централізованою і децентралізованою (Yivi) архітектурою.

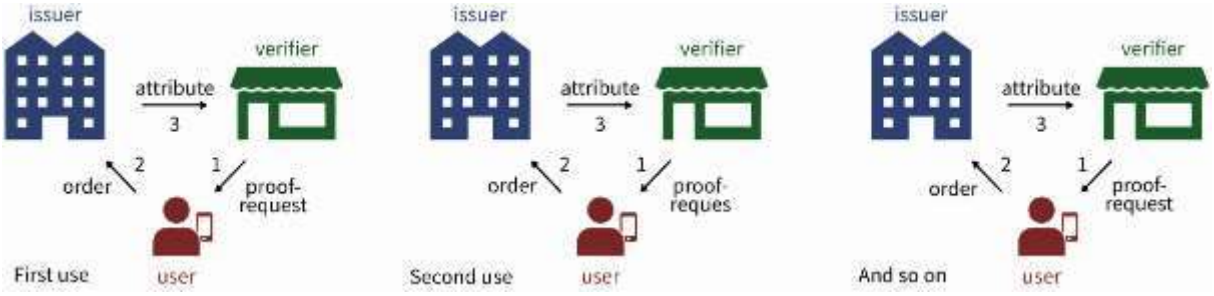


Рисунок 1.4 – Централізована архітектура технології цифрового підпису

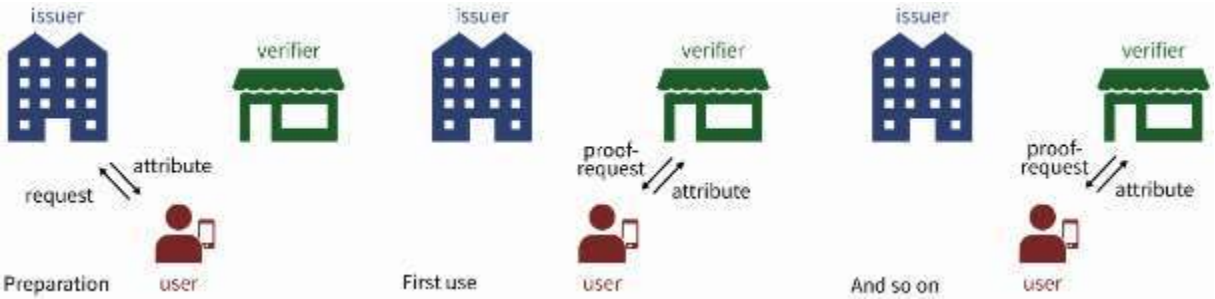


Рисунок 1.5 – Децентралізована архітектура технології цифрового підпису

В контексті Yivi відсутні штучні витрати, пов'язані із централізованою архітектурою, надаючи більш ефективний та економічний підхід.

У відмінності від Yivi, в централізованих сервісах емітент атрибутів виступає як центр конфіденційності, який фіксує та відслідковує всі транзакції. Така централізована архітектура відкриває можливість для зловмисного емітента повністю захопити вашу ідентичність та видати себе за вас. У такому випадку користувач практично не має засобів припинити це або навіть виявити проблему до її настання або пізніше, коли наслідки стають очевидними.

Децентралізована структура Yivi надає користувачеві реальний контроль над використанням його атрибутів. Кожен користувач самостійно розкриває свої

атрибути лише після явної згоди, і це відбувається без (непотрібного) втручання третіх сторін. Порівняйте це з тим, як користувач може самостійно пред'явити свій фізичний паспорт, незалежно від будь-якого посередника.

У централізованій архітектурі, яка не використовує Yivi, користувач має кожного разу надсилати запит емітенту, коли йому потрібно підтвердити певні атрибути. Це означає, що третя сторона (емітент) завжди повинна взаємодіяти з верифікатором. Такий підхід дозволяє цій третій стороні "відстежувати" запити користувача, що може негативно впливати на конфіденційність користувача.

Окрім Yivi, існує декілька проєктів, які прагнуть досягти схожих цілей за допомогою технологій ЕЦП, заснованих на атрибутах [39].

Експериментальний проєкт Decode є спрямованим на розробку практичних альтернатив використання Інтернету. Він надає інструменти, що дозволяють людям контролювати конфіденційність своєї особистої інформації та вирішувати, чи ділитися нею для суспільного блага.

Проєкт Schluss повертає контроль над інформацією атрибутів користувача технології цифрових підписів користувачам і використовує відкриті технології для досягнення своєї мети.

Технологія Serto дозволяє користувачам зробити дані більш портативними, приватними та цінними за допомогою децентралізованої технології. Вони створили платформу, яка дозволяє перевіряти джерело даних і контролювати їх видачу.

Блокчейн-стартап SelfKey пропонує рішення для цифрової ідентифікації. Один з їхніх продуктів – електронний гаманець SelfKey, призначений для забезпечення повного контролю користувачів над своїми даними, документами та цифровими активами.

Некомерційна організація Sovrin, аналогічна фонду Privacy by Design, сприяє самосуверенній ідентичності через мережу Sovrin, що базується на відкритому вихідному коді.

В таблиці 1.1 наведено порівняльну інформацію щодо можливостей розглянутих технологій ЕЦП на основі атрибутів.

Таблиця 1.1 – Можливості технологій ЕЦП на основі атрибутів

№ з/п	Техно-логія	Аутенти-фікація	Сигнатура ЕЦП	Децентра-лізація	Відкритий код	Робоча версія
1	YIVI	+	+	+	+	+
2	DECODE	+	-	-	+	+
3	Schluss	+	-	-	+	+
4	Serto	+	-	+	+	-
5	Sovrin	+	-	+	+	+
6	SelfKey	+	-	+	+	+

Аналіз даних таблиці 1.1 і результатів вивчення можливостей проєктів-технологій використання цифрового підпису із застосуванням атрибутів дозволяє дійти ряду висновків.

Загальною тенденцією цих альтернативних проєктів технологій ЕЦП з використання атрибутів є використання атрибутів та облікових даних, які користувачі можуть надавати або розкривати під час аутентифікації у постачальника послуг. Іноді це також називається спільним використанням атрибутів. Основна ідея всіх цих проєктів полягає в тому, що вони дозволяють користувачам краще контролювати свої дані, як особисті, так і неособисті.

На відміну від інших ініціатив, Yivi вирізняється можливістю використовувати атрибути для підпису цифрового контенту. Здається, що всі інші проєкти сконцентровані лише на створенні безпечного простору для зберігання облікових даних і розкриття чи передачі їх постачальникам послуг за бажанням користувача. Ще однією актуальною різницею між цими проєктами є застосування різних підходів щодо децентралізації. Yivi, Serto, Sovrin і SelfKey використовують принципи децентралізації, однак існує відмінність у способі реалізації цього принципу. Serto, Sovrin і SelfKey використовують технологію блокчейн.

Yivi обирає інший підхід до децентралізації без застосування технології блокчейн. Під час використання YIVI жодна третя сторона не втручається, коли

користувач розкриває атрибути або виконує підписи на основі атрибутів. Це означає, що технологія відповідає лише рівню "розширених" цифрових підписів в рамках правил eIDAS. Однак, такий підхід сприяє децентралізації без участі третьої сторони, утворюючи однорангову структуру, в якій користувач може розкривати атрибути безпосередньо постачальнику послуг.

Існує багато альтернативних проєктів, що намагаються впроваджувати технології із застосуванням атрибутів для аутентифікації або для підписів. Проте можна відзначити, що всі ці проєкти, окрім Yivi, фокусуються переважно на ідеї самосуверенної ідентичності і не пропонують жодного рішення для використання технологій із застосуванням атрибутів у цифровому підписі контенту, тобто, не здатні формувати сигнатури ЕЦП.

1.5 Постановка задачі

Використання атрибутів для поліпшення зрозумілості цифрових підписів виглядає перспективно, але наступний крок - перетворення теоретичної концепції у реальність. У наступних розділах потрібно розглянути, як саме можна здійснити цей перехід від теорії ідеї до практики алгоритмів і технічної реалізації, використовуючи технологію цифрового підпису із застосуванням атрибутів підписанта в системах електронного документообігу.

Багатьом поточним реалізаціям технологій цифрових підписів бракує соціального аспекту – зрозумілості і можливості безпечного використання в нетрадиціних застосуваннях у різноманітних сервісах. Особі-верифікатору, яка перевіряє підписаний документ, необхідно мати достатньо інформації для того, щоб визначити, чи є отриманий вміст дійсним. Важливо, щоб було зрозуміло, хто саме підписав цей вміст. Це дозволяє самому користувачу, який проводить верифікацію, самостійно вирішувати, як далі діяти з отриманим контентом.

Знання джерела вмісту цифрового контенту у системі електронного документообігу є ключовим для забезпечення автентичності, і важливо, щоб

верифікатор розумів семантику цифрового підпису.

Якщо особисті дані підписанта, пов'язаний документ та сам підпис можуть бути легко прочитані і зрозуміті, інформаційна цінність цифрового підпису значно зростає. Це, в свою чергу, сприяє боротьбі з впливом інформаційної фальсифікації, оскільки забезпечує чіткість та довіру щодо автентичності та походження підписаного цифрового контенту.

Мета кваліфікаційної роботи полягає у вдосконаленні і розширенні можливостей технології використання цифрового в системах електронного документообігу та інших електронних сервісах з авторизацією користувачів за рахунок застосування у сигнатурі підпису особових атрибутів підписанта.

Щоб реалізувати програму досліджень необхідно:

а) виявити перспективні напрямки та способи вдосконалення технології використання цифрового підпису в системах електронного документообігу, що можуть бути використані у підвищенні її ефективності;

б) визначити основні положення технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу;

в) розробити математичну модель технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу;

г) здійснити алгоритмічну реалізацію технології;

д) провести апробацію дієвості прийнятих теоретичних і алгоритмічних рішень технології.

Потрібно також розглянути конкретні застосування цифрового підпису у сферах електронної документації та надати практичні рекомендації, які забезпечать зрозумілість та надійність застосування цього інноваційного підходу.

2 МАТЕМАТИЧНА МОДЕЛЬ ДЛЯ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ЦИФРОВОГО ПІДПИСУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1 Базові положення розробки математичної моделі

Однією з важливих функцій математичної моделі ЕЦП є забезпечення довіри в цифровому середовищі. Вона створює механізм, який гарантує, що електронна інформація залишається недоторканною та автентичною під час обміну.

Якісна математична модель технології ЕЦП враховує сучасні методи захисту від криптоаналізу. Це включає в себе вдосконалені математичні алгоритми, які роблять надійність та стійкість ключів відповідним чином довговічними, зменшуючи ймовірність невдачі в системах електронного документообігу. Таким чином, математична модель технології ЕЦП набуває критичного значення для забезпечення безпеки, автентичності та цілісності електронної інформації, відкриваючи шлях до нових можливостей для розвитку цифрового суспільства.

Для синтезу математичної моделі нашої технології використання цифрового підпису в системах електронного документообігу спочатку проаналізуємо особливості традиційних моделей сучасних технологій аналогічного призначення.

Традиційно, надійний механізм для захисту від несанкціонованого доступу та змін електронних документів надає використання асиметричної криптографії та хеш-функцій. Використання асиметричної криптографії та хеш-функцій утворює міцний фундамент для ефективного функціонування електронних цифрових підписів, надаючи гарантії конфіденційності та цілісності електронної інформації.

Математичні принципи асиметричної криптографії є основою для забезпечення захисту від несанкціонованого доступу та неправомірних змін. Використання пари ключів – конфіденційного та загальнодоступного, дозволяє ефективно підписувати та перевіряти електронні документи, забезпечуючи конфіденційність та ідентифікацію авторства.

Математично-обґрунтовані механізми хеш-функцій у моделі грають важливу роль у забезпеченні цілісності даних в системах електронного документообігу. Генерація унікального "відбитку" вмісту документа дозволяє ефективно виявляти будь-які зміни в підписаних ЕЦП електронних документах. Це не лише надає інструмент для виявлення порушень цілісності, але й впливає на високий рівень довіри до електронних підписів.

Використання математичних принципів аутентифікації дозволяє перевіряти, чи є підпис валідним, чи він був створений особою, яка має відповідний приватний ключ. Якісна математична модель дозволяє розпізнавати автентичність електронних підписів та підтверджувати їх достовірність.

Використання особових атрибутів підписанта в технології і математичній моделі значим чином розширює можливості і універсальність технології використання цифрового підпису в системах електронного документообігу.

В математичній моделі технології ЕЦП із застосуванням особових атрибутів, розглядається врахування різноманітних атрибутів підписанта для забезпечення високого рівня безпеки та гнучкості системи. Таким чином модель із застосуванням особових атрибутів дозволяє реалізувати ефективний контроль доступу із застосуванням атрибутів користувачів. Кожен атрибут може мати вагу або рівень довіри, і доступ до конкретної інформації може залежати від комбінації цих атрибутів. Це дозволяє гнучко налаштовувати політики безпеки з урахуванням контексту використання.

Однією з переваг моделі ЕЦП із застосуванням особових атрибутів є її здатність динамічного оновлення атрибутів в реальному часі. Зміни в атрибутах користувача можуть автоматично відображатися в цифровому підписі, що робить систему більш гнучкою та реактивною до змін у середовищі. Математичний апарат дозволяє динамічно оновлювати атрибути користувачів, що робить систему адаптабельною до змін в індивідуальних характеристиках користувачів і дозволяє системі ефективно взаємодіяти з реальними змінами в обставинах.

В математичній моделі, що використовує атрибути, може застосовуватись асиметрична криптографія на основі характеристик користувача. Замість

використання загального ключа, приватний та публічний ключі генеруються із застосуванням атрибутів особи, що робить систему більш гнучкою та адаптованою до специфічних властивостей користувачів.

Модель передбачає можливість використання мультиатрибутної аутентифікації, де комбінація різних атрибутів, таких як біометричні дані, геолокація, часові параметри тощо, формує унікальний підпис. Це підсилює рівень безпеки та запобігає несанкціонованому доступу, оскільки для підпису необхідна відповідність не одного, а кількох атрибутів.

Таким чином, математична модель технології ЕЦП із застосуванням атрибутів відкриває нові перспективи для забезпечення безпеки та ефективності в цифровому середовищі. Цей підхід не лише покращує безпеку підписів, але й забезпечує адаптабельність системи до різних сценаріїв використання та динамічних змін в атрибутах користувачів.

2.2 Криптографічні складові математичної моделі технології використання цифрового підпису

Одним із широко використовуваних алгоритмів цифрового підпису є алгоритм Ель-Гамаля.

Особливість цього алгоритму в тому, що на основі відкритого тексту $M = \{m_1\}$ і пари чисел $\{P, G\,(G < P)\}$ (ці числа розповсюджені серед користувачів системи), пара ключів генерується у реалізації самого алгоритму шифрування, а не в спеціалізованому модулі генерації. Конфіденційний ключ $K_B\,(K_B < P)$ обирається випадковим чином. Відкритий ключ вираховують за формулою:

$$K_K = G^{K_B} \bmod P\,. \qquad (2.1)$$

Крім ключа шифрування K_a відкритого тексту M задіюється випадкове ціле

число *K*, що задовольняє умовам:

$$\begin{cases} 1 < N < P-1 \\ \text{НСД}(N, P-1) = 1 \end{cases} \tag{2.2}$$

де НСД – найменший спільний дільник.

Потім вираховуються числа *a* і *b*:

$$a = G^N \bmod P \tag{2.3}$$

$$b = {K_K}^N * M \bmod P \tag{2.4}$$

Пара чисел (*a*, *b*) стає шифртекстом. Недоліком є те, що довжина шифртексту подвоює довжину вихідного відкритого тексту *M*.

Для розшифрування шифртексту використовують формулу перетворення:

$$M = \frac{b}{a^{K_B}} \bmod P \tag{2.5}$$

Математична дійсність оберненого перетворення шифртексту грунтується на принципі:

$$\frac{b}{a^{K_B}} \equiv \frac{{K_K}^K * M}{a^{K_B}} \equiv \frac{G^{K_B N} * M}{G^{K_B N}} \equiv M \,(\bmod P) \tag{2.6}$$

Це загальні принципи шифрування за алгоритмом Эль-Гамаля.

Технологія цифрового підпису з використанням алгоритму Ель-Гамаля передбачає використання тих самих ключів K_K й K_B, що й у шифруванні.

Технологія ЕЦП має передбачати дві процедури:

1) процедуру накладання ЕЦП;

2) процедуру перевірки ЕЦП.

У процедурі накладання ЕЦП використовується конфіденційний (відомий також як секретний або приватний тощо) ключ K_K підписанта-відправника повідомлення, у процедурі ж перевірки ЕЦП – відкритий (загальнодоступний або загальнорозповсюджений) ключ K_a підписанта.

У процедурі накладання ЕЦП підписант першочергово формує хеш-функцію $h(M)$ відкритого тексту M, який завіряється ЕЦП. Отримуване значення хеш-функції $h(M)$ являє з себе бітовий рядок фіксованої довжини, що і характеризує весь текст M в цілому. Бітовий рядок хеш-функції $h(M)$ шифрується конфіденційним ключем K_K підписанта-відправника повідомлення. Пара чисел, що отримується при шифруванні бітового рядка хеш-функції $h(M)$, являє собою ЕЦП для тексту M.

При верифікації ЕЦП цифрового підпису отримувач повідомлення повторно здійснює розрахунки бітового рядка хеш-функції від прийнятого каналом відкритого тексту повідомлення $m=h(M)$, після чого із використанням відкритого ключа підписанта перевіряє ідентичність отриманого бітового рядка хеш-функції з ЕЦП обчисленому значенню m.

Роботу технології ЕЦП в описаному математичному базисі можна представити схематично (рис. 2.1).

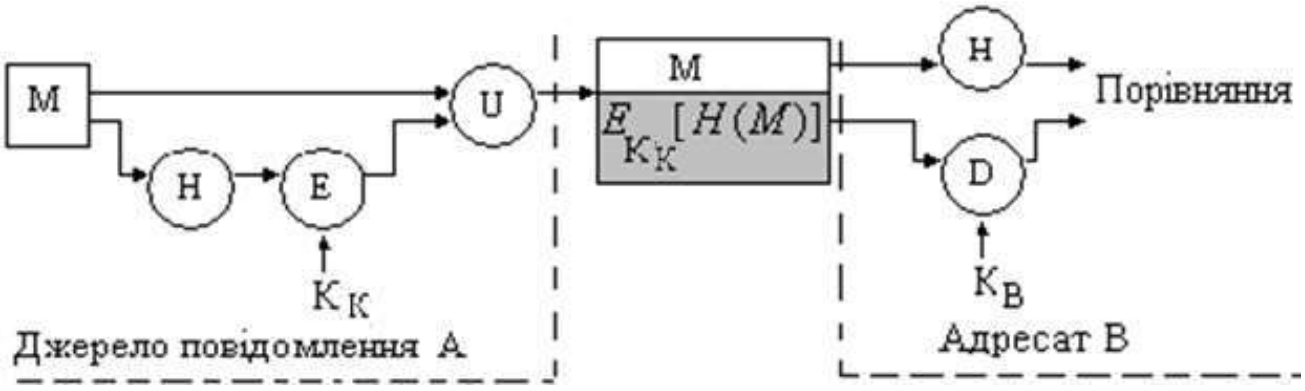


Рисунок 2.1 – Схема реалізації ЕЦП традиційними методами

У технології ЕЦП ключовим моментом постає неможливість підробки користувацького цифрового підпису без знання конфіденційного ключа підписанта

K_K. Також важливо, що у технології ЕЦП будь-який файл може бути використаний як відкритий текст для підписування – цифровий документ будь-якого формату сприймається як двійковий код тексту, зображення, електронних таблиць або іншого формату абсолютно ідентично.

Універсалізації технології ЕЦП додає підхід, при якому підписаний файл може формуватися шляхом додавання до нього як одного, так і кількох електронних підписів.

Щодо функції хешування $h(M)$, то тут важливо, щоб вона була відповідна кільком властивостям:

– необерненість перетворення – за значенням хешу $h(M)$ неможливо відтворити відкритий текст M;

– неповторність значень хешу двох текстів M_1 і M_2, за якою будь-якого коду $h(M_1)$ має бути практично неможливо обчислити $M_2 \neq M_1$ з виконанням вимоги $h(M_1)=h(M_2)$, тобто, практично неможливо знайти два різні відкритих тексти блоки M_1 і M_2, щоб їхні хеш-значення $h(M_1)$ і $h(M_2)$ співпали;

– застосовуваність до коду відкритого тексту M будь-якої довжини;

– простота і однотипність процедури формування значення $h(M)$ до двійкового коду відкритого тексту M будь-якої довжини;

– фіксована довжина значення $h(M)$ для будь-якої довжини вхідного двійкового коду M;

– алгоритм обчислення $h(M)$ повинен бути ефективним як у програмній реалізації, так і у апаратній.

2.3 Складові математичної моделі для реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта

Технологія цифрового підпису із застосуванням особових атрибутів підписанта, як це слідує з назви, базується на використанні у підписі особових

атрибутів підписанта.

Математична модель технології електронного цифрового підпису, реалізовуваної на основі особових атрибутів підписанта, має орієнтувати математичний апарат на класичний набір ключових функцій ЕЦП, спрямованих на підвищення безпеки, достовірності та гнучкості процесу електронного підписування, але з урахуванням особливостей атрибутивного підпису. Призначення цієї математичної моделі у пропонованій технології використання цифрового підпису в системах електронного документообігу є вирішальним для успішного впровадження та використання цієї технології.

Математична модель може враховувати різноманітні атрибути, такі як біометричні дані, геолокаційні параметри та інші, для ідентифікації та аутентифікації користувачів. Це робить технологію цифрового підпису більш надійною.

Застосування атрибутів, таких як унікальні біометричні характеристики або контекстуальні параметри, допомагає ускладнити можливість фальсифікації електронних підписів. Це стає важливою перевагою в умовах, де забезпечення нерозсекречуваності та цілісності даних є критичним.

Для визначення складових математичної моделі для реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта першочергово слід класифікувати атрибути, які можуть і доцільно використовувати в технології.

Проведений аналіз дозволив виділити три типових категорії атрибутів особи:

– ідентифікаційні атрибути;
– неідентифікаційні атрибути;
– контекстуальні атрибути.

Як ідентифікаційні атрибути будемо розглядати такі, які 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 (псевдонім, який однозначно пов'язаний з особою);
– ідентифікатор (номер або серія-номер) посвідчення з місця роботи;
– серія-номер водійського посвідчення;
– номер телефона (за умови індивідуального користування) тощо;
– особистий ідентифікатор електронної пошти (e-mail) або соціальних мереж.

Як неідентифікаційні атрибути будемо розглядати 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;
– освіта;
– фах;
– місце роботи;
– посада;
– неідентифікуючий особу псевдонім (широко розповсюджений або такий, що відомий тільки довіреній особі або обмеженому колу довірених осіб);
– дата народження;
– вік;
– дата видачі паспорту (будь-якого іншого документа тощо);
– орган, що видав паспорт (будь-який інший документа тощо);
– номер телефона загального користування тощо.

З наведених прикладів слідує, що неідентифікуючими атрибутами можуть бути як широко розповсюджені дані особи, так і нікому не відомі дані.

Якщо ідентифікаційні атрибути служать для точної ідентифікації особи, то неідентифікаційні атрибути надають контекст і додаткову інформацію без прямої ідентифікації. У контексті електронного цифрового підпису, комбінація обох типів атрибутів спрямована на створення безпечних та адресно-орієнтованих підписів.

Особливістю неідентифікуючих атрибутів є можливість отримання на їх основі у певних ситуаціях ідентифікаційного атрибута або ідентифікаціного набору атрибутів. Розповсюджені прізвище, ім’я та по батькові при об’єднанні утворюють ідентифікаційний атрибут ПІБ. Освіта, посада, місце роботи підписанта тощо можуть ідентифікувати його особу, якщо при аналізі визначиться відсутність конкурентів за відповідним атрибутом в колі здійснення ідентифікаційного аналізу. Така можливість повинна враховуватись в технології використання цифрового підпису в системах електронного документообігу, що є предметом подальших досліджень.

Як контекстуальні атрибути підпису будемо розглядати 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 підписанта 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);

– змінювані біометричні параметри фізичного стану особи (пульс, температура тощо);

– зовнішні умови оточуючого середовища;

– тип пристрою, задіяний для накладання ЕЦП;

– дані аутентифікації під час входу в систему;

– права та повноваження підписанта;

– роль підписанта у певному конкретному контексті тощо.

Контекстуальні атрибути, такі як інформація про географічне положення підписанта і час накладання підпису, не є основними, але можуть бути застосовані для забезпечення додаткового рівня безпеки ЕЦП.

Зрозуміло, що не всі перелічені атрибути при реалізації технології доцільно включати до ЕЦП одночасно і загалом не всі вони є зручними для використання в технології та доцільними відповідно кожному окремо взятому застосуванню.

При формуванні технології використання цифрового підпису в системах електронного документообігу і розробці її математичної моделі будемо спиратись на наданні їм властивостей гнучкості, адаптивності та мультиатрибутності. Зазначені принципи передбачають надання підписанту можливості формувати цифровий підпис з довільної кількості атрибутів та визначати їх склад за власним побажанням або у відповідності до потреб.

Для гнучкості вибору атрибуту і забезпечення математичного підґрунтя адаптивності мультиатрибутного формування ЕЦП в технології використання цифрового підпису введемо до математичної моделі множини відповідних атрибутів. В якості ідентифікаторів множин атрибутів використаємо абревіатури англомовного перекладу назв множин:

– IA – ідентифікаційні атрибути (Identifying Attributes);
– NIA – неідентифікаційні атрибути (Non-Identifying Attributes);
– CA – контекстуальні атрибути (Contextual Attributes).

З цього ми отримуємо в математичній моделі три множини атрибутів:

$$IA:\{IA_1, IA_2, \dots, IA_i, \dots, IA_k\}, \tag{2.7}$$

$$NIA:\{NIA_1, NIA_2, \dots, NIA_j, \dots, NIA_m\}, \tag{2.8}$$

$$CA:\{CA_1, CA_2, \dots, CA_l, \dots, CA_n\}, \tag{2.9}$$

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

Кожне значення атрибутів $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$ є двійковим представленням відповідного атрибуту, тому далі будемо ідентифікувати елементи множин як двійкові коди або двійкові вектори атрибутів математичної моделі технології використання цифрового підпису в системах електронного документообігу.

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

Схематично процедура формування цифрового підпису в примітивах математичної моделі технології представлена на рисунку 2.2.

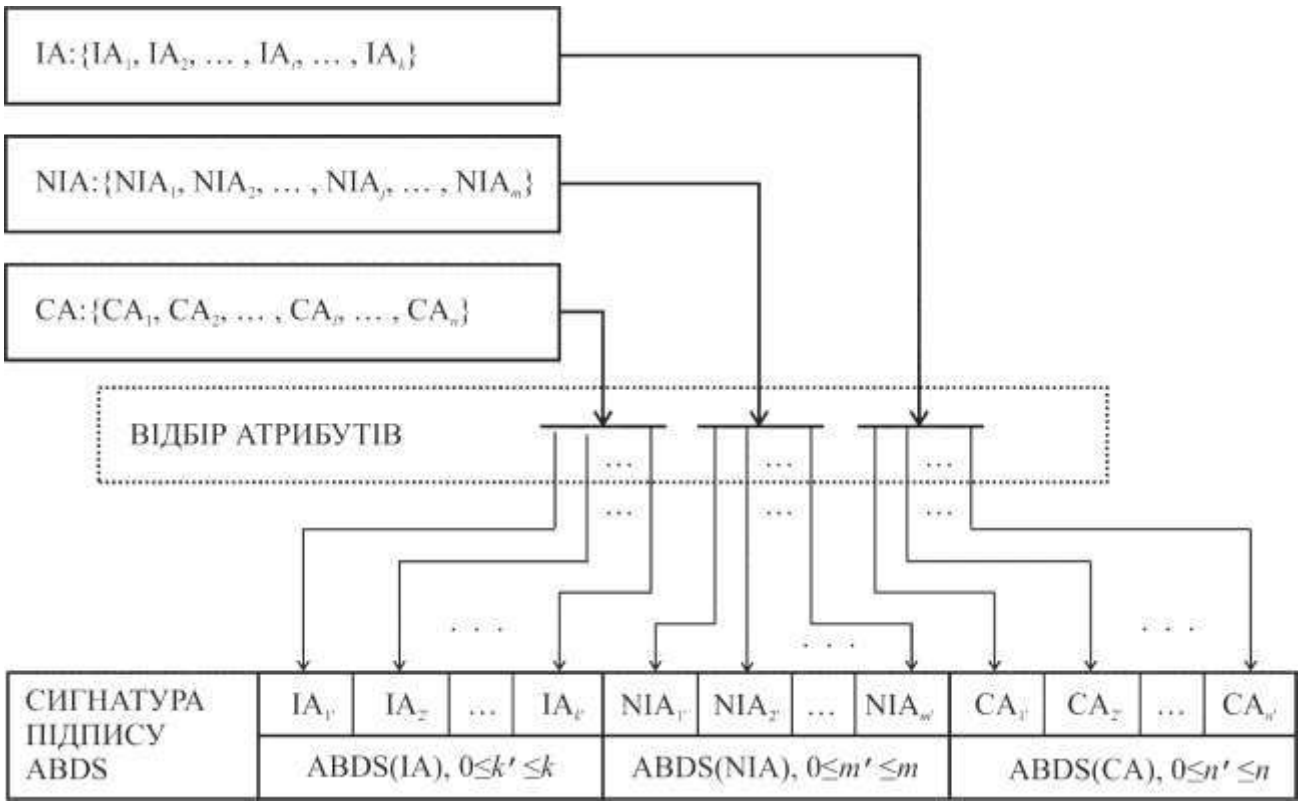


Рисунок 2.2 – Схема утворення сигнатури цифрового підпису із застосуванням особових атрибутів

Наведені на рисунку 2 для полів ABDS(IA), ABDS(NIA), ABDS(CA) сигнатури цифрового підпису ABDS обмеження $0 \le k' \le k$, $0 \le m' \le m$, $0 \le n' \le n$ ілюструють, що в ході утворення сигнатури цифрового підпису із застосуванням атрибутів до її складу можуть включатися атрибути кожного класу у будь-якій кількості від нуля (атрибути відповідного класу і саме поле цих атрибутів в сигнатурі цифрового підпису будуть відсутні) до максимальної кількості задекларованих атрибутів відповідної полю множини атрибутів.

В іншій інтерпретації обмеження $0 \le k' \le k$, $0 \le m' \le m$, $0 \le n' \le n$ можна записати у вигляді:

$$0 \le |ABDS(IA)| \le |IA)|, \quad (2.10)$$

$$0 \le |ABDS(NIA)| \le |NIA)|, \quad (2.11)$$

$$0 \le |ABDS(CA)| \le |CA)|. \quad (2.12)$$

Таким чином, математична модель враховує можливість максимально гнучкої і адаптивної потребам підписанта мультиатрибутного ЕЦП, що використовує комбінацію різних атрибутів для створення підпису. Це збільшує безпеку та точність ідентифікації, оскільки для визначення особи використовується не один, а довільна кількість атрибутів різних класів.

Сигнатура ABDS цифрового підпису із застосуванням особових атрибутів , за раніше описаними класичними принципами, разом з хеш-сигнатурою відкритого тексту може піддаватися криптографічному шифруванню (закриттю) і додаватися до відкритого тексту. Можливе використання сигнатури цифрового підпису із застосуванням атрибутів ABDS і у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта. Ці дві передбачувані математичною моделлю перспективи роблять можливим використання технології цифрового підпису в системах електронного документообігу більш широкими, а саму технології гнучкішою і універсальнішою.

2.4 Висновки

Математична модель технології синтезована з орієнтацією на функції, спрямовані на поліпшення якості та безпеки ЕЦП як ключового елемента систем електронного документообігу та сервісів цифрового середовища. Математична модель повністю враховує інноваційний підхід до електронного підписування, надаючи необхідний математичний інструментарій, щоб забезпечити високий рівень ідентифікації та безпеки в електронних комунікаціях та в обміні даними.

Математична модель є основою для створення адаптивних систем, які можуть реагувати на зміни в атрибутах особи. Здатність динамічно адаптуватися до нових атрибутів або їх змін робить такі підписи більш гнучкими та ефективними в різних сценаріях використання.

Математична модель технології електронного цифрового підпису із застосуванням атрибутів враховує різноманітні характеристики та атрибути підписанта для створення надійних та гнучких цифрових підписів. Модель дозволяє включати контекстуальні атрибути, такі як часові та геолокаційні параметри, у підпис. Це додає додатковий рівень інформації, що стає корисним в різноманітних сценаріях використання, включаючи правові аспекти та внутрішні організаційні політики.

Математична модель використовує асиметричну криптографію та атрибутні ключі, щоб забезпечити високий рівень безпеки електронних підписів. Генерація унікальних ключів із застосуванням атрибутів особи ускладнює можливість несанкціонованого доступу та фальсифікації.

Ці атрибути ідентифікуються та враховуються в математичній моделі для створення ідентифікатора особи, який служить основою для створення безпечного та гнучкого електронного цифрового підпису. Урахування цих атрибутів забезпечує більш високий рівень безпеки та точності в процесі електронного підписування.

3 СИНТЕЗ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ЦИФРОВОГО ПІДПИСУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

3.1 Принципи реалізації технології цифрового підпису

Основною фокусною точкою цього розділу є технічні можливості технології цифрового підпису із застосуванням особових атрибутів підписанта, а також можливості її впровадження в системи електронного документообігу. Важливо визначити, як ця технологія може додати внесок у розвиток електронного документообігу та призвести до покращення розуміння цифрових підписів із застосуванням атрибутів серед звичайних користувачів Інтернету. Розуміння принципів реалізації запропонованої технології цифрового підпису із застосуванням особових атрибутів підписанта має визначити успіх її впровадження в щоденне використання.

Вимоги до набору атрибутів і інструментів мають бути доцільними для реалізації протягом заданого часу, що перетворюється на обсяг дослідження, виключаючи фокусування на основних можливостях, таких як досвід користувача. Дослідження щодо того, чи відповідає технологія цифрового підпису із застосуванням особових атрибутів підписанта усім юридичним зобов’язанням і чи дійсно набір інструментів буде використовуватися на практиці, вважається поза цілями кваліфікаційної роботи. Однак ми обговоримо, які можливості відкриваються під час використання набору інструментів технології цифрового підпису із застосуванням особових атрибутів підписанта.

Однією з переваг технології ЕЦП із застосуванням особових атрибутів є її здатність динамічного оновлення атрибутів в реальному часі. Зміни в атрибутах користувача можуть автоматично відображатися в цифровому підписі, що робить систему більш гнучкою та реактивною до змін у середовищі. Технологія дозволяє динамічно оновлювати атрибути користувачів, що робить систему адаптабельною до змін в індивідуальних характеристиках користувачів і дозволяє системі

ефективно взаємодіяти з реальними змінами в обставинах.

Важливим аспектом технології використання цифрового підпису із застосуванням атрибутів в системах електронного документообігу є мінімізація даних, коли йдеться про підвищення конфіденційності користувачів. Це вимагається законодавством України [40] і ЄС [41]. Проте мінімізація даних може призвести до зниження рівня інформаційної цінності цих даних. Коли розкривається менше даних, отримувач (читач) може мати менше інформаційних даних. Слід розглянути баланс між збереженням високої інформаційної цінності виявлених даних і розкриттям лише мінімальних (особистих) даних. У випадку цифрових підписів ми не хочемо розкривати занадто багато (особистої) інформації про підписанта, але ми також хочемо, щоб розкрита (особиста) інформація була достатньо інформативною та зрозумілою. Це можна порівняти з наміром аутентифікувати себе у постачальника послуг, не розкриваючи якомога більше особистої інформації, тобто, не більше ніж це необхідно. Тут можуть бути доречні облікові дані на основі атрибутів.

Що стосується аутентифікації, облікові дані із застосуванням атрибутів можна використовувати для вирішення проблеми розкриття занадто великої кількості особистої інформації під час аутентифікації постачальнику послуг, зберігаючи при цьому високу інформаційну цінність розкритої інформації. У традиційних системах керування ідентифікацією довірений постачальник ідентифікаційної інформації (або емітент) видає користувачеві автентичні атрибути, як-от водійські права чи студентський квиток, або будь-які інші особисті дані (атрибути), які можна використовувати для підтвердження особи користувача. Постачальник ідентифікаційної інформації несе відповідальність за керування особистими даними користувача, які необхідні для ідентифікації користувача.

Потенційна перевага використання підписів із застосуванням атрибутів полягає у збільшенні інформаційної цінності цифрового підпису. Можна побачити перевагу надання користувачам контролю над тим, чи хочуть вони розкривати певні атрибути, але варто зосередитися на стороні одержувачів (верифікатора підпису), тобто тих, хто хоче перевірити підпис. Одержувач підпису із

застосуванням атрибутів може отримати більше інформації про особу відправника (підписанта), якщо роль підписанта чітка та видима в підписі. Завдяки наданню підписанту можливості додавати до підпису певні (особисті) атрибути, інформаційна цінність підпису зростає. Одержувач цього підпису може побачити особу підписанта в більш структурованому та зрозумілому вигляді.

Загальний тип підпису показує одержувачу лише загальне (ім’я) підписанта, підтвердження того, що документ підписано (за допомогою певного конфіденційного ключа), і сертифікат, доданий довіреним органом, щоб гарантувати дійсність підпису. Загальне ім’я підписанта в більшості випадків не надає одержувачу достатньо ідентифікаційної інформації. У той же час назва центру сертифікації не звучить у більшості отримувачів. Загалом, цей підхід не надає одержувачу великої кількості інформації, особливо не про особу підписанта та джерело вмісту документа.

Зауважимо, що видавець атрибута має обов’язково відповідати гарантованому рівню довіри. Це означає, що, наприклад, атрибут диплома доктора наук має видавати лише видавець, який має «ліцензію» на це, наприклад, Хмельницький національний університет. Проте цьому ж університету не слід довіряти видавати-підтверджувати такі атрибути, як водійські права.

Тепер, коли ми визначили обмеження технології з теоретичної точки зору, слід розглянути, що важливо здійснити на практиці. Ми можемо посилити наше теоретичне дослідження, проводячи прикладні дослідження – дослідження і визначення того, що необхідно для створення набору інструментів, який зможе:

– прикріпляти підпис із застосуванням атрибутів до будь-якого типу цифрового контенту;

– перевіряти цей підпис при включенні його до конкретного цифрового вмісту;

– робити це доступним для кожного користувача.

Завданням таких досліджень є практично визначити, які кроки потрібно здійснити для розробки ефективного і універсального інструментарію. Такий набір інструментів не лише міг би дозволити прив'язувати цифрові підписи із

застосуванням атрибутів до різних видів контенту, але й забезпечити їх перевірку та доступність для широкого кола користувачів.

Перед розробкою технології використання цифрового підпису із застосуванням атрибутів в системах електронного документообігу важливо розуміти, як саме ЕЦП буде включений до цифрового вмісту. Цифровий вміст може включати файли різних типів, таких як текстові документи, зображення або відео. Існують три різні методи "зберігання" підпису: відокремлений, у конверті (інтеграція) та на конверті (обгортання).

Відокремлений підпис зберігається у окремому файлі, формат ЕЦП може бути вибраний за бажанням користувача.

Підпис у конверті - це технологія, при якій ЕЦП вбудовується безпосередньо в оригінальний цифровий вміст. Для цього оригінальний формат цифрового вмісту повинен підтримувати цей процес. Прикладами таких форматів, які дозволяють вбудовувати підписи, є PDF і XML.

Обгортання підписів використовується, якщо новий файл створюється у визначеному форматі підпису і виступає контейнером, що відображає оригінальний цифровий вміст. Найпоширенішим форматом для обгортання підписів є синтаксис криптографічного повідомлення [42,43].

Оскільки нам доводиться впоратися з обмеженнями, які дозволяють лише підписувати повідомлення (рядок) за допомогою підпису на основі атрибутів, було прийнято рішення використовувати схему хешування та підпису. Хешоване кодування цифрового вмісту використовується як вхідні дані об’єкта повідомлення в підписі на основі атрибутів. Це призводить до огортаючого підпису, де цифровий вміст вбудовано в підпис як рядок. Після цього підпис із застосуванням атрибутів вбудовується в щойно підписаний файл, який містить, серед іншої інформації, оригінальний файл (може бути зашифрований) і підпис із застосуванням атрибутів (закодований, наприклад, base64 [44]).

Практичний продукт подібних технологій – це програма для ПК або мобільний додаток, що функціонує як постачальник послуг у співпраці з сервісом підтвердження атрибутів. Програмна реалізація дає користувачеві можливість

підписувати будь-який тип файлу (цифровий вміст) за допомогою підписів із застосуванням атрибутів та перевіряти будь-який тип файлу, який підписаний підписом на основі атрибутів.

Ціллю цієї роботи є зробити семантику цифрового підпису зрозумілою. Таким чином, користувач повинен мати можливість підписувати та перевіряти підписи, які відображають зрозумілу семантику. Оскільки ця кваліфікаційна робота виконується в галузі інформаційних технологій, увага в алгоритмічних рішеннях далі буде зосереджена саме на технічних функціях. Незважаючи на те, що функціональна деталізація важлива для того, щоб зробити набір інструментів доступним і простим у використанні, вона виходить за межі цієї роботи.

При реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу важливо розділити основні і другорядні вимоги до технології, тобто, здійснити пріоритезацію вимог для визначення набору інструментів і визначення пріоритетності функціональних можливостей.

Обов’язкові вимоги і відповідні їм функції необхідні для того, щоб технологія працювала належним чином. В перших обов’язкових вимогах технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу можна вказати:

– реалізацію «схеми хеш-та-знак» (хешування та підписування електронного документу);

– можливість вибору будь-яких атрибутів для формування підпису під потреби або побажання підписанта

– можливість додавання-вилучення атрибутів при формуванні ЕЦП;

– можливість для користувача підписувати будь-який тип цифрового документа (будь-який формат файлу);

– можливість захищати атрибути шифруванням;

– можливість підписувати електронний документ та перевіряти цифровий вміст і підпис;

– можливість відкликати ЕЦП;

– можливість застосовувати атрибути в електронних сервісах, що не є типовими застосуваннями криптографічної технології ЕЦП.

Другорядними можна визначити вимоги:

– зміна назви результуючого (підписаного) файлу;

– відображення хешу закодованого файлу тощо.

Зміна назви результуючого (підписаного) файлу і відображення хешу закодованого файлу не є важливими для функціонування програми. Замість вибору назви можна залишити назву вибраного файлу оригінальною, а хеш-сигнатуру користувачу можна не показувати – вона не є інформативною для нефахівця. Однак це призведе до того, що користувач не зможе перевірити хеш-коди за бажанням.

Також при реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу важливо розділити категорії суб’єктів, долучених до реалізації або використання пропонованої технології ЕЦП.

Дослідження існуючих технологій відповідного спрямування [39,45-51] та визначення актуальних напрямків застосування технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу дозволяє ідентифікувати наступні категорії суб’єктів (ролі) в реалізації пропонованої технології ЕЦП:

– користувачі-підписанти;

– сервіс користувача-підписанта (мобільний додаток, програмний застосунок на комп’ютері тощо);

– запитувач;

– верифікатори або постачальники послуг;

– емітенти;

– менеджер технології.

Деталізуємо роль кожної категорії суб’єктів в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного

документообігу.

Роль користувача або підписанта відіграють суб’єкти, які хочуть використовувати переваги технології цифрового підпису із застосуванням особових атрибутів і при цьому максимально контролювати свою конфіденційність.

Сервіс користувача-підписанта може бути реалізований у вигляді мобільного додатка чи програмного застосунку на комп'ютері. Цей сервіс повинен мати здатність отримувати та розкривати атрибути, а також зберігати їх конфіденційно. Для забезпечення конфіденційності збережуваних атрибутів рекомендується їх криптографічне закриття.

Сервіс користувача-підписанта в рамках технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу виконує роль клієнта. Такий сервіс надає користувачеві можливість ефективно взаємодіяти з системою та використовувати свої ідентифікаційні атрибути. Сервіс користувача-підписанта повинен відрізнятися зручністю для користувача, тому в технології рекомендовано реалізувати два варіанти сервісу – у вигляді мобільного додатка та у вигляді програмного застосунку для комп'ютера (ПК, ноутбук тощо).

Роль постачальник послуг або верифікатора в технології відіграє суб’єкт або сторона, перед якою користувач-підписант ідентифікує себе. Постачальник послуг або верифікатор перевіряє атрибути підписанта для надання певної замовленої користувачем послуги або для підтвердження дійсності ЕЦП в системі електронного документообігу.

Емітенти – це перевірені організації або служби (сервіси тощо) високої довіри, здатні видавати перевірені атрибути користувачам, тобто, постачальники гарантовано достовірних атрибутів як ідентифікаційної інформації користувача-підписанта.

Роль емітентів доцільно пояснити більш детально.

Емітентом, першочергово, може виступати державний орган, який видає певний документ. Реквізити диплому може видавати університет, який видав цей

документ, одночасно засвідчуючи гарантовану наявність та дійсність самого документа у підписанта, а також всіх приналежних диплому атрибутів. Реквізити паспорту громадянина України можуть видавати територіальні підрозділи Державної міграційної служби України, якими видаються відповідні документи, одночасно засвідчуючи гарантовану наявність та дійсність самого документа у підписанта, а також всіх приналежних паспорту атрибутів. Емітентом атрибутів паспорту можуть виступати різні органи. Для нашого міста до їх числа можна віднести: відділ у справах громадянства, імміграції та реєстрації фізичних осіб управління МВС України в Хмельницькі області; паспортний сервіс «ДП Документ»; сектор громадянства, імміграції та реєстрації фізичних осіб Хмельницького міського відділу УМВС України в Хмельницький області, паспортний стіл; паспортно-візовий сервіс тощо. Подібні служби-емітенти можна визначити і для інших документів державного зразка, таких, як ідентифікаційний код, водійські права, посвідчення пенсіонера, медична картка, посвідчення медичного працівника або іншої сфери тощо.

В цьому аспекті доцільно також відзначити основні, другорядні і похідні атрибути документів. Це найзручніше зробити на прикладі паспорту громадянина України (аналогічний аналіз можна провести для ID-картки або іншого документу).

Основними реквізитами (атрибутами) паспорту громадянина України є його індивідуальні серія і номер.

До другорядних атрибутів можна віднести:

- ПІБ особи-власника паспорту;
- дата народження;
- місце народження;
- стать;
- адреса місцепроживання;
- інформацію про сімейний стан та склад сім’ї;
- дата видачі паспорту;
- дані про орган видачі паспорту;

– група крові та інша інформація тощо.

Ці атрибути розглядаються як другорядні для документа, але аж ніяк не для особи-власника паспорту, оскільки значна частина з цих атрибутів є конфіденційними даними.

Похідними атрибутами паспорту громадянина України можуть бути:

– ім’я;

– по батькові;

– прізвище;

– число дати народження (рік, місяць по окремості тощо);

– вік;

– кількість дітей тощо.

Таким чином, один окремий документ від довіреного надійного емітента може слугувати джерелом визначення великої кількості достовірних атрибутів для застосування в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу. Крім того, атрибути різних документів можуть дублюватися (прізвище є майже в усіх документах) і це може слугувати як елементом перевірки достовірності даних атрибутів, так і самих емітентів.

Головне призначення ролі емітентів в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу полягає в забезпеченні достовірності даних атрибутів і запобігання їх фальсифікації, що могло б постати простою схемою навмисного створення фіктивних осіб-підписантів при суто ручному заповненні атрибутів або виникнення ненавмисних помилок людського фактору при ручному заповненні тих же атрибутів.

Зазначимо, що в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу залишається можливість приховування конфіденційної інформації користувача-підписанта через використання атрибутів-псевдонімів та контроль-блокування застосування

атрибутів, які підписант не має бажання оприлюднювати в кожному окремо взутому випадку.

Найпотужнішим емітентом в умовах цифровізації документообігу в Україні постає бренд цифрової держави – застосунок «Дія», реалізований Міністерством цифрової трансформації України. Цей застосунок вже зараз є джерелом атрибутів для авторизації, ідентифікації користувачів в різних віртуальних сервісах, а також в технологіях ЕЦП, тому розглядається як потенційний основний емітент атрибутів технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу в нашій державі.

Роль запитувача відіграють суб'єкти технології, які можуть виконувати функції постачальників послуг у ролі верифікатора, а також постачальників ідентифікаційної інформації у якості емітентів. Запитувач має здатність видавати атрибути користувачеві, проводити перевірку атрибутів та підписів на основі атрибутів, а також підписувати електронний документ за допомогою атрибутів. Це ще один інструмент запобігання фальсифікації даних в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу.

З використанням технології користувачі можуть, окрім збільшення контролю над своєю конфіденційністю, розкривати свої атрибути для аутентифікації або підписувати певний цифровий вміст. Саме тому користувачеві потрібен запитувач для спілкування. Запитувач може створюватись реалізується у формі веб-додатку або програми для робочого столу. Запитувач використовує серверні та зовнішні пакети, надані програмним забезпеченням. Це дозволяє запитувачу спілкуватися з сервером-менеджер технології. Запитувач ініціює сеанс із сервером-менеджером, а потім сервер ініціює сеанс із сервісом користувача-підписанта.

На рисунку 3.1 представлена схема рольової взаємодії суб’єктів реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу.

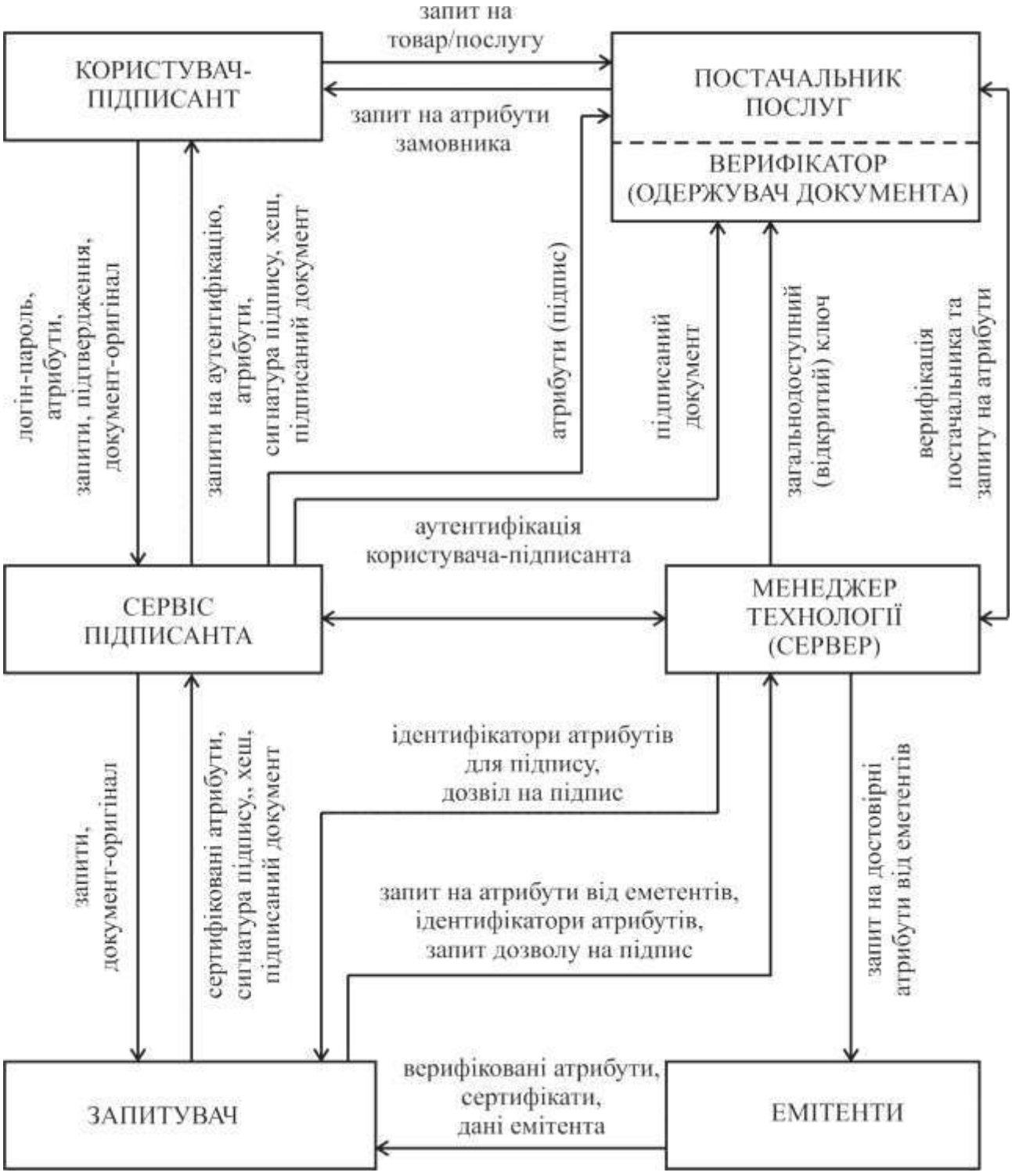


Рисунок 3.1 – Рольова схема взаємодії суб’єктів технології

Менеджер (сервер) технології є невід’ємною і надважливою роллю системи, як і багатьох подібних технологій. Менеджер технології цифрового підпису відповідає за визначення та поширення відкритих ключів, типів атрибутів й інформації про їх видавця-емітента. Менеджер технології приймає рішення

стосовно того, які типи облікових атрибутів можуть бути видані-підтверджені емітентами, а також визначає, які емітенти можуть приєднатися до домену менеджера технології. Менеджер має визначати ступінь довіри до замовника атрибутів (постачальника послуг) та надавати користувачу рекомендації щодо видачі атрибутів, тобто, протидіяти незаконному заволодінню атрибутами або розповсюдженню атрибутів понад реальну потребу (дотримання вимог Загального регламенту про захист даних [41] діючих вимог законодавства Європейського Союзу) При цьому роль сервера-менеджера технології не передбачає доступу до значень самих атрибутів користувача-підписанта, оскільки це є пріоритетною функцією користувача і використовуваного ним в технології.

Рольова схема взаємодії суб'єктів технології відображує загальні напрямки передачі запитів, документів, даних між суб'єктами, також представленими на схемі технології, а також основні процеси, що протікають під час реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу (аутентифікація користувача, верифікація постачальника послуг та коректності його запиту на отримання атрибутів, наприклад, на дотримання вимог Загального регламенту про захист даних Європейського Союзу, отримання хеш-коду документа та сигнатури ЕЦП із застосуванням атрибутів підписанта тощо.

Подальший розвиток технології полягає в алгоритмічній реалізації розглянутих в цьому розділі і відображених на схемі процесів і процедур.

3.2 Алгоритми реалізації технології цифрового підпису

Основні процеси технології цифрового підпису із застосуванням особових атрибутів підписанта поділяються на дві частини:

- підпис (накладання ЕЦП);
- перевірка підпису (верифікація).

Відповідно, алгоритм підпису стосується функцій, необхідних для роботи процесу підписання, а алгоритм верифікації стосується функціональних можливостей, необхідних для роботи процесу перевірки.

З наведеної на рисунку 3.1 рольової схема взаємодії суб'єктів технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу та опису, що передував зазначеній схемі, можна побачити два напрямки застосування технології:

– підпис цифрового контенту електронного документа ЕЦП для системи електронного документообігу, що є традиційним застосуванням технології цифрового підпису в Україні;

– надання даних атрибутів підписанта на вимогу постачальника послуг (товару тощо), ініційоване замовлення цих послуг зі сторони підписанта.

Другий напрямок застосування технології цифрового підпису не є традиційним для України і тому сприймається не зовсім зрозуміло, але в Європейському Союзі і іншому цивілізованому світі будь-яке підтвердження запиту особистими даними сприймається як різновид накладання підпису, навіть якщо запит має форму питання, чи є особі 18 років.

Процес підпису цифрового контенту електронного документа (файлу будь-якого формату) накладанням ЕЦП в технології складається з таких кроків:

1. Аутентифікація в системі ЕЦП – електронному сервісі підписанта (мобільному додатку або в програмі обслуговування ЕЦП на ПК – перша аутентифікація).
2. Запит сеансу підпису на основі атрибутів.
3. Отримання запиту на повторну аутентифікацію (дзвінок, QR-код для сканування за допомогою мобільного додатку тощо).
4. Повторна аутентифікація.
5. Вибір файлу для підпису.
6. Вибір атрибутів, передбачених як частина «політики» підписання (шаблон підпису).

7. Запит на формування підпису на основі атрибутів.
8. Отримання дозволу на накладання ЕЦП, тобто, на видачу атрибутів.
9. Шифрування файлу (за потреби).
10. Формування сигнатури підпису.
11. Шифрування сигнатури, наприклад, у варіанті base64 (за потреби).
12. Додавання сигнатури підпису із застосуванням атрибутів до підготовленого файлу.
13. Хешування файлу з сигнатурою.
14. Додавання хеш-сигнатури до файлу.
15. Підписаний файл з сигнатурами ЕЦП із застосуванням атрибутів і хеш-коду можна зберегти або передати.
16. Завершення сеансу.

Процедура відображує загальний алгоритм дій технології у випадку позитивної реалізації на всіх етапах, але можливі і відмови або додаткові погодження стосовно розголошення атрибутів у випадках виявлення певних загроз або ризиків.

Очевидною причиною відмови може бути неуспіх проходження процедури аутентифікації. Причиною отримання попередження технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу, наприклад, може бути підозрілий вибір атрибутів або вибір до включення особових даних, які є конфіденційними.

Важливою особливістю пропонованої технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу є те, що аналіз набору атрибутів здійснюється сервером (менеджером) сервісу ЕЦП, але при цьому сервіс отримує тільки запит на атрибути у вигляді ідентифікаторів атрибутів, таких, як ім’я, прізвище, ключ ЕЦП класичний, вік, ключ ЕЦП класичний, сертифікат ЕЦП тощо, але самі ці атрибути не є доступними серверу.

Для більш наочного і детального відображення особливостей реалізації технології в процесі підпису цифрового контенту електронного документа накладанням ЕЦП з атрибутів синтезовано блок-схему алгоритму (рисунок 3.2).

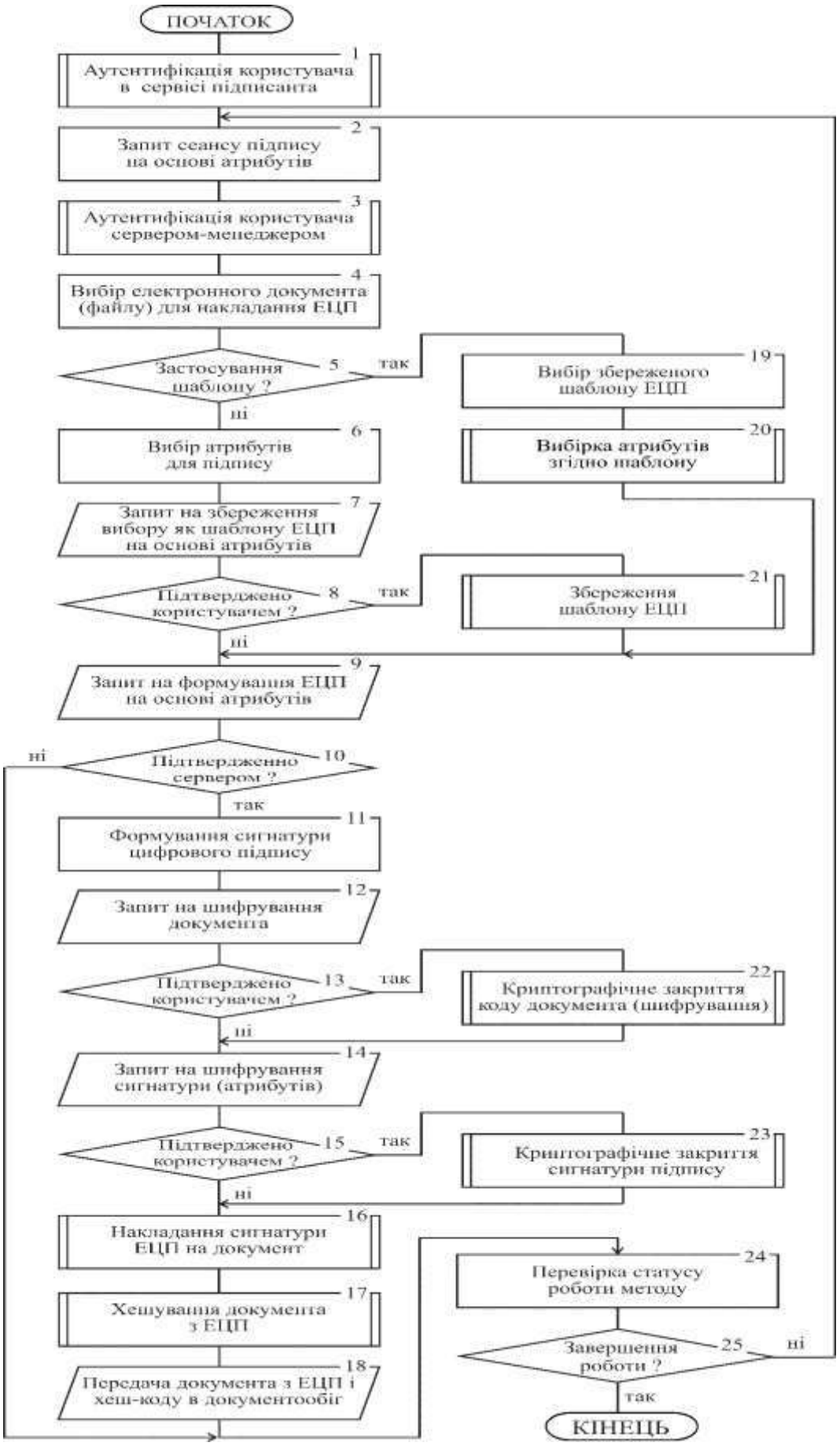


Рисунок 3.2 – Алгоритм накладання сигнатури ЕЦП на документ

Як видно з рисунку 3.2, користувач може створювати і зберігати типові шаблони ЕЦП для використання в майбутньому. При цьому шаблон не є секретним, оскільки визначає тільки схему формування сигнатури з атрибутів, але не містить жодного конкретного значення атрибутів. На етапі збереження обраного в поточному сеансі набору атрибутів як шаблону користувач повинен дати шаблону підпису ім’я-ідентифікатор. Цей ідентифікатор буде використано як ім’я для вибору шаблону і для накладання відповідного підпису в подальшому. Користувач може вибрати атрибути, які будуть призначені підпису як частину політики шаблону. Цю політику запроваджено, оскільки відсутність додавання жодного атрибута під час підписання порушить мету зробити семантику підпису зрозумілою. Тепер можна ініціювати запит на підпис з використанням заготовленого заздалегідь шаблону і не витрачати час на повторний підбір атрибутів.

Далі розглянемо алгоритм верифікації, який стосується функціональних можливостей технології, необхідних для роботи процесу перевірки ЕЦП.

Процес верифікації складається з таких кроків:

1. Обрати підписаний файл (процедуру транспортування, скачування і зберігання файлу не розглядаємо).
2. Перевірити хеш-сигнатуру, додану до підписаного файлу електронного документа.
3. Сформувати запит на перевірку підпису, вбудованого в підписаний електронний документ (файл).
4. Запитувач отримує статус підпису.
5. За потреби – здійснити декодування атрибутів з сигнатури
6. Запитувач відображає користувачу статус підпису, пов’язані атрибути та метадані файлу-документа.
7. Завершення сеансу верифікації.

Для більш наочного і детального відображення особливостей реалізації технології в процесі верифікації ЕЦП цифрового контенту електронного документа синтезовано блок-схему алгоритму, яку представлено на рисунку 3.3.

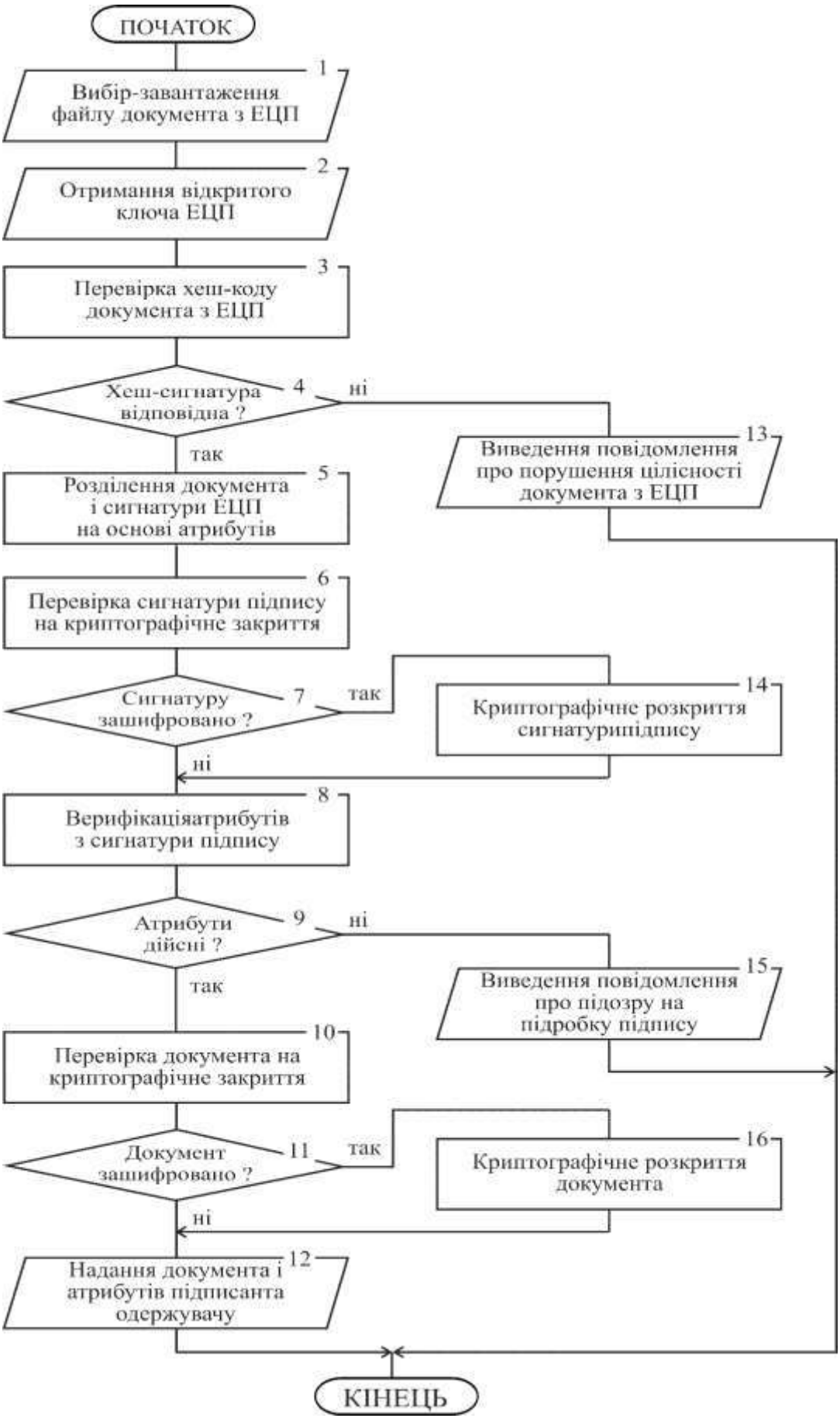


Рисунок 3.3 – Алгоритм верифікації сигнатури ЕЦП

Коли користувач має намір перевірити підписаний файл, він може зробити це локально на своєму комп’ютері або ж у мобільному додатку. Обидві програми в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу діють як запитувач.

Оригінальний вихідний файл і підпис із застосуванням атрибутів отримуються з підписаного файлу.

Спочатку перевіряється хеш-сигнатура на відповідність до файлу. Для цього має бути витягнуто з отриманого підписаного файлу поле повідомлення, яке містить хеш-сигнатуру вихідного файлу і накладеного підпису із застосуванням атрибутів. Щоб перевірити, чи не було змін у вихідному файлі або підписі, код вихідного файлу з підписом хешується повторно. Потім отриманий хеш порівнюється з хешем із поля повідомлення підпису на основі атрибутів. Це є класичним процесом і не містить оригінальності як у перевірці, так і у діях з результатами перевірки.

Далі обробляється та перевіряється сигнатура підпису на основі атрибутів. Для цього сигнатура теж має бути витягнута з отриманого підписаного файлу. Якщо виконане шифрування сигнатури – здійснюється зворотній процес розшифрування. Вихідний файл також зберігається в підписаному файлі.

У випадку, коли підпис є дійсним і два хеші співпадають, перевірка успішна. Статус підпису та інша пов’язана інформація відображається отримувачу. Запитувач може отримати інформацію про статус підпису, а також інші пов'язані дані, такі як вбудовані атрибути та початкові метадані електронного документа.

Ще одним призначенням технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу є надання даних атрибутів підписанта на вимогу постачальника послуг (товару тощо), ініційоване замовлення цих послуг зі сторони підписанта.

Процес формування і накладання підпису як сукупності атрибутів на вимогу постачальника послуг в технології складається з таких кроків:

1. Ініціація процесу замовлення послуг користувачем технології, який відіграє при цьому роль замовника-підписанта.

2. Отримання запиту на авторизацію замовника (наприклад, у вигляді реєстраційної форми веб-застосунку постачальника послуг).

3. Аутентифікація замовника-підписанта в електронному сервісі підписанта (мобільному додатку або в програмі обслуговування ЕЦП на ПК – перша аутентифікація).

4. Запит сеансу підпису на основі атрибутів.

5. Отримання запиту на повторну аутентифікацію (дзвінок, QR-код для сканування за допомогою мобільного додатку тощо).

6. Повторна аутентифікація.

7. Перевірка надійності постачальника послуг зі сторони менеджера технології (верифікація постачальника послуг сервером).

8. За виникнення підозр щодо надійності постачальника послуг – запит користувачу на продовження роботи з підозрілим постачальником.

9. При відмові користувача від роботи з підозрілим постачальником – завершення сеансу роботи.

10. Перевірка коректності запиту на атрибути постачальника послуг зі сторони менеджера технології (верифікація коректності запиту в розрізі вимог GDPR – Загального регламенту про захист даних Європейського Союзу).

11. За виникнення підозр щодо коректності запиту постачальника послуг – запит користувачу на продовження роботи з підозрілим постачальником з повідомленням про виявлені ризики.

12. При відмові користувача від роботи з некоректним запитом постачальника – завершення сеансу роботи.

13. Вибір атрибутів, передбачених як частина «політики» підписання (шаблон підпису).

14. Запит на формування підпису на основі атрибутів.

15. Отримання дозволу на видачу атрибутів.

16. Підтвердження видачі атрибутів замовником-підписантом.

17. Видача атрибутів (наприклад, перенесення атрибутів в реєстраційну форму постачальника послуг і відправка форми постачальнику).

18. Завершення сеансу.

Для більш наочного і детального відображення особливостей реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу в процесі формування і накладання підпису як сукупності атрибутів на вимогу постачальника послуг синтезовано блок-схему алгоритму, яку представлено на рисунку 3.4.

Як видно з рисунку 3.4 та слідує з попередньо наданого опису, алгоритм формування і накладання підпису на вимогу постачальника послуг має спільні складові з алгоритмом підпису цифрового контенту електронного документа накладанням ЕЦП (рисунок 3.2), але при цьому має і суттєві відмінності від останнього.

Першочергово, в алгоритмі формування і накладання підпису на вимогу постачальника послуг не передбачається класичного накладання ЕЦП і відсутній об’єкт для накладання ЕЦП – електронний документ. Накладання підпису на вимогу постачальника послуг передбачає завірення особи замовника-підписанта перед постачальником послуг достовірними атрибутами замовника. Це схоже на паперову заяву-замовлення на послугу, форму якої заповнювали в часи паперового документообігу і завіряли власним підписом. Тут підпис особи відсутній, але роль підпису відіграють самі верифіковані і підтверджені менеджером атрибути.

Ще одна особливість, в алгоритмі формування і накладання підпису на вимогу постачальника послуг користувач не може створювати і зберігати типові шаблони ЕЦП для використання в майбутньому. Шаблоном стає сам запит постачальника послуг, в якому перелічені вимоги до різновидів атрибутів, які необхідні для виконання замовлення. Тут слід звернути увагу, що сам запит постачальника послуг має містити лише вимогу на ті атрибути, які дійсно необхідні для виконання замовлення. В технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу акцент зроблено на верифікації коректності запиту постачальника в розрізі вимог Загального регламенту про захист даних ЄС.

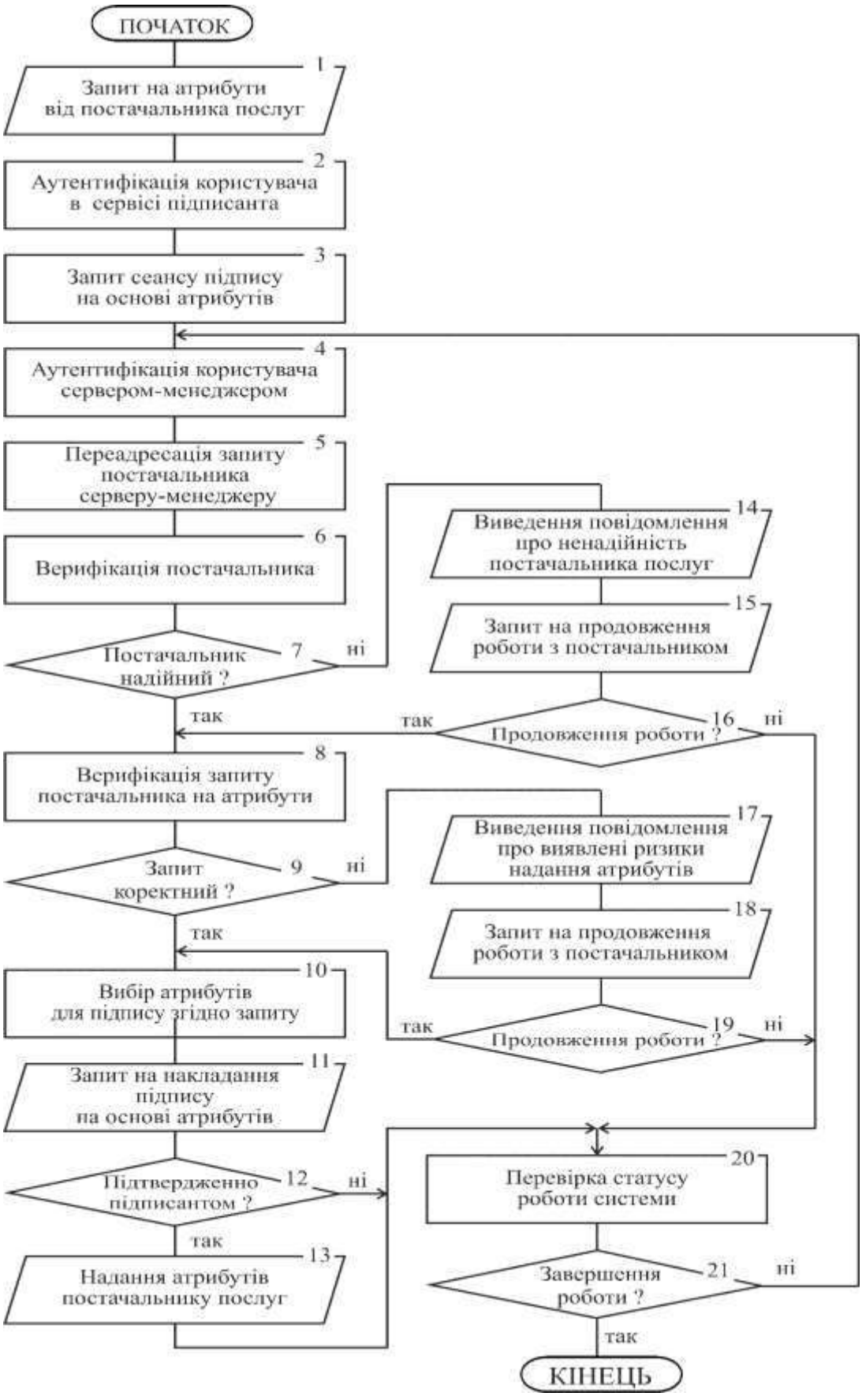


Рисунок 3.4 – Алгоритм формування і накладання підпису на вимогу постачальника послуг

На шляху України до ЄС важливим постає питання дотримання вимог Європейських нормативних документів з організації систем електронного документообігу тощо. При визначенні базових положень технології цифрового підпису з використанням атрибутів актуальності набувають саме вимоги Загального регламенту про захист даних ЄС GDPR [7] щодо мінімізації розголошення особової інформації суб'єктів даних. Тому будь-яка підозра на недотримання цих вимог сприймається як ризик розкриття надлишкових даних замовника-підписанта і потребує підтвердження самого підписанта. При цьому підписант може формувати неповністю заповнену атрибутами форму (проігнорувати необов’язкові атрибути) або відмовитися від замовлення, а в подальшому вирішити питання з постачальником або оскаржити його вимоги за принципових питань згідно закону.

Цій самій меті служить і верифікація постачальника послуг. Найкращим способом верифікації є перевірка GDPR-сертифікації постачальника, що є гарантією в країнах ЄС, але, нажаль, не популярне поки в Україні. Тому верифікація може базуватись на рейтингових оцінках або за іншими критеріями, деталізація яких не є ціллю цієї роботи.

Також слід звернути увагу в даному алгоритмі на те, що атрибути надаються постачальнику послуг у відкритому форматі (не шифруються), що є типовим для заповнення реєстраційних форм і тому обґрунтованим.

Для підвищення конфіденційності підпису замовник-підписант може використовувати систему псевдонімів та альтернативних атрибутів (поштових скриньок замість реальних адрес, додаткових e-mail тощо), що є поширеною практикою в цивілізованих країнах.

3.3 Висновки

В розділі надано опис технології використання цифрового підпису в системах електронного документообігу, в якому уточнено загальні принципи реалізації

запропонованої технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу.

Для визначення загальних принципів реалізації технології здійснено розподіл вимог щодо її функціональних можливостей на першочергові та другорядні, що дозволило здійснити поетапний підхід до розробки технології цифрового підпису.

Дослідження існуючих технологій та визначення актуальних напрямків застосування пропонованої технології дозволило ідентифікувати категорії суб'єктів (ролі) в реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу, користувачі-підписанти, сервіс користувача-підписанта, запитувач, верифікатори або постачальники послуг, емітенти, менеджер (сервер) технології.

Рольова декомпозиція технології використана за основу для визначення рольової схеми взаємодії суб'єктів технології, яка, в свою чергу, стала базисом в алгоритмічної реалізації розглянутих в розділі і відображених на схемі процесів і процедур.

Алгоритми реалізації технології цифрового підпису технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу представлена трьома алгоритмами:

– алгоритм накладання сигнатури ЕЦП на документ;

– алгоритм верифікації сигнатури ЕЦП;

– алгоритм формування і накладання підпису на вимогу постачальника послуг.

В технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу акцент зроблено на дотриманні вимог Загального регламенту про захист даних ЄС GDPR [7] як одного із базових положень щодо роботи з особистими даними (атрибутами) в системах електронного документообігу, який має враховуватись на шляху України до ЄС.

4 АПРОБАЦІЯ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ЦИФРОВОГО ПІДПИСУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

4.1 Визначення можливостей і сценаріїв використання технології цифрового підпису ідентифікаційних особових атрибутів підписанта

В попередніх розділах розглянуто математичну модель технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу та надано опис принципів її реалізації та алгоритми її функціонування в різних варіантах застосування.

Цей розділ присвячений апробації технології, що передбачає перевірку можливостей технології та уточнення принципів користування цими можливостями для користувачів.

Першочергово слід відзначити, що в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу користувач може реалізовувати різні види сеансів взаємодії з технологією:

- сеанси випуску;
- сеанси розкриття;
- сеанси підпису;
- комбіновані сеанси.

Сеанс випуску передбачає отримання нового набору атрибутів. Процес сеансів випуску включає в себе можливість отримання нового набору атрибутів завдяки технології. Сервіс користувача-підписанта отримує цей новий набір, включаючи підпис емітента, який передається від менеджера (сервера) технології. Підпис емітента використовується для майбутніх сеансів підпису та розкриття даних користувача на основі атрибутів. Перед тим як отримати новий набір атрибутів, може виникнути необхідність запросити в користувача розкриття

певних атрибутів, які вже зберігаються у сервісі користувача-підписанта. Цей етап може представляти собою комбінований сеанс випуску та розкриття даних атрибутів, де об'єднуються операції випуску нових атрибутів і розкриття існуючих, забезпечуючи комплексний та гнучкий підхід до обробки даних атрибутів.

Сеанс розкриття надає можливість підписантам розкривати конкретні атрибути, які можуть бути запитані, наприклад, постачальником послуг. Користувач-підписант може виступати як ініціатор розкриття атрибутів, формуючи цифровий підпис з використанням цих атрибутів для електронного документа у системі електронного документообігу.

Основна мета розкриття атрибутів полягає у їхній верифікації – зовнішньому підтвердженні достовірності.

В процесі цього сеансу користувач може ініціювати запит на розкриття до менеджера (сервера) технології, використовуючи запитувач. Це спричиняє старт сеансу розкриття даних атрибутів. Після цього менеджер (сервер) технології надсилає запит на розкриття атрибутів сервісу користувача-підписанта. Якщо користувач-підписант підтверджує запит, розкриті атрибути відсилаються менеджеру (серверу) технології.

Менеджер (сервер) технології перевіряє отримані атрибути та надсилає свій статус дійсності, включаючи перевірені розкриті атрибути, запитувачу. При цьому сервер може ініціювати звернення до емітента для додаткової перевірки атрибутів. Це єдиний сценарій в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу, при якому дані атрибутів потрапляють до менеджера (сервера) технології.

Сеанси підпису із застосуванням атрибутів є основним сеансом технології.

Ця категорія сеансів дозволяє користувачам додавати підпис із застосуванням атрибутів до електронних документів або повідомлень, або надавати атрибути за запитом постачальника послуг. У процесі підписання документів технологія працює аналогічно до будь-якого іншого цифрового підпису, але перевагою перед типовим цифровим підписом є можливість додавати особисті атрибути в системі електронного документообігу.

Це не тільки забезпечує підписанта додатковим контролем над конфіденційністю, але також приносить користь верифікатору. У цьому контексті верифікатор, який отримує та переглядає підписане повідомлення, отримує корисну інформацію про співавтора у вигляді особистих атрибутів. Гарантії підпису включають в себе переконання у тому, що повідомлення не піддавалося змінам та атрибути, додані до підпису, були актуальними на момент створення ЕЦП. Перевірити підпис із застосуванням атрибутів можна у будь-який майбутній момент часу.

Детальний опис сеансів підпису із застосуванням атрибутів за запитом постачальника послуг наведений у попередньому розділі, який включає презентацію алгоритмічної реалізації даної технології.

Перед тим як розпочати певні сеанси в рамках цієї технології, сервіс користувача-підписанта вимагає від користувача введення логіна та пароля. Цей процес допомагає запитувачу переконатися, що користувач, який розпочинає сеанс, дійсно має володіти відповідним атрибутом.

Введення логіна та пароля є важливим кроком у забезпеченні безпеки та уникненні можливих зловживань, наприклад, використання зловмисником викраденого телефону для несанкціонованого розкриття атрибутів, які можуть бути на телефоні.

Відповідальність за перевірку правильності даних для аутентифікації покладена на менеджера технології (сервер). Якщо ідентифікаційний набір (логін і пароль) виявляється неправильним, сеанс повинен бути припинений, щоб уникнути недозволених дій. Перед кожним сеансом, який включає атрибути, менеджер схеми має використовувати сервер спільного доступу до ключів. Цей сервер бере участь у всіх сеансах, де використовуються атрибути, за якими відповідає менеджер схеми. Користувачі реєструються на серверах спільного доступу, керованих відповідними менеджерами схем, при першому встановленні та відкритті сервісу користувача-підписанта. На цьому етапі користувач може вибрати свій логін і пароль. Починаючи з цього моменту, при кожному сеансі роботи з технологією користувачу необхідно вводити логін і пароль перед тим, як менеджер технології

дозволить успішно завершити сеанс.

Для реалізації сеансу розкриття необхідно отримати підтвердження нульового розголошення, також відомого як докази нульового знання (Zero-knowledge proofs). Ці докази служать засобом підтвердження того, що певне число відповідає певній властивості, при цьому не розкриваючи саме це число.

В облікових даних може бути ряд атрибутів. Коли користувач вирішує розкрити лише певний набір атрибутів у своїх облікових даних, інші атрибути, включаючи секретний ключ, залишаються прихованими завдяки використанню доказів нульового знання. Таким чином, користувач може переконати верифікатора, що він насправді має дійсний підпис емітента для всіх атрибутів, що належать йому в межах пов’язаних облікових даних, при цьому не розголошуючи конкретних прихованих атрибутів.

Підпис атрибута користувача емітентом є необхідним кроком для подальшого підтвердження того, що конкретні атрибути були надані відповідними (автентичними) емітентами, які пов'язані з конкретним користувачем-підписантом. Існують емітенти, які бажають безпечно підписувати атрибути користувача, не маючи доступу до секретного ключа користувача. З метою збереження секретного ключа користувача у таємниці (і, таким чином, збереження його приватності) використовується підтвердження з нульовим знанням.

Технологія використовує підтвердження з нульовим знанням для того, щоб оберігати як секретний ключ технології, так і підпис від верифікатора. Це забезпечує додатковий рівень конфіденційності, оскільки верифікатор не отримує доступу до важливих облікових даних технології цифрового підпису. Секретний ключ і підпис у технології зберігаються прихованими, щоб забезпечити відсутність зв'язку між ними та забезпечити безпеку облікових даних підписанта. Першим атрибутом кожного отриманого облікового запису завжди є секретний ключ підписанта. Користувач доводить емітенту, що він знає перший атрибут (секретний ключ), використовуючи доказ нульового знання. Таким чином, емітент розпізнає свого користувача як правильного, не розкриваючи секретний ключ користувача емітенту. Надалі емітент може безпечно підписати атрибути.

Як зазначалося в попередньому розділі, в технології передбачено реалізацію двох схем підпису: аутентифікації та підпису. В схемі аутентифікації атрибути можуть бути вибірково розкриті користувачем-підписантом під час аутентифікації певному постачальнику послуг. В схемі підпису підписант може вибірково розкривати та додавати атрибути до ЕЦП на основі атрибутів. Таким чином, підтвердження вибіркового розкриття використовується або для аутентифікації, або для створення підпису (з хешем повідомлення).

Технологія цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу складається з чотирьох етапів: генерація ключа, видача атрибутів, генерація підпису та перевірка підпису.

Генерація ключа відбувається при ініціалізації сервісу користувача-підписанта, коли він встановлюється на комп'ютер або мобільний телефон та вперше запускається користувачем. У цей момент генерується секретний ключ у вигляді випадкового 256-розрядного двійкового числа, який безпечно зберігається сервісом. Цей секретний ключ використовується для видачі атрибутів, аутентифікації при запиті атрибутів і підписання цифрового вмісту.

Процес видачі атрибутів вже був описаний і передбачає, що користувач може отримати атрибути від авторизованих емітентів. Емітент підписує облікові дані, що містять запитувані атрибути, своїм закритим ключем. Під час перевірки підпису відкритий ключ емітента використовується верифікаторами. Такий підхід забезпечує відправника атрибутів довіреною підписаною інформацією, яку можна перевірити та використовувати в майбутньому.

Процес створення підпису при використанні обох схем (сеансів підпису та аутентифікації) реалізації технології детально розглядався у попередньому розділі і представлений алгоритмами для накладання ЕЦП на документ (рисунок 3.2) та формування підпису на запит постачальника послуг (рисунок 3.4).

На рисунку 4.1 представлена рольова декомпозиція взаємодії суб’єктів технології в процесі накладання сигнатури ЕЦП на документ та верифікації сигнатури ЕЦП одержувачем завіреного підписом файлу документа.

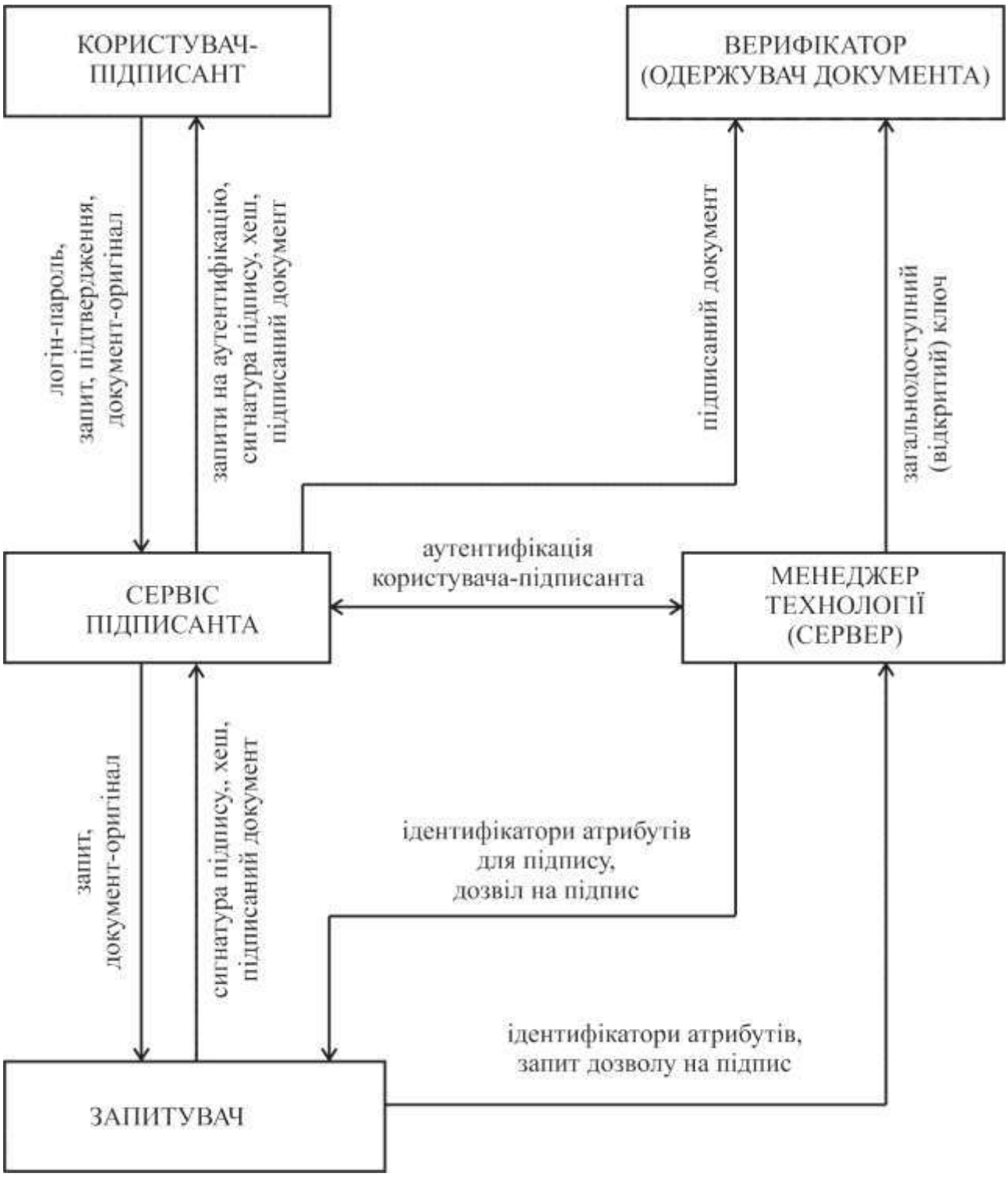


Рисунок 4.1 – Рольова декомпозиція взаємодії суб’єктів при накладанні сигнатури ЕЦП на документ та її верифікації

На рисунку 4.2 представлена рольова декомпозиція взаємодії суб’єктів технології в процесі формування і накладання підпису на вимогу постачальника послуг (надання атрибутів постачальнику послуг).

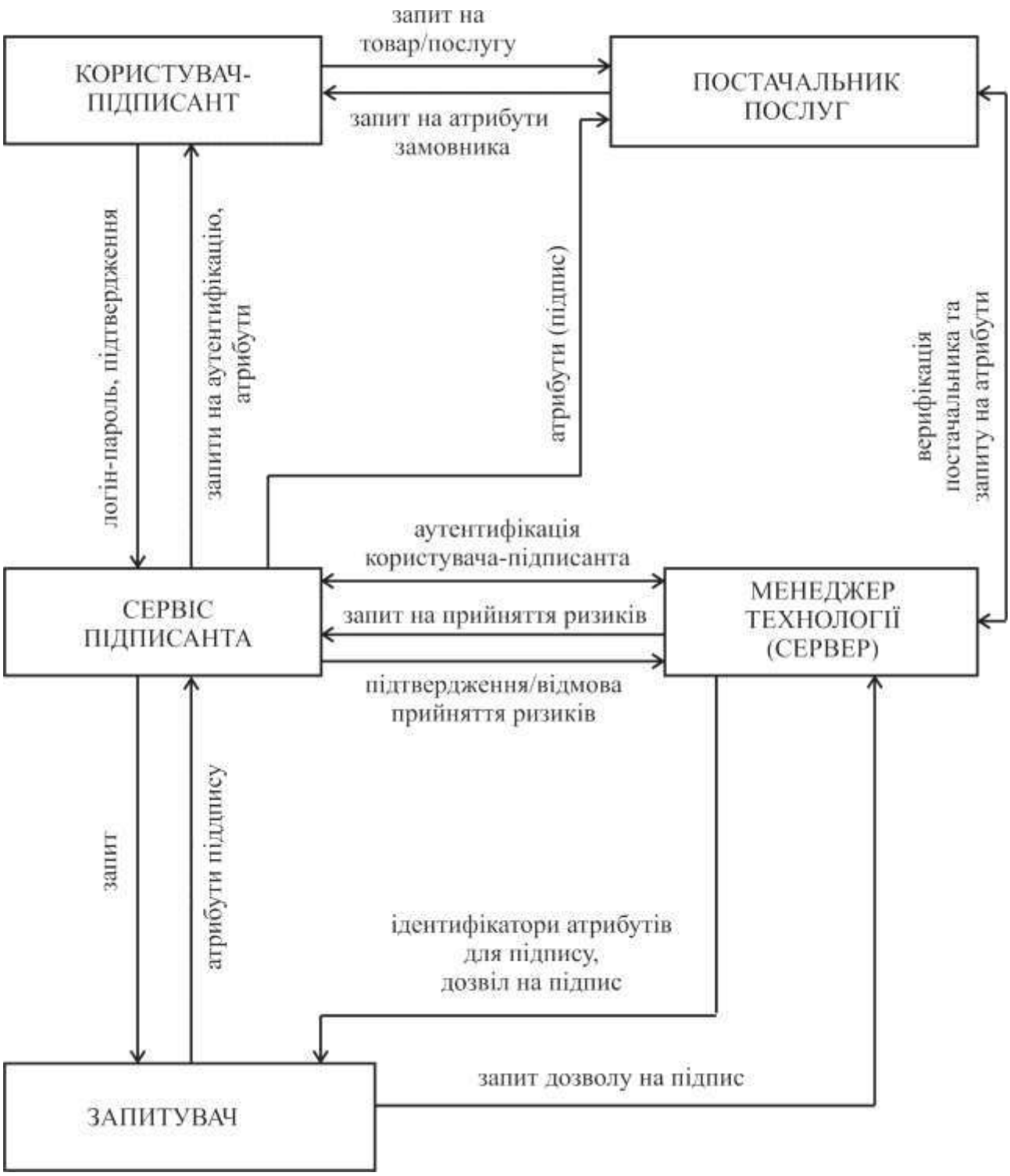


Рисунок 4.2 – Рольова декомпозиція взаємодії суб’єктів при формуванні-накладанні підпису на вимогу постачальника послуг

Фактично, в обох сценаріях створення підпису здійснюється сервісом користувача-підписанта (мобільним додатком або програмним застосунком на ПК) під контролем та керівництвом підписанта, а також під контролем менеджера

технології (серверного застосунку). Сервіс користувача-підписанта надає необхідні атрибути, мітку часу та вибірковий доказ розкриття інформації, щоб переконатися, що саме користувач сервісу підписав повідомлення та має відповідні атрибути, що були видані емітентом.

Перевірка підпису реалізується за допомогою алгоритму верифікації сигнатури ЕЦП (рисунок 3.3). Верифікатори, які бажають підтвердити підпис на основі атрибутів, повинні мати відкритий ключ відповідного емітента, який надав пов'язані атрибути мобільному додатку. Відкритий ключ емітента використовується для перевірки підпису. Верифікатор перевіряє дійсність мітки часу та переконується, що повідомлення (в межах підпису) було підписано користувачем-підписантом, який має відповідні атрибути, видані емітентом.

4.2 Аналіз кіберзагроз та дослідження технології на вразливості і стійкість до атак

Заключним етапом виконуваних робіт є апробація технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу на кіберстійкість та безпечність, що передбачає здійснення дослідження технології на вразливості та стійкість до атак.

Аналіз публікацій [49-51,54,55] дозволив відзначити, що вадами подібних технологій є можливість ураження атаками різних видів, тому актуально дослідити наявні загрози технологій цифрового підпису та визначити наявність контрзаходів щодо реалізації цих загроз при реалізації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу.

Розглянемо загрози інформаційної безпеки технології і контрзаходи.

4.2.1 Загроза повторного використання підпису (Non-re-usability) в системах електронного документообігу полягає в тому, що зловмисник може намагатися використати підпис, який вже був здійснений, для виконання неправомірних дій або отримання доступу до ресурсів. Це може виникнути, якщо підпис витягнуто з

попереднього сеансу та повторно вставлено в інший контекст чи для іншої транзакції.

Підпис повинен бути нероздільним від цифрового вмісту та непридатним для подальшого використання. Це означає, що цифровий вміст, до якого додається підпис, в спочатку хешується і зберігається як "повідомлення" в підписі, заснованому на атрибутах технології. Використовуючи процес хешування цифрового вмісту та введення цього хешу як частини об'єкта повідомлення, можна гарантувати, що підпис неможливо буде використовувати повторно.

Якщо підпис із застосуванням атрибутів буде доданий до іншого цифрового вмісту, хеш нового цифрового вмісту не буде співпадати з хешем оригінального документа, зробивши підпис недійсним. Перевірку дійсності підпису може виконувати сторона, що перевіряє, хешуючи цифровий вміст із доданим підписом на основі атрибутів, а потім порівнюючи отриманий хеш з хешем, що міститься в об'єкті повідомлення доданого підпису на основі атрибутів. Ідентичність хешів свідчить про те, що підпис був доданий до оригінального документа, тоді як їхня різність свідчить про те, що підпис не відноситься до доданого вмісту.

4.2.2 Загроза використання застарілих атрибутів в системах електронного документообігу може виникнути, коли вже неактуальна інформація про користувача чи об'єкт зберігається або використовується в системі документообігу. Такий атрибут, як «викладач», має бути дійсним лише до тих пір, поки користувач офіційно є викладачем.

Якщо атрибути застаріли і не відображають поточний стан користувача чи об'єкта, може статися неправильне прийняття рішень або надання послуг на основі застарілих даних. Якщо застарілі атрибути містять конфіденційну інформацію, то використання цих даних може призвести до порушення конфіденційності та витоку чутливої інформації. Використання застарілих атрибутів при процесі ідентифікації може призвести і до помилкової ідентифікації користувача.

Технологія цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу передбачає наявність механізму для відкликання і верифікації атрибутів.

Емітенти мають можливість відкликати облікові дані, які раніше були надані сервісу користувача. Це може відбуватися у випадках, коли один чи кілька атрибутів у складі цих облікових даних втратили свою актуальність. Зокрема, емітенти можуть визначати атрибути, які більше не є дійсними, і проводити їх відкликання. Верифікатори, які бажають перевірити актуальність атрибутів, можуть здійснювати перевірку, запитуючи підтвердження невідкликання через мобільний додаток. Проте важливо зазначити, що верифікатори мають залежати від емітента, який є органом відкликання, для відкликання атрибутів, що втратили свою дійсність, включаючи відповідні облікові дані. У своєму запиті на сеанс розкриття верифікатор може включати масив відкликання, який стосується певного типу облікових даних, для отримання підтвердження їхньої актуальності.

4.2.3 Загроза застосування атаки повторення (Replay Attacks) в системах електронного документообігу – це потенційна загроза, при якій зловмисник може захопити та повторно передати раніше зареєстрований чи перехоплений електронний обмін даними. Ця атака може призвести до небажаного відтворення вже відправленого електронного документа чи підпису, порушуючи цілісність та автентичність інформації.

Атаки повторення мають такі схеми:

– зловмисник може зафіксувати електронний підпис на документі та повторно передати його, вигідно користуючись дубльованою аутентифікацією;

– зловмисник може повторити раніше відправлені запити, такі як запити на отримання атрибутів або доступ до конфіденційної інформації;

– зловмисник може повторити попередні транзакції, що може призвести до некоректних або небажаних результатів;

Відтворення попередньо переданих даних може призвести до порушення цілісності та автентичності інформації електронного документообігу.

Захист від атаки повторення в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу включає в себе використання механізмів аутентифікації та авторизації на основі часу (контекстуальних атрибутів), а також застосування криптографічних методів для

підпису та перевірки повідомлень.

Ініціаторам атаки повторення повинно бути неможливо відтворити сеанс розкриття атрибутів. Коли атрибути перевіряються, верифікатор висилає випадкову кількість бітів, відому як nonce, на сервіс користувача. Сервіс користувача відповідає розкритими атрибутами та доказами знань, які точно відповідають цьому nonce. Верифікатор не може повторно використовувати nonces, оскільки це порушить захист від атак повтору.

Також верифікатори не мають можливості виконувати атаки повтору. Для запобігання цьому технологія ніколи не передає повну копію підпису облікових даних верифікатору. Замість цього частини підпису заховані за допомогою доказів знань, що гарантує їхню незв'язність. Таким чином, верифікатори не можуть використовувати інформацію, яку вони дізналися під час попереднього сеансу, наприклад, розкриті атрибути, для передачі іншим верифікаторам і вживання ролі сервісу користувача.

4.2.4 Ще один вид загроз – фальшива ідентифікація (False-Identity).

Фальшива ідентифікація в системах електронного документообігу вказує на намагання неправомірно представити себе або іншу особу, шляхом введення неправдивих чи підроблених ідентифікаційних даних або ідентифікаційних атрибутів. Це може включати в себе використання фіктивних персональних даних, підробку документів або інші хитрощі з метою набуття неправомірного доступу до системи, ресурсів чи інформації.

Важливо визначити, що в системах електронного документообігу фальшива ідентифікація може виникнути як внаслідок недостатньої аутентифікації користувача, так і через підробку електронних даних, введення неправдивих атрибутів чи недостовірних електронних документів. Попередження фальшивої ідентифікації вимагає ефективних методів аутентифікації та засобів валідації ідентифікаційної інформації, а також вдосконалення заходів кібербезпеки для запобігання шахрайствам та неправомірному доступу до систем.

В технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу фальшива ідентифікація

запобігається через систему перевірених атрибутів, що надаються і гарантуються емітентами.

4.2.5 Загроза надлишкового розкриття атрибутів в системах електронного документообігу виникає, коли користувач розголошує більше інформації, ніж необхідно для виконання конкретної задачі чи отримання певної послуги. Це може виникнути через неправильні запити постачальників послуг або несвідомі дії користувача. Надлишкове розкриття атрибутів створює ризик, оскільки зайва інформація може бути використана зловмисниками чи недобропорядними постачальниками послуг для неправомірних цілей. Наприклад, якщо система запитує більше особистих даних, ніж необхідно для проведення транзакції, це може призвести до порушення конфіденційності користувача.

Захист від цієї загрози включає в себе усвідомлення користувача щодо того, яка саме інформація запитується та чому. Користувачі повинні бути обережними і не розголошувати більше даних, ніж це необхідно для здійснення певної операції. Постачальники послуг також повинні бути відповідальними та дотримуватися принципів обмеження обробки особистих даних, щоб мінімізувати ризик надлишкового розкриття атрибутів.

Оскільки користувачі в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу видають лише важливі особисті атрибути, створення повного профілю особи для шахрайства стає важким завданням, можливо, навіть неможливим. Якщо деякі атрибути залишаються конфіденційними, їх неможливо використовувати для шахрайства за допомогою ідентифікації. Зловмисний постачальник послуг може спробувати отримати занадто багато (особистої) інформації, яка не є необхідною для надання послуги. Мета шахрая – отримати якнайбільше (особистої) інформації від користувача. Технічно це можливо, але користувач може відмовити від такого запиту. Підписант може просто відхилити запит, і ніякі атрибути не будуть розкриті, залишаючи шахрая з порожніми руками. Користувачу слід зрозуміти, які саме атрибути запитуються, щоб уникнути непорозумінь та випадкової згоди на ризикований запит, що передбачено в технології .

Крім того, облікові дані, що включають атрибути в сервісі користувача, мають цифровий підпис емітента. Це означає, що зловмисник не може створити "фейковий" атрибут. Проте, емітент повинен бути довіреним та проходити перевірку, перш ніж може діяти як емітент, тобто лише після визнання його ліцензованою організацією чи органом влади.

4.2.6 Загроза розкриття емітента в системах електронного документообігу виникає, коли конфіденційна інформація, пов'язана з емітентом, виходить за межі і стає доступною неповноважній стороні. Це може стати наслідком недостатнього захисту ключів, систем або недбалості щодо безпеки в обробці атрибутів емітента.

Загроза розкриття атрибутів емітента може призвести до небажаного доступу до конфіденційної інформації, такої як закриті ключі, що використовуються для підпису облікових даних. Це може дозволити зловмисникам використовувати ці ключі для створення підроблених атрибутів або інших шахрайських дій.

Для запобігання цій загрозі в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу передбачене вживання заходів безпеки, таких як шифрування конфіденційних даних, захист від несанкціонованого доступу до систем та ретельний контроль за ключами.

4.2.7 Підробка ідентифікаційних і неідентифікаційних атрибутів підписанта в системах електронного документообігу вказує на спробу змінити, підробити або представити неправдиві інформаційні атрибути підписанта з метою введення в оману систем або отримання неправомірного доступу.

Це може охоплювати різні аспекти, такі як зміна особистих даних, електронного підпису, інших ідентифікуючих атрибутів, що стосуються підпису. Підробка атрибутів підписанта може призвести до виникнення проблем із захистом від несанкціонованого доступу, аутентифікації та цілісності електронних документів.

В технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу змогу видачі облікових даних (атрибутів) мають лише ті емітенти, які володіють приватним ключем видачі

Idemix. Закритий ключ Idemix емітента використовується для створення підпису облікових даних за допомогою підпису-сертифіката. Цей підпис-сертифікат емітента гарантує цілісність облікових даних, що означає, що верифікатор може виявити будь-які додавання, зміни або вилучення атрибутів з облікових даних. Такий підхід забезпечує верифікаторам впевненість у тому, що отримані атрибути є дійсними та були видані конкретним емітентом.

4.2.8 Фальсифікація часу в системах електронного документообігу вказує на намагання змінити часові позначення або введення неправдивої інформації про час з метою обману систем або викликання неправдивого враження щодо послідовності подій.

Це може включати в себе такі дії, як зміна часових міток на документах, електронних повідомленнях чи транзакціях з метою приховання справжнього часу подій або створення фальшивого враження про порядок виникнення подій.

Забезпечення надійності інформації про час є ключовим елементом забезпечення цілісності та достовірності даних в технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу і реалізується через систему контекстуальних атрибутів технології, які, фактично, є метаданими цифрового підпису і супроводжують електронний документ та захищаються механізмом хешування.

4.2.9 Загроза порушення цілісності в системах електронного документообігу включає в себе можливі атаки та сценарії, які ставлять під сумнів або змінюють цілісність документів або інших цифрових ресурсів. В технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу реалізується традиційний механізм запобігання порушенню цілісності електронних документів та сигнатури підпису на основі атрибутів, а саме – хешування електронного документа і сигнатури. Оскільки механізм хешування вважається ефективним контрзаходом атакам з порушенням цілісності цифрового контенту, загроза порушення цілісності в технології цифрового підпису із застосуванням особових атрибутів підписанта може вважатися мінімізованою

4.2.10 Загроза відмови від авторства ЕЦП включає в себе потенційні сценарії

та атаки, які можуть піддавати сумніву чи відкидати валідність підпису. Особливістю технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу є те, що в ній використовуються верифіковані емітентами атрибути та систему приватних ключів, а також механізми захисту цілісності документа і сигнатури підпису що, фактично, усуває можливість відмови від авторства.

4.2.11 Фальсифікація особи – одна із найпоширеніших вад систем підпису із використанням атрибутів.

Фальсифікація особи в системах електронного документообігу вказує на спробу представити недостовірні або змінені інформаційні атрибути з метою обману систем або отримання неправомірного доступу. Це може включати створення фіктивних або підроблених особистих даних, документів або інших ідентифікуючих атрибутів.

Системи аутентифікації не завжди можуть гарантувати повністю запобігти фальсифікації особи. Розглянемо ситуацію, коли користувач, що не досяг 18-річного віку, намагається придбати квиток на концерт, доступний лише для осіб старше 18 років. В цьому випадку веб-сайт, де здійснюється покупка квитка, може запитувати лише адресу та вік покупця. Адреса використовується для доставки квитка, а вік - для перевірки відповідності вимогам концерту. Однак оскільки користувач може подати неправдиві дані, існує загроза фальсифікації особи. Продавець квитків не може впевнитися, що квиток буде відправлений саме тій особі. Таким чином, постачальник послуг повинен бути обережним у визначенні та перевірці атрибутів, які запитуються для забезпечення достовірності ідентифікації користувача.

У контексті електронного документообігу, де використовуються цифрові технології, фальсифікація особи може мати різні форми, такі як підробка цифрових підписів, неправдиве представлення атрибутів користувача чи намагання вдатися до ідентифікаційного обману.

В технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу передбачено двофакторну

аутентифікацію, що запобігає несанкціонованому використанню сервісу користувача-підписанта сторонньою особою. Ефективні методи аутентифікації, шифрування атрибутів та захист конфіденційної інформації, є важливими для запобігання фальсифікації особи в електронному документообігу і в технології цифрового підпису. Крім того, більшість атрибутів є верифікованими емітентами, тому фальсифікувати особу при використанні технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу досить важко. Для наведеного прикладу вік особи буде похідним атрибутом від дати народження, що є другорядним атрибутом паспорта громадянина України, а всі атрибути паспортних даних, як зазначалося раніше, в технології мають бути сертифіковані емітентом.

Таким чином, фальсифікація особи загалом передбачена технологією і в технології існують засоби протидії цій загрозі, але для повноцінної протидії атакам з використанням цієї загрози потрібна усвідомлена позиція користувача-підписанта щодо його ролі в захисті свого сервісу від несанкціонованого доступу, зокрема, в протидії атакам типу серфінгу через плече.

4.2.12 Серфінг через плече (Shoulder surfing) – це тип соціальної інженерії і активний метод атаки, при якому зловмисник спостерігає за введенням конфіденційної інформації чи виконанням користувачем дій, спостерігаючи ззаду чи зі сторони. У системах електронного документообігу цей термін вказує на можливість отримання несанкціонованого доступу до чутливої інформації, коли користувач взаємодіє з електронними документами чи вводить конфіденційні дані.

Загроза "серфінгу через плече" (Shoulder surfing) в системах електронного документообігу виникає, коли несанкціонована особа намагається отримати доступ або зловживати конфіденційною інформацією, спостерігаючи за діями користувача з використанням терміналу чи комп'ютера.

Атрибути в технології використовуються для формування унікального ідентифікаційного «паспорта» користувача. Цей паспорт можна використовувати для вибіркового розкриття конкретних особистих даних про користувача, що дає можливість підглядати за розкриттям. Як вже було зазначено, ця технологія

забезпечує кілька важливих властивостей безпеки, таких як перевірка джерела та цілісність атрибутів.

Однак на сьогодні в технології відсутня певна властивість безпеки, що захищала б користувача цієї технології від потенційного серфінгу через плече". Зловмисник може спостерігати за атрибутами користувача та використовувати їх для цифрового підпису контенту, фактично не маючи належних атрибутів. Це обмеження можна порівняти з ситуацією, коли зловмисник придивляється через плече користувача, спостерігаючи, як той вводить пароль, та використовує ці дані для подальших дій.

Важливо відзначити, що ця проблема є складною і вимагає зусиль самого користувача у сфері захисту його конфіденційності. Прийняття стандартних заходів безпеки та усвідомлення ризиків є важливими аспектами для запобігання подібним видам атак. Зокрема, щоб запобігти атакам серфінгу через плече у використанні технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу, рекомендується вживати наступні заходи:

– застосування захисних фільтрів або екранів на пристроях, що використовуються для роботи з електронними документами, щоб зменшити можливість спостереження за екраном з боку інших осіб;

– організація робочого місця користувача та використання пасивних методів захисту, щоб робоче місце користувача було розташоване так, щоб зменшити можливість спостереження інших осіб за діями користувача;

– використання фізичних або електронних засобів для обмеження видимості екрана з боку (наприклад, захисних непрозорих екранів);

– використання моніторів з обмеженим кутом огляду;

– застосування методів безпеки при введенні, таких як введення паролей або інших ідентифікаторів, таким чином, щоб було важко спостерігати за процесом введення;

– перекриття технічних каналів витоку інформації для запобігання зчитуванню інформації з електронних ресурсів користувача (монітор, клавіатура,

провідні лінії зв’язку) віддалено;

– профілактичні інформаційні заходи та інструктажі з метою формування у користувачів свідомості щодо можливості такого виду атак та надання їм рекомендації з безпеки.

Такі загрози, як серфінг на плечі та фальсифікація особи, є суспільними проблемами, які непросто вирішити жодною системою чи набором інструментів, включаючи інструменти технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу. Хоча користувачі все ще мають певні обов’язки щодо захисту власної конфіденційності, в технології переслідувалась ціль якомога більше допомогти користувачеві захистити свою конфіденційність. Набір інструментів технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу спрямований на пошук правильного балансу між розкриттям відповідної особистої інформації підписанта верифікатору та уникненням надмірної кількості особистої інформації підписанта під час підписання електронного документа.

4.3 Висновки

Четвертий розділ присвячений апробації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу, що передбачає перевірку можливостей технології та уточнення принципів користування цими можливостями для користувачів.

Першочергово відзначено, що в технології користувач може реалізовувати різні види сеансів взаємодії з технологією: сеанси випуску; сеанси розкриття; сеанси підпису; комбіновані сеанси.

В розділі надано деталізацію зазначених сценаріїв використання технології і дій користувача-підписанта, а також взаємодії користувача-підписанта з іншими суб’єктами реалізації сценаріїв.

Реалізацію сценаріїв використання технології продемонстровано двома схемами рольової декомпозиції:

– рольова декомпозиція взаємодії суб’єктів при накладанні сигнатури ЕЦП на документ та її верифікації;

– рольова декомпозиція взаємодії суб’єктів при формуванні-накладання підпису на вимогу постачальника послуг.

Рольова декомпозиція пояснена і обґрунтована у зв’язку з алгоритмами реалізації технології.

В розділі також здійснено аналіз типових кіберзагроз у використанні технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу та здійснене дослідження технології на вразливості і стійкість до атак. В ході дослідження визначено наявність в технології засобів протидії загрозам порушення цілісності, відмови від авторства ЕЦП, фальсифікації особи, фальшивої ідентифікації, повторного використання підпису, підробки атрибутів підписанта, використання застарілих атрибутів, надлишкового розкриття атрибутів, розкриття емітента, застосування атаки повторення, фальсифікації часу. Також було визначено вразливість технології да атак серфінгу через плече, для протидії яким надані рекомендації і описані контрзаходи організаційно-інформаційного характеру.

ВИСНОВКИ

В роботі за результатами теоретичних та практичних досліджень здійснено розробку удосконаленої технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу. При розробці методу переслідувалась мета, що полягає у вдосконаленні і розширенні можливостей технології використання цифрового в системах електронного документообігу та інших електронних сервісах з авторизацією користувачів за рахунок застосування у сигнатурі підпису особових атрибутів підписанта.

Для реалізації програми досліджень виконано наступні роботи:

– проведене дослідження існуючих технологій використання цифрового підпису в системах електронного документообігу, виявлено перспективні напрямки та способи вдосконалення, що можуть бути використані у підвищенні їх ефективності;

– запропоновано математичну модель технології та визначено схему формування мультиатрибутивної адаптивної сигнатури цифрового підпису в термінах запропонованої математичної моделі;

– визначено основні положення удосконаленої технології використання цифрового підпису;

– здійснено алгоритмічну реалізацію технології, в ході якої розроблено алгоритм формування і накладання сигнатури підпису на електронний документ, алгоритм верифікації сигнатури підпису та алгоритм надання атрибутів для авторизації підписанта на запит постачальника послуг;

– здійснено апробацію технології моделюванням взаємодії її суб’єктів в реалізації різних сценаріїв;

– виконане дослідження технології на вразливості і стійкість до атак.

Оцінка отриманих результатів дозволила дійти загального висновку, що в роботі виконані всі поставлені задання і досягнуто загальної мети дослідження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Електронний документообіг: види систем та їхні функції. URL: https://dealssign.com/blog/elektronnij-dokumentoobig-vidi-sistem-ta-yixni-funkciyi/ (дата звернення: 12.10.2023).

2. Асанова Л. Місце електронного документообігу в загальній системі діловодства. Адміністративне право і процес. 2021. №3. С. 156-160.

3. Системи електронного документообігу в Україні. URL: https://expresssoft.com.ua/uk/sistemi-elektronnogo-dokumentoobigu-vidi-prikladi-gotovi-rishennja/ (дата звернення: 12.10.2023).

4. Вибір системи електронного документообігу. URL: https://fossdoc.com/vybor-sed (дата звернення: 12.10.2023).

5. Сулима Д. Система електронного документообігу факультету. Безпека даних. Інформаційно-комунікаційні технології в освіті. 2018. №5. С 45-48

6. Севастєєв Є.О. Безпека електронного документообігу. Одеса, ДУІТЗ. 2022. 18 с.

7. Siti Salbiah Zainal Abidin and Mohd Heikal Husin. Improving accessibility and security on document management system: A Malaysian case study. Applied Computing and Informatics. 2018. ISSN: 2634-1964. P. 137-154.

8. Aderonke Ikuomola, Ezekiel Abiodun Oyekan, Olutomisin M. Orogbemi. A Secured Cloud-Based Electronic Document Management System. International Journal of Innovative Research and Development. 2022. Vol 11, Issue 1. ISSN 2278-0211. P. 38-45.

9. Balogun Naeem A., L.A. Raheem, Musbau Dogo Abdulrahaman, Balogun U.O. Adoptability of electronic document management system in Ilorin businesses. Nigerian Journal of Technology. 2019. №38(3). P. 701-715.

10. Захист систем електронного документообігу: юридичні й технічні моменти. Статті проєкту КАДРОВИК.UA. 2023. URL: https://www.kadrovik.ua/content/zahyst-system-elektronnogo-dokumentoobigu-yurydychni-j-tehnichni-momenty (дата звернення: 12.10.2023).

11. Копняк К. В., Покиньчереда В. В. Електронний документообіг в

публічному управлінні: проблеми впровадження, переваги та перспективи. Електронне фахове видання "Державне управління: удосконалення та розвиток". 2020. №10. URL: http://www.dy.nayka.com.ua/pdf/10_2020/37.pdf (дата звернення: 15.10.2023).

12. Ясінська А. Проблеми та перспективи електронного документообігу в умовах цифрової трансформації. Молодий вчений. 2022. №11 (111). С. 128-134.

13. Ali R.N., Abdullayev V.H., Abbasova V.S. Analysis of main requirements for electronic document management systems. ScienceRise. 2020. № 1. P. 28-31.

14. Електронний підпис і сертифікація документів. URL: https://pidru4niki.com/19590809/informatika/elektronniy_pidpis_sertifikatsiya_dokumentiv (дата звернення: 14.10.2023).

15. Краус К.М., Краус Н.М., Манжура О.В. Електронна комерція та Інтернет-торгівля: навчально-методичний посібник. Київ: Аграр Медіа Груп, 2021. – 454 с.

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

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

18. Whitfield Diffie and Martin Hellman. New directions in cryptography. IEEE transactions on Information Theory. 1976. №22(6). P. 644-654,

19. Ronald L Rivest, Adi Shamir, Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978. №21(2). P. 120-126.

20. Zubov V. An Electronic Signature Within The Digital Economy. Proceedings of the II International Scientific Conference GCPMED 2019 - "Global Challenges and Prospects of the Modern Economic Development". 2019. P.621-625.

21. Providing documents via a digital signature. Paperless service. URL: https://support.nic.ua/en-us/article/212-providing-documents-via-a-digital-signature-paperless-service (дата звернення: 14.10.2023).

22. Pooja M., Yadav M. Digital signature. International Journal of Scientific Research in Computer Science. Eng. Inf. Technol. 2018. №3. P. 71-75.

23. Шевченко К.Л., Карпенко І.І. Принципи та підходи щодо сертифікації електронного підпису. Матеріали ІІІ Міжнародної науково-практичної конференції «Мехатронні системи: інновації та інжиніринг». 2019. С. 167-168.

24. Ідентифікація і аутентифікація користувачів. URL: http://pmf.uad.lviv.ua/storage/uploads/лекції%201%20інформаційна%20безпека.pdf (дата звернення: 14.10.2023).

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

26. Hemanta K Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In Cryptographers' track at the RSA conference. Springer. 2011. P. 376-392.

27. Gergely Alpar and BPF Jacobs. Credential design in attribute-based identity management. URL: https://www.cs.ru.nl/~gergely/objects/TILTing_Alpar-Jacobs_CredentialDesign.pdf (дата звернення: 18.10.2023).

28. ABC4Trust Attribute-based Credentials for Trust. URL: https://abc4trust.eu/download/ABC4Trust-OnePager-About-ABC4Trust.pdf (дата звернення: 18.10.2023).

29. Ahmad Sabouri, Ioannis Krontiris, Kai Rannenberg. Attribute-based Credentials for Trust (ABC4Trust). URL: http://ioanniskrontiris.de/publications/ABC4Trust_TrustBus2012.pdf (дата звернення: 18.10.2023).

30. Jan Bobolz, Fabian Eidens, Stephan Krenn, Sebastian Ramacher, Kai Samelin. Issuer-Hiding Attribute-Based Credentials ? An extended abstract of this paper appeared in the 20th International Conference on Cryptology and Network Security CANS 2021. 2021. Vienna, Austria. Springer. 2021. P. 1-18.

31. D2.2 - Architecture for Attribute-based Credential Technologies - Final Version. / Patrik Bichsel et. al. 2014. 149 p.

32. How Yivi works? URL: https://www.yivi.app/en/for-me/how-yivi-works (дата звернення: 18.10.2023).

33. About IRMA. URL: https://privacybydesign.foundation/irma-en/ (дата

звернення: 18.10.2023).

34. Ashley Bringer, Candice Gordon, Sean Mackey, Reba Smith. Idemix: Identity Mixer URL: https://faculty.uca.edu/ronmc/INFO3321/Spring_2007/ET%20Pres/ET1/G4/Idemix%20Group%204.htm (дата звернення: 19.10.2023).

35. Privacy by Design Foundation URL: https://privacybydesign.foundation/en/ (дата звернення: 19.10.2023).

36. Brinda Hampiholi, Gergely Alpar, Fabian van den Broek, and Bart Jacobs. Towards practical attribute-based signatures. In International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer. 2015. P. 310-328.

37. Yivi in detail. URL: https://privacybydesign.foundation/irma-explanation/ (дата звернення: 19.10.2023).

38. iDIN. URL: https://www.idin.nl/ (дата звернення: 19.10.2023).

39. 10 кращих програм для цифрового підпису. URL: https://apix-drive.com/ua/blog/reviews/10-krashih-program-dlja-cifrovogo-pidpisu (дата звернення: 19.10.2023).

40. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022р. URL: https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text (дата звернення: 09.11.2023).

41. Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС. URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення: 09.11.2023).

42. J. Schaad, August Cellars. Cryptographic Message Syntax (CMS) Content Types for Concise Binary Object Representation (CBOR). Internet Engineering Task Force (IETF). 2020. ISSN:2070-1721. RFC 8769.

43. Gerard Wawrzyniak, Imed El Fray. New xml signature scheme that is resistant to some attacks. IEEEAccess. 2020.Vol. 8, P. 35815-35831.

44. A virtual teacher who reveals to you the great secrets of Base64. URL: https://base64.guru/converter/decode (дата звернення: 23.10.2023).

45. Rupeng Yang, Man Ho Au, Qiuliang Xu, and Zuoxia Yu. Decentralized

blacklistable anonymous credentials with reputation. ACISP 18: 23rd Australasian Conference on Information Security and Privacy. Springer, Heidelberg/ 2018. Vol. 10946. P. 720–738.

46. Alberto Sonnino, Mustafa Al-Bassam, Shehar Bano, Sarah Meiklejohn, George Danezis. Threshold issuance selective disclosure credentials with applications to distributed ledgers. In ISOC Network and Distributed System Security Symposium – NDSS 2019. 2019.

47. Rafael Torres Moreno, Jorge Bernal Bernab´e, Jes´us Garc´ıa Rodr´ıguez, Tore Kasper Frederiksen, Michael Stausholm, Noelia Mart´ınez, Evangelos Sakkopoulos, Nuno Ponte, and Antonio F. Skarmeta. The OLYMPUS architecture - oblivious identity management for private user-friendly services. Sensors. №20(3):945. 2020. P. 131–145.

48. Ulrich Hab¨ock and Stephan Krenn. Breaking and fixing anonymous credentials for the cloud. CANS 19: 18th International Conference on Cryptology and Network Security. Springer. 2019. Vol. 11829. P. 249–269.

49. Mehmet Cinci, Ceren Cubukcu Cerasi, Muaz Gultekin. Token Based Novel Approach To Web Service Security. International Conference on Electrical, Computer and Energy Technologies (ICECET). 2022. P. 1-6.

50. Said El Kafhali, Iman El Mir, Mohamed Hanini. Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. Archives of Computational Methods in Engineering. 2022. Vol.29, №1. P. 223.

51. Sancar N., Cavus N. Determining the awareness of users towards E-signature: A scale development study. AIP Conf. Proc. 2021, P. 2325-2334.

52. 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). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 30.10.2023).

53. Sharma, A.K.; Mittal, S.K. A comprehensive study on digital-signatures with Hash-functions. Int. J. Comput. Sci. Eng. 2019. №7. P. 604-607.

54. Afrianto I., Heryandi A., Finandhita A., Atin S. E-document autentification with

digital signature model for smart city in Indonesia. J. Eng. Sci. Technol. 2020. №15. P. 28-35.

55. Cavus N., Sancar N. The Importance of Digital Signature in Sustainable Businesses: A Scale Development Study. Sustainability. 2023. №15(6). 5008. URL: https://doi.org/10.3390/su15065008 (дата звернення: 19.10.2023).

56. Електронні підписи на базі DocuSign, PandaDoc, AdobeSign, InStaSign та їх чинність в Україні URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/elektronni-pidpisi-na-bazi-docusign-pandadoc-adobesign-instasign-ta-yih-chinnist-v-ukrayini.html (дата звернення: 19.10.2023).

57. Класифікація атрибутів особи і формування цифрового підпису на їх основі / Рижий Я.О. та ін. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький. 2023. С.252-256.

58. Рижий Я.О., Мельник М.М., Стецюк В.М. Технологія цифрового підпису з використанням атрибутів в системах електронного документообігу. Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції, 20-21.11.2023 р. Суми/Вінниця: НІКО/КЗВО «Вінницька академія безперервної освіти», 2023. С.223-225.

59. Рижий Я.О., Стецюк В.М. Підсистема цифрового підпису систем корпоративного електронного документообігу на базі криптографічних модулів ОС. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції, 20-21.11.2023 р. Суми/Вінниця: НІКО/КЗВО «Вінницька академія безперервної освіти», 2023. С.272-275.

ДОДАТОК А

Копії наукових публікацій

УДК 004
ББК 32.97
Е50

Рекомендовано до видання Вченою радою КЗВО «Вінницька академія безперервної освіти» (протокол № 8 від 20.11.2023 р.)

Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції 20-21 листопада 2023 р. – Суми/Вінниця: НІКО/ КЗВО «Вінницька академія безперервної освіти», 2023. – 336 с.

ISBN 978-617-7422-23-4

Збірник містить матеріали Міжнародної науково-практичної Інтернет конференції «Електронні інформаційні ресурси: створення, використання, доступ. Матеріали збірника подано у авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, статистичних даних, власних імен та інших відомостей. Матеріали відтворюються зі збереженням змісту, орфографії та синтаксису текстів, наданих авторами.

УДК 004
ISBN 978-617-7422-23-4

Google Drive (диск) - забезпечує зашифрований і безпечний доступ до ваших файлів. Ми можемо заздалегідь сканувати файли, до яких вам надали доступ, і вилучати їх, якщо виявимо зловмисне програмне забезпечення, спам, програми-шантажисти або фішинг. Диск повністю працює в хмарі та не використовує локальні файли, що зменшує ризики для ваших пристроїв. https://www.google.com/drive/

Google Sites (сайт) - ви можете створити веб-сайт, щоб ділитися інформацією з іншими. https://support.google.com/sites/?hl=en&sjid=5020266745628554616-EU#topic=7184580

Google Calendar - об'єднує всі календарі, щоб ви могли ефективно планувати робочі, особисті й інші справи. Поділіться календарями з колегами, щоб вони знали, коли ви зайняті. Завдяки спільному календарю в Google Workspace ви будете витрачати менше часу на планування й більше – на роботу. https://support.google.com/calendar

YouTube – платформа для пошуку готового навчального матеріалу, завантаження власних навчальних робіт; можливість асинхронного онлайн-викладання (запис з мобільного, завантажити відео, запис за допомогою розширень Google Chrome, редагування відео в YouTube Студії) та синхронного онлайн-викладання (лекція в прямому ефірі без демонстрації екрана, чат в режимі прем'єри, трансляція через OBS, трансляція через студію у веб переглядачі). Можливість створення власних списків відтворення. https://support.google.com/youtube/?sjid=5020266745628554616-EU#topic=9257498

Цифрові інструменти Google:

ПЕРЕВАГИ:

- багатофункціональність,
- доступність,
- швидкість,
- синхронність,
- мобільність,
- захист,
- практичність,
- довготривалість.

НЕДОЛІКИ:

- обмежений обсяг пам'яті на Google Drive (15 Гб),
- мережа інтернет,
- кібербезпека,
- приватність.

Використані джерела:

1. Офіційний сайт Google: https://support.google.com/

РИЖИЙ Я.О., МЕЛЬНИК М.М., СТЕЦЮК В.М.
Хмельницький національний університет

ТЕХНОЛОГІЯ ЦИФРОВОГО ПІДПИСУ З ВИКОРИСТАННЯМ АТРИБУТІВ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Анотація: Поряд із традиційними реалізаціями простого, удосконаленого і кваліфікованого електронного підпису останнім часом все більше уваги приділяється технологіям безпечного застосування в системах електронного документообігу підписів, що не знеособлюють підписанта. В роботі розглядаються базові положення технології цифрового підпису з використанням атрибутів особистих даних підписанта, яка орієнтована на надання мінімально-необхідних особистих даних користувача у відповідності до вимог GDPR, а також на убезпечення постачальників послуг від надання неправдивої інформації підписантом.

Ключові слова: захист інформації, електронний цифровий підпис, атрибути користувача, система електронного документообігу

В епоху тотальної цифровізації суспільства електронний цифровий підпис (ЕЦП) в системах електронного документообігу стає одним з ключових інструментів для забезпечення надійності, цілісності та конфіденційності електронних документів.

Основна перевага ЕЦП у системах електронного документообігу полягає в здатності впевнено ідентифікувати особу, яка підписала документ, і гарантувати, що сам документ не піддавався маніпуляціям після його підписання. Це робить ЕЦП надважливим елементом для забезпечення правової чинності електронних документів, таких як контракти, угоди та інші юридично значущі матеріали.

Нормативно-правовою базою України [1] та ЄС [2] регламентовано три традиційних види ЕЦП: простий, удосконалений і кваліфікований. В той же час, в Законі України «Про електронну комерцію» [3] водиться поняття електронного підпису з одноразовим ідентифікатором, що свідчить про можливість використання різноманітних підходів до трактування і класифікації поняття і технологій цифрового підпису.

Згідно [1], «електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис», що потенційно передбачає можливість сприйняття в якості електронного підпису будь-яких даних користувача, які дозволяють ідентифікувати підписанта в системах електронного документообігу згідно вимог цих систем.

Останнім часом актуальності набувають технології та сервіси, що базуються на використанні атрибутів користувача в якості цифрового підпису. До переваг технологій цифрового підпису з використанням атрибутів слід віднести:

- урізноманітнення варіацій цифрового підпису в системах електронного документообігу через можливість вибору різних атрибутів підписанта для формування підпису;
- відхід від практики повного знеособлення підписанта, оскільки атрибути користувача ідентифікують підписанта в чітко визначених аспектах;
- можливість використання єдиного сервісу цифрового підпису для різних систем ідентифікації підписанта;
- можливість застосування технологій цифрового підпису для ідентифікації користувача в найрізноманітніших системах електронної реєстрації.

Реалізації технологій цифрового підпису з використанням атрибутів розглядаються в наукових роботах [4,5] та мають практичні реалізації в системах CocoSign, DocuSign, PandaDoc тощо [6] і продовжують розвиватися та вдосконалюватись. В той же час, в Україні розробці і впровадженню технологій ЕЦП з використанням атрибутів на сьогодні приділяється мало уваги, що зумовлює інтерес до досліджень в цьому напрямку.

На шляху України до ЄС важливим постає питання дотримання вимог Європейських нормативних документів з організації систем електронного документообігу тощо. При визначенні базових положень технології цифрового підпису з використанням атрибутів актуальності набувають вимоги Загального регламенту про захист даних ЄС GDPR [7] щодо мінімізації розголошення особової інформації суб'єктів даних.

Технологія цифрового підпису з використанням атрибутів в системах електронного документообігу передбачає зберігання усіх атрибутів суб'єкта даних (підписанта) на власних ресурсах зазначеного суб'єкта (на гаджеті, з яким підписант працює в системі документообігу). До атрибутів відноситься будь-яка традиційна і нетрадиційна інформація, що може знадобитись у різноманітних електронних сервісах: ПІБ, дата народження, адреса, електронні адреси, паспортні дані та дані різноманітних посвідчень, псевдоніми, електронні ключі тощо. За збереження конфіденційності цієї інформації на власному гаджеті відповідальність несе сам її власник. В ідеальному варіанті для збереження власної інформації використовується надійний додаток з функцією криптографічного захисту інформації, що є складовою системи цифрового підпису.

При зверненні суб'єкта до будь-якого електронного сервісу, що потребує певних особистих даних, доступ до цих даних надається тільки за згоди і під контролем суб'єкта захищеним додатком під управлінням сервісу служби контролю за наступним алгоритмом:

- звернення суб'єкта до електронного сервісу ініціює запит сервісу щодо отримання даних атрибутів;
- для безпечного надання атрибутів суб'єкт здійснює авторизований вхід до додатку підпису на основі атрибутів;
- додаток надає запит щодо сеансу обміну атрибутами сервісу служби контролю;
- сервіс здійснює повторну аутентифікацію користувача (дзвінком, надсиланням цифрового коду на телефон або QR коду тощо);
- після авторизації користувача сервіс перевіряє наявність GDPR-сертифікації електронного сервісу, визначає перелік атрибутів, які вимагає сервіс і передає інформацію-запит підписанту;
- підписант приймає рішення щодо передачі кожного атрибуту в електронному сервісу і підтверджує своє рішення позначенням атрибутів для передачі та наданням загального підтвердження;
- за згодою підписанта сервіс надає дозвіл додатку передати атрибути сервісу.

Для сервісів, якими підписант користується постійно, процедура може бути спрощена через створення в додатку шаблонів заздалегідь погоджених (в попередніх сеансах) наборів атрибутів для взаємодії з сервісом.

Застосування технології цифрового підпису з використанням атрибутів дозволяє спростити дії власника особистих даних при підписанні документів в системах електронного документообігу, збільшити захищеність конфіденційних (особистих) даних, реалізувати надання мінімально-необхідного набору даних у відповідності до вимог GDPR, а також убезпечити постачальників послуг від надання неправдивої інформації замовником-підписантом.

Список використаних джерел

1. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022р. URL:https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text (дата звернення: 09.11.2023).
2. РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС. URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення: 09.11.2023).
3. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII, редакція від 19.11.2022. URL:https://zakon.rada.gov.ua/laws/show/675-19. (дата звернення: 09.11.2023).
4. Ke Gu, Keming Wang, Lulu Yang Traceable attribute-based signature. Journal of Information Security and Applications. Volume 49. 2019. Article ID 102400.
5. F2P-ABS: A Fast and Secure Attribute-Based Signature for Mobile Platforms. Security and Communication Networks. Volume 2019, Article ID 5380710. 12p.
6. 10 кращих програм для цифрового підпису. Apix-drive блог. URL:https://apix-drive.com/ua/blog/reviews/10-krashih-program-dlja-cifrovogo-pidpisu (дата звернення: 09.11.2023).
7. 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.

РИЖКОВ А. К., ВОЙЦЕХОВСЬКА О. В., ГОРОДЕЦЬКА О. С.
Вінницький національний технічний університет

АНАЛІЗ МЕТОДІВ АВТОРИЗАЦІЇ ПРИ ПРОЕКТУВАННІ СЕРВЕРНОЇ ЧАСТИНИ ВЕБ-ЗАСТОСУНКУ

Анотація: В роботі проведено аналіз методів авторизації користувачів у веб-застосунку. Розглянуто основні аспекти використання JWT токенів для авторизації, зокрема їх структуру, генерацію та перевірку, а

The article highlights the approach of building a subsystem for the protection of corporate electronic document flow. Attention is focused on aspects related to the support of public key infrastructure and electronic digital signature. The authors propose a method of building a digital signature subsystem of electronic document management systems based on cryptographic modules of the basic operating system.Ключові слова: Корпоративні системи документообігу, електронний підпис,security subsystem.

Вступ У недавні роки обсяги електронного документообігу значно збільшилися, що зробило необхідним впровадження такої системи захисту інформації в системах електронного документообігу, яка забезпечувала б надійність, конфіденційність та підтвердження справжності вмісту документів. Одним із способів досягнення цих цілей є використання електронного цифрового підпису (ЕЦП).

Електронний цифровий підпис — це унікальний код, створений на основі документа за допомогою спеціального алгоритму з використанням ключів шифрування. Вважається, що існують два ключі: приватний (закритий), який знає лише автор, та публічний, який є доступним для всіх. Щоб обидві сторони мали можливість отримати ці ключі, необхідний посередник — третя сторона, яка могла б виступати гарантом таких відносин. Цю роль виконує інфраструктура відкритих ключів (PKI - Public Key Infrastructure)[1].

На сьогодні кожна організація має власне бачення системи Public Key Infrastructure (інфраструктури відкритих ключів) для вирішення питань захисту електронного документообігу. Це пов'язано з відсутністю єдиного міжнародного стандарту, який був би законодавчо прийнятий у багатьох розвинутих країнах. Для захисту документів в корпоративних системах документообігу необхідно розробити підсистему, яка грунтується на використані криптографічних модулів операційної системи та відкритих стандартах крипто алгоритмів з можливістю додавання нових функцій та розширення для потреб систем документообігу.

Для розробки такої підсистеми необхідно провести дослідження сучасних асиметричних крипто алгоритмів і односторонніх хеш-функцій, а також проаналізувати криптографічні модулі сучасних операційних систем.

Основна частина. Вибір архітектури підсистеми здійснювався на основі базової моделі PKI, яка передбачає наявність наступних складових:

- центр сертифікації - елемент PKI, якому довіряють створювати та/або завіряти сертифікати, авторитетне джерело сертифікатів
- центр реєстрації або просто реєстратор - елемент PKI, уповноважений виконувати реєстрацію, тобто проводити ідентифікацію користувачів та їх реєстрацію у списку таким чином, щоб забезпечити можливість захищеного присвоєння сертифікатів цьому користувачеві.
- сховище сертифікатів - служба довідників або база даних, яка містить всю інформацію про сертифікати;
- адміністратор системи - виконує функції управління сертифікатами;
- користувач системи.

Рисунок 1 – Структура підсистеми захисту документообороту

Структура даних Stack керується принципом LIFO: Last-In-First-Out, останній елемент, доданий у стек, вийде з нього першим. Базовими операціями стека є: push (додати на вершину) і pop (вилучити з вершини). Stack використовується для розв'язання задач, для яких важливим є порядок видалення елементів, як-от рекурсія.

Структура даних Queue послуговується принципом FIFO: First-In-First-Out, перший, доданий у чергу елемент вийде першим. Queue використовується для розв'язання задач, для яких важливим є відповідний порядок оброблення елементів. Stack і Queue використовуються для конкретних сценаріїв й обмежуються в термінах доступу та операцій [1].

Окрім розглянутих базових структур, у Java є структура Map, яку організовано за принципом «ключ-значення»:

```
public Map<String, Object> getSupplierAdditionalParametersMap() {
    Map<String, Object> additionalParameters = new HashMap<>();
    additionalParameters.put(PARAM_CONTRACT_UUID, getContractUUID());
    return additionalParameters;
}
```

Тут getSupplierAdditionalParametersMap виконує збір параметрів, які потім можуть передаватися через інтерфейс Map. Поширено відома реалізація HashMap використовує хешкод (адресу пам'яті) для швидкого доступу до значення. HashMap використовують для передачі даних по запиту від сервера до клієнта, оскільки ключ завжди є унікальним. Крім того, є структура HashTable, яка використовується вкрай рідко, оскільки є синхронізованою та неефективною щодо часу виконання операцій над даними.

Окрім HashMap та HashTable, у Java є ще структура HashSet, яка теж використовує хешування для зберігання даних і зберігає пари «ключ-значення». Однак, на відміну від HashMap, HashSet зберігає лише унікальні об'єкти. Якщо в HashMap унікальними повинні бути лише ключі і при цьому значення можуть однаковими бути, то в HashSet всі об'єкти повинні бути унікальними. Саме тому HashMap використовують, коли треба швидко отримати доступ до значення через ключ, а HashSet – коли потрібно швидко перевірити наявність конкретного елемента.

Керування базами даних у back-end є критично важливим аспектом розробки серверної частини вебсайту і вимагає досвіду співпраці зі структурами бази даних. Backend-розробник прагне забезпечити ефективне та масштабоване функціонування серверної частини, проводячи оптимізацію коду, застосування ефективних структур даних та налаштувань сервера. На вибір тих чи інших структур даних для конкретної задачі впливає кількість даних, частота операцій додавання, видалення і пошуку, а також необхідність сортування або гарантії унікальності елементів. Правильний їх вибір може значно покращити продуктивність та ефективність програмного забезпечення, тому важливо глибоко розуміти всі наявні опції та вміти їх використовувати.

Список використаних джерел

1. Колекції в Java. Частина 2: HashSet, HashMap та інші. URL: https://mate.academy/blog/java-development/java-collections-2/

СТЕЦЮК М.В, РИЖИЙ Я.О.
Хмельницький національний університет

ПІДСИСТЕМА ЦИФРОВОГО ПІДПИСУ СИСТЕМ КОРПОРАТИВНОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА БАЗІ КРИПТОГРАФІЧНИХ МОДУЛІВ ОС.

У статті висвітлено підхід побудови підсистеми захисту корпоративного електронного документообігу. Зосереджено увагу на аспектах, пов'язаних із підтримкою інфраструктури відкритих ключів та електронного цифрового підпису. Автори пропонують метод побудови підсистеми цифрового підпису систем електронного документообігу на базі криптографічних модулів базової операційної системи.

Модуль генерації ключів створює ключову пару RSA для створення сертифіката. Після створення сертифікатів ключі видаляються. Таким чином, повторне створення сертифікату неможливе - сертифікати обов'язково будуть відрізнятися серійним номером та ключами[4].

Модуль створення сертифіката закритого ключа дає сертифікат, що містить другий ключ[5].

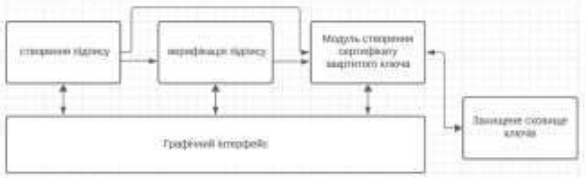


Рисунок 4 – Структура модуля створення і верифікації електронного підпису

Файл сертифіката відкритого ключа передається адміністратору для публікації у сховищі. Файл закритого ключа передається користувачеві установки на його робочій станції.

Процес верифікації підпису складається з наступних кроків:

- обчислюється хеш повідомлення за алгоритмом SHA-2;
- відбувається розшифрування хеша з підпису за допомогою відкритого ключа;
- порівнюються хеші, якщо вони співпадають, підпис вважається правильним.

Висновок Отже, запропонована підсистема захищеного обігу документів дозволяє створювати та розподіляти цифрові сертифікати безпеки, забезпечує доступ користувачів системи до бази сертифікатів, виконує відгуки сертифікату у разі компрометації закритого ключа користувача, підписує електронні документи цифровою підписом, перевіряє електронні цифрові підписи, створені системою, та керує сховищем сертифікатів. Безпека в системі забезпечується криптографічною стійкістю використовуваних алгоритмів. Ця система надає мінімальний набір функцій, що гарантує захист електронного обігу документів. Функціональність системи може бути легко розширена за потреби.

Список використаних джерел

1. Xiaojie Zhao; Shangping Wang; Yaling Zhang; Yu Wang. Attribute-based access control scheme for data sharing on hyperledger fabric /Journal of Information Security and Applications Volume 67, June 2022, Page 103182
2. Peraturan Menteri Negara Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 Tentang Pedoman Umum Tata Naskah Dinas Elektronik, Jakarta:Republik Indonesia, 2011
3. Mirosław Kutyłowski, Przemysław Błaśkiewicz. (2022). "Advanced Electronic Signatures and eIDAS – Analysis of the Concept." Journal of Computer Science and Telecommunication, Wrocław University of Science and Technology, Wybrzeze Wyspianskiego 27, Wrocław, 50-370, Poland.
4. Kutyłowski, M., Błaśkiewicz, P. (2023). "Advanced Electronic Signatures and eIDAS – Analysis of the Concept." Computer Standards & Interfaces, 83, 103644. Faculty of Computer Science and Telecommunication, Wrocław University of Science and Technology, Wybrzeze Wyspianskiego 27, Wrocław, 50-370,
5. Aumasson, J. P., Endignoux, G. (2018). "Improving Stateless Hash-Based Signatures." In: Cryptographers' Track at the RSA Conference. Springer, Cham, pp. 219–242.

Для забезпечення рівномірного розподілу навантаження на функціональні блоки пропонується відійти від базової моделі PKI шляхом об'єднання центру сертифікації з центром реєстрації, оскільки користувачі реєструються лише один раз і навантаження на центр реєстрації є недостатнім, щоб виділяти його в окремий Сервіс.

Існують дві базові моделі загальної служби PKI: ієрархічна модель, що базується на цепі сертифікатів, та модель, що базується на взаємній (крос-) сертифікації. В ієрархічній моделі центри сертифікації розташовані в ієрархічному підпорядкуванні "кореневого" центру сертифікації, який надає їм сертифікати. У моделі, заснованої на взаємній (крос-) сертифікації, незалежні центри сертифікації здійснюють взаємну сертифікацію.

Для підвищення масштабованості підсистеми було використано модель, засновану на взаємній сертифікації.

Одним із обов'язків адміністратора підсистеми є керівництво нею та її відновлення у випадках збою, публікації нових сертифікатів користувачів у сховище, видалення застарілих та недійсних сертифікатів, відкликання сертифікатів, а також резервування бази даних сертифікатів.

Адміністратор системи виступає в ролі арбітра при розгляді конфліктних ситуацій, лише він має доступ до сховища сертифікатів та інформації про учасників системи [2].

Структура програми "Адміністрування сховища" представлена на рисунку 2.

Рисунок 2 – Структура модуля Адміністративне сховище сертифікатів

Модуль запису в сховище сертифікатів бере участь у всіх транзакціях запису, таких як: додавання сертифіката, видалення сертифіката, публікація списку відкликаних сертифікатів, відкликання сертифікату [3].

Модуль читання зі сховища сертифікатів бере участь у таких транзакціях читання: отримання сертифікату, оформлення списку відкликаних сертифікатів, отримання статусу сертифіката, отримання сертифіката влади. "Графічний інтерфейс" використання для відображення інформації.

Центр реєстрації та сертифікації (ЦРС) реалізований у модулі "Створення сертифіката", яка виконує наступні функції: генерація та видача сертифікатів закритого ключа користувачам, створення та передача адміністратору сертифікатів відкритих ключів для публікації у сховище, зміна ключів користувачів. Структура модуля "Створення сертифіката" представлена на рисунку 3.

Рисунок 3 – Структура модуля створення сертифікату

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2023

XV Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. Комп'ютерні науки та прикладні інформаційні технології.
2. Комп'ютерна інженерія та системи захисту інформації.
3. Математичне моделювання та інженерія програмного забезпечення
4. Телерадіокомунікації, медійні та комунікаційні системи.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

Робочі мови конференції: українська, англійська

ОРГКОМІТЕТ:

Олег СИНЮК – голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

Олег САВЕНКО – заступник голови оргкомітету, декан факультету Інформаційних технологій ХНУ, доктор технічних наук, професор

Олександр БАРМАК – заступник голови оргкомітету, завідувач кафедри Комп'ютерних наук ХНУ, доктор технічних наук, професор

Тетяна ГОВОРУЩЕНКО – завідувач кафедри Комп'ютерної інженерії та інформаційних систем ХНУ, доктор технічних наук, професор

Олена ВИСОЦЬКА – доктор технічних наук, завідувач кафедри Радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», професор

Євгеній ЛАВРОВ – доктор технічних наук, професор (Сумський державний університет)

Людмила ТІМОФЄЄВА – відповідальна за студентську науково-дослідну роботу ХНУ

Олександр МАЗУРЕЦЬ – секретар конференції, к.т.н., доцент кафедри Комп'ютерних наук ХНУ

Марина МОЛЧАНОВА – секретар конференції, викладач кафедри Комп'ютерних наук ХНУ

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: *apkt.khnu@gmail.com*

УДК 004.056.5

Рижий Я.О., Мельник М.М., Чешун О.В., Орленко В.С.

Хмельницький національний університет

КЛАСИФІКАЦІЯ АТРИБУТІВ ОСОБИ І ФОРМУВАННЯ ЦИФРОВОГО ПІДПИСУ НА ЇХ ОСНОВІ

Здійснено ідентифікацію та класифікацію атрибутів для реалізації технології атрибутивного цифрового підпису в системах електронного документообігу, запропоновано спосіб формалізованого представлення різних класів атрибутів в математичній моделі та презентовано схему синтезу сигнатури підпису на основі формалізованого представлення особових атрибутів підписанта. Технологія синтезу підпису базується на принципах гнучкості, адаптивності та мультиатрибутності ЕЦП.

The identification and classification of attributes for the implementation of the technology of attributive digital signature in electronic document circulation systems is carried out, a method of formalized representation of various classes of attributes in a mathematical model is proposed, and a scheme of signature synthesis based on a formalized representation of the signatory's personal attributes is presented. The signature synthesis technology is based on the principles of flexibility, adaptability and multi-attribute EDS.

Невід'ємною складовою сучаних технологій автоматизованого документообігу є електронні цифрові підписи (ЕЦП). ЕЦП забезпечує безпеку і юридичну дійсність віртуальних документів, ефективність їх обробки, ідентифікує автора документа, гарантує цілісність вмісту та має в електронному середовищі юридичний статус традиційного підпису на паперовому носії.

Згідно Закону України [1], «електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис».

Традиційна технологія формування ЕЦП базується на застосуванні асиметричної криптографії з використанням пари ключів (приватного і публічного) та алгоритмів обчислення хеш-фнкцій електронного документа[2]. Такий підхід забезпечує високий рівень безпеки та можливість перевірки цілісності документа, що робить криптографічний ЕЦП важливим інструментом для забезпечення конфіденційності та автентифікації в електронному документообігу.

В той же час, криптографічний ЕЦП має в певних аспектах використання ряд недоліків, до яких відносять знеособлення підписанта, вузькоспеціалізоване

Актуальні проблеми комп'ютерних наук

УДК 004.056.5

Рижий Я.О., Мельник М.М., Чешун О.В., Орленко В.С.

Хмельницький національний університет

КЛАСИФІКАЦІЯ АТРИБУТІВ ОСОБИ І ФОРМУВАННЯ ЦИФРОВОГО ПІДПИСУ НА ЇХ ОСНОВІ

Здійснено ідентифікацію та класифікацію атрибутів для реалізації технології атрибутивного цифрового підпису в системах електронного документообігу, запропоновано спосіб формалізованого представлення різних класів атрибутів в математичній моделі та презентовано схему синтезу сигнатури підпису на основі формалізованого представлення особових атрибутів підписанта. Технологія синтезу підпису базується на принципах гнучкості, адаптивності та мультиатрибутності ЕЦП.

The identification and classification of attributes for the implementation of the technology of attributive digital signature in electronic document circulation systems is carried out, a method of formalized representation of various classes of attributes in a mathematical model is proposed, and a scheme of signature synthesis based on a formalized representation of the signatory's personal attributes is presented. The signature synthesis technology is based on the principles of flexibility, adaptability and multi-attribute EDS.

Невід'ємною складовою сучаних технологій автоматизованого документообігу є електронні цифрові підписи (ЕЦП). ЕЦП забезпечує безпеку і юридичну дійсність віртуальних документів, ефективність їх обробки, ідентифікує автора документа, гарантує цілісність вмісту та має в електронному середовищі юридичний статус традиційного підпису на паперовому носії.

Згідно Закону України [1], «електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис».

Традиційна технологія формування ЕЦП базується на застосуванні асиметричної криптографії з використанням пари ключів (приватного і публічного) та алгоритмів обчислення хеш-фнкцій електронного документа[2]. Такий підхід забезпечує високий рівень безпеки та можливість перевірки цілісності документа, що робить криптографічний ЕЦП важливим інструментом для забезпечення конфіденційності та автентифікації в електронному документообігу.

В той же час, криптографічний ЕЦП має в певних аспектах використання ряд недоліків, до яких відносять знеособлення підписанта, вузькоспеціалізоване

252 АПКН-2023

ідентифікації.

З наведених прикладів слідує, що неідентифікуючими атрибутами можуть бути як широко розповсюджені дані особи, так і нікому не відомі дані про особу.

Особливістю неідентифікуючих атрибутів є можливість отримання на їх основі у певних ситуаціях ідентифікаційного атрибута або ідентифікаційного набору атрибутів. Розповсюджені прізвище, ім'я та по батькові при об'єднанні утворюють ідентифікаційний атрибут ПІБ. Освіта, посада, місце роботи підписанта тощо можуть ідентифікувати його особу, якщо при аналізі визначиться відсутність конкурентів за відповідним атрибутом в колі здійснення ідентифікаційного аналізу. Така можливість повинна враховуватись в технології використання цифрового підпису в системах електронного документообігу, що є предметом подальших досліджень.

Як контекстуальні атрибути підпису будемо розглядати 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 підписанта 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); змінювані біометричні параметри фізичного стану особи (пульс, температура тощо); зовнішні умови оточуючого середовища; тип пристрою, задіяний для накладання ЕЦП; дані автентифікації під час входу в систему; права та повноваження підписанта; роль підписанта у певному конкретному контексті тощо.

У контексті електронного цифрового підпису саме комбінація різних типів атрибутів спрямована на створення безпечних та адресно-орієнтованих підписів. Зрозуміло, що не всі перелічені атрибути при реалізації технології доцільно включати до ЕЦП одночасно і загалом не всі вони є зручними для використання в технології та доцільними відповідно кожному окремо взятому застосуванню.

При визначенні базових принципів технології будемо акцентувати увагу на забезпеченні гнучкості, адаптивності та мультиатрибутності ЕЦП. Зазначені принципи передбачають надання підписанту можливості формувати цифровий підпис з довільної кількості атрибутів та визначати їх склад за власним побажанням або у відповідності до потреб.

Для гнучкості процедур автоматизованого вибору атрибутів і забезпечення математичного підґрунтя адаптивності мультиатрибутного формування ЕЦП

формуються множини відповідних атрибутів. В якості ідентифікаторів множин атрибутів використано абревіатури англомовного перекладу назв множин:

– *IA* – ідентифікаційні атрибути (Identifying Attributes);
– *NIA* – неідентифікаційні атрибути (Non-Identifying Attributes);
– *CA* – контекстуальні атрибути (Contextual Attributes).

Таким чином ми отримуємо три множини атрибутів:

$$IA:\{IA_1, IA_2, \dots, IA_i, \dots, IA_k\}, \quad (1)$$
$$NIA:\{NIA_1, NIA_2, \dots, NIA_j, \dots, NIA_m\}, \quad (2)$$
$$CA:\{CA_1, CA_2, \dots, CA_l, \dots, CA_n\}, \quad (3)$$

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

Схематично процедура формування цифрового підпису в примітивах математичної моделі технології представлена на рисунку 1.

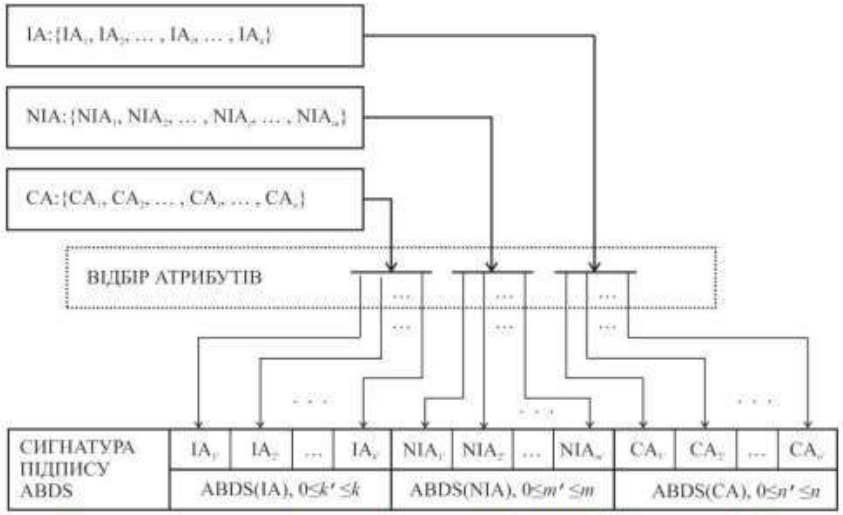


Рисунок 1 – Схема утворення сигнатури цифрового підпису з атрибутів

Кожне значення атрибуту $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$ є двійковим представленням відповідного атрибуту, тому далі будемо ідентифікувати елементи

множин як двійкові коди або двійкові вектори атрибутів. Формування цифрового підпису в примітивах математичної моделі технології зводиться до вибору елементів множин $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$, які відповідають потребам-побажанням підписанта, та поєднання їх у єдину двійкову послідовність – вектор (сигнатуру) цифрового підпису на основі атрибутів ABDS (Attribute-Based Digital Signature).

Сигнатура ABDS цифрового підпису, синтезована на основі двійкових векторів атрибутів, разом з хеш-сигнатурою відкритого тексту, може піддаватися криптографічному шифруванню (закриттю) і додаватися до відкритого тексту за класичними технологіями накладання ЕЦП. В той же час, можливе використання сигнатури цифрового підпису на основі атрибутів ABDS і у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта. Ці дві передбачувані перспективи роблять можливим використання технології цифрового підпису в системах електронного документообігу більш широкими, а саму технології гнучкішою і більш універсальною.

Перелік посилань

1. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022р. URL:https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text (дата звернення: 09.11.2023).
2. Метьолкін А.О., Кардашук В.С. Дослідження методів підвищення криптографічної стійкості. Вісник східноукраїнського національного університету імені Володимира Даля. 2018. № 6 (247). С. 90-95.
3. Ke Gu, Keming Wang, Lulu Yang. Traceable attribute-based signature. Journal of Information Security and Applications. Volume 49. 2019. Article ID 102400.
4. Victor Sucasas, Georgios Mantas, Maria Papaioannou, Jonathan Rodriguez. Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services. IEEE Transactions on Cloud Computing. 2023.Vol.11, №.1. pp.168-184.
5. Qianqian Su, Rui Zhang, Rui Xue, You Sun, Sheng Gao. Distributed Attribute-Based Signature With Attribute Dynamic Update for Smart Grid. IEEE Transactions on Industrial Informatics, 2023. Vol.19, №.9. pp. 9424-9435.

УДК 004.056:004.942

ОРЛЕНКО ВІКТОРІЯ
Хмельницький національний університет
https://orcid.org/0000-0001-9601-1916
e-mail: orlenkovs@khmnu.edu.ua
РИЖИЙ ЯРОСЛАВ
Хмельницький національний університет
e-mail: mirsvqwertyi@gmail.com
ЧЕШУН ВІКТОР
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ЧЕШУН ОЛЕКСАНДР
Хмельницький національний університет
Sashacn228@gmail.com

МОДЕЛЬ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ ОСОБОВИХ АТРИБУТІВ

Стаття присвячена презентації моделі технології синтезу сигнатури цифрового підпису на основі особових атрибутів. В роботі здійснено аналіз і класифікацію атрибутів підписанта для використання в сигнатурі цифрового підпису, визначено спосіб представлення і розподілу атрибутів в математичній моделі, презентована схема утворення сигнатури цифрового підпису в термінах математичної моделі. Сигнатура цифрового підпису, синтезована на основі двійкових векторів атрибутів, разом з хеш-сигнатурою відкритого тексту може піддаватися криптографічному шифруванню (закриттю) і додаватися до відкритого тексту за класичними технологіями накладання ЕЦП. Також можливе використання сигнатури цифрового підпису на основі атрибутів і у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта.

Ключові слова: захист інформації, електронний цифровий підпис, атрибути користувача, система електронного документообігу.

ORLENKO VIKTORIIA, RYZHYI YAROSLAV, CHESHUN VIKTOR, CHESHUN OLEKSANDR
Khmelnytsky National University

MODEL OF DIGITAL SIGNATURE TECHNOLOGY BASED ON PERSONAL ATTRIBUTES

Abstract. The article is devoted to the presentation of a mathematical model of the digital signature synthesis technology based on personal attributes. The paper analyzes and classifies the attributes of the signatory for use in a digital signature, defines the method of presentation and distribution of attributes in a mathematical model. In the model of technology, sets of identifying, non-identifying and contextual attributes are defined. Each value of the attribute is a binary representation of the corresponding attribute, which allows you to identify the elements of the sets as binary codes or binary vectors of attributes and use methods of working with binary numbers.

To implement the technology, a scheme for generating signatures using elements of a mathematical model is proposed. The formation of a digital signature is reduced to the selection of elements of sets of identification, non-identification and contextual attributes that meet the needs or wishes of the signatory, and combining them into a single binary sequence - attribute-based digital signature (ABDS). A digital signature synthesized on the basis of binary attribute vectors, together with the plain text, can be subjected to cryptographic encryption (closing) and added to a packet with a hash signature using classic electronic digital signature technologies. It is also possible to use a digital signature ABDS attributes and in open form, without encryption, determined by the goals and needs of the signer. These two expected prospects make it possible to use the digital signature technology in electronic document management systems more widely, and the technology itself to be more flexible and more universal. The solutions are the basis of the algorithmic implementation of digital signature technology using attributes.

Keywords: information protection, electronic digital signature, user attributes, electronic document management system.

Вступ

Сучасний світ невпинно рухається у напрямку цифрової трансформації, змінюючи спосіб, яким ми працюємо і спілкуємося. У цьому контексті системи електронного документообігу стають ключовим інструментом для забезпечення ефективного обміну даними та документами між організаціями, установами та приватними особами [1]. Подібні системи є невід'ємною складовою сучасного підприємства чи організації, вони дозволяють значно зменшити витрати часу та ресурсів, пов'язаних з обробкою, зберіганням та передачею паперових документів. Вони сприяють автоматизації рутинних процесів, забезпечуючи швидкий доступ до необхідної інформації в будь-який час і в будь-якому місці. У зв'язку з розвитком роботи на віддалених робочих місцях, системи електронного документообігу дозволяють забезпечити ефективний обмін документами в реальному часі, незалежно від місцезнаходження користувачів. Це сприяє підвищенню продуктивності та зручності роботи, що є особливо важливим у сучасному глобалізованому світі.

Системи електронного документообігу також сприяють і поліпшенню безпеки даних [2]. Вони дозволяють керувати доступом до конфіденційної інформації, забезпечуючи шифрування даних та механізми перевірки цілісності. Це допомагає запобігти несанкціонованому доступу до важливих даних та зменшити ризик витоку інформації. Одним із основних інструментів кібербезпеки систем електронного документообігу є використання цифрових підписів [3].

Постановка задачі

Електронний цифровий підпис (ЕЦП) – це технологічний механізм, який дозволяє вам електронно підписувати документи або інші електронні повідомлення [4]. Ігнорування ЕЦП – одна з найбільш поширених слабких сторін систем електронного документообігу [3].

До недоліків традиційних технологій ЕЦП, що базуються на використанні криптографічних алгоритмів, можна віднести знеособлення підписанта і централізацію дій з підписом. Для формування, накладання і підтвердження ЕЦП підписант і верифікатор підпису повинні звертатися до послуг спеціалізованих сервісів високої довіри і не мають змоги ні сформувати ЕЦП власноруч, ні отримати з нього інформацію про підписанта.

Альтернативним напрямком розвитку технологій цифрового підпису є формування підпису на основі атрибутів підписанта, що робить підпис безпосередньо інформаційно пов'язаним з особою його надавача і максимально інформативним для верифікатора підпису, а самого підписанта перетворює у автора і власника підпису, як це є при використанні власноручного підпису.

Поняття підписів із застосуванням атрибутів було явно введено науковцями з Китаю в роботі [6], а Hemanta K Маji з співавторами [7] продовжив цю роботу і описує підпис із застосуванням атрибутів як «універсальний примітив, що дозволяє стороні підписувати повідомлення з детальним контролем над ідентифікаційною інформацією».

Існуючий, але в основному теоретичний проєкт під назвою ABCJTrust [8] мав на меті розробити структуру під ідентифікатором ABC (Attribute-based Credentials – облікові дані на основі атрибутів) на основі існуючої технології використання атрибутів в системах електронного документообіг.

Подібним, але більш практичним проєктом є Yivi [9] – технологія, спрямована на реалізацію функціонального потенціалу облікових даних на основі атрибутів. Для впровадження облікових даних із застосуванням атрибутів Yivi (частково) покладається на систему ідентифікації Identity Mixer (Idemix), розроблену IBM Research [10]. Система IBM Idemix надає різні функціональні можливості для підтвердження володіння обліковими даними із застосуванням атрибутів та їхніми властивостями.

Важливим аспектом технології використання цифрового підпису із застосуванням атрибутів в є мінімізація і актуалізація даних, коли йдеться про забезпечення конфіденційності користувачів. Це вимагається законодавством України [11] і ЄС [12]. Проте, мінімізація даних може призвести до зниження рівня інформаційної цінності цих даних.

Коли розкривається менше даних, отримувач (верифікатор) може мати менше актуальної йому інформації. Слід розглянути баланс між збереженням високої інформаційної цінності виявлених даних і їх мінімальних розкриттям.

Для досягнення балансу між розкриттям і забезпеченням конфіденційності особових атрибутів у цифровому підписі виникає потреба визначення математичного апарату для формалізації даних і процесів їх обробки при формуванні підпису, а також розробки технології формування сигнатури атрибутивного цифрового підпису в термінах математичної моделі.

Основна частина

У випадку цифрових підписів є потреба розкривати не занадто багато особистої інформації про підписанта, але розкрита інформація повинна бути достатньо інформативною та зрозумілою. Це потребує аналізу і класифікації атрибутів, які можуть бути використані при формуванні сигнатури атрибутивного підпису.

Проведений аналіз дозволив виділити три типових категорії атрибутів особи:

- 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 (псевдонім, який однозначно пов'язаний з особою); ідентифікатор (номер або серія-номер) посвідчення з місця роботи тощо.

Як неідентифікаційні атрибути визначено 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); дата народження; вік; дата 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 особисту інформацію без прямої ідентифікації.

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 підписанта 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 підписанта; роль підписанта у певному контексті тощо.

При визначенні базових принципів увага акцентується на забезпеченні гнучкості, адаптивності та мультиатрибутності ЕЦП. Зазначені принципи передбачають надання підписанту можливості формувати цифровий підпис з довільної кількості атрибутів та визначати їх склад за власним побажанням або у відповідності до потреб.

Для гнучкості процедур автоматизованого вибору атрибутів і забезпечення математичного підґрунтя адаптивності мультиатрибутного формування ЕЦП формуються множини відповідних атрибутів:

– $IA:\{IA_1, IA_2, \dots, IA_i, \dots, IA_k\}$ – множина ідентифікаційних атрибутів (Identifying Attributes) особи-підписанта;

– $NIA:\{NIA_1, NIA_2, \dots, NIA_j, \dots, NIA_m\}$ – множина неідентифікаційних атрибутів (Non-Identifying

Attributes) особи-підписанта;

– $CA:\{CA_1, CA_2, \dots, CA_i, \dots, CA_n\}$ – множина контекстуальних атрибутів (Contextual Attributes) особи-підписанта або самого підпису.

Схема формування цифрового підпису в примітивах математичної моделі представлена на рисунку 1.

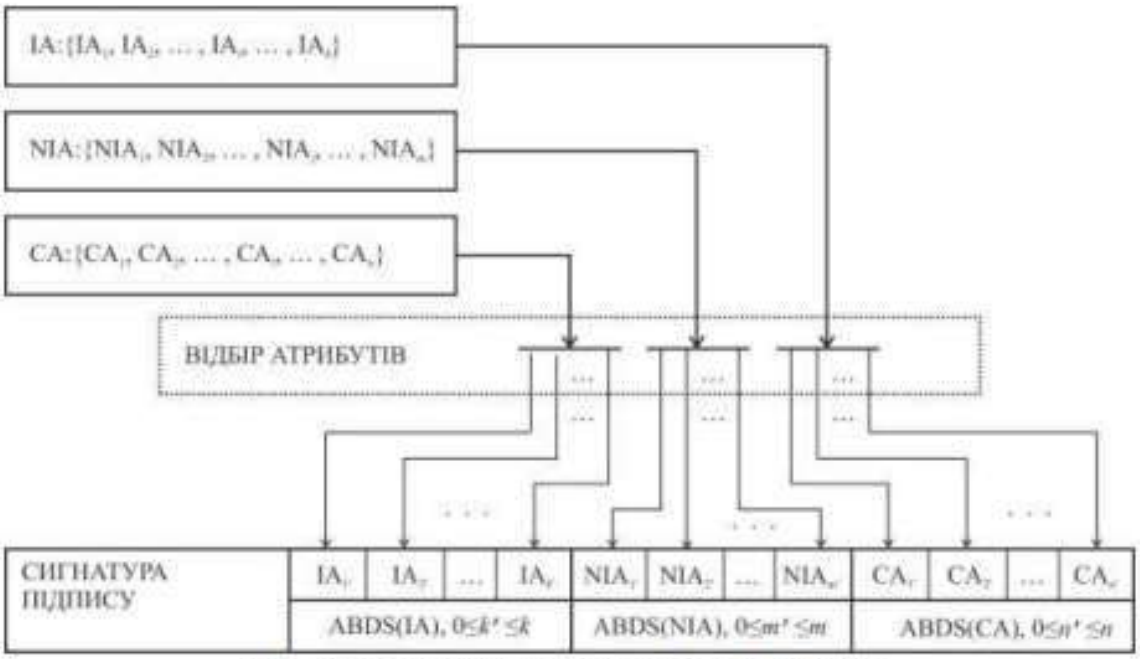


Рис. 1 – Схема утворення сигнатури цифрового підпису з атрибутів

Кожне значення атрибуту $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$ є двійковим представленням відповідного атрибуту, що дозволяє ідентифікувати елементи множин як двійкові коди або двійкові вектори атрибутів. Формування цифрового підпису зводиться до вибору елементів множин $IA_i \in IA$, $NIA_j \in NIA$ і $CA_l \in CA$, які відповідають потребам-побажанням підписанта, та поєднання їх у єдину двійкову послідовність – вектор (сигнатуру) цифрового підпису на основі атрибутів ABDS (Attribute-Based Digital Signature).

Наведені на схемі для полів ABDS(IA), ABDS(NIA), ABDS(CA) обмеження $0 \le k' \le k$, $0 \le m' \le m$, $0 \le n' \le n$ ілюструють, що в ході утворення сигнатури цифрового підпису ABDS до її складу можуть включатися атрибути кожного класу у будь-якій кількості від нуля (атрибути відповідного класу і саме поле цих атрибутів в сигнатурі цифрового підпису будуть відсутні) до максимальної кількості задекларованих атрибутів.

Висновки

В статті розглянута модель технології цифрового підпису із використанням атрибутів підписанта та презентована схема утворення сигнатури цифрового підпису в термінах математичної моделі. Сигнатура ABDS цифрового підпису, синтезована на основі двійкових векторів атрибутів, разом з файлом відкритого тексту, може піддаватися криптографічному шифруванню (закриттю) і з хеш-сигнатурою додаватися до відкритого тексту за класичними технологіями накладання ЕЦП. В той же час, можливе використання сигнатури цифрового підпису на основі атрибутів ABDS і у відкритому вигляді, без закриття шифруванням, що визначається цілями та потребами підписанта. Ці дві передбачувані перспективи роблять можливим використання технології цифрового підпису в системах електронного документообігу більш широкими, а саму технології гнучкішою і більш універсальною.

Література

1. Асанова Л. Місце електронного документообігу в загальній системі діловодства. *Адміністративне право і процес*. 2021. №3. С. 156-160.
2. Севастєєв Є.О. Безпека електронного документообігу. Одеса, ДУІТЗ. 2022. 18 с.
3. Rauniyar K. Role of FinTech and innovations for improvising digital financial inclusion. *Int. J. Innov. Sci. Res. Technol.* 2021. №6. P. 1419-1424.
4. Електронний підпис і сертифікація документів. URL: https://pidru4niki.com/19590809/informatika/elektronniy_pidpis_sertifikatsiya_dokumentiv (дата звернення: 27.11.2023).
5. Політанський В. С. Теоретико-правові засади системи електронного документообігу в Україні. *Право і суспільство*. 2021. №1. С. 22-27.
6. Guo Shanqing and Zeng Yingpei. Attribute-based signature scheme. In *2008 International Conference on Information Security and Assurance (ISA 2008)*. IEEE, 2008. P. 509-511.
7. Hemanta K Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In *Cryptographers' track at the RSA conference. Springer*. 2011. P. 376-392.
8. ABC4Trust Attribute-based Credentials for Trust. URL: https://abc4trust.eu/download/ABC4Trust-OnePager-About-ABC4Trust.pdf (дата звернення: 28.11.2023).
9. How Yivi works? URL: https://www.yivi.app/en/for-me/how-yivi-works (дата звернення: 28.11.2023).
10. Ashley Bringer, Candice Gordon, Sean Mackey, Reba Smith. Idemix: Identity Mixer URL: https://faculty.uca.edu/ronmc/INFO3321/Spring_2007/ET%20Pres/ ET1/G4/Idemix%20Group%204.htm (дата звернення: 29.11.2023).
11. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022р. URL: https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text (дата звернення: 29.11.2023).
12. 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.

References

1. Asanova L. Mistse elektronnoho dokumentoobihu v zahalnii systemi dilovodstva. Administratyvne pravo i protses. 2021. №3. S. 156-160.
2. Sevastieiev Ye.O. Bezpeka elektronnobo dokumentoobibu. Odesa, DUITZ. 2022. 18 s.
3. Rauniyar K. Role of FinTech and innovations for improvising digital financial inclusion. Int. J. Innov. Sci. Res. Technol. 2021. №6. P. 1419-1424.
4. Elektronnyi pidpys i sertyfikatsiia dokumentiv. URL: https://pidru4niki.com/19590809/informatika/elektronniy_pidpis_sertifikatsiya_dokumentiv (date of access: 27.11.2023).
5. Politanskyi V. S. Teoretyko-pravovi zasady systemy elektronnoho dokumentoobihu v Ukraini. Pravo i suspilstvo. 2021. №1. S. 22-27.
6. Guo Shanqing and Zeng Yingpei. Attribute-based signature scheme. In 2008 International Conference on Information Security and Assurance (ISA 2008). IEEE, 2008. P. 509-511.
7. Hemanta K Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In Cryptographers' track at the RSA conference. Springer. 2011. P. 376-392.
8. ABC4Trust Attribute-based Credentials for Trust. URL: https://abc4trust.eu/download/ABC4Trust-OnePager-About-ABC4Trust.pdf (date of access: 28.11.2023).
9. How Yivi works? URL: https://www.yivi.app/en/for-me/how-yivi-works (date of access: 28.11.2023).
10. Ashley Bringer, Candice Gordon, Sean Mackey, Reba Smith. Idemix: Identity Mixer URL: https://faculty.uca.edu/ronmc/INFO3321/Spring_2007/ET%20Pres/ ET1/G4/Idemix%20Group%204.htm (date of access: 29.11.2023).
11. Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy: Zakon Ukrainy vid 01.12.2022r. URL: https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text (date of access: 29.11.2023).
12. 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.

ДОДАТОК Б

Презентація кваліфікаційної роботи

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

Рижий Ярослав Олександрович

Технологія використання цифрового підпису
в системах електронного документообігу

спеціальність 125 – Кібербезпека

Науковий керівник: к.т.н., доцент **Орленко Вікторія Сергіївна**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ МАГІСТРА

Мета кваліфікаційної роботи полягає у вдосконаленні і розширенні можливостей технології використання цифрового в системах електронного документообігу та інших електронних сервісах з авторизацією користувачів за рахунок застосування у сигнатурі підпису особових атрибутів підписанта.

Об'єктом дослідження є процеси захищеної авторизації користувачів інформаційних послуг систем електронного документообігу.

Предметом дослідження є технології формування електронного цифрового підпису в електронних сервісах та системах електронного документообігу з адаптованою потребам підписанта структурою сигнатури.

Наукова новизна отриманих результатів:

1. Визначено спосіб формування мультиатрибутивної адаптивної сигнатури цифрового підпису в термінах запропонованої математичної моделі;

2. Удосконалено технологію електронного цифрового підпису систем електронного документообігу забезпеченням гнучкості формування сигнатури підпису із застосуванням атрибутів та її адаптивності до потреб підписанта.

Практична значимість отриманих результатів полягає у визначенні положень і розробці алгоритмів технології використання цифрового підпису в системах електронного документообігу більш широкого застосування і зрозумілого нефаховому користувачу формату.

Задачі досліджень у роботі формулюються наступним чином:

а) виявити перспективні напрямки та способи вдосконалення технології використання цифрового підпису в системах електронного документообігу, що можуть бути використані у підвищенні її ефективності;

б) визначити основні положення технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу;

в) розробити математичну модель технології використання цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу;

г) здійснити алгоритмічну реалізацію технології;

д) провести апробацію дієвості прийнятих теоретичних і алгоритмічних рішень технології.

В основі методів дослідження лежать базові положення інформаційної безпеки, теорії ідентифікації та аутентифікації, криптографії, теорії множин.

Апробація роботи. Наукові результати і основні положення магістерської роботи доповідались і обговорювались на Всеукраїнській і міжнародній науково-практичних конференціях.

Публікації. За темою магістерської роботи підготована до видання 1 стаття у фаховому журналі та опубліковано 2 тези доповідей науково-практичних конференцій.

ДОСЛІДЖЕННЯ ПРОБЛЕМ ТА ПЕРСПЕКТИВ В ПРЕДМЕТНІЙ ОБЛАСТІ

Таблиця 1 – Можливості технологій цифрового підпису

Технологія	Сигнатура ЕЦП	Аутенти-фікація	Децентра-лізація	Використання атрибутів	Поєднання ЕЦП і атрибутів	Практична реалізація
ЕЦП	+	-	-	-	-	+
Serto	-	+	+	+	-	-
YIVI	+	+	+	+	-	+
DECODE	-	+	-	+	-	+
Schluss	-	+	-	+	-	+
Sovrin	-	+	+	+	-	+
SelfKey	-	+	+	+	-	+

Висновок 1 : Класична технологія цифрового підпису (ЕЦП) має вади надмірної централізації, незрозумілості для користувача і малої презентативності для одержувача.

Висновок 2 : В ЄС широко ведуться дослідження в напрямку створення технологій цифрового підпису з гнучким і зрозумілим для користувача синтаксисом, але більшість з цих технологій орієнтовані на аутентифікацію підписанта в системах надання послуг.

Висновок 3 : Удосконалення технології використання цифрового підпису в системах електронного документообігу забезпеченням гнучкості формування сигнатури підпису із застосуванням атрибутів підписанта є актуальною задачею дослідження.

Перший науковий результат

МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ

Загальне представлення

$$M = < IA, NIA, CA >$$

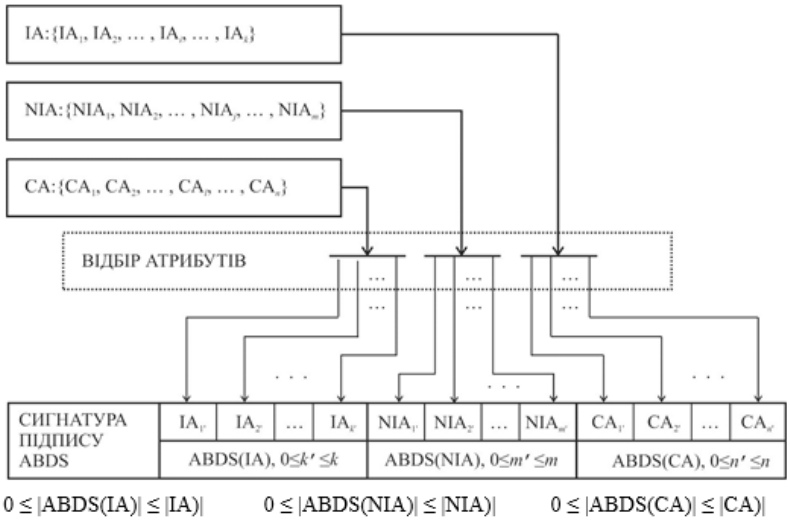
Елементи моделі

IA:{IA$_1$, IA$_2$, … , IA$_i$, … , IA$_k$} – множина ідентифікаційних атрибутів IA$_i$∈IA особи-підписанта

NIA:{NIA$_1$, NIA$_2$, … , NIA$_j$, … , NIA$_m$} – множина неідентифікаційних атрибутів NIA$_j$∈NIA особи-підписанта

CA:{CA$_1$, CA$_2$, … , CA$_l$, … , CA$_n$} – множина контекстуальних атрибутів CA$_l$∈CA особи-підписанта або підпису

Схема утворення сигнатури цифрового підпису



Другий науковий результат

РОЛЬОВА ДЕКОМПОЗИЦІЯ ТЕХНОЛОГІЇ ЦИФРОВОГО ПІДПИСУ

Суб'єкти (ролі) технології

Користувач-підписант – суб'єкт, який використовує технологію цифрового підпису із застосуванням своїх особових атрибутів.

Сервіс користувача-підписанта – мобільного додаток або програмний застосунок на комп'ютері.

Запитувач – сервіс запиту, підтвердження і використання верифікованих емітентом атрибутів.

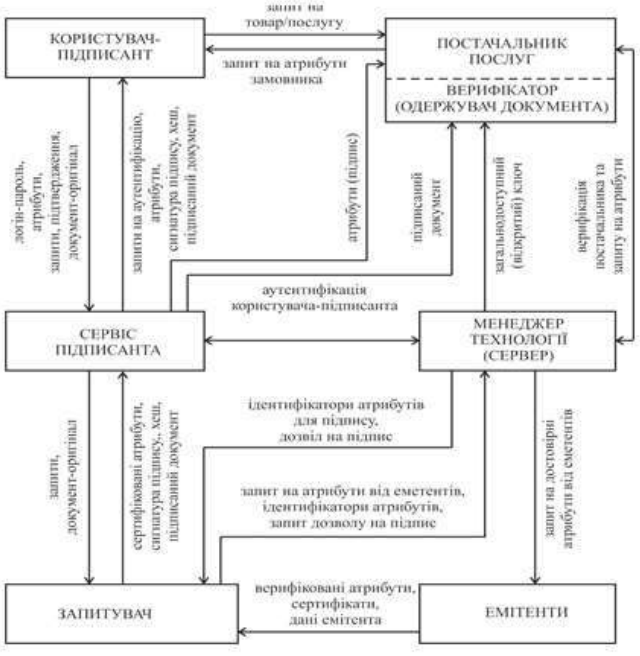
Емітент – перевірена організація або служба (сервіс тощо) високої довіри, здатна видавати гарантовано достовірні атрибути особи (паспортний стіл, ДІЯ тощо).

Менеджер (сервер) – відповідає за визначення та поширення відкритих ключів, типів атрибутів, перевірку постачальників і запитів та взаємодію ролей.

Верифікатор – суб'єкт системи електронного документообігу, одержувач документа з цифровим підписом.

Постачальник послуг – суб'єкт (фірма, організація тощо), який видає запит на атрибути замовника для надання послуги.

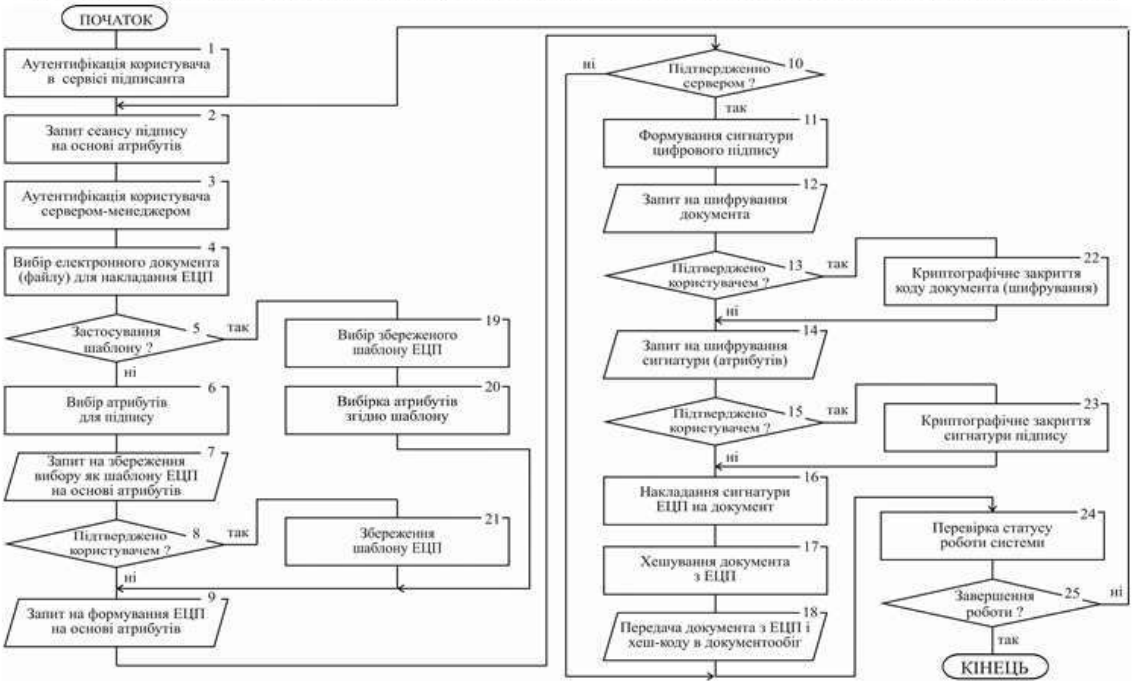
Схема взаємодії ролей



Другий науковий результат

АЛГОРИТМІЧНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ

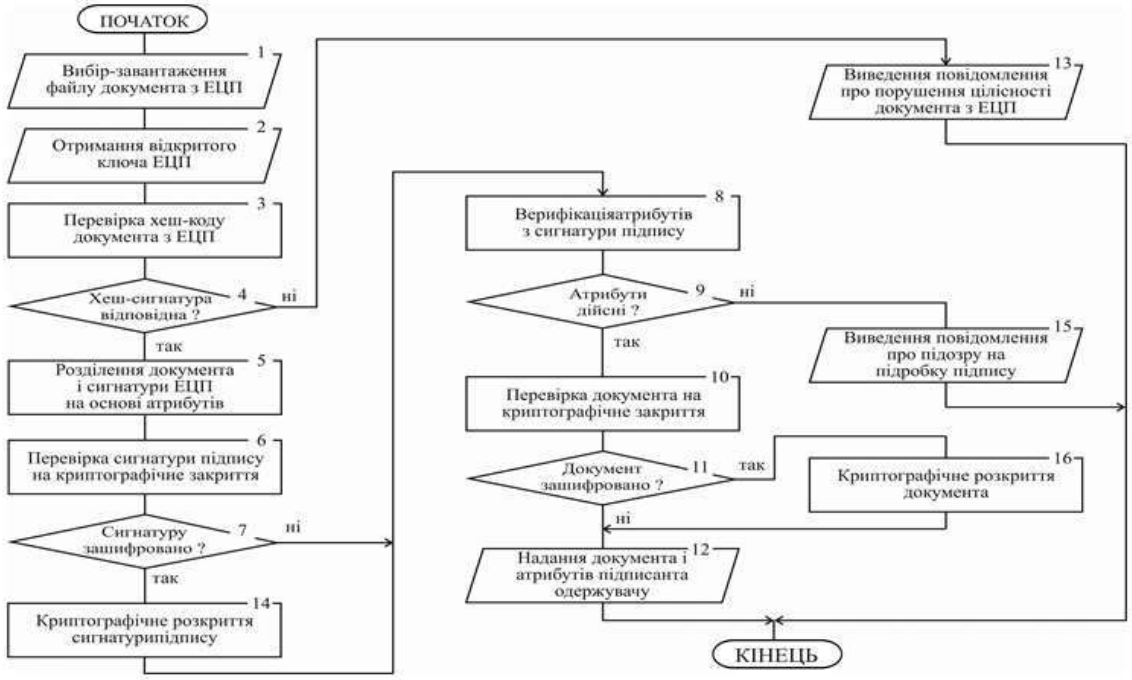
Алгоритм формування і накладання сигнатури підпису на електронний документ



Другий науковий результат

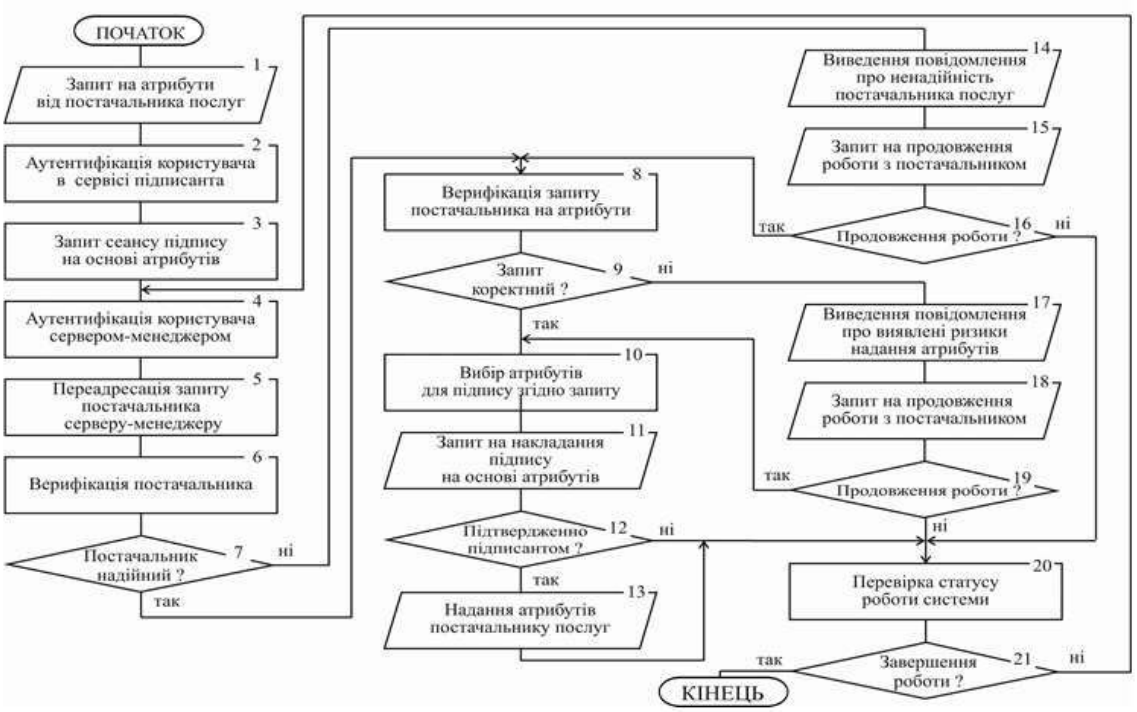
АЛГОРИТМІЧНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ

Алгоритм верифікації сигнатури підпису



АЛГОРИТМІЧНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ

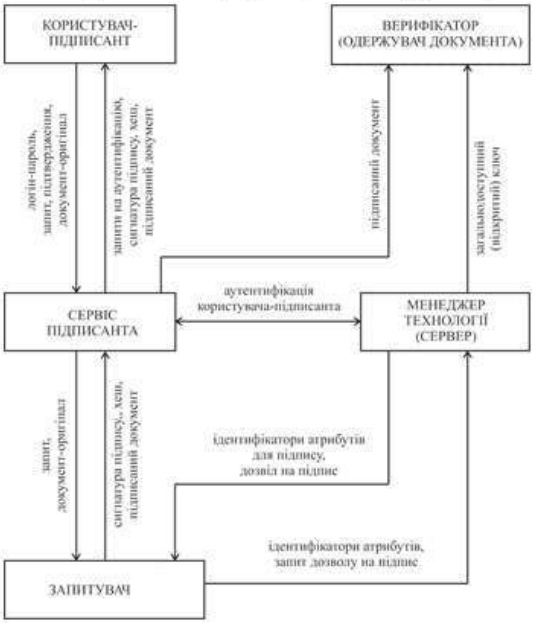
Алгоритм надання атрибутів для авторизації підписанта на запит постачальника послуг



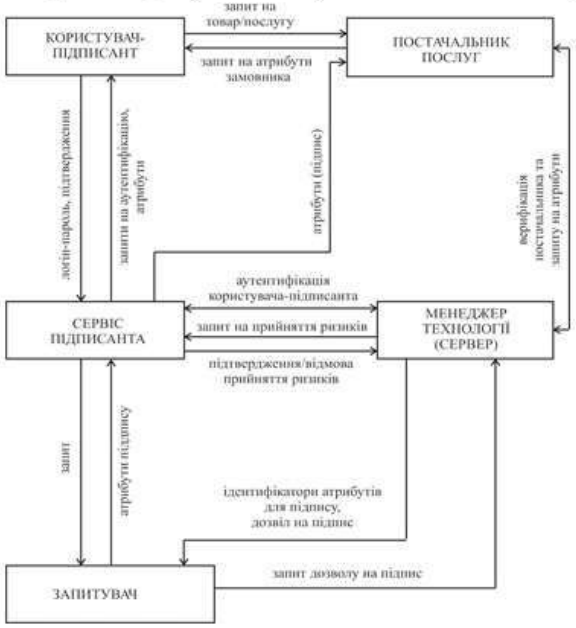
АПРОБАЦІЯ ТЕХНОЛОГІЇ

Моделювання сценаріїв реалізації технології на схемах рольової декомпозиції

Рольова декомпозиція взаємодії суб'єктів при накладанні та верифікації сигнатури ЕЦП



Рольова декомпозиція взаємодії суб'єктів при накладанні підпису на вимогу постачальника послуг



АПРОБАЦІЯ ТЕХНОЛОГІЇ
Дослідження технології на вразливості і стійкість до атак

Вид атаки/вразливості	Стійкість	Примітка
Повторне використання підпису (Non-Re-Usability)	+	
Порушення цілісності (Integrity Violation Of)	+	
Відмови від авторства (Repudiation Of Origin)	+	
Використання застарілих атрибутів (Using Legacy Attributes)	+	
Надлишкове розкриття атрибутів (Redundant Attribute Disclosure)	+	
Розкриття емітента (Issuer Disclosure)	+	
Підробка атрибутів (Attributes Forgery)	+	
Фальшива ідентифікація (False Identification)	+	
Фальсифікація особи (Identity Falsification)	+	
Фальсифікація часу (Time Falsification)	+	
Атаки повторення (Replay Attacks)	+	
Серфінг через плече (Shoulder Surfing)	-	Надані рекомендації

ВИСНОВКИ

В роботі за результатами теоретичних та практичних досліджень виконано розробку удосконаленої технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу. При розробці переслідувалась мета, що полягає у вдосконаленні і розширенні можливостей технології використання цифрового в системах електронного документообігу та інших електронних сервісах з авторизацією користувачів за рахунок застосування у сигнатурі підпису особових атрибутів підписанта.

Для реалізації програми досліджень виконано наступні роботи:

– проведене дослідження існуючих технологій використання цифрового підпису в системах електронного документообігу, виявлено перспективні напрямки та способи вдосконалення, що можуть бути використані у підвищенні їх ефективності;

– запропоновано математичну модель технології та визначено схему формування мультиатрибутивної адаптивної сигнатури цифрового підпису в термінах запропонованої математичної моделі;

– визначено основні положення удосконаленої технології використання цифрового підпису;

– здійснено алгоритмічну реалізацію технології, в ході якої розроблено алгоритм формування і накладання сигнатури підпису на електронний документ, алгоритм верифікації сигнатури підпису та алгоритм надання атрибутів для авторизації підписанта на запит постачальника послуг;

– здійснено апробацію технології моделюванням взаємодії її суб'єктів в реалізації різних сценаріїв;

– виконане дослідження технології на вразливості і стійкість до атак.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Рижого Ярослава Олександровича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

01.12.2023
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015978045

Дата перевірки:
06.12.2023 21:57:42 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.12.2023 22:00:36 EET

ID користувача:
100008300

Назва документа: **Рижий_магістерська_ПЛ**

Кількість сторінок: **79** Кількість слів: **15748** Кількість символів: **130653** Розмір файлу: **984.80 KB** ID файлу: **1015657765**

1%
Схожість

Найбільша схожість: **0.39%** з джерелом з Бібліотеки (ID файлу: **1015641973**)

0.77% Джерела з Інтернету	156	Сторінка 81
0.66% Джерела з Бібліотеки	47	Сторінка 81

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	1

Wed Dec 06 21:02:21 EET 2023, Мостовий Сергій Володимирович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 121965 Назва: Технологія використання цифрового підпису в системах електронного документообігу Додано в БД: 2023-12-06 Автора: Рижий Я.О. Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	113841	1611	750 (1%)	10 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Технологія використання цифрового підпису в системах електронного документообігу

Автор: Рижий Ярослав Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Орленко Вікторія Сергіївна, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 99%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ В.С. Орленко

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Рижий Ярослав Олександрович

Тема Технологія використання цифрового підпису в системах електронного документообігу

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 85

1. Короткий зміст роботи та прийнятих рішень В кваліфікаційній роботі здійснено ідентифікацію та класифікацію атрибутів для реалізації технології цифрового підпису в системах електронного документообігу, визначено спосіб формалізованого представлення різних класів атрибутів в математичній моделі та презентовано схему синтезу сигнатури підпису, розроблені алгоритми та рольові схеми реалізації технології, здійснено апробацію отриманих результатів.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність; визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. В першому розділі зроблене дослідження технологій використання цифрового підпису в системах електронного документообігу, дослідження технологій використання цифрового підпису в системах електронного документообігу. Математична модель технології, запропонована в другому розділі, враховує різноманітні характеристики та атрибути підписанта для створення надійних та гнучких цифрових підписів. В третьому розділі надано опис технології використання цифрового підпису в системах електронного документообігу, в якому уточнено загальні принципи реалізації запропонованої технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу, зроблена рольова декомпозиція, яка використана за основу для визначення рольової схеми взаємодії суб'єктів технології, яка, в свою чергу, стала базисом в алгоритмічної реалізації. Четвертий розділ присвячений апробації технології цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу.

4. Позитивні сторони роботи Кваліфікаційна робота містить актуальні рішення і пропозиції, орієнтовані на вдосконалення і розширення можливостей технології використання цифрового в системах електронного документообігу та інших електронних сервісах з авторизацією користувачів за рахунок застосування у сигнатурі підпису особових атрибутів підписанта .

5. Негативні сторони роботи В роботі не деталізовані принципи посднання класичного ЕЦП та цифрового підису на основі атрибутів. Не деталізовані принципи програмної реалізації необхідних для реалізації технології програмних сервісів

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та наскрізно пов'язаний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Презентаційний та ілюстративний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження -

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони предетавленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Підченко Сергій Костянтинович
Завідувач кафедри ТМІТ, доктор технічних наук, професор

« 5 » 12 2023. (підпис)